УДК 512.552+519.95

V. V. Skobelev, Cand. Phys.-Math. Sci

Satisfiability modulo linear arithmetic over a finite ring

There are developed mathematical methods intended for resolving the problem of analysis of satisfiability modular linear arithmetic over any finite associative (not necessary commutative) ring with non-zero multiplication. General schemes for solvers intended for analysis of satisfiability of formulae presented via any system of linear equations or linear disequalities are proposed. Time complexity of proposed solvers is estimated for finite fields and rings of residues.

Key Words: finite rings, linear arithmetic, satisfiability of formulae.

Institute of Applied Mathematics and Mechanics of NAS of Ukraine, 83114, Rose Luxemburg str., 74,
e-mail: vv_skobelev@iamm.ac.donetsk.ua

Скобелєв В.В., к.ф.-м.н.

Виконання формул лінійної арифметики над скінченним кільцем

Розроблено математичний апарат, який призначено для розв'язання задачі дослідження виконання формул лінійної арифметики над скінченним асоціативним (не обов'язково комутативним) кільцем з операцією ненульового множення. Запропоновано загальні схеми, які призначено для дослідження виконання формул, які представлено системою лінійних рівнянь, або лінійних нерівностей. Досліджено часову складність запропонованих схем у випадках скінченого поля та кільця лишків.

Ключові слова: скінченні кільця, лінійна арифметика, виконання формул.

Інститут прикладної математики і механіки НАН України, 83114, м. Донецьк, вул. Рози Люксембург, 74,
e-mail: vv_skobelev@iamm.ac.donetsk.ua

Статтю представив чл.-кор. НАН України, Анісімов А.В.

Introduction.

Satisfiability modulo theory (*SMT*) is an NP-complete problem intended for deciding satisfiability of a first-order formula (usually presented via conjunction of literals) in some decidable first-order theory T ($SMT(T)$).

At present the lazy approach [1] (also referred as $DPLL(T)$ [2]) is predominant for construction of $SMT(T)$. It is based on integration of some Boolean satisfiability (*SAT*) solver with some procedure intended to handle basic atomic constraints of the theory T. Elaboration of the last procedure is the basic step for construction of $SMT(T)$ under the lazy approach.

It is worth to note the following aspects of architecture of modern *SMT* solvers.

Firstly, besides output *sat* or *unsat* some formulae valid in the theory T (i.e. some lemmas of the theory T) can be produced (if output is *sat* they are called theory-deduction clauses, while if output is *unsat* they are called theory-conflict clauses).

Secondly, layering technique [3] is used, i.e. it is implemented some hierarchy

$$S_1,\dots,S_n$$

of solvers of increasing expressivities and complexity, such that S_i $(i=1,\dots,n-1)$ is intended to decide some sub-theory T_i $(T_i \subset T_{i+1})$, while S_n is intended to decide full theory T.

Thirdly, the splitting-on-demand-technique [4] is used, i.e. it can be produced the output *unknown* with some list of T-lemmas containing new T-atoms, which will be taken into account in the *DPLL* search.

The most well studied case of $SMT(T)$ is linear rational arithmetic [1,5,6], i.e. $T = LA(\mathbf{Q})$ and atoms are of the form

$$\sum_{i=1}^{n} a_i x_i + b \lozenge 0 \quad (\lozenge \in \{\le, <, \ne, =, \ge, >\}).$$

Some efficient support for linear integer arithmetic $LA(\mathbf{Z})$ under condition $\lozenge \in \{\le, =\}$ was developed in [7].

But situation is much more complicated for linear arithmetic over any finite ring $\mathsf{K} = (K, +, \cdot)$ (i.e. if $T = LA(\mathsf{K})$), since any finite ring as an algebraic system differs essentially from the ring of integers.

It is worth to note that there are important applications of $LA(\mathsf{K})$ (K is a finite ring) in cryptography [8]. Thus, satisfiability of formulae of linear arithmetic over a finite ring is actual problem from theoretic and applied point of view, both.

Investigation of $SMT(T)$ for $T = LA(\mathsf{K})$, where K is any associative finite ring is the main aim of the given paper.

1. Typical structure of $LA(\mathbf{Z})$-solvers.

Typical modern $LA(\mathbf{Z})$-solver intended for analysis of atoms of the form

$$\sum_{i=1}^{n} a_i x_i + b \lozenge 0 \quad (\lozenge \in \{=, \le\}).$$

is proposed in [7]. This solver is organized in the following way.

Firstly, the rational relaxation of the problem is analyzed by Simplex-based $LA(\mathbf{Q})$-solver. If its output is *unsat* (i.e. some conflict is detected), then $LA(\mathbf{Z})$-solver also returns *unsat* and halts. If its output is *sat* (i.e. no conflict is detected), then it is checked, whether all assigned values for variables are integers. If this happens, then $LA(\mathbf{Z})$-solver also returns *sat* and halts.

Otherwise, module intended to analyze system of linear Diophantine equations is activated. Corresponding algorithm runs in polynomial time, and is based on integration of procedure intended for checking consistency for analyzed system of equations with procedure intended for reducing this system of equations to triangular form, i.e. to the form

$$x_j = \sum_{i \ne j} a_{ji} x_i + c_j \quad (a_{ji}, c_j \in \mathbf{Z}),$$

where variable x_j does not occur in the right part of any equation.

The first procedure is based on the factor that if it is obtained equation

$$\sum_i a_{hi} x_i + b_h = 0,$$

such that GCD of a_{hi}'s does not divide b_h then analyzed system of linear Diophantine equations is inconsistent.

The second procedure is organized in the following way. Let

$$\sum_i a_{hi} x_i + b_h = 0$$

is analyzed equation and a_{hk} be the non-zero coefficient with the smallest absolute value.

If $|a_{hk}| = 1$ then analyzed equation is rewritten in the form

$$x_k = -\sum_{i \ne k} \alpha_{hk} a_{hi} x_i - \alpha_{hk} b_h \quad (\alpha_{hk} = a_{hk} \,|\, a_{hk} |^{-1}).$$

This substitution is then applied to all the other equations.

If $|a_{hk}| > 1$ then analyzed equation is rewritten in the form

$$a_{hk}(x_k + \sum_{i \ne k} a_{hi}^{(q)} x_i + b_h^{(q)}) + \sum_{i \ne k} a_{hi}^{(r)} x_i + b_h^{(r)} = 0,$$

where $a_{hi}^{(q)}$ and $a_{hi}^{(r)}$ (similarly, $b_h^{(q)}$ and $b_h^{(r)}$) are the quotient and the remainder of the division of a_{hi} by a_{hk} (similarly, of b_h by a_{hk}). Substitution

$$x_t = x_h + \sum_{i \ne k} a_{hi}^{(q)} x_i + b_h^{(q)}$$

where x_t is some fresh variable is applied to all equations and then this equation is included in analyzed system of linear Diophantine equations.

If output of considered module is *unsat*, then $LA(\mathbf{Z})$-solver also returns *unsat* and halts.

Otherwise, resulted system of linear Diophantine equations is used for substitutions

$$x_j = \sum_{i \ne j} a_{ji} x_i + c_j$$

of variables into all analyzed inequalities.

Then module intended to analyze system of linear inequalities is activated.

