International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 2, Issue. 6, Nov-Dec. 2012 pp-4133-4137 ISSN: 2249-6645

The Computational Algorithm for Supported Solutions Set of Linear Diophantine Equations Systems in a Ring of Integer Numbers

Serigiy L. Kryvyi[1], Paweł Dymora[2], Mirosław Mazurek[3]
[1](Department of Distributed Systems, Rzeszow University of Technology, Poland)

ABSTRACT:*The algorithm for computation of minimal supported set of solutions and base solutions of linear Diophantine equations systems in a ring of integer numbers is proposed. This algorithm is founded on the modified TSS-method.*

Keywords:*ring of integer numbers, linear Diophantine equations, supported set, supported set of solutions*

I. INTRODUCTION

Linear Diophantine equations and also their systems are often present in a wide variety of sciences with heavy usage of computations. In order to solve many different systems these equations are brought to taskof integerlinear programming, pattern recognitionandmathematicalgames[2], cryptography[3], unification[4], parallelizationof cycles[5], etc. In this case, the sets of parameters of the equations are usuallysetsof integers, residue ringor residue field of any number modulo and sets in which solutions to the equations are found in ringsof integers, the set ofnatural numbersorfinitefieldsandresidue rings. Algorithms forfinding solutionsoflinearDiophantineequations system (SLDE) in the setof natural numbershave been described inmany publications [6] -[12]. In this work we will focus on analyzes of the computation of SLDE algorithm in a ringof integers. The basisof the proposedalgorithmis theTSSmethodusedfor the constructing the minimalsetof solutionsforming ahomogeneous system of linearDiophantineequations(HSLDE) on thesetof natural numbers[1].

II. PRELIMINARIES

The systems of linear Diophantine equations. The system of linear Diophantine equations in a ring Z is described as follows:

$$S=\begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \ldots \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n = b_q, \end{cases} \qquad (1)$$

Where: $a_{ij}, b_i, x_i \in Z$, $i=1,\ldots,n$, $j=1,\ldots,q$. Solution to SLDE (1) we will call a vector $c=(c_1,c_2,\ldots,c_n)$, which by substitution in $L_i(x)$ for the value x_j , c_j transforms $L_i(c)\equiv b_i$ into identity for all $i=1,2,\ldots,q$. SLDE is called Homogenous (HSLDE), where all b_i are equal to 0, otherwise the system is called inhomogeneous (ISLDE).

A. 2.1. The TSS method of HSLDE solution

Let's consider HSLDE S presented as (1) and $e_1=(1,0,\ldots,0)$, $e_2=(0,1,\ldots,0)$, …, $e_n=(0,\ldots,0,1)$ which are unitary vectors of canonical set base Z^n. Let's have M as solutions set for the system S . Since it is homogeneous, than the zero vectors is always valid solution. Such a solution is called trivial and any other non- zero solution of S is called non-trivial. The HSLDE is called contrary, only when the set M is composed exclusively with the trivial solution; otherwise it is called non contrary.

The TSS method and its implementation for linear equations systems in a set of natural numbers have been described in detail in [1]. Let's consider a modification of this method in case of the ring of integer numbers Z .

The case of homogeneous linear Diophantine equation (HLDE). Let's define the HLDE with the following form:

$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0,$ (2)

Where: $a_i, x_i \in Z, i=1,\ldots,n$.

Let's consider a set of canonical base vectors $M=\{e_1,\ldots,e_n\}$ and a function $L(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ HLDE (2). Without limiting the generality, assume that in the function $L(x)$ the first non-zero coefficient is a_1 and $a_1>0$.

Let's build a set of vectors $B=\{e_1=(-a_2,a_1,0,\ldots,0), e_2=(-a_3,0,a_1,0,\ldots,0),$ $e_{q-1}=(-a_q,0,0,\ldots,0,a_1)\}\cup M_0$ where $M_0=\{e_r : L(e_r)=0\}$, $a_j\neq 0$, while, if for some a_i GCD (Great Common Divisor) $(a_1,a_1)\neq 1$, than the coordinates of this vector can be reduced to this GCD. Selected non-zero coefficient a_1 will be called a primary. This way, one can assume, that all vectors in the set B are such, that a_i and a_1 are mutually simple. In other words, set B is constructed by combining the first non-zero coefficient with the last non-zero coefficient, having different signs and being complemented with canonical base vectors, which correspond to zero coefficients HLDE (2). This kind of constructed set is called the TSS set or base set. It is obvious that vectors from the set B are solutions of HLDE (2), and the set B is closed in a respect to summation, subtraction and multiplication by an element from the ring Z .

