UDC 621.37:621.391

THE METHOD OF PSEUDORANDOM CODES DECODING ON THE BASIS OF THE MODIFIED METHOD OF BRANCHES AND BOUNDARIES

T. Lavrovska, S. Rassomakhin

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
lavrovska92@gmail.com, rassomakhin@karazin.ua

Reviewer: Victor Krasnobayev, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine;
krasnobayev@karazin.ua

Received on November 2016

Abstract. *Reasons of crisis of error-correcting coding are considered. Underlined the urgency of application of pseudo random codes in modern systems transmission of information. Presented constructive mathematical method of decoding pseudorandom codes based on the use of the method of branches and borders. Is proposed for modification of the classical algorithm of branch and bound. Is proposed, assessment of computing complexity of methods of decoding of pseudorandom codes on basis of the classical and modified algorithm of branches and boundaries is made, and also assessment of computing complexity of the offered method in comparison with exhaustive search method. Program implementation of method of decoding of pseudorandom codes is developed.*

Keywords*: pseudorandom code, branch and bound method, computational complexity, error-correcting coding.*

1 Introduction

Formulation of the problem. Scientific and technical progress in the field of telecommunications in the modern society gives ample opportunities for information exchange. It is a powerful method for development of different information technologies, which strongly enter in daily life of humanity. Business by means of electronic commerce, using Blockchain, application of cloud computing – is not the complete list of achievements of IT area. At the same time the nomenclature and number of technical means of processing and information transfer which work on wireless communication networks are increased from year to year. Therefore, search of new solutions of rational use of frequency and energy resource of transmission channels for creation of the technologies allowing to increase data transmission rate and reduce the required power of transmitters is urgent.

In the theory of information transfer is known the historical role of the methodology based on use of random codes in the proof of fundamental theorems for noisy channels [1,2]. However, proofs on the basis of an random choice of a code usually are called nonconstructive as till today random (pseudorandom) codes (PRC) for support of error correcting and confidentiality of process of information transfer are not used. It is a consequence of absence of acceptable computing complexity of methods of creation and decoding of PRC which provide ability of correction, the close to maximum likelihood.

Implementation of constructive algorithms of creation and processing of PRC can be expected only when using of determinate algorithms of generation of pseudorandom characters of code words. Attractiveness of PRC technologies consist in a possibility of creation of signal and code constructions, which will allow to raise at the same time as the frequency, and energetic efficiency of information transmission systems. However, the main barrier to broad use of PRC is absence of methods of decoding not based on algorithm of exhaustive search.

Computing complexity of the algorithms based on computation of Euclidean distances increases exponentially with increase in block length of a code and in case of required values of block length

is unacceptable. Receiving simple linear algebraic methods of decoding is encountered with difficulties following from nonlinearity of the determined algorithms of generation of the pseudorandom sequence. Thus, the ideas of application of PRC will be applied constructive if develop the linear (linearized) methods of decoding of such codes.

Objective: development of a constructive mathematical method of decoding of PRC on the basis of application of the modified method of branches and boundaries, assessment of computing complexity of operation of decoding and its comparing with exhaustive search algorithms based on use of the rule of maximum likelihood.

MAIN PART

2 Statement of the task of decoding, as main objective of the linear programming

The procedure of obtaining of code book of arbitrary pseudorandom code can be provided as follows. The general flow of binary characters of a source is subject to coding whishes divided on the sequences by length of **k** bits. These sequences are intended for creation of pseudorandom error correcting code. At the same time each combination from **k** binary characters of a source is transferred to decimal value x_0 – sequence number by which is determined appropriate sequence of pseudorandom numbers $x_1, x_2, \ldots, x_{n-1}$, that is x_0 –is ancestor number of the code word $X_j=\left\{x^j{}_0, x^j{}_1, \ldots, x^j{}_{n-1}\right\}$ with appropriate number $j = x^j{}_0$, $j \in \left[0,\ldots,\left(2^k\text{-}1\right)\right]$. Thus, for each block from **k** binary characters of a source are put in compliance block from **n** not binary numbers of a code. Numbers of code words determine informative parameters of a signal. For example, amplitudes of the quadrature components of subcarrier frequencies [3]. Magnitude

$$R = k/n, \tag{1}$$

is speed of error correcting code and shows a ratio of amount of information binary characters of the message with amount of not binary characters of a codewhich are used for transmissions on communication link. Speed of a code (1) can be both more and less than one. Reason of this property is ability of a choice of length of the code word PRC irrespective of length of the initial block of binary characters **k**.

On an output of the channel after impact of noise the sequence has an form:

$$X^*_j = X_j + \Xi = \left\{x^j{}_0 + \xi_0, x^j{}_1 + \xi_1, \ldots, x^j{}_{n-1} + \xi_{n-1}\right\} = \left\{x^*{}_0, x^*{}_1, \ldots, x^*{}_{n-1}\right\},$$

where $\Xi = \left\{\xi_0, \xi_1, \ldots, \xi_{n-1}\right\}$ is vector of coordinates of noise. These codes allow to provide rather low probability of decoding with an error on the block of a code in case of simple increase in block length n if throughput of the channel was not exceeded.

Now pseudorandom codes are not applied in information transmission systems because the known methods of decoding of such codes are based on implementation of the rule of maximum likelihood and are possible only in case of symbol-by-symbol comparing, the received channel word with all possible options which are stored in the receiver. Decoding procedure is based on search of the minimum value of length of the difference vector of Euclidean distances between points X_j^* i X_i:

$$\min\left|X_j^* - X_i\right| = \sqrt{(x_0{}^{j*} - x_0{}^i)^2 + \ldots + (x_{n-1}{}^{j*} - x_{n-1}{}^i)^2},$$

where $i \in \left[0\ldots\left(2^k\text{-}1\right)\right]$.

Thus, computing complexity of such methods of decoding increases exponentially with length of block code **n**.

For solution of this problem of decoding in case of creation of PRC is offered to use a procedure of computation of characters of code words by recurrent rule of the linear congruent generation

(LCG). This rule allows to linearize the issue of decoding of PRC and essential to reduce its computing complexity. It is possible by replacement of computation Euclidean distances on rule of smallest projections (SP) which are identical on the end result

$$\min\sum_{q=0}^{n-1}\left|x_q^{j*}-x_q^{i}\right|, \quad \text{where} \quad i\in\left[0\ldots\left(2^k-1\right)\right].$$

Using of SP in a complex with method of decoding of PRC on the basis of the modified method of branches and boundaries will allow to provide polynomial computing complexity. Process of obtaining code words PRC on the basis of the linear congruent generation is as follows [3,4]. Each next i number of the pseudorandom sequence of arbitrary **j** code word is generated by the recurrent rule of generation of the sequence of LCG in case x_0^j:

$$x_i^j=(a\cdot x_{i-1}^j+b)\bmod m, \tag{2}$$

where a – multiplicative parameter, b – additive parameter of conversion, *mod* – operation of computation of the module m. Magnitude $m=2^k$ is power of the alphabet of words PRC. For simplification of mathematical calculations the upper index in designation of variables x_i^j will not be used, that is number of the code word is fixed $x_i^j \to x_i$.