Firstly, it tighten every inequality $\sum_i a_i x_i + b \le 0$, such that GCD g of a_i's does not divide b, by transforming it to inequality

$$\sum_i a_i g^{-1} x_i + \lceil b g^{-1} \rceil \le 0.$$

Then $LA(\mathbf{Q})$-solver is activated. If its output is *unsat* (i.e. some conflict is detected), then $LA(\mathbf{Z})$-solver also returns *unsat* and halts. If its output is *sat* (i.e. no conflict is detected), then it is checked, whether all assigned values for variables are integers. If this happens, then $LA(\mathbf{Z})$-solver also returns *sat* and halts.

Otherwise, the branch-and-bound module is activated. This module recursively divides analyzed problem in two sub-problems by adding to original formula additional constraint in the following way. Let $LA(\mathbf{Q})$-solver has assigned to variable x_k some non-integer value α_k. For the first sub-problem additional constraint is $x_k - \lfloor \alpha_k \rfloor \le 0$, while for the second one it is $-x_k + \lceil \alpha_k \rceil \le 0$. Then $LA(\mathbf{Q})$-solver is activated for analyzed sub-problem.

These computations are produced until either $LA(\mathbf{Z})$-solver returns *sat*, or it would be established that all sub-problems are unsatisfiable ones and, thus, $LA(\mathbf{Z})$-solver returns *unsat*.

2. Preliminary analysis.

If we compare the ring $\mathsf{Z}=(\mathbf{Z},+,\cdot)$ of integers with any finite ring K, considering them as algebraic systems, then the following essential distinctions can be detected, at least:

1. In a ring K operation of multiplication can be non-commutative [9]. In this case it is necessary to consider terms ab and ba as different ones.

2. There is no natural relation $\le$ of total ordering in any finite ring K. Thus, only atoms of the form

$$\sum_{i=1}^{n} a_i' x_i a_i'' + b \Diamond 0 \quad (\Diamond \in \{=,\neq\})$$

can be considered in any linear arithmetic $LA(\mathsf{K})$.

3. Any finite ring K is not an algebraic subsystem of the ring Z of integers (and, thus, of the ring $\mathsf{Q}=(\mathbf{Q},+,\cdot)$ of rational numbers). This implies that any $LA(\mathbf{Q})$-solver and any module intended to analyze system of linear Diophantine equations, both, cannot be applied in any linear arithmetic $LA(\mathsf{K})$, in principle.

4. Division in a ring K can be partial operation. If this happens, then in the process of analysis of linear equations it is necessary to consider separately two essentially different situations: when selected coefficient is an invertible element and when it is a non-invertible one.

5. There can be zero divisors for non-zero elements of a ring K. If this happens, then in the process of analysis of linear equations these divisors can be considered in details.

Taking all these factors into account, we analyze basic modules of $LA(\mathsf{K})$-solver under supposition that K is any associative finite ring with non-zero multiplication, i.e. there exist $a,b\in K$ such that $ab\neq 0$ or $ba\neq 0$.

Remark 1. Arithmetic in any ring $\mathsf{K}=(K,+,\cdot)$ with zero multiplication can be directly reduced to arithmetic in the abelian group $(K,+)$.

3. Some backgrounds of the ring theory.

By supposition, for any considered ring $\mathsf{K}=(K,+,\cdot)$ inequality $|K|\ge 2$ holds.

If $|K|=2$ then K is finite field GF(2).

If $|K|\ge 3$ then the following two lemmas hold.

Lemma 1. Let $\mathsf{K}=(K,+,\cdot)$ be any ring such that $|K|\ge 3$. For any $a\in K$ if there exist $b\in K$ such that $ax=b$ for all $x\in K\setminus\{0\}$ then $b=0$.

Proof. Let $ax=b$ for all $x\in K\setminus\{0\}$.

If $a=0$ then $b=0$.

Let $a\neq 0$. Since $|K|\ge 3$ there exist two different elements $x_1,x_2\in K\setminus\{0\}$ such that $ax_1=b$ and $ax_2=b$. Thus, $a(x_1-x_2)=0$.

Since $x_1\neq x_2$, i.e. $x_1-x_2\neq 0$ we get $b=0$.

Q.E.D.

Lemma 2. Let $\mathsf{K}=(K,+,\cdot)$ be any ring such that $|K|\ge 3$. For any $a\in K$ if there exist $b\in K$ such that $xa=b$ for all $x\in K\setminus\{0\}$ then $b=0$.

Proof is similar to proof of lemma 1.

Lemma 3. Let $\mathsf{K}=(K,+,\cdot)$ be any ring such that $|K|\ge 3$. For any $a_1,a_2\in K$ if there exist $b\in K$ such that $a_1xa_2=b$ for all $x\in K\setminus\{0\}$ then $b=0$.

Proof is similar to proof of lemma 1.

For any considered ring $\mathsf{K}=(K,+,\cdot)$ we set

$$K^{l-zero}=\{a\in K\setminus\{0\}\,|\,(\forall x\in K\setminus\{0\})(ax=0)\},$$

$$K^{r-zero}=\{a\in K\setminus\{0\}\,|\,(\forall x\in K\setminus\{0\})(xa=0)\}.$$

Taking into account the notion of "division" we can extract the following three non-empty sets of considered finite rings $\mathsf{K}=(K,+,\cdot)$:

1. The set D^l of all rings $\mathsf{K}=(K,+,\cdot)$ with left division, i.e. $\mathsf{K}\in D^l$ if and only if for any $a\in K\setminus\{0\}$ and any $b\in K$ the set of solutions of equation $ax=b$ is non-empty.

2. The set D^r of all rings $\mathsf{K}=(K,+,\cdot)$ with right division, i.e. $\mathsf{K}\in D^r$ if and only if for any $a\in K\setminus\{0\}$ and any $b\in K$ the set of solutions of equation $xa=b$ is non-empty.

3. The set $D=D^l\cap D^r$ of all rings with two-sided division.

Taking into account the notion of "unit" we can partition all considered rings into the following six non-empty sets:

1. The set C_1 of all commutative rings $\mathsf{K}=(K,+,\cdot)$ with the unit, i.e. with such element $1\in K$ that $1x=x1=x$ for all $x\in K$.

2. The set C_2 of all commutative rings without the unit.

3. The set C_3 of all non-commutative rings $\mathsf{K}=(K,+,\cdot)$ with the unit $1\in K$.

4. The set C_4 of all non-commutative rings $\mathsf{K}=(K,+,\cdot)$ with some left unit $1_l\in K$ (i.e. $1_l x=x$ for all $x\in K$) and without any right unit (i.e. without any such element $1_r\in K$ that $x1_r=x$ for all $x\in K$).

5. The set C_5 of all non-commutative rings $\mathsf{K}=(K,+,\cdot)$ with some right unit $1_r \in K$ and without any left unit $1_l \in K$.

6. The set C_6 of all non-commutative rings $\mathsf{K}=(K,+,\cdot)$ without any left unit $1_l \in K$ and without any right unit $1_r \in K$, both.