Lemma 1. Let $x=(c_1,c_2,\ldots,c_q)$ - be a some solution of HLDE (2), than, if $x\notin B$, than x can be represented as a nonnegative linear combination in the form:

$$a_1x = c_2e_1 + c_3e_2 + \ldots + c_qe_{q-1},$$

where: $e_i \in B, i=1,\ldots,q-1$.

Proof. If $x=(c_1,\ldots,c_q)\in M$, than the vector has a following representation:

$$a_1x = c_2e_1 + c_3e_2 + ... + c_qe_{q-1} =$$
$$(-c_2a_1 - c_3a_3 - ... - c_qa_q, c_2a_1, ..., c_qa_1) =$$
$$= (c_1a_1, c_2a_1, ..., c_qa_1) = a_1(c_1, c_2, ..., c_q)$$

Due to the fact that x is a solution of HLDE (2), i.e. $a_1c_1 = -a_2c_2 - a_3c_3 - ... - a_qc_q$.

Note, that if a vector e_j from B is a canonical base vector and the j-th coordinate of the vector x is equal to c_j, than in the vector x representation, the vector e_j enters with a coefficient a_1c_j. Lemma proved.

The proved lemma results with the following conclusion.

Conclusion 1. If among the coefficients HLDE is even one coefficient equal 1, than the set B is a base of all HLDE solutions set. Then indeed, the elements of the set B have the form:

$$\{e_1 = (-a_2, 1, 0, ..., 0), e_2 = (-a_3, 0, 1, 0, ..., 0), e_{q-1} = (-a_q, 0, 0, ..., 0, 1)\} \cup M_0,$$

i.e. if in the distribution of any solution x into vectors of the set B the basic coefficient is equal one, then this means, that the set B will be the base.

Example 1. Let's build TSS HLDE

$$L(x) = 3x_1 + y - z + 2u + v = 0$$

The base set or the TSS base of the HLDE has the following form:

$$e_1 = (-1, 3, 0, 0, 0), e_2 = (1, 0, 3, 0, 0), e_3 = (-2, 0, 0, 3, 0), e_4 = (-1, 0, 0, 0, 3)$$

The solutions LJRD $x_1 = (0, 2, 3, 0, 1), x_2 = (1, 1, 0, -2, 0)$ have the representation $3x_1 = 2e_1 + 3e_2 + e_4$, $3x_2 = e_1 - 2e_3$.

All the solutions to any set of HLDE is presented as a set:

$$B = \{e_1 = (1, -3, 0, 0, 0), e_2 = (0, 1, 1, 0, 0), e_3 = (0, -2, 0, 1, 0), e_4 = (0, -1, 0, 0, 1)\}$$

In this vector's base x_1 and x_2 have the representation: $x_1 = 3e_2 + e_4$, $x_2 = e_1 - 2e_3$.

The case of homogenous system of linear Diophantine equations. Let's consider the HSLDE:

$$S = \begin{cases} L_1(x) = a_{11}x_1 + ... + a_{1n}x_n = 0, \\ L_2(x) = a_{21}x_1 + ... + a_{2n}x_n = 0, \\ ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \\ L_q(x) = a_{q1}x_1 + ... + a_{qn}x_n = 0, \end{cases}$$

Where: $a_{ij}, x_i \in Z$, $i = 1, ..., q$, $j = 1, ..., n$.

Let's build the base set $B_1 = \{e_1^1, e_2^1, ..., e_{q-1}^1\}$ for the first equation $L_1(x) = 0$ and let's calculate values $L_2(e_i^1) = b_i$ where $e_i^1 \in B_1, b_i \in Z$. Then, let's create an equation:

$$b_1y_1 + ... + b_iy_i + ... + b_{q-1}y_{q-1} = 0 \qquad (4)$$

Then let's build its base set $B_1^{'} = \{s_1, ..., s_{q-2}\}$. Vectors s_i from $B_i^{'}$ corresponds to solutions vectors $B_2 = \{e_1^2, ..., e_{q-2}^2\}$ HSLDE $L_1(x) = 0 \wedge L_2(x) = 0$.