In a general view the offered method of decoding of a pseudorandom error correcting code in the conditions of distortions of characters is considered. This method is based on use of a mathematical algorithm of branches and boundaries for directional search of the decision.

Operation of decoding is reached if in the conditions of possible distortions, the ancestor number x_0 of a segment of the pseudorandom sequence (PRS) is correctly defined. Magnitude x_0 (the first number in code word of length **n**) in binary representation correctly defines the transferred binary sequence of a source. For search of number all characters of PRS of a code are used, as all of them are connected to ancestor number a recurrent chain of non-linear computation (2).

Whereas in (2) non-linear operation of computation of the module is used, it is a hindrance to implementation of directional search of the decision. Necessary perform linearization of operation of decoding by introduction of additional integer non-negative numerical parameter y.

Quantitative value y is equal to a multiplier by equivalent linear algebraic operation of computation of the module m. Then mathematical expression (2) changes the next way:

$$x_{i+1}=ax_i+b-y_i m, \quad i\in\left[0,\ldots,(n-1)\right]. \tag{3}$$

Mathematical expression (3) is fair only in case of execution of restrictions which follow from a mathematical gist of an algorithm of LCG PRC:

$$0\le y_i\le\left\lfloor\frac{(m-1)a+b}{m}\right\rfloor, \quad y_i \ - \text{integer}, \ i\in\left[0,\ldots,(n-2)\right]. \tag{4}$$

For compensating of distortions of arbitrary initial code word of a source **x** in result of summing with elements of a vector of Gaussian random variables Ξ for each of numbers of the code word x_i^*, $i\in[0,\ldots,n-1]$ will be entered couple of auxiliary non-negative variables w_{2i+1}, w_{2i+2}.

This pair characterizes possible double-sided deviations of number x_i^* which are a consequence of action of a vector of a noise Ξ. One variable from this pair enters in calculation with sign "+", it means that it is added to the number distorted by a noise x_i^*, other–with sign «-», it means that it is subtracted from x_i^*. Then for observed code word $X^*=\left\{x^*_0,\ldots,x^*_{n-1}\right\}$ system of equations is formed:

$$\begin{cases} x_0 = x^*_0 - w_1 + w_2; \\ x_1 = x^*_0 - w_3 + w_4; \\ \vdots \\ x_{n-1} = x^*_{n-1} - w_{2n-1} + w_{2n}. \end{cases} \quad (5)$$

In each of the equations (5) one of pair of auxiliary variables **w** with an even or odd index will equal zero because the deviation from action of a noise can be only towards reduction, or towards increase of true number. At the same time variables x_i must satisfy to inequality $0 \le x_i \le (m-1)$. For decision of the task of decoding is planned to use the linear programming (LP), then the left inequality of this restriction (non negativity support) is automatically executed according to terms of the canonical task LP.

Issue LP-in a canonical form requires of representation of all restrictions of area of admissible decisions in the form of equalities. Therefore, for changeover from the right inequality to equality non-negative integer auxiliary variables $\tilde{x}_n, \tilde{x}_{n+1}, \ldots, \tilde{x}_{2n-1}$ is entered:

$$\begin{cases} \tilde{x}_n = (m-1-x^*_0) + w_1 - w_2; \\ \tilde{x}_{n+1} = (m-1-x^*_1) + w_3 - w_4; \\ \vdots \\ \tilde{x}_{2n-1} = \left(m-1-x^*_{\frac{n-1}{2}}\right) + w_{2n-1} - w_{2n}. \end{cases} \quad (6)$$

In case of execution of restrictions (6) is reached execution of the following system of equalities:

$$\begin{cases} x_0 + \tilde{x}_n = m-1; \\ x_1 + \tilde{x}_{n+1} = m-1; \\ \vdots \\ x_{n-1} + \tilde{x}_{2n-1} = m-1. \end{cases} \quad (7)$$

On the basis of (3) and (4) are defined values y_i corresponding to multipliers of equivalent algebraic representation of operation of computation of the module m:

$$\begin{cases} y_0 = \frac{1}{m}(ax^*_0 - x^*_1 + b) - \frac{a}{m}w_1 + \frac{a}{m}w_2 + \frac{1}{m}w_3 - \frac{1}{m}w_4; \\ \vdots \\ y_{n-2} = \frac{1}{m}(ax^*_{n-2} - x^*_{n-1} + b) - \frac{a}{m}w_{2n-3} + \frac{a}{m}w_{2n-2} + \frac{1}{m}w_{2n-1} - \frac{1}{m}w_{2n}. \end{cases} \quad (8)$$

Minimum of objective function **L**, which needs to be provided when decoding PRC according to the rule of the smallest projections considered above, has an appearance:

$$L = \sum_{i=1}^{2n} w_i = w_1 + w_2 + \ldots + w_{2i-1} + w_{2i}. \quad (9)$$

The physical sense of objective function consists in finding of the minimum sum of projections of the ends of the difference vector between a point X^* on an output of noisy channel and a point X of the code book of PRC which is closest to X^*.

Mathematical expressions (5), (6), (8) and (9) represent a canonical statement of the main problem of the linear programming (MPLP). For solution MPLP is applied simplex a method and its implementation in the form of table algorithm. MPLP contains $3n-1$ equations and has $5n-1$ unknown variables 2n variables choosing as the free, and remaining $3n-1$ is as basis variables expressed through free. The free variables are $\underbrace{w_1, \ldots, w_{2n}}_{2n}$.

Then conversions of the equations (5), (6), (8) and (9) gives the following statement of the integer task LP. It is necessary to find the non-negative values of variables x_i, y_j, w_q satisfying to

system of restrictions equalities (5), (6), (8) and providing a minimum of objective function (9). For decision of formulated integer task LP is applied table algorithm of simplex method. On the basis of the received expressions the simplex table is built (Table 1).

Rules of filling of the table are as follows:

– names of basis variables to the first column of basis variables (B.V.)are entered;

– names of the free variables to the first line of the free variables (F.V.) are entered;

– free terms from the equations (5), (6), (8) and (9) are entered to the second column of free terms (S.Ch.);

– starting with the third column are entered coefficients of free variables from the equations (5), (6), (8) and (9) with changing signs on opposite.