Lemma 4. There hold identities

$$(C_1 \cup C_2) \cap D^{\alpha} = (C_1 \cup C_2) \cap D \quad (\alpha \in \{l,r\}). \quad (1)$$

Proof. Since $D \subset D^l$ and $D \subset D^r$ there hold inclusions

$$(C_1 \cup C_2) \cap D^l \subseteq (C_1 \cup C_2) \cap D, \quad (2)$$

$$(C_1 \cup C_2) \cap D^r \subseteq (C_1 \cup C_2) \cap D. \quad (3)$$

For any ring $\mathsf{K} \in (C_1 \cup C_2) \cap D^l$ the set of solutions of any equation $ax=b$ $(a \in K \setminus \{0\}, b \in K)$ is non-empty.

Since for any ring $\mathsf{K} \in C_1 \cup C_2$ equations $ax=b$ and $xa=b$ are equivalent to each other, then for any ring $\mathsf{K} \in (C_1 \cup C_2) \cap D^l$ the set of solutions of any equation $xa=b$ $(a \in K \setminus \{0\}, b \in K)$ is also non-empty.

This implies that $\mathsf{K} \in (C_1 \cup C_2) \cap D$. Thus, it holds inclusion

$$(C_1 \cup C_2) \cap D \subseteq (C_1 \cup C_2) \cap D^l. \quad (4)$$

Inclusion

$$(C_1 \cup C_2) \cap D \subseteq (C_1 \cup C_2) \cap D^r \quad (5)$$

can be proved similarly.

Inclusions (2)-(5) imply that identities (1) hold.

Q.E.D.

Lemma 4 implies that the following corollary holds.

Corollary 1. There hold identities

$$(C_1 \cup C_2) \setminus D^{\alpha} = (C_1 \cup C_2) \setminus D \quad (\alpha \in \{l,r\}).$$

Remark 2. There can be several one-sided units elements in a ring $\mathsf{K} \in C_4 \cup C_5$.

The simplest ring $\mathsf{K} \in C_4$ with two distinct left units contains four elements and its operations are determined in the following way

$+$	0	a	b	c	$\cdot$	0	a	b	c
0	0	a	b	c	0	0	0	0	0
a	a	0	c	b	a	0	a	b	c
b	b	c	0	a	b	0	a	b	c
c	c	b	a	0	c	0	0	0	0

To get the simplest ring $\mathsf{K} \in C_5$ with two distinct right units it is sufficient to transpose the matrix that determines multiplication.

We would use the following denotation for considered ring $\mathsf{K}=(K,+,\cdot)$:

1. If $\mathsf{K} \in C_1$, then K^{inv} is the set of all invertible elements of the ring K. Thus, $(K^{inv},\cdot)$ is the multiplicative (commutative) group of the ring K.
2. If $\mathsf{K} \in C_3$, then

$$K^{l-inv} = \{u \in K \mid (\exists v \in K)(vu=1)\}$$

is the set of all left-invertible elements of the ring K, and

$$K^{r-inv} = \{u \in K \mid (\exists w \in K)(uw=1)\}$$

is the set of all right-invertible elements of the ring K.

Thus, $(K^{l-inv} \cap K^{r-inv},\cdot)$ is the multiplicative (not necessary commutative) group of the ring K.

3. If $\mathsf{K} \in C_4$, then for any left unit $1_l \in K$

$$K^{l-inv}(1_l) = \{u \in K \mid (\exists v \in K)(vu=1_l)\}$$

is the set of all elements of the ring K, left invertible relatively to the left unit 1_l.

4. If $\mathsf{K} \in C_5$, then for any right unit $1_r \in K$

$$K^{r-inv}(1_r) = \{u \in K \mid (\exists v \in K)(uv=1_r)\}$$

is the set of all elements of the ring K, right invertible relatively to the right unit 1_r.

Let $\mathsf{K}=(K,+,\cdot) \in C_1$. Subsets $<x> = K^{inv}x$ $(x \in K)$ are called classes of associated elements of the ring K. It is well known that $<0>=\{0\}$, $<\alpha>=K^{inv}$ $(\alpha \in K^{inv})$ and

$$<x> * <y> = <xy>$$

for all $x, y \in K$.

The following generalization of the notion 'associated elements' was investigated in [10] for rings $\mathsf{K}=(K,+,\cdot) \in C_3$.

Let $K^{inv} = K^{l-inv} \cap K^{r-inv}$. Subsets $<x>_l = K^{inv}x$ $(x \in K)$ are called classes of l-associated elements and subsets $<x>_r = K^{inv}x$ $(x \in K)$ are called classes of r-associated elements. Thus, to determine any specific element $y \in <x>_l$ $(x \in K \setminus \{0\})$, as well as any specific element $z \in <x>_r$ $(x \in K \setminus \{0\})$ it is sufficiently to determine corresponding element of the set K^{inv}.

It is evident that:

1) $<0>_l = <0\}_r = \{0\}$;

2) $<\alpha>_l = <\alpha>_r = K^{inv}$ for any $\alpha \in K^{inv}$;

3) $<x>_l = <x>_r$ for any $x \in K^{cntr}$, where K^{cntr} is the center of the ring K;

4) $x \in <x>_l \cap <x>_r$ for any $x \in K$.

For any subsets A and B of the set K we set

$$A * B = \{ab \mid a \in A, b \in B\}.$$

Remark 3. For any ring $\mathsf{K} \in C_3$ if $K^{inv} \subseteq K^{cntr}$ then identities

$$< x >_l = < x >_r = < x > \quad (x \in K)$$

hold. Moreover, in this case in a ring K identities

$$< x > * < y > = < xy > \quad (x, y \in K)$$

also hold.

It was established in [10] that the following theorems hold.

Theorem 1. For any ring $\mathsf{K} \in C_3$

$$< xy >_l \subseteq < x >_l * < y >_l,$$
$$< xy >_r \subseteq < x >_r * < y >_r$$

for all $x, y \in K$.

Theorem 2. For any ring $\mathsf{K} \in C_3$

$$< x >_l * < y >_r = < xy >_l * K^{inv} = K^{inv} * < xy >_r,$$
$$xy \in < x >_r * < y >_l$$

for all $x, y \in K$.

4. Analysis of satisfiability of the simplest atoms.

In any associative finite ring $\mathsf{K} = (K, +, \cdot)$ with non-zero multiplication the simplest atoms are $ax \Diamond b$, $xa \Diamond b$ and $a_1 x a_2 \Diamond b$, where $a, a_1, a_2, b \in K$ are fixed elements and $\Diamond \in \{=, \neq\}$.

Remark 4. In any commutative ring atoms $ax \Diamond b$, $xa \Diamond b$ and $a_1 x a_2 \Diamond b$ are indistinguishable. Thus, when K is commutative ring only the simplest atoms $ax \Diamond b$ $(\Diamond \in \{=, \neq\})$ can be analyzed.

Let us consider architecture of $LA(\mathsf{K})$-solver $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ intended for analysis of satisfiability of atoms

$$ax = b, \quad (6)$$
$$xa = b \quad (7)$$

and

$$a_1 x a_2 = b, \quad (8)$$

where $a, a_1, a_2, b \in K$ are fixed elements.

This solver can be designed on the base of layering technique with the following hierarchy $M^{(1)}_1, M^{(1)}_2, M^{(1)}_3$ of modules.