Lemma 2. Vectors set B_2 describes the base set of HSLDE $L_1(x) = 0 \wedge L_2(x) = 0$, i.e. any solution x of this system has a representation $kx = l_1e_1^2 + ... + l_{q-2}e_{q-2}^2$, where: $e_i^2 \in B_2$, $l_i \in Z$, $i = 1, ..., q-2$.

Proof. Let's have x to be any solution to HSLDE $L_1(x) = 0 \wedge L_2(x) = 0$. Because x is a solution $L_1(x) = 0$, and taking into account lemma 1, x can be represented as:

$$dx = a_1e_1^1 + ... + a_{q-1}e_{q-1}^1,$$

Where: $e_i^1 \in B_1$, $a_i \in Z$, $i = 1, ..., q-1$. Then, due to the fact that x is the solution $L_2(x) = 0$ we obtain:

$$L_2(dx) = a_1b_1 + ... + a_{q-1}b_{q-1} = 0,$$

Where $b_j = L_2(e_j^1)$, $j = 1, ..., q-1$. Respectively, vector $a = (a_1, ..., a_{q-1})$ is a solution of HLDE (4) and due to lemma 1 we get:

$$ka = d_1s_1 + ... + d_{q-2}s_{q-2},$$

Where: $s_i \in B_1^{'}$, $d_i \in Z$, $i = 1, ..., q-2$, and k - is the main coefficient of given HLDE . Thus:

$$kdx = d_1e_1^2 + ... + d_{q-2}e_{q-2}^2$$

where $e_i^2 \in B_2$, $i = 1, ..., q-2$.

The lemma 2 proved.

The following theorem can be proven with a help of mathematical induction, directly from lemma 1 and 2.

Theorem1. TSS HSLDE B_1 (2) is built using the described above manner and it is a base of all solutions set of a given HSLDE.

Example 2. Let's describe the base set of HSLDE:

$$S = \begin{cases} L_1(x) = 3x_1 + x_2 - x_3 + 2x_4 + x_5 = 0, \\ L_2(x) = 2x_1 + 3x_2 + 0x_3 - x_4 + 2x_5 = 0. \end{cases}$$

The base set for the first equation was described in a first example.

$$B_1 = \{e_1^1 = (1, -3, 0, 0, 0), e_2^1 = (0, 1, 1, 0, 0), e_3^1 = (0, -2, 0, 1, 0), e_4^1 = (0, -1, 0, 0, 1)\}.$$

Values $L_2(x)$ for a given vectors respectively equal to: -7, 3, -7, 1. let's construct the equation $-7y_1 + 3y_2 - 7y_3 - y_4 = 0$ and let's transform the base set of this HLDE:

$$B_1^{'} = \{s_1 = (3, 7, 0, 0), s_2 = (-1, 0, 1, 0), s_3 = (-1, 0, 0, 7)\}.$$

These vectors correspond with TSS vectors (base set):

$$B_2 = \{e_1^2 = (3, -2, 7, 0, 0), e_2^2 = (-1, 1, 0, 1, 0), e_3^2 = (-1, -4, 0, 0, 7)\}.$$

If during the construction of the base equation $-7y_1 + 3y_2 - 7y_3 - y_4 = 0$ we perform combining in accordance (4)with the last value (ie. in respect to -1), we will obtain such a base for a set of all solutions of a given HSLDE:

$\{e_1^2 = (1,4,0,0,7), e_2^2 = (0,-2,1,0,3), e_3^2 = (0,5,0,1,-7)\}.$

In regards to conclusion 1, the theorem 1 result can be detailed. Indeed, since the coefficients values in the equation $L_1(x) = a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0$ are mutually simple, it is always possible to have number one among the values $L_1(x)$. Without limiting the generality of considerations we assume that GCD $(a_{11}, a_{12}, a_{13}) = 1$, i.e. the first three factors are mutually simple in $L_1(x)$. Then there are such numbers d_1, d_2, d_3, that in vector $y = (d_1, d_2, d_3, 0, ..., 0)$ values $L_1(y) = 1$. once we obtain this, let's calculate the value $L_1(x)$ for the canonical base vectors. First let's construct a base set B_1 by combining the spare vector y with the other vectors in order to obtain the base set. Let's note now that vectors from B_1 have the form:

$$e'_1 = -a_{11}y + e_1, e'_2 = -a_{12}y + e_2, e'_3 = -a_{13}y + e_3,$$
$$e'_4 = -a_{14}y + e_4, ..., e'_n = -a_{1n}y + e_n,$$

where e_i – canonical base vectors; a_{ij} – coefficient in an equation $L_1(x) = 0$.

