The article considers the method of effective processing of error-correcting codes combinations. The method is based on the possibility of lexicographical partitioning of code words space into clusters. This process allows to realize the list decoding method of code vectors on a regular basis with the use of a single list, which refers to the cluster number zero. The authors show that the vector of any other cluster with simple transformations can be brought to a vector of the cluster zero. The article proves that the method is applicable to binary and non-binary codes.

Key words: error-correcting codes, list decoding, binary codes, non-binary codes.

MATHEMATICAL MODELING
Introduction

The transfer of large data amount and objectively increasing requirements to management efficiency of modern and advanced information-management complexes (IMC) reveal the necessity of applying the short management cycles (SMC). For example, it concerns the final stage of the high-accuracy process or the realization of brief hypersonic technology commands. Regarding this, in order to protect the real-time data from the errors it is advisable to use a noise-resistant short codes. In light of IMC specificity short codes are universal concerning their long analogues.

In addition, such codes provide relatively fast mode switch of parametric adaptation of the error protection system in the communication channels of IMC. If the large multimedia data amount needs to be exchanged, the short codes transform into the cascade structure or into the 3D-codes (and above) product. It is possible due to the codecs structural adaptation.

The reducing of code sequences length and specific requirements for the IMC-data reliability on the one hand lead to the problem of flexible synthesis of information about signals, obtained from a continuous communication channel. And on the other hand to the need of effective soft algorithms for the processing of the redundant codes used in a communication system IMC. Regarding this the telecommunication technologies play a crucial role in the organization of mobile IMC and specialized management systems (MS), aimed to collect information about controlled objects and manage these objects in accordance with the target function $F(V, U, T, P)$.

The set of objects $V$ is considered to be given in SM. At that time as a set of operation conditions $U$ can vary and stochastically affect the achievement $F(\ast)$ in the actual time intervals $T$ and with a given reliability $P$ of the information circulating in the MS [1, 2]. Usually, the boundaries of parameter $T$ are determined by the duration of the management cycle $T_{mc}$, the execution of which indicates the efficiency of achievement $F(\ast)$.

Under the intense interference parameter $T_{mc}$ can be reduced only by using the integrated MS and IMC on the basis of material carrier in the form of a communication system, capable of transmitting not only the short control signals, but also the large amounts of multimedia data. For example, during the interaction