Decoding of the code word PRC that was distorted by noises comes down to the correct determination of value x_0 – ancestor number of the code word PRC that correctly defines k bit combination of binary characters of a source.

The initial table contains the basic plan (*a task has variant of solution*), where B.V. values are equal to elements in the corresponding lines of the F.T. column, and values of the free variables are equal to zero. In a line of objective function in the F.T. column is a value of size of objective function. This value is used for realization of directional searching of the decision on a method of branches and borders. Decoding on the basis of a method of branches and borders is iterated that means creation of a tree of decisions with tops of minimum values of basic plans. Route by a tree from initial top to some fixed top determines the admissible sequence of the choice of integer values for task variables. Main goal of decoding by proposed method is receiving integer variables of $\boldsymbol{x}$ and $\boldsymbol{y}$ at minimum possible value of objective function **L**.

Table 1 - The initial simplex table

F.V / B.V.	F. T.	w_1	w_2	w_3	w_4	…	w_{2n-3}	w_{2n-2}	w_{2n-1}	w_{2n}
x_0	x^*_0	1	-1	0	0	…	0	0	0	0
x_1	x^*_1	0	0	1	-1	…	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
x_{n-1}	x^*_{n-1}	0	0	0	0	…	0	0	1	-1
x_n	$\left(m-1-x^*_0\right)$	-1	1	0	0	…	0	0	0	0
x_{n+1}	$\left(m-1-x^*_1\right)$	0	0	-1	1	…	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
x_{2n-1}	$\left(m-1-x^*_{n-1}\right)$	0	0	0	0	…	0	0	-1	1
y_0	$\frac{1}{m}\left(ax^*_0-x^*_1+b\right)$	$\frac{a}{m}$	$-\frac{a}{m}$	$-\frac{1}{m}$	$\frac{1}{m}$	…				
⋮	⋮	⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮
y_{n-2}	$\frac{1}{m}\left(ax^*_{n-3}-x^*_{n-2}+b\right)$					…	$\frac{a}{m}$	$-\frac{a}{m}$	$-\frac{1}{m}$	$\frac{1}{m}$
L	0	-1	-1	-1	-1	…	-1	-1	-1	-1

Formally the method of branches and borders can be described by the sequence of the following stages.

On the first iteration the plan of Table 1 is analyzed on permissibility on the basis of content of cells of a column F.T.. If all elements of column of the free terms are not the negative then the plan is permissible. If all elements of line of objective function **L** (except an element in the F.T. column) are negative, then the plan is optimum.

If any element of F.T. column is negative, plan is not permissible and the table is modified according to an algorithm of the solution of a dual problem of LP. The line with the negative element is allowing. If such lines are several, then the line is chosen which has maximal on an absolute value negative element. In the allowing line is looked for an element which has the negative sign. If such elements are several, then among them is selected maximum on an absolute value. The column which has this element is considered allowing. On crossing of the allowing column and line is an allowing element.

Modification of the table with exchange between couple a "free-basic" variables from headings of allowing line and column and recalculation of maintenance of cells must make for transition to the next plan of task as follows:

- headings of variables which correspond to the allowing column and line are interchanged the position;
- an allowing element changes on inverse;
- elements of an allowing line are divided into the allowing element;
- elements of allowing column are divided into the allowing element and are changed their sign on inverse;
- to all other elements from old table is added multiplication of an element of the allowing line from old table which is in the same column, on an element of the allowing column from new table which is in the same line.

After modification, received table repeatedly is analyzed on permissibility. After obtaining permissible plan, it is analyzed on an optimality.

If in a line of objective function is at least one positive element, then the plan not optimum and the table is modified according to an algorithm of the decision of the direct task LP. Column which has positive element is selected as allowing column. If such elements are several then among them is selected maximum. In the allowing column are analyzed elements which match on a sign with element of F.T. column. If such couples of elements a few, then it is necessary to calculate the relation of the free term to appropriate element of allowing column. The allowing line is the line which has the minimum value of this relation. On crossing of the allowing column and line is an allowing element.

The table is modified and content of cells is recalculated by rules which are considered above. After modification of table, table repeatedly is analyzed on permissibility and optimality. These iterations cyclically repeat till that moment will not be found permissible and optimum plan which is called the basic plan of the task.

Further the received basic plan is analyzed on existence of integral numbers in F.T. column. Variables $x_i,\ i \in [0,\ldots,(2n-1)]$ and $y_j,\ j \in [0,\ldots,(n-2)]$ which are contained in the cells of F.T. column must contain integral numbers. The first line which has not integer, specifies the name of the variable (x_i, y_j or w_k) for which will be created an additional constraint of integrality.

For reduction of computing complexity of this method of decoding is offered to use the modified method of branches and boundaries. Gist of this modification consists in provision of priority of the analysis of integrality only of variables $\mathbf{y_j}$. Experimentally proved that when the integrality of those variables provides integrality of other variables of decoding task. This modification significantly reduces the number of iterations of search of the decision, as a result, reduces computing complexity of decoding procedure of PRC. Additional restriction is created by introduction to the basic plan of an additional line for an additional auxiliary basis variable. The mechanism of introduction of additional restrictions in details will be considered below in case of presentation of a specific example of implementation of the decision of the task of decoding. On the basis of additional restrictions is executed branching of a decision tree. Let's assume that for providing of

integrality is selected variable $\mathbf{y_j}$. Area of admissible solutions of zero step of the task breaks on two not crossed subareas for the following step $G_1^{(1)}$ and $G_2^{(1)}$ on the basis of the rule:

$$G_1^{(1)} = \left\{ Y \in G^{(0)}, y_i \le \lfloor y_i \rfloor \right\};$$
$$G_2^{(1)} = \left\{ Y \in G^{(0)}, y_i \ge \lceil y_i \rceil \right\}. \quad (10)$$

The rule (10) means that in new areas value of variable needs to be reduced to the next smaller integer number $\lfloor y_i \rfloor$, or on the contrary, be to increased to the next bigger integer number $\lceil y_i \rceil$. Then, on the technology described above, it is necessary to find sequentially basic plans of tasks for areas $G_1^{(1)}$ and $G_2^{(1)}$. After execution of branching and formation of restrictions, basic plans are analyzed on permissibility and optimality, if necessary is executed modification and recalculation of tables, and also analysis of integrality. Actions is iterated until all elements in lines of the F.T. column will be integers. At the same time some integer variables can be in composition of the free, it means that they are equal to zero.