Firstly, the module $M^{(1)}_1$ is activated. It produces the following computations.

If some atom (6) or (7) is analyzed it is checked, if $a = 0$, while if some atom (8) is analyzed it is checked, if $a_1 = 0$ or $a_2 = 0$.

Let $a = 0$ for an atom (6) or (7) (correspondingly, $a_1 = 0$ or $a_2 = 0$ for an atom (8)). It is checked, if $b = 0$. If this happens, $M^{(1)}_1$ returns *sat* and halts (thus, $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ also returns *sat* and halts). Otherwise, $M^{(1)}_1$ returns *unsat* and halts (thus, $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ also returns *unsat* and halts).

Let $a \neq 0$ for an atom (6) or (7) (correspondingly, $a_1 \neq 0$ and $a_2 \neq 0$ for an atom (8)).

Remark 5. Let it is analyzed some atom (8) under supposition that $a_1 \neq 0$ and $a_2 \neq 0$. If $\mathsf{K} \in D^l \setminus D^r$ then (8) can be transformed into (7), while if $\mathsf{K} \in D^r \setminus D^l$ then (8) can be transformed into (6).

The following two situations can take the place:

1. Let $\mathsf{K} \in D^l$ and some atom (6) is analyzed, or $\mathsf{K} \in D^r$ and some atom (7) is analyzed, or $\mathsf{K} \in D$ and some atom (8) is analyzed.

The module $M^{(1)}_1$ returns *sat* and halts (thus, $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ also returns *sat* and halts).

2. Let $\mathsf{K} \notin D^l$ and some atom (6) is analyzed, or $\mathsf{K} \notin D^r$ and some atom (7) is analyzed, or $\mathsf{K} \notin D^l \cup D^r$ and some atom (8) is analyzed.

If $\mathsf{K} \in C_1 \cup C_3 \cup C_4 \cup C_5$ then the module $M^{(1)}_2$ is activated, while if $\mathsf{K} \in C_2 \cup C_6$ then the module $M^{(1)}_3$ is activated.

The module $M^{(1)}_2$ produces some computations in the following four cases (in all other cases $M^{(1)}_2$ directly activates $M^{(1)}_3$).

1. Let $\mathsf{K} \in C_1 \setminus D$ (taking into account remark 4, we can restrict ourselves with atoms (6) only).

The module $M^{(1)}_2$ checks if $a \in K^{inv}$. If this happens, $M^{(1)}_2$ returns *sat* and halts (thus, $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ also returns *sat* and halts). Otherwise, the module $M^{(1)}_3$ is activated.

2. Let $\mathsf{K} \in C_3$ (we emphasize that if some atom (6) is analyzed then $\mathsf{K} \in C_3 \setminus D^l$, if some atom (7) is analyzed then $\mathsf{K} \in C_3 \setminus D^r$, and if some atom (8) is analyzed then (see remark 5) $\mathsf{K} \in C_3 \setminus (D^l \cup D^r)$).

The module $M^{(1)}_2$ produces the following computations.

For any atom (6) it is checked, if $a \in K^{l-inv}$. For any atom (7) it is checked, if $a \in K^{r-inv}$. For any atom (8) it is checked, if $a_1 \in K^{l-inv}$ and $a_2 \in K^{r-inv}$.

If this happens, $M_2^{(1)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *sat* and halts). Otherwise, the module $\mathsf{M}_3^{(1)}$ is activated.

3. Let $\mathsf{K} \in C_4 \setminus D^l$ The module $M_2^{(1)}$ produces the following computations.

For any atom (6) it is checked, if there exists some left unit $1_l \in K$ such that $a \in K^{l-inv}(1_l)$. If this happens, $M_2^{(1)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *sat* and halts). Otherwise, the module $M_3^{(1)}$ is activated.

For any atom (7) the module $M_3^{(1)}$ is activated.

For any atom (8) it is checked, if there exists some left unit $1_l \in K$ such that $a_1 \in K^{l-inv}(1_l)$. If this happens, then (8) is transformed into (7). The module $M_3^{(1)}$ is activated.

4. Let $\mathsf{K} \in C_5 \setminus D^r$ The module $M_2^{(1)}$ produces the following computations.

For any atom (7) it is checked, if there exists some right unit $1_r \in K$ such that $a \in K^{r-inv}(1_r)$. If this happens, $M_2^{(1)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *sat* and halts). Otherwise, the module $M_3^{(1)}$ is activated.

For any atom (6) the module $M_3^{(1)}$ is activated.

For any atom (8) it is checked, if there exists some right unit $1_r \in K$ such that $a_2 \in K^{r-inv}(1_r)$. If this happens, then (8) is transformed into (6). The module $M_3^{(1)}$ is then activated.

Architecture of the module $M_3^{(1)}$ depends essentially on the structure of considered ring K.

The simplest case is when $\mathsf{K} \in C_1 \cup C_3$. The following two approaches are possible, at least.

The first approach is based on direct checking satisfiability of atoms (possibly, by exploring these or the others algebraic properties of the structure of the ring K).

The second approach is based on exploring notion of 'associated elements' considered in the previous section and lies in the following.

Let $\mathsf{K} \in C_1 \setminus D$ (taking into account remark 4, we can restrict ourselves with atoms (6) only).

Satisfiability of (6) is reduced to satisfiability of the atom $< a > * < x > = < b >$ in the semigroup $(\{< x > | x \in K\}, *)$.

If the last atom is satisfiable then $M_3^{(1)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *sat* and halts). Otherwise, $M_3^{(1)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *unsat* and halts).

It is well known that cardinality of the set of classes of associated elements can be sufficiently less than cardinality of the set K. In this case considered approach seems to be promising.

Let $\mathsf{K} \in C_3$. Satisfiability of (6) is reduced to satisfiability of the formula $b \in < a >_r * < x >_l$, satisfiability of (7) is reduced to satisfiability of the formula $b \in < x >_r * < a >_l$, and satisfiability (8) is reduced to satisfiability of the formula $b \in < a_1 >_r * < x >_r * < a_2 >_l$.

If analyzed formula is satisfiable then $M_3^{(1)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *sat* and halts). Otherwise, $M_3^{(1)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ also returns *unsat* and halts).

Cardinality of the set of classes of l-associated elements as well as cardinality of the set of classes of r-associated elements can be sufficiently less than cardinality of the set K. In this case considered approach seems to be promising.

If $\mathsf{K} \in C_2 \cup C_4 \cup C_5 \cup C_6$ (especially in the absence of effective technique intended for solving factorization problem in a ring K) the module $M_3^{(1)}$ executes exhaustive searching over some subset $S \subseteq K$ which cardinality can be comparable with cardinality of the set K.

Since all considered rings could be partitioned into the sets C_i $(i = 1,\ldots,6)$, we get that the following theorem holds.

Theorem 3. $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ is complete and consistent.

Let us consider architecture of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$ intended for analysis of satisfiability of atoms

$$ax \neq b, \quad (9)$$

$$xa \neq b, \quad (10)$$

and

$$a_1 x a_2 \neq b, \quad (11)$$

where $a, a_1, a_2, b \in K$ are fixed elements.

Remark 6. Taking into account remark 4, we emphasize that when K is commutative ring only an atom (9) can be considered.