Vectors e'_i can be presented also in the following form:

$$e'_1 = (-a_{11}d_1 + 1, -a_{11}d_2, -a_{11}d_3, 0, ..., 0),$$
$$e'_2 = (-a_{12}d_1, -a_{12}d_2 + 1, -a_{12}d_3, 0, ..., 0),$$
$$e'_3 = (-a_{13}d_1, -a_{13}d_2, -a_{13}d_3 + 1, 0, ..., 0),$$
$$e'_4 = (-a_{14}d_1, -a_{14}d_2, -a_{14}d_3, 1, ..., 0),$$
$$\ldots\ldots\ldots$$
$$e'_n = (-a_{1n}d_1, -a_{1n}d_2, -a_{1n}d_3, 0, ..., 1).$$

In this form the following theorem take places.

Theorem 2. TSS HLDE B_1, is a set base of all solutions for a given HLDE $L_1(x) = 0$ and is constructed using the method described above. The complexity of base construction is proportional to the value l^3, where l - is a maximal number of numbers m and n, n - the number of unknowns in HLDE, and m - the maximum length of the binary representation of HLDE coefficients.

Proof. Having $x = (c_1, c_2, ..., c_n)$ - is the solution of HLDE $L_1(x) = 0$. Then vector x has the following representation:

$$x = c_1e'_1 + c_2e'_2 + c_3e'_3 + c_4e'_4 + ... + c_ne'_n =$$
$$= [(-c_1a_{11}d_1 + c_1 - c_2a_{12}d_1 - c_3a_{13}d_1 - c_4a_{14}d_1 - ... - c_na_{1n}d_1],$$
$$[c - c_1a_{11}d_2 - c_2a_{12}d_2 + c_2 - c_3a_{13}d_2 - c_4a_{14}d_2 - ... - c_na_{1n}d_2],$$
$$[-c_1a_{11}d_3 - c_2a_{12}d_3 - c_3a_{13}d_3 + c_3 - c_4a_{14}d_3$$
$$- ... - c_na_{1n}d_3], c_4, ..., c_n) =$$
$$= (c_1, c_2, c_3, c_4, ..., c_n)$$

because $L(x) = a_{11}c_1 + a_{12}c_2 + ... + a_{1n}c_n = 0$.

The given algorithm complexity is described as a complexity of the extended Euclidean algorithm, defined along with the GCD and linear combination representing this GCD. It is obvious (see [3]), that the complexity is expressed as a value of $O(m \log m)$, where m - is the length of the binary representation of the maximal HLDE coefficient. Algorithm this is used no more than n times and it is measured as a form of $O(mn \log m)$. Building the base B_1 requires no more than n^3 operations. As a result, the summary measure of the time complexity is described as a value $O(l^3)$, where $l = \max(m, n)$.

The theorem is proved.

The above theorem leads to the following conclusion.

Conclusion 2. The time complexity of constructing all solutions base set for the HSLDE with the form (5) is proportional to a value $O(ql^3)$, where: q - is a number of equations HSLDE, and $l = \max(m, n)$.

III. THE TSS METHOD OF ISLDE SOLUTION

Having S be the ISLDE with the form of (1) and $b_q \neq 0$. Executing the free segments eliminations in the first $q-1$ equations, we transform the input ISLDE into the following form:

$$S' = \begin{cases} L'_1(x) = a'_{11}x_1 + ... + a'_{1n}x_n = 0, \\ L'_2(x) = a'_{21}x_1 + ... + a'_{2n}x_n = 0, \\ \quad ... \\ L'_{q-1}(x) = a'_{q-11}x_1 + ... + a'_{q-1n}x_n = 0, \\ L'_q(x) = a'_{q1}x_1 + ... + a'_{qn}x_n = b_q. \end{cases} \qquad (5)$$

Let's build the HSLDE base solutions set, composed of the first $q-1$ equations of the system (5). Having vectors $\{s_1, ..., s_k\}$. we specify $L_q(s_j) = a_j, j = 1, ..., k$. For this values the following theorem is true.

Theorem 3. The ISLDE with the form (1) is consistent only if the ISLDE $a_1y_1 + a_2y_2 + ... + a_ky_k = b_q$ has at least one solution in the set of integer numbers set.