3 Decoding of PRC on basis of modified method of branches and boundaries

Example of application of offered method for decoding of a pseudo random error correcting code on the basis of use of the modified method of branches and boundaries is considered.

Parameters of a pseudorandom error correcting code are values: k=5; n=5. For LCG technology parameters are selected: $m = 2^k = 32,\ a = 5,\ b = 19$. Sequentially changing numbers of the binary sequences on length $k = 5$ characters $x_0 = 0,1,\ldots,31$ and using the rule (2) for computation of characters of code words and is obtained code book of PRC which is provided in Table 2.

Table 2 – Code sequences of the complete code book of PRC

x_0	X	x_0	X	x_0	X	x_0	X
0	0, 19, 18, 13, 20	8	8, 27, 26, 21, 28	16	16, 3, 2, 29, 4	24	24, 11, 10, 5, 12
1	1, 24, 11, 10, 5	9	9, 0, 19, 18, 13	17	17, 8, 27, 26, 21	25	25, 16, 3, 2, 29
2	2, 29, 4, 7, 22	10	10, 5, 12, 15, 30	18	18, 13, 20, 23, 6	26	26, 21, 28, 31, 14
3	3, 2, 29, 4, 7	11	11, 10, 5, 12, 15	19	19, 18, 13, 20, 23	27	27, 26, 21, 28, 31
4	4, 7, 22, 1, 24	12	12, 15, 30, 9, 0	20	20, 23, 6, 17, 8	28	28, 31, 14, 25, 16
5	5, 12, 15, 30, 9	13	13, 20, 23, 6, 17	21	21, 28, 31, 14, 25	29	29, 4, 7, 22, 1
6	6, 17, 8, 27, 26	14	14, 25, 16, 3, 2	22	22, 1, 24, 11, 10	30	30, 9, 0, 19, 18
7	7, 22, 1, 24, 11	15	15, 30, 9, 0, 19	23	23, 6, 17, 8, 27	31	31, 14, 25, 16, 3

For transmission on the channel is selected code word generated by number $x_0 = 0$ or $X = \{0,19,18,13,20\}$, which as a result of summing with a noise vector Ξ and is changed $X^* = \{0,18,22,15,20\}$. For simplification of an example the numbers of the code word distorted by transmission are rounded to integer values. On the basis of expressions (5), (6), (8) and (9) and according to rules of filling of initial simplex table (Table 1) is formed starting table of this example (Table 3).

Table 3 contains the permissible, optimum basic plan of not integer problem of LP (elements of column FT are not negative, elements of line L – are not positive). However the plan does not meet of condition of integrality (FT column contains in lines $y0 \div y3$ not integer values). According to developed of modified method of branches and borders additional restriction is formed for area $G_1^{(1)}$. Firstly (in the analysis of lines of Table 3 from top to down), not integer variable $y0$ is chosen. That variable $y0$, which is equal in the Table 3 to size 0,0312 will got value of the next smaller integer $\lfloor y0 \rfloor = 0$.

Performance of inequality is required $y0 \le 0$. For formation of a line of constraint for new table it is necessary to execute transition from restriction inequality to restriction equality, by introduction of an additional non-negative variable v: $y0 + v = 0$. Let's express a variable v as basic:

$$v = 0 - y0 . \quad (11)$$

Table 3 – First iteration *(Step 1)*

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,031	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,718	0	0	0,1562	-0,1562	-0,0312	0,03125	0	0	0	0
y2	3,562	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Definition $y0$ in the form of a linear combination of free variables is set by line $y0$ of Table 3:

$$y_0 = 0,1562w1 - 0,1562w2 - 0,0312w3 - \\ - 0,0312w4 + 0,0312. \quad (12)$$

Using (12) in (11), the equation of additional restriction is created:

$$v = -0,0312 - 0,1562w1 + 0,1562w2 + \\ + 0,0312w3 - 0,0312w4. \quad (13)$$

On the basis of (13) the additional line for a fictitious variable v is entered into the basic plan. As a result size of the table increases, and it is transformed to Table 4.

Table 4 – First iteration *(Step 1)* with additional restriction

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,0312	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
v	-0,031	-0,1562	0,1562	0,0312	-0,0312	0	0	0	0	0	0
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Table 4 for subarea $G_1^{(1)}$ contains the impermissible plan because FT column has a negative element. According to the rules described above is necessary to execute the solution of a dual task. Allowing line – a line of restriction v, the allowing column – a column of a variable w1 and the allowing element which is located on crossing of a line v and column w1 are chosen (look at shaded elements in Table 4).

For transition to the permissible plan is necessary to execute modification and recalculation of Table 4 according to rules which were considered above. Modification of the plan gives Table 5.

Table 5 – Modification of initial Table 4 *(Step 1)*

	FT	v	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	-0,2	6,4	0	0,2	-0,2	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31,2	-6,4	0	-0,2	0,2	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0,2	-6,4	-1	-0,2	0,2	0	0	0	0	0	0
L	0,2	-6,4	-2	-1,2	-0,8	-1	-1	-1	-1	-1	-1

The decision received in Table 5 is analyzed on permissibility. As the plan is not permissible then its modification is executed. As allowing line is selected x0, and allowing the column - w4. Recalculation gives Table 6.

Table 6 – Modification of Table 5 *(Step 1)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Table 6 contains permissible and optimum basic plan. This plan is noted on a tree of decisions (Fig. 1) by corresponding top $G_1^{(1)}$ which has value of objective function L=1.

Restriction for area $G_2^{(1)}$ is formed so that the variable $y0$ will got value of the next bigger integer $\lceil y0 \rceil = 1$. For this purpose, performance of inequality $y0 \geq 1$ is required. $y0 \leq 0$. For transition from restriction inequality to restriction equality is entered an additional non-negative variable v: $y0 - v = 0$, or:

$$v = y0 - 1. \quad (14)$$

For designation of an additional variable in (14) is used the same name v, all fictitious variables are auxiliary and their size at achievement of the final decision of a task does not matter. When obtaining of intermediate basic plan any additional fictitious variable is appeared as a part of basic variables of a task (in heading of any line) for reduction of dimension of tables the corresponding line will delete.

Definition $y0$ through values of free variables gives:

$$v = -0,968 + 0,1562w1 - 0,1562w2 - \\ - 0,0312w3 + 0,0312w4, \quad (16)$$

What to allows to enter a line of additional restriction into the Table 7.