$LA(\mathsf{K})$-solver $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ can be designed on the base of layering technique with the following hierarchy $M^{(2)}_1, M^{(2)}_2, M^{(2)}_3$ of modules.

Firstly, the module $M^{(2)}_1$ is activated. It produces the following computations.

If some atom (9) or (10) is analyzed it is checked, if $a = 0$, while if some atom (11) is analyzed it is checked, if $a_1 = 0$ or $a_2 = 0$.

Let $a = 0$ if an atom (9) or (10) is analyzed (correspondingly, $a_1 = 0$ or $a_2 = 0$ if an atom (11) is analyzed).

It is checked, if $b = 0$. If this happens, $M^{(2)}_1$ returns *unsat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *unsat* and halts). Otherwise, $M^{(2)}_1$ returns *sat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *sat* and halts).

Let $a \neq 0$ if an atom (9) or (10) is analyzed (correspondingly, $a_1 \neq 0$ and $a_2 \neq 0$ if an atom (11) is analyzed).

The module $M^{(2)}_2$ is activated. It checks, if $b = 0$. If this happens, $M^{(2)}_2$ returns *sat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *sat* and halts). Otherwise, the module $M^{(2)}_3$ is activated.

Computations produced by the module $M^{(2)}_3$ depend on the following three situations:

1. Some atom (9) is analyzed. The module $M^{(2)}_3$ checks, if $a \in K^{l-zero}$. If this happens, $M^{(2)}_3$ returns *unsat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *unsat* and halts). Otherwise, $M^{(2)}_3$ returns *sat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *sat* and halts).

2. Some atom (10) is analyzed. The module $M^{(2)}_3$ checks, if $a \in K^{r-zero}$. If this happens, $M^{(2)}_3$ returns *unsat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *unsat* and halts). Otherwise, $M^{(2)}_3$ returns *sat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *sat* and halts).

3. Some atom (11) is analyzed. The module $M^{(2)}_3$ checks, if $a_1 \in K^{l-zero}$ or $a_2 \in K^{r-zero}$. If this happens, $M^{(2)}_3$ returns *unsat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *unsat* and halts). Otherwise, $M^{(2)}_3$ returns *sat* and halts (thus, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ also returns *sat* and halts).

Since all considered rings could be partitioned into the sets C_i $(i = 1,\ldots,6)$, we get that the following theorem holds.

Theorem 4. $LA(\mathsf{K})$-solver $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ is complete and consistent.

4. Analysis of satisfiability of a system of linear equations.

Let us consider architecture of $LA(\mathsf{K})$-solver $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ intended for analysis of satisfiability of atoms presented via systems of linear equations

$$a_{i1}x_1 + \ldots + a_{in}x_n = b_i \quad (i = 1,\ldots,m), \qquad (12)$$

$$x_1 a_{i1} + \ldots + x_n a_{in} = b_i \quad (i = 1,\ldots,m) \qquad (13)$$

and

$$u_{i1} + \ldots + u_{in} = b_i \quad (i = 1,\ldots,m), \qquad (14)$$

where u_{ij} $(i \in \mathbf{N}_m; j \in \mathbf{N}_n)$ is $a_{ij}x_j$, $x_j a_{ij}$ or $a'_{ij}x_j a''_{ij}$ and at least two of these three types of terms are presented.

Remark 7. Taking into account remark 4, we emphasize that when K is commutative ring only atom (12) can be considered.

$LA(\mathsf{K})$-solver $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ can be designed on the base of layering technique with the following hierarchy $M^{(3)}_1, M^{(3)}_2, M^{(3)}_3$ of modules.

Firstly, the module $M^{(3)}_1$ is activated. This module is based on usual Gauss method and it is intended to transform:

1) system (12) into equivalent diagonal form

$$e_{i_h}x_{i_h} = \sum_{j \in \mathbf{N}_n \setminus \{i_1,\ldots i_r\}} c_{i_h j}x_j + d_{i_h} \quad (h \in \mathbf{N}_r), \qquad (15)$$

where $e_{i_h} \neq 0$ $(h \in \mathbf{N}_r)$;

2) system (13) into equivalent diagonal form

$$x_{i_h}e_{i_h} = \sum_{j \in \mathbf{N}_n \setminus \{i_1,\ldots i_r\}} x_j c_{i_h j} + d_{i_h} \quad (h \in \mathbf{N}_r), \qquad (16)$$

where $e_{i_h} \neq 0$ $(h \in \mathbf{N}_r)$;

3) system (14) into equivalent diagonal form

$$e'_{i_h}x_{i_h}e''_{i_h} = \sum_{j \in \mathbf{N}_n \setminus \{i_1,\ldots i_r\}} c'_{i_h j}x_j c''_{i_h j} + d_{i_h} \quad (h \in \mathbf{N}_r), \qquad (17)$$

where $e'_{i_h}, e''_{i_h} \in K \setminus \{0\}$ $(h \in \mathbf{N}_r)$.

If some inconsistency is checked then $M^{(3)}_1$ returns *unsat* and halts (thus, $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ also returns *unsat* and halts). If transformation of analyzed system of linear equations into corresponding equivalent diagonal form is successful then the module $M^{(3)}_2$ is activated. Otherwise, the module $M^{(3)}_3$ is activated.

Remark 8. Any of equivalent diagonal forms (15)-(17) can be considered as a system of linear equations with parameters x_j $(j \in \mathbf{N} \setminus \{i_1,\ldots,i_r\})$.

The module $M_2^{(3)}$ is intended to check satisfiability of corresponding equivalent diagonal form.

This module is based on sequential analysis of equations of equivalent diagonal form by applying corresponding $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$.

Besides, if it is necessary, it is executed some analysis of non-emptiness of the set of admissible parameters x_j $(j \in \mathbf{N} \setminus \{i_1,\ldots,i_r\})$. This analysis is based on these or the others algebraic properties of the structure of the ring K.

Remark 9. It is evident that if the set of admissible of parameters x_j $(j \in \mathbf{N} \setminus \{i_1,\ldots,i_r\})$ is empty then corresponding initial system of equations is unsatisfiabe. Thus, if it is checked that set of admissible of parameters x_j $(j \in \mathbf{N} \setminus \{i_1,\ldots,i_r\})$ is empty then $M_2^{(3)}$ immediately returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts).

If $M_2^{(3)}$ establishes that corresponding equivalent diagonal form is consistent it returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *sat* and halts). If $M_2^{(3)}$ establishes that corresponding equivalent diagonal form is inconsistent it returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts). Otherwise the module $M_3^{(3)}$ is activated.

The module $M_3^{(3)}$ is intended to check if is non-empty the set of solutions of initial system of equations (correspondingly, of equivalent diagonal form). This module is based on searching (possibly restricted by exploring these or the others algebraic properties of the structure of the ring K).

If it is checked that the set of solutions of initial system of equations (correspondingly, of equivalent diagonal form) is non-empty then $M_3^{(3)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *sat* and halts). Otherwise, $M_3^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts).

Taking into account theorem 3, we get that the following theorem holds.

Theorem 5. $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ is complete and consistent.