Proof. If equation $a_1y_1 + a_2y_2 + ... + a_ky_k = b_q$ has solution $(c_1, c_2, ..., c_k)$, then it is obvious that vector $s = c_1s_1 + c_2s_2 + ... + c_ks_k$ is a SNLRS solution.

If ISLDE is consistent and $s = (k_1, k_2, ..., k_n)$ then its solution s is presented in the linear combination form constructed of the first $q-1$ homogenous equations of the system (5), i.e..:

$$s = c_1s_1 + c_2s_2 + ... + c_ks_k.$$

Then $L_q(s) = c_1a_1 + c_2a_2 + ... + c_ks_k = b_q$ should has at least one solution, because s is a solution of ISLDE.

The theorem is proved.

It is known that generalized solution of ISLDE has the form $y = x + \sum_{i=1}^{k} a_ix_i$, where: x – is a partial solution of ISLDE, x_i - is a base solution of a given HSLDE, a_i - any integer numbers, and k - is the number of base solutions. In this case, for a comprehensive solution of the ISLDE we should construct its HSLDE base and find one of the ISLDE solutions. Finding such a solution, as a result from the above considerations, is reduced into finding the solution of the equation $a_1y_1 + a_2y_2 + ... + a_ky_k = b_q$. This solution can be found with the use of the least coefficients method.

Example 3. The consistency of the ISLDE should be checked:

$$S = \begin{cases} L_1(x) = 2x_1 - 3x_2 + x_3 + x_4 + 0x_5 = 1, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -2. \end{cases}$$

The transformed ISLDE has the following form:

$$S' = \begin{cases} L'_1(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -2. \end{cases}$$

The HLDE $L_1(x)' = 0$ base is combined with the vectors (in this case the computation of GCD coefficients is not necessary, because coefficient equals 1):

$$(1,0,0,0,7),(0,1,0,0,-5),(0,0,1,0,3),(0,0,0,1,2).$$

Values $L_2(x)$ for these vectors equals: -4, 6, -2, -2. The greatest common divisor of these values equals 2 and is a divisor of the free member $b_2 = -2$. As a result the ISLDE has a solution, this is it is consistent.

If the system is determined:

$$S' = \begin{cases} L'_1(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -3, \end{cases}$$

Therefore it has not solutions in a ring of integer numbers, because GCD (-4, 6, -2, -2) = 2 and doesn't divide the free member -3 and then the equation $-4x + 6y - 2z - 2u = -3$ has no solutions.

In conclusion, we find that the given measurements of the time complexity can be more detailed, if we follow all the details of the processed calculations in the TSS algorithm. In this work it is limited to determining the polynominality of these algorithms.

IV. The Example Use of the Algorithm in the Interconnection Network Designing Process

Let's consider the problem of designing the interconnection network with the configuration presented in the Fig. 1.

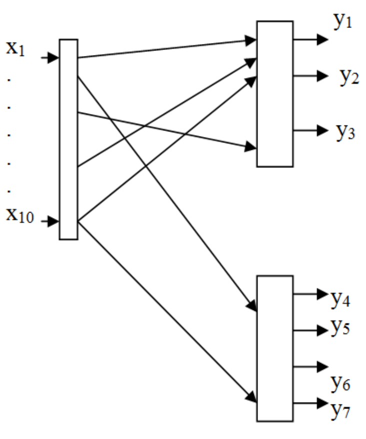

Fig. 1. The designed interconnection network configuration schema.

The designed interconnection network has 10 inputs $x_1 - x_{10}$ and two panels with outputs $y_1 - y_3$ and $y_4 - y_7$ respectively. We should power supply the minimal amount of inputs, in order to satisfy the following conditions: $y_1 = -10$, $y_2 = 20$, $y_3 = -5$, $y_4 = -20$, $y_5 = 50$, $y_6 = -10$, $y_7 = 20$ [V]. To solve this problem we construct the following equations system:

$$\begin{cases} x_1 + x_2 + x_3 + x_9 = -10 \\ x_3 - x_4 + x_5 + x_{10} = 20 \\ x_2 + x_6 - x_7 + x_9 = -5 \\ x_1 + x_3 + x_7 + x_{10} = -20 \\ -x_3 + x_5 + x_6 - x_9 = 20 \\ x_1 - x_4 - x_5 + x_7 + x_8 + x_9 = -10 \\ x_2 + x_3 - x_4 + x_6 + x_7 + x_8 = 20 \end{cases}$$

Such equations system has the following solutions: $x^0 = (0,80,-50,-35,5,-45,0,0,-40,30)$. Therefore, we obtain that: $x_1 = 0$, $x_2 = 80$, $x_3 = -50$, $x_4 = -35$, $x_5 = 5$, $x_6 = -45$, $x_7 = 0$, $x_8 = 0$, $x_9 = -40$, $x_{10} = 30$ [V]. This means that inputs x_1, x_7, x_8 may not be connected to any outputs.