Table 7 – The second iteration with additional restriction *(Step 1)*

	FT	w1	w2	w3	w4	w5	w6	w7	w8	w9	w10
x0	0	1	-1	0	0	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	-1	1	0	0	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0,0312	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
v	-0,968	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0	0	0
L	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Table 7 for subarea $G_2^{(1)}$ contains impermissible plan, because column FT has negative element. According to the rules described above are chosen as the allowing line – a line of restriction v, and as the allowing column – a column $w2$. For achievement of permissibility of plan is executed modification of Table 7.

As a result Table 8 is obtained permissible and optimum basic plan of Table 8 is noted on a tree of decisions (Fig. 1) by corresponding top $G_2^{(1)}$ which has value of objective function L = 6,2.

Tops $G_1^{(1)}$ and $G_2^{(1)}$ of first step of the decision, which correspond to Tables 6 and 8 must be branched for the purpose of achievement of integer values of other integer variables.

The choice of the next top (table) among the "hanging" tops of a tree of decisions for the subsequent branching is carried out from the point of view of its greatest prospects. For obtaining next basic plan is chosen table which has the smallest (*among the "hanging" tops*) value of objective function. Then next top of tree of decisions which will be used for branching, is Table 6 with value L = 1.

Table 8 – Modification of Table 7 *(Step 1)*

	FT	w1	v	w3	w4	w5	w6	w7	w8	w9	w10
x0	6,2	0	-6,4	0,2	-0,2	0	0	0	0	0	0
x1	18	0	0	1	-1	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	24,8	0	6,4	-0,2	0,2	0	0	0	0	0	0
x6	13	0	0	-1	1	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	1	0	-1	0	0	0	0	0	0	0	0
y1	2,7187	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0	0	0
y2	3,562	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w2	6,2	-1	-6,4	0,2	-0,2	0	0	0	0	0	0
L	6,2	-2	-6,4	-0,8	-1,2	-1	-1	-1	-1	-1	-1

On the second step is chosen next not integer variable $y1$ for formation of additional restriction of area $G_1^{(2)}$. So that chosen variable $y1$ is equal in the Table 6 to size 2,875 will have value of the next smaller integer $\lfloor y1 \rfloor = 2$. Additional restriction is formed by an example of expressions (12) and (16) that leads to Table 9.

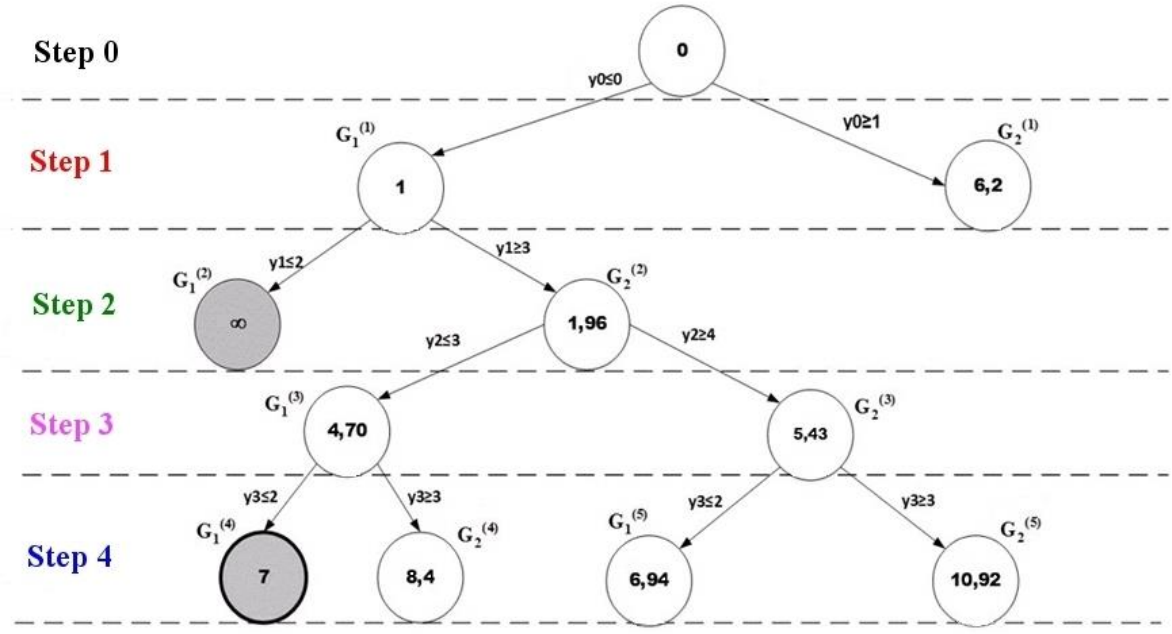

Fig. 1 – The tree of decisions for the modified method of branches and borders

Table 9 for subarea $G_1^{(2)}$ contains impermissible plan, because column FT has negative element. According to the rules described above are chosen as the allowing line – a line of restriction v, and as the allowing column – a column $w6$.

Modification of the table lead to the plan presented in Table 10.

Table 9 – First iteration *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	-0,875	5	0	0	0,7812	0,0312	-0,0312	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Table 10 contains impermissible plan (*a negative number in a line* $x7$ *of the FT column*). As other numbers in this line are not negative, then continuation of calculations for this table does not make sense, because getting permissible decision is impossible.

Table 10 – Modification of the Table 9 *(Step 2)*

	FT	v	w2	w3	x0	w5	v	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	50	-160	0	0	-25	0	-32	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	-19	160	0	0	25	0	32	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2	0	0	0	0	0	1	0	0	0	0
y2	7,937	-25	0	0	-3,9062	0	-5	-0,0312	0,0312	0	0
y3	2,312	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
w6	28	-160	0	0	-25	-1	-32	0	0	0	0
L	29	-192	-2	-2	-29	-2	-32	-1	-1	-1	-1

Plan of Table 10 is noted on a tree of decisions (Fig. 1) by corresponding top $G_1^{(2)}$ which has value of objective function $L = \infty$. The top $G_1^{(2)}$ is final of branch, and is not subject to further branching.

The next restriction for area $G_2^{(2)}$ is built so that the variable $y1$ will have got value of the next bigger integer number $\lceil y1 \rceil = 3$. Additional restriction was created by an example of expression (16) leads to plan of Table 11. Table 11 contains impermissible plan because FT column has a negative number. According to described above by the rules allowing line and column are additional variables v (*exchange of positions between two additional fictitious variables*).

Table 11 – Second iteration *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1	-32	0	-1	-5	0	0	0	0	0	0
x1	19	-32	0	0	-5	0	0	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	12	32	0	0	5	0	0	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	0	1	0	0	0	0	0	0	0	0	0
y1	2,875	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	-0,125	-5	0	0	-0,7812	-0,0312	0,0312	0	0	0	0
L	1	-32	-2	-2	-4	-1	-1	-1	-1	-1	-1

Modification leads to Table 12.