5. Analysis of satisfiability of a system of linear disequalities.

Let us consider architecture of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ intended for analysis of satisfiability of atoms presented via systems of linear disequalities

$$a_{i1}x_1 + \ldots + a_{in}x_n \neq b_i \quad (i = 1,\ldots,m), \qquad (18)$$

$$x_1 a_{i1} + \ldots + x_n a_{in} \neq b_i \quad (i = 1,\ldots,m), \qquad (19)$$

and

$$u_{i1} + \ldots + u_{in} \neq b_i \quad (i = 1,\ldots,m), \qquad (20)$$

where u_{ij} $(i \in \mathbf{N}_m; j \in \mathbf{N}_n)$ is $a_{ij}x_j$, $x_j a_{ij}$ or $a'_{ij}x_j a''_{ij}$ and at least two of these three types of terms are presented.

We associate with analyzed system of disequalities (18), (20) and (21), correspondingly, the system of linear equations

$$a_{i1}x_1 + \ldots + a_{in}x_n = b_i + \alpha_i \quad (i = 1,\ldots,m), \qquad (21)$$

$$x_1 a_{i1} + \ldots + x_n a_{in} = b_i + \alpha_i \quad (i = 1,\ldots,m) \qquad (22)$$

and

$$u_{i1} + \ldots + u_{in} = b_i + \alpha_i \quad (i = 1,\ldots,m), \qquad (23)$$

where $\alpha_1,\ldots,\alpha_m \in K \setminus \{0\}$ are parameters.

It is evident that:

1) system of disequalities (18) is satisfiable if and only if associated system of equations (21) is satisfiable;

2) system of disequalities (19) is satisfiable if and only if associated system of equations (22) is satisfiable;

3) system of disequalities (20) is satisfiable if and only if associated system of equations (23) is satisfiable.

This factor implies that $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ can be designed on the base of layering technique with the following hierarchy $M_1^{(4)}, M_2^{(4)}, M_3^{(4)}$ of modules.

Firstly, the module $M_1^{(4)}$ is activated. It transforms analyzed system of disequalities into corresponding associated system of linear equations. Then the module $M_2^{(4)}$ is activated.

The module $M_2^{(4)}$ is based on applying $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ to corresponding associated system of linear equations.

Besides, if it is necessary, it is executed some analysis of non-emptiness of the set of admissible parameters $\alpha_1,\ldots,\alpha_m \in K \setminus \{0\}$. This analysis is based on these or the others algebraic properties of the structure of the ring K.

Remark 10. It is evident that if the set of admissible parameters $\alpha_1,\ldots,\alpha_m \in K \setminus \{0\}$ is empty then corresponding initial system of disequalities is unsatisfiabe. Thus, if it is checked that set of admissible of parameters $\alpha_1,\ldots,\alpha_m \in K \setminus \{0\}$ is empty then $M_2^{(4)}$ immediately returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ also returns *unsat* and halts).

If $M_2^{(4)}$ establishes that corresponding associated system of linear equations is consistent it returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ also returns *sat* and halts). If $M_2^{(4)}$ establishes that corresponding associated system of linear equations is inconsistent it returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ also returns *unsat* and halts). Otherwise the module $M_3^{(4)}$ is activated.

The module $M_3^{(4)}$ is intended to check if is non-empty the set of solutions of initial system of disequalities and is based on searching (possibly restricted by exploring these or the others algebraic properties of the structure of the ring K) and applying corresponding $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$, when it is necessary.

If it is checked that the set of solutions of initial system of disequalities is non-empty then $M_3^{(4)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ also returns *sat* and halts). Otherwise, $M_3^{(4)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ also returns *unsat* and halts).

Taking into account theorems 4 and 5, we get that the following theorem holds.

Theorem 6. $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ is complete and consistent.

6. Time complexity of $LA(\mathsf{K})$-solvers.

We would analyze time complexity of proposed $LA(\mathsf{K})$-solvers in terms of logarithmic weight [11].

Time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ can be characterized in the following way.

Theorem 7. For any finite field $\mathrm{GF}(p^k)$ ($p \in \mathbf{N}$ is prime integer and $k \in \mathbf{N}$) time complexity of $LA(\mathrm{GF}(p^k))$-solver $\mathsf{S}_{LA(\mathrm{GF}(p^k))}^{(1)}$ is

$$T = \begin{cases} O(\log p), \text{if } p \to \infty \text{ and } k \text{ is fixed} \\ O(k), \text{if } k \to \infty \text{ and } p \text{ is fixed} \\ O(k \log p), \text{if } p \to \infty \text{ and } k \to \infty \end{cases}. \quad (24)$$

Proof. For any finite field $\mathrm{GF}(p^k)$ ($p \in \mathbf{N}$ is prime integer and $k \in \mathbf{N}$) the modules $M_2^{(1)}$ and $M_3^{(1)}$ are not needed at all.

For any finite field $\mathrm{GF}(p^k)$ ($p \in \mathbf{N}$ is prime integer and $k \in \mathbf{N}$) time complexity of the module $M_1^{(1)}$ is determined by formula (24).

Thus, time complexity of $LA(\mathrm{GF}(p^k))$-solver $\mathsf{S}_{LA(\mathrm{GF}(p^k))}^{(1)}$ is also determined by formula (24).

Q.E.D.

The simplest finite rings $\mathsf{K} \in C_1 \setminus (D^l \cup D^r)$ are rings of residues $\mathsf{Z}_{p^k} = (\mathbf{Z}_{p^k}, +, \cdot)$, where $p \in \mathbf{N}$ is prime integer and $k \geq 2$.

Theorem 8. For any ring of residues $\mathsf{Z}_{p^k} = (\mathbf{Z}_{p^k}, +, \cdot)$ ($p \in \mathbf{N}$ is prime integer and $k \geq 2$) time complexity of $LA(\mathsf{Z}_{p^k})$-solver $\mathsf{S}_{LA(\mathsf{Z}_{p^k})}^{(1)}$ is

$$T = \begin{cases} O(\log p), \text{if } p \to \infty \text{ and } k \text{ is fixed} \\ O(\log k), \text{if } k \to \infty \text{ and } p \text{ is fixed} \\ O(\log pk), \text{if } p \to \infty \text{ and } k \to \infty \end{cases}. \quad (25)$$

Proof. Any non-zero element of a ring Z_{p^k} ($p \in \mathbf{N}$ is prime integer and $k \geq 2$) can be presented in the form αp^i, where $\alpha \in \mathbf{N}_{p-1}$ and $i \in \mathbf{Z}_p$, while zero of the ring Z_{p^k} can be presented as $0 p^0$.

Thus, checking if $\alpha p^i = 0$ is reduced to checking if $\alpha = 0$ and $i = 0$. Thus, time complexity of the module $M_1^{(1)}$ is

$$T_1 = \begin{cases} O(\log p), \text{if } p \to \infty \text{ and } k \text{ is fixed} \\ O(\log k), \text{if } k \to \infty \text{ and } p \text{ is fixed} \\ O(\log pk), \text{if } p \to \infty \text{ and } k \to \infty \end{cases}. \quad (26)$$

Checking if $\alpha p^i \in \mathbf{Z}_{p^k}^{inv}$ is reduced to checking if $\alpha \neq 0$ and $i = 0$. Thus, time complexity of the module $M_2^{(1)}$ is

$$T_2 = \begin{cases} O(\log p), \text{if } p \to \infty \text{ and } k \text{ is fixed} \\ O(\log k), \text{if } k \to \infty \text{ and } p \text{ is fixed} \\ O(\log pk), \text{if } p \to \infty \text{ and } k \to \infty \end{cases}. \quad (27)$$

Classes of associated elements of the ring Z_{p^k} ($p \in \mathbf{N}$ is prime integer and $k \geq 2$) are $<0>=\{0\}$, $C_1 = \mathbf{N}_{p-1}$ and $C_{i+1} = \{\alpha p^i \mid \alpha \in \mathbf{N}_{p-1}\}$ $(i \in \mathbf{N}_{k-1})$.