The solutions of the homogenous equations system, which corresponds to a given inhomogeneous equations system may be described as follows:

$e = (-1,11,-6,21,-3,-7,-23,46,-4,30)$,
$s = (-1,11,-6,22,-3,-7,-24,48,-4,31)$,
$t = (8,-90,49,-175,25,54,192,-383,33,-249)$,
$r = (5,-169,92,-329,47,107,361,-720,62,-468)$.

Using these solutions the interconnection network designer has a choice, because he can select a special variant which suits him best. Thus, the interconnection network designer can use the general solution equation of a given equations system:

$$x = x^0 + ae + bs + ct + dr,$$

Where a,b,c,d are arbitrary integers?

V. Conclusion

In this paper we have presented the algorithm for computation the minimal supported set of solutions and base solutions of linear Diophantine equations systems in a ring of integer numbers. Linear Diophantine equations and their systems are often found in a wide variety of sciences which have heavy usage of computations. Solving the Diophantine equations is one of the main issues in computing the data, dependences in algorithm's code especially nested loop programs with memory access which very often occurs in numerical computing. Recently, the Diophantine equations are used to obtain an accurate and predictable computational model in many multi-disciplinary scientific fields especially in bimolecular networks studies.

The most crucial task in such models is to check the model's correctness – model validation problem. In the validation process finding of basic state equations is the most important task which may be checked by existence of integer solutions of Diophantine equations systems. Moreover, one of the motivations of this problem comes from the coding theory which may be implemented in many different fields of cryptography, encryption and users authentication (symmetric-key encryption and public-key cryptosystems) where the nonuniqueness of Diophantine equations solutions is analyzed. Thus, the proposed research is an actual scientific problem.

REFERENCES

[1] С. Л. Крывый, *Алгоритмырешениясистемлинейныхдиофантовыхуравнений в целочисленныхобластях*..Кибернетика и СистемныйАнализ, 2006, N 2, pp. 3-17.

[2] Г. А. Донец, *Решениезадачи о сейфена (ОД)-матрицах*, Кибернетика и СистемныйАнализ, 2002, N1, pp. 98-105.

[3] А. В. Черемушкин, *Лекциипоарифметическималгоритмам в криптографии,*МЦНМО, 2002, 103 p.

[4] F. Baader, J. Ziekmann, *Unification theory*, Handbook on Logic in Artificial Intelligence and Logic Programming, Oxford University Press, 1994, pp. 1-85.

[5] R. Allen, K. Kennedy, *Automatic translation of FORTRAN program to vector form,* ACM Transactions on Programming Languages and systems, 1987, v. 9, N4, pp. 491-542.

[6] E. Contejan, F. Ajili, *Avoiding slack variables in the solving of linear Diophantine equations and inequations*, Theoretical Comp. Science, 1997, pp. 183 -208.

[7] L. Pottier, *Minimal solution of linear Diophantine systems: bounds and algorithms*,In Proc. of the Fourth Intern. Conf. on Rewriting Techniques and Applications, Italy, 1991, pp. 162-173.

[8] E.Domenjoud, *Outils pour la deduction automatiquedans les theories associatives-commutatives*, Thesis de Doctoral d'Universite: Universite de Nancy I, 1991.

[9] M. Clausen, A. Fortenbacher, *Efficient solution of linear Diophantine equations*, J. Symbolic Computation, 1989, N 1,2, pp. 201-216.

[10] J. F. Romeuf , *A polinomial algorithm for solving systems of two linear Diophantine equations*, *TCS, 1990, pp. 329-340.*

[11] M. Filgueiras, A.P. Tomas, *A Fast Method for Finding the Basis of Non-negative Solutions to a Linear Diophantine Equation*, J. Symbolic Computation, 1995, v.19, N2, pp. 507-526.

[12] H. Comon, Constraint *solving on terms: Automata techniques (Preliminary lecture notes)*, Intern. Summer School on Constraints in Computational Logics: Gif-sur-Yvette, France, September 5-8, 1999, 22 p.