Table 12 – Modification of Table 11 *(Step 2)*

	FT	v	w2	w3	x0	w5	w6	w7	w8	w9	w10
w4	1,8	-6,4	0	-1	0	0,2	-0,2	0	0	0	0
x1	19,8	-6,4	0	0	0	0,2	-0,2	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	0	1	0	0	0	0	0	0
x6	11,2	6,4	0	0	0	-0,2	0,2	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
y0	-0,025	0,2	0	0	-0,1562	-0,0062	0,0062	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0	0	-1	0	1	0	0	0	0	0	0
v	0,025	-0,2	0	0	0,1562	0,0062	-0,0062	0	0	0	0
L	1,8	-6,4	-2	-2	1	-0,8	-1,2	-1	-1	-1	-1

For disposal of impermissible plan is necessary to execute exchange – values $y0 \leftrightarrow x0$.

This transformation leads to plan which is presented in Table 13.

Table 13 contains permissible and optimum basic plan. Important point is possibility of removal of a line of a fictitious variable v in Table 13 during transition to next basic plan and its place will have used for record of new restriction. The basic plan, which was received in Table 13, is noted by top $G_2^{(2)}$ on a tree of decisions (Fig. 1) and corresponds to value of objective L = 1,96. This top corresponds to the smallest value of objective function among all available "hanging" tops. That's why this top and its Table 13 are chosen for further branching for achievement of integer of value $y2$.

Table 13 – Modification of Table 12 *(Step 2)*

	FT	v	w1	w3	y0	w5	w6	w7	w8	w9	w10
w4	1,8	-6,4	0	-1	0	0,2	-0,2	0	0	0	0
x1	19,8	-6,4	0	0	0	0,2	-0,2	0	0	0	0
x2	22	0	0	0	0	1	-1	0	0	0	0
x3	15	0	0	0	0	0	0	1	-1	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	30,84	1,28	0	0	6,4	-0,04	0,04	0	0	0	0
x6	11,2	6,4	0	0	0	-0,2	0,2	0	0	0	0
x7	9	0	0	0	0	-1	1	0	0	0	0
x8	16	0	0	0	0	0	0	-1	1	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
x0	0,16	-1,28	0	0	-6,4	0,04	-0,04	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3,5625	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312	0	0
y3	2,3125	0	0	0	0	0	0	0,1562	-0,1562	-0,0312	0,0312
w1	0,16	-1,28	-1	0	-6,4	0,04	-0,04	0	0	0	0
v											
L	1,96	-7,68	-2	-2	-6,4	-0,76	-1,24	-1	-1	-1	-1

Steps of the decision is repeated to achievement of integer of all elements of the FT column. At the same time perspective and final tops of a tree of decisions gradually are defined. From a step to a step quantity of final (not perspective and not subject to branching) tops begins to increase, and task quickly strives for the only optimum integer decision which corresponds to the smallest achievable value of objective function. Received value L corresponds to the minimum size of the sum of lengths of projections of a vector of hindrance Ξ. It allows of implement offered rule of decoding (SP). Full process of decoding for the reviewed example is illustrated by a tree in fig. 1. The top $G_1^{(4)}$ is final, which corresponds to the plan of the decision presented in Table 14, at the same time value of objective function is equal L = 7. Value of a variable determines the most probable (by MLE) the decoded code word.

Table 14 – Final table *(Step 4)*

	FT	v	w1	w3	y0	v	w6	v	w8	w9	w10
w4	1	0	0	0	0	1	0	0	0	0	0
x1	19	0	0	1	0	1	0	0	0	0	0
x2	18	32	0	5	0	5	0	0	0	0	0
x3	13	160	0	25	0	25	0	32	0	0	0
x4	20	0	0	0	0	0	0	0	0	1	-1
x5	31	0	0	-0,2	6,4	-0,2	0	0	0	0	0
x6	12	0	0	-1	0	-1	0	0	0	0	0
x7	13	-32	0	-5	0	-5	0	0	0	0	0
x8	18	-160	0	-25	0	-25	0	-32	0	0	0
x9	11	0	0	0	0	0	0	0	0	-1	1
x0	0	0	0	0,2	-6,4	0,2	0	0	0	0	0
y1	3	-1	0	0	0	0	0	0	0	0	0
y2	3	0	0	0	0	0	0	-1	0	0	0
y3	2	25	0	3,9062	0	3,9062	0	5	0	-0,0312	0,0312
w2	0	0	-1	0,2	-6,4	0,2	0	0	0	0	0
w5	4	-32	0	-5	0	-5	-1	0	0	0	0
w7	2	-160	0	-25	0	-25	0	-32	-1	0	0
L	7	-192	-2	-30,8	-6,4	-28,8	-2	-32	-2	-1	-1

On Fig. 2 for an example the tree of decisions received by decoding of PRC on the basis of the classical method of branches and borders which does not use priority at search of variables for achievement of integer values is shown. In the analysis of a tree of decisions is seen that the objective of decoding are achieved already at 4-th step, however process of branching continues to the 7th step that is caused by need of check of all "hanging" perspective tops and confirmations of correctness of decoding.