Any atom $ax=b$, where $a\in C_i$ $(i\in \mathbf{N}_k)$ and $b\in C_j$ $(j\in \mathbf{N}_k)$ can be transformed into the atom $C_i * < x >= C_j$. Satisfiability of the last atom is reduced to checking if $i\le j$. Thus, time complexity of the module $M_3^{(1)}$ is

$$T_3=\begin{cases}O(1), \text{if } k \text{ is fixed}\\ O(\log k), \text{if } k\to\infty\end{cases}. \qquad (28).$$

Since $T=T_1+T_2+T_3$, formulae (26)-(28) imply that the formula (25) holds.

Q.E.D.

Let $\mathsf{K}\in C_2\cup C_4\cup C_5\cup C_6$ under condition that there is no effective technique intended for solving factorization problem in the ring K. In this case the module $M_3^{(1)}$ executes exhaustive searching over some subset $S\subseteq K$ which cardinality can be comparable with cardinality of the set K.

Thus, in this case time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$ is some sub-exponent, at least.

Time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$ can be characterized in the following way.

Theorem 9. For any finite field $\mathrm{GF}(p^k)$ ($p\in\mathbf{N}$ is prime integer and $k\in\mathbf{N}$) time complexity of $LA(\mathrm{GF}(p^k))$-solver $\mathsf{S}_{LA(\mathrm{GF}(p^k))}^{(2)}$ is determined by formula (24).

Proof. For any finite field $\mathrm{GF}(p^k)$ time complexity of each of the modules $M_1^{(2)}$ and $M_2^{(2)}$ is determined by formula (24).

For any finite field $\mathrm{GF}(p^k)$ time complexity of the module $M_3^{(2)}$ is some constant, since $K^{l-zero}=K^{r-zero}=\varnothing$.

Thus, time complexity of $LA(\mathrm{GF}(p^k))$-solver $\mathsf{S}_{LA(\mathrm{GF}(p^k))}^{(2)}$ is determined by formula (24).

Q.E.D.

Theorem 10. For any ring of residues $\mathsf{Z}_{p^k}=(\mathbf{Z}_{p^k},+,\cdot)$ ($p\in\mathbf{N}$ is prime integer and $k\ge 2$) time complexity of $LA(\mathsf{Z}_{p^k})$-solver $\mathsf{S}_{LA(\mathsf{Z}_{p^k})}^{(2)}$ is determined by formula (26).

Proof is similar to proof of theorem 9.

Time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$ could depend essentially on time complexity of the module $M_3^{(2)}$. Time complexity of checking, if $\alpha\in X$ $(X\in\{K^{l-zero},K^{r-zero}\})$ do not exceed

$T=O(\max\{|K^{l-zero}|,|K^{r-zero}|\}\log|K|)$ $(|K|\to\infty)$.

This estimation is upper bound for time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$.

Time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ can be characterized in the following way.

Theorem 11. For any finite field $\mathrm{GF}(p^k)$ ($p\in\mathbf{N}$ is prime integer and $k\in\mathbf{N}$) time complexity of $LA(\mathrm{GF}(p^k))$-solver $\mathsf{S}_{LA(\mathrm{GF}(p^k))}^{(3)}$ is

$$T=(O(\min\{m,n\}(t_1+mn^2t_2)) \ (p^k\to\infty), \qquad (29)$$

where t_1 is time complexity of computing of inverse element and t_2 is time complexity of multiplication in the field $\mathrm{GF}(p^k)$.

Proof. For any finite field $\mathrm{GF}(p^k)$ the module $M_3^{(3)}$ is not needed at all.

The module $M_1^{(3)}$ tries to transform initial system of equations into equivalent diagonal form

$$x_{i_h}=\sum_{j\in\mathbf{N}_n\setminus\{i_1,\dots i_r\}}c_{i_hj}x_j+d_{i_h} \quad (h\in\mathbf{N}_r). \qquad (30)$$

Transformation of any equation

$$a_{ij}x_j+a_{i,j+1}x_{j+1}+\dots+a_{in}x_n=b_i$$

into equation

$$x_j+a'_{i,j+1}x_{j+1}+\dots+a'_{in}x_n=b'_i$$

needs one operation of computing of inverse element a_{ij}^{-1} and $n-j$ operations of multiplication. Thus, time complexity of this step is

$$T_1'(j)=O(t_1+(n-j)t_2) \ (p^k\to\infty). \qquad (31)$$

Deleting of variable x_j from any other equation of analyzed system needs $n-j$ operations of multiplication and $n-j$ operations of addition. Since time complexity of addition is much more less then time complexity of multiplication we can ignore time complexity of addition.

Thus, time complexity of this step is also determined by formula

$$T_1''(j)=O((n-j)t_2) \ (p^k\to\infty).$$

This implies that time complexity of deleting of variable x_j from all the others equation of analyzed system is

$$T_1''(j)=O(m(n-j)t_2) \ (p^k\to\infty). \qquad (32)$$

Time complexity of module $M_1^{(3)}$ is

$$T_1 = \sum_{j=1}^{\min\{m,n\}} (T_1'(j) + T_2'''(j)).$$

Taking into account formulae (31) and (32), we get

$$T_1 = O(\min\{m,n\}(t_1 + mn^2 t_2)) \ (p^k \to \infty).$$

If some inconsistency is checked then $M_1^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts).

Otherwise, the module $M_2^{(3)}$ directly returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *sat* and halts), i.e. time complexity of the module $M_1^{(2)}$ is

$$T_2 = O(1) \ (p^k \to \infty).$$

Since $T = T_1 + T_2$, we get that formula (29) holds. Q.E.D.

The situation differs essentially for any ring of residues $\mathsf{Z}_{p^k} = (\mathbf{Z}_{p^k}, +, \cdot)$ ($p \in \mathbf{N}$ is prime integer and $k \geq 2$). In this case the module $M_3^{(3)}$ also is not needed.

The module $M_1^{(3)}$ tries to transform initial system of equations into equivalent diagonal form

$$\alpha_{i_h} p^{v_h} x_{i_h} = \sum_{j \in S_{i_h}} \beta_{i_h j} p^{w_{i_h j}} x_j + \gamma_{i_h} p^{l_h} \ (h \in \mathbf{N}_r), \quad (33)$$

where $S_{i_h} \subseteq \mathbf{N}_n \setminus \{i_1, \ldots, i_r\}$, $\alpha_{i_h}, \beta_{i_h j} \in \mathbf{Z}_{p^k}^{inv}$, and $\gamma_{j_h} = 0$ or $\gamma_{i_h} \in \mathbf{Z}_{p^k}^{inv}$,.