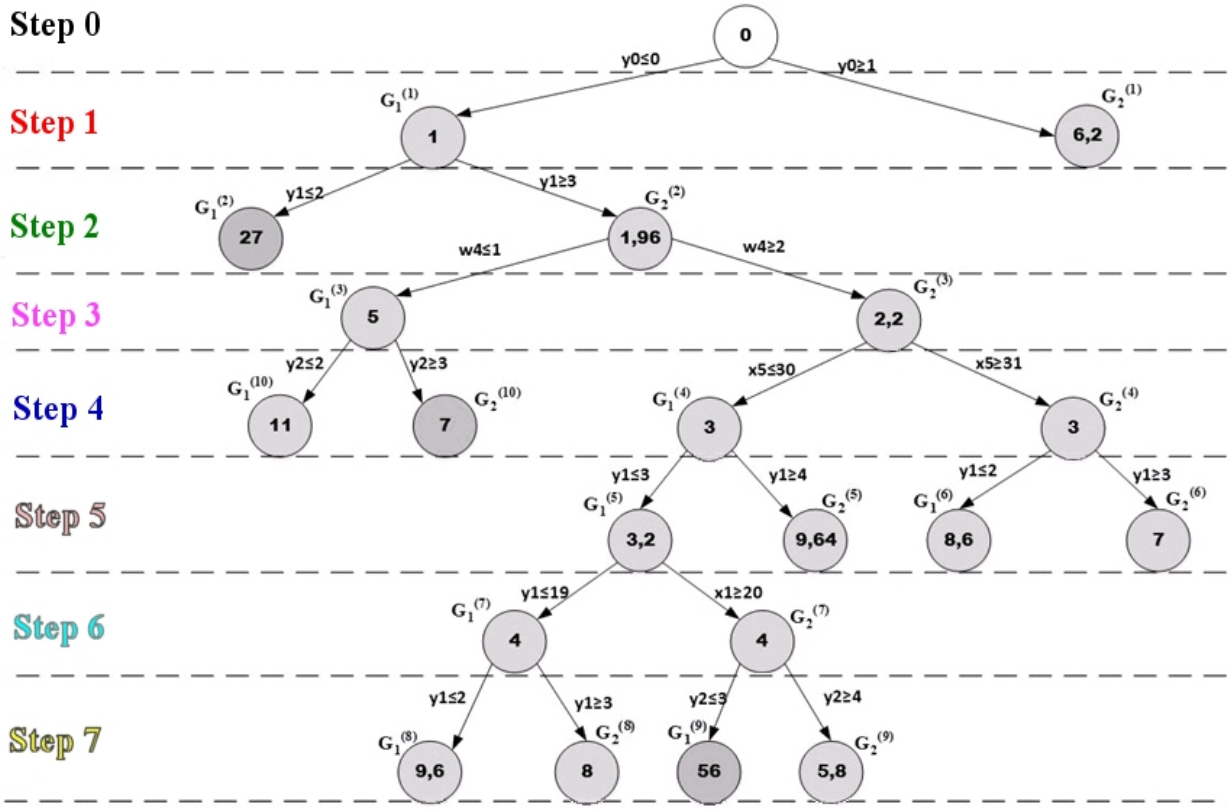

Fig. 2 – Tree of decisions for a classical method of branches and borders

Important result of use of the offered modified method of search of integer variables is that values of objective function in nodes of a tree are increased quicker (at increase of number of step of branching), unlike values by Fig. 2. It allows to conclude that computing complexity of method of decoding of PRC on the basis of the modified method of branches and borders significantly decreases by putting of a priority for achievement of integrality of the variables y performing function of linearization of operations of calculation of the module m. Approximate estimate of increment of computing efficiency in the reviewed example can be defined by simple calculation of the relation of quantity of nodes of trees of the decisions which are shown in Fig. 1 and Fig. 2: $21/11 \approx 1,91$.

4 Assessment of computing complexity of decoding of PRC

For confirmation of the fact of receiving a constructive method of decoding of PRC which has polynomial computing complexity is necessary to held comparison with method of simple search. For assessment of computing complexity of decoding of PRC by modified method of branches and borders uses the known result [5] where is described that чтоupper limit of quantity of tops of a tree of decisions for a classical algorithm amount:

$$S \approx N^5 \log_2 N, \qquad (17)$$

where N – effective value of quantity of unknown variables of a task.

The number of elementary operations (multiplication and addition) which are performed at modification one simplex of the table by size of $(3n-1)\cdot(2n)$ cells (as in the example reviewed above) problems of LP, using (17), it is possible to define total of elementary operations for solution of problem of decoding:

$$S=N^5 \log_2 N \cdot 2 \cdot (3n-1) \cdot (2n) \ . \tag{18}$$

It is known [6] that at the solution of problems of linear programming for obtaining of any permissible and optimum basic plan it is necessary to execute, approximately, no more N/2 iterations of recalculation of tables. Therefore final assessment of quantity of executed elementary operations constitutes:

$$\begin{aligned} S&=N^5 \log_2 N \cdot 2 \cdot (3n-1) \cdot (2n) \cdot \frac{N}{2} = \\ &= N^6 \log_2 N \cdot (3n-1) \cdot (2n). \end{aligned} \tag{19}$$

Total of variables of basis task in the starting table constitutes 3n-2, where n - length of block PRC. At branching of nodes of tree of decisions according to the modified method of branches and borders the priority is given to achievement of integer of variables $y_i, i \in [0,\ldots,n-2]$. Achievement of integrality of variables y_i, practically, guarantees achievement of the full solution of a task (*all variables will be integer*). At the same time the quickest approximation to decision is observed (*the decision is reached for smaller quantity of steps*).

Also, variables x and $\tilde{x}$ are a part of basic variables (Table 15). But appeal to lines of these variables at conditions of integrality are executed extremely seldom. For variables x restrictions only are formed in case the corresponding variable is outside the admissible range of values $[0\ldots m-1]$. The probability of this case on condition of uniform distribution of numbers, and an exception of a possibility of emergence in the code word of two identical numbers is equal $2/2^n$ – for variable x and $1/2^n$ – for variable $\tilde{x}$. The corresponding probabilistic weight coefficients which determine the weight of variables x, $\tilde{x}$, y and at calculation of effective quantity of variables N of problem of LP are presented in Table 15 .

Table 15 – Weight coefficients of variables

Quantity of variables	Name and range of placement	Weight coefficients
n	$x_i, i \in [0,\ldots,n-1]$	$2^{-(n-1)}$
n	$\tilde{x}_i, i \in [i,\ldots,2i-1]$	2^{-n}
n-1	$y_i, i \in [2i,\ldots,3i-2]$	1

Using of the weight coefficients presented in Table 15 allow to determine size of effective value of quantity of unknown variables of a task N:

$$N=(n-1)+n \cdot 2^{-n} + n \cdot 2^{-(n-1)}. \tag{20}$$

On the basis of expressions (19) and (20) computing complexity of a method of decoding of PRC on the basis of the modified method of branches and borders is estimated. Results of comparison of computing efficiency of developed decoding method with similar parameter of simple directional search of the decision at decoding of PRC are presented in Fig. 3.

As appears from the dependences presented in Fig. 3 with growth of length of the block computing complexity of directional search of the decision algorithm of decoding grows exponential, and using of the offered decoding method computing complexity grows to polynomial law. With lengths of PRC blocks $n \geq 37$ is reached advantage of offered decoding method on computing complexity comparison with directional search of the decision. For example, with a block length PRC

n = 50 advantage is equal almost 1000, and n = 60 – approximately by 10^6 times. It is confirmation of achievement of the object of this work.

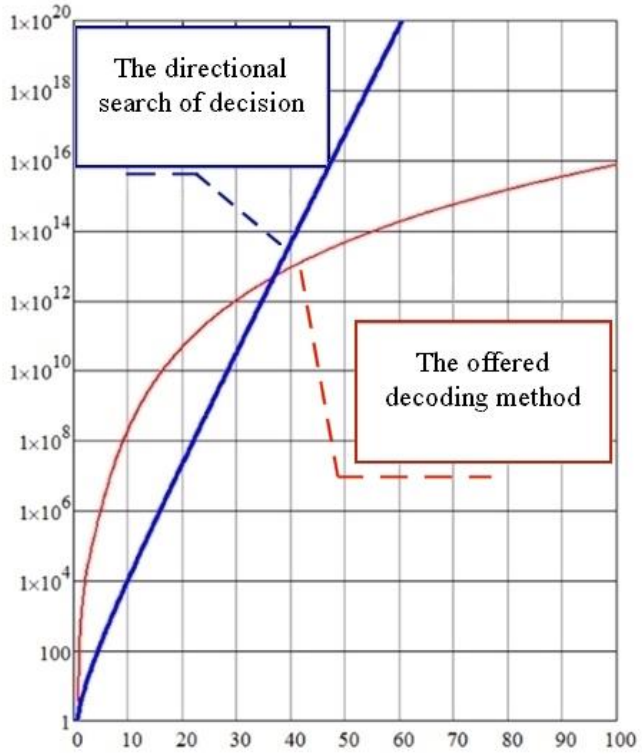

Fig. 3 – Comparison of computational complexity

5 Conclusions

The main result of this article consists in receiving a constructive method of construction and decoding of the LKG pseudorandom codes on the basis of the offered modified mathematical method of branches and borders. The possibility of representation of a problem of decoding in the form of tasks of integer linear programming due to insignificant decrease in objectivity of the rule of definition of the next code word is proved. This result disproves the settled stereotypes concerning a possibility of decoding of random and pseudorandom codes by exclusively methods of directional search of the decision on the basis of the rule of maximum like hood. The offered rule of the smallest projections of different vectors is a basis for linearization of objective function of the decoder. Decrease in objectivity of decoding is compensated by increase of lengths of PRC blocks.

The most acceptable method for the solution of an integer problem of decoding of PRC is the mathematical method of the directed search of the optimal solution – a method of branches and granits. The instrument of linearization of objective function is replacement of nonlinear operation of calculation of the module on its algebraic equivalent. Using of this replacement in the equations of recurrent interrelation of symbols of code words allows to formalize a problem of decoding in the form of an initial problem of integer linear programming.

Modification of a classical method of branches and borders by introduction of a priority of search of integer variables of a task in nodes of branching of a tree of decisions, allows to reduce several times quantity of the steps necessary for obtaining the optimal integer solution of a problem of decoding.

The complex consideration of the main problematic issues connected with creation and processing of pseudorandom codes and also the received strict mathematical solution of a problem of decoding PRC which have done in this work allow to make the reasonable assumption of a possibility of practical realization of PRC technologies in perspective systems of information transfer.

References

[1] Shannon C. E. A Mathematical Theory of Communication / C. E. Shannon // Bell Syst. Tech. J. – 1948. – Vol. 27. – P. 379 – 423, 623 – 656. (In English)
[2] Shannon C. E. Communication in the presence of noise / Shannon C. E. // Proc. IRE. – 1949. – Vol. 37. – P. 10 – 21. (In English)
[3] Lavrovskaya T.V. Matematicheskie modeli sluchaynyih i psevdosluchaynyih kodov // T.V. Lavrovskaya, S.G. Rassomahin // Sistemi obrobki Informatsiyi. – 2016. – Vip.9 (146) . – S. 55-61. (In Russian)
[4] Lavrovskaya T.V. Fizicheskaya model psevdosluchaynyih kodov v mnogomernom Evklidovom prostranstve / T.V. Lavrovskaya, S.G. Rassomahin // Sistemi Ozbroennya i Viyskova TehnIka. – 2016. – Vip. 3 (47). – S. 79-84. (In Russian)
[5] Nazaryants E.G. Polinomialnaya slozhnost parallelnoy formyi metoda vetvey i granits resheniya zadachi kommivoyazhera // Ya.E. Romm, E.G. Nazaryants // Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki. – 2015. – Vip.4 (165). – S. 44. (In Russian)
[6] Akulich I.L. Matematicheskoe programmirovanie v primerah i zadachah: ucheb. posobie dlya studentov ekonom. spets. vuzov / I.L. Akulich – Moskva: Vyissh. Shkola. – 1986. – 319 s. (In Russian)

Рецензент: Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: krasnobayev@karazin.ua

Надійшло: Листопад 2016.

Автори:
Таміла Лавровська, аспірантка, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: lavrovska92@gmail.com
Сергій Рассомахін, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: rassomakhin@karazin.ua

Метод декодування псевдовипадкових кодів на основі модифікованого методу гілок і меж.

Анотація: Розглянуто причини кризи завадостійкого кодування. Підкреслюється актуальність застосування псевдовипадкових кодів в сучасних системах передачі інформації. Наведено конструктивний математичний метод декодування псевдовипадкових кодів на основі використання методу гілок і меж. Запропонована модифікація класичного алгоритму гілок і меж. Проведена оцінка обчислювальної складності методів декодування псевдо-випадкових кодів на основі класичного та модифікованого алгоритму гілок і меж, а також оцінка обчислювальної складності запропонованого методу у порівнянні з перебірним алгоритмом. Розроблена програмна реалізація метода декодування псевдовипадкових кодів.

Ключові слова: псевдовипадковий код, метод гілок і меж, обчислювальна складність, завадостійке кодування.

Рецензент: Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: krasnobayev@karazin.ua

Поступила: Ноябрь 2016.

Авторы:
Тамила Лавровская, аспирантка, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: lavrovska92@gmail.com
Сергей Рассомахин, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: rassomakhin@karazin.ua

Метод декодирования псевдослучайных кодов на основе модифицированного метода ветвей и границ.

Аннотация: Рассмотрены причины кризиса помехоустойчивого кодирования. Подчеркивается актуальность применения псевдослучайных кодов в современных системах передачи информации. Представлен конструктивный математический метод декодирования псевдослучайных кодов на основе использования метода ветвей и границ. Предложена модификация классического алгоритма ветвей и границ. Проведена оценка вычислительной сложности методов декодирования псевдослучайных кодов на основе классического и модифицированного алгоритма ветвей и границ, а также оценка вычислительной сложности предложенного метода по сравнению с переборным алгоритмом. Разработана программная реализация метода декодирования псевдослучайных кодов.

Ключевые слова: псевдослучайный код, метод ветвей и границ, вычислительная сложность, помехоустойчивое кодирование.