Dealing as in proof of theorem 11, we establish that time complexity of the module $M_1^{(3)}$ is determined by formula

$$T_1 = O(\min\{m,n\}(t_1 + mn^2 t_2)) \ (p^k \to \infty), \quad (34)$$

where t_1 is time complexity of computing of inverse element and t_2 is time complexity of multiplication in the ring Z_{p^k}.

If some inconsistency is checked then $M_1^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts). Otherwise, the module $M_2^{(3)}$ is activated.

The module $M_2^{(3)}$ executes sequential analysis of equations of equivalent diagonal form (33) in accordance with the following scheme.

Step 1. $U := K^n$, $h := 1$.

Step 2. If $\gamma_{i_h} = 0$ then go to step 8.

Step 3. If $l_h \geq \min\{\min\{w_{i_h j} \mid j \in S_{i_h}\}, v_h\}$ then go to step 5.

Step 4. The module $M_2^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts).

Step 5. Compute the set V_h of solutions of h-th equation of equivalent diagonal form.

Step 6. If $V_h = \varnothing$ then $M_2^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts), else $U := U \cap V_h$.

Step 7. If $U = \varnothing$ then $M_2^{(3)}$ returns *unsat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *unsat* and halts).

Step 8. If $h = r$ then $M_2^{(3)}$ returns *sat* and halts (thus, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ also returns *sat* and halts), else $h := h + 1$ and go to step 2.

It is evident that time complexity of the module $M_2^{(3)}$ is much more higher then (34) and is the same as time complexity of searching the set of solutions of equivalent diagonal form (33).

Moreover, let $\mathsf{K} \in C_2 \cup C_4 \cup C_5 \cup C_6$ under condition that there is no effective technique intended for solving factorization problem in the ring K. In this case the module $M_2^{(3)}$ executes exhaustive searching over some subset $S \subseteq K$ which cardinality can be comparable with cardinality of the set K. Thus, in this case time complexity of $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ is some sub-exponent, at least.

It was established that analysis of satisfiability of any system of disequalities is equivalent to analysis of satisfiability of associated system of linear equations. Thus, time complexity of any $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$ is not less than time complexity of corresponding $LA(\mathsf{K})$-solver $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$.

Conclusions.

In the given paper there are developed mathematical methods intended for resolving the problem of analysis of satisfiability modular linear arithmetic over any finite associative (not necessary commutative) ring with non-zero multiplication. General schemes for solvers intended for analysis of satisfiability of formulae presented via any system of linear equations or linear disequalities are proposed.

It is evident that if analyzed formula is presented via some system of linear equations and disequalities then its analysis is reduced to sequential application of corresponding $LA(\mathsf{K})$-solvers $\mathsf{S}_{LA(\mathsf{K})}^{(1)}$, $\mathsf{S}_{LA(\mathsf{K})}^{(2)}$, $\mathsf{S}_{LA(\mathsf{K})}^{(3)}$ and $\mathsf{S}_{LA(\mathsf{K})}^{(4)}$.

It is worth to note that if $LA(\mathsf{K})$-solver $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$ concludes that all analyzed simplest atoms (6)-(8) are satisfiable then these atoms can be used for substitution into all other atoms of analyzed formula. And only after this substitution $LA(\mathsf{K})$-solver $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$ can be applied.

Similarly, let $LA(\mathsf{K})$-solver $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ has produced equivalent diagonal form for analyzed system of equations. If this solver concludes that all analyzed atoms are satisfiable then equivalent diagonal form can be used for substitution into all disequalities. And only after this substitution $LA(\mathsf{K})$-solver $\mathsf{S}^{(4)}_{LA(\mathsf{K})}$ can be applied.

In the given paper time complexity of proposed solvers is estimated for finite fields and rings of residues. It was established that even for the simplest rings, i.e. for rings of residues time complexity of $LA(\mathsf{K})$-solvers $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ and $\mathsf{S}^{(4)}_{LA(\mathsf{K})}$ is much more higher than time complexity of corresponding $LA(\mathsf{K})$-solvers intended for finite fields.

Detailed analysis of time complexity for the simplest non-commutative rings forms one of trends for future research.

It is well known that any system of equations over some finite ring determines some variety over this ring (see [12], for example).

Proposed in the given paper $LA(\mathsf{K})$-solvers $\mathsf{S}^{(1)}_{LA(\mathsf{K})}$, $\mathsf{S}^{(2)}_{LA(\mathsf{K})}$, $\mathsf{S}^{(3)}_{LA(\mathsf{K})}$ and $\mathsf{S}^{(4)}_{LA(\mathsf{K})}$ can be applied for analysis of structure of linear varieties over finite rings.

Analysis of general schemes for solvers intended for analysis of satisfiability of formulae presented via systems of non-linear equations or non-linear disequalities over finite rings forms another trend for future research.

List of references

1. *Sebastiani R.* Lazy satisfiability modulo theories // Journal on Satisfiability, Boolean Modeling and Computation. – 2007. – N 3. – P. 141-224.
2. *Nieuwenhuis R., Oliveras A., Tinelli C.* Solving SAT and SAT modulo theories: from an abstract Davis-Putnam-Longemann-Loveland procedure to DPLL(T) // Journal of ACM. – 2006. – N 6. – P. 937-977.
3. *Bozzano M., Brutomesso R., Cimatti A., et al.* MathSAT5: Tight integration of SAT and mathematical decision procedures // Journal of Automated Reasoning. – 2005. – N 1-3. – P. 265-293.
4. *Barret C., Nieuwenhuis R., Oliveras A., et al.* Splitting on demand in SAT modulo theories // LNCS. – 2006. – 4246. – P. 512-526.
5. *Duterte B., de Morura L.* A fast linear-arithmetic solver for DPLL(T) // LNCS. – 2006. – 4144. – P. 81-94.
6. *Faure G., Nieuwenhuis R., Oliveras A., et al.* SAT modulo the theory of linear arithmetic: exact, inexact and commercial solvers // LNCS. – 2008. – 4996. – P. 77-90.
7. *Griggio A.* A practical approach to satisfiability modulo linear integer arithmetic // Journal on Satisfiability, Boolean Modeling and Computation. – 2012. – N 8. – P. 1-27.
8. *Charin Yu.S., Bernik V.I., Matveev G.V., et al.* Mathematical and computer backgrounds of cryptology. – Minsk: Novoye znanie, 2003. – 382 p. (in Russian).
9. *Kurosh A.G.* Lectures in general algebra. – Moscow: Nauka, 1973. – 400 p. (in Russian).
10. *Skobelev V.V.* On systems of polynomial equations over finite rings // Naukovy zapiski NaUKMA. – 2012. – V.138. – P. 15-19.
11. *Aho A., Hopcroft Jh., Ullman Jh.* The design and analysis of computer algorithms. – Moscow: Mir, 1979. – 536 p. (in Russian).
12. *Skobelev V.V., Glazunov N.M., Skobelev V.G.* Varieties over rings. Theory and applications. – Donetsk: IAMM of NAS of Ukraine, 2011. – 323 p. (in Russian).

Надійшла до редколегії 29.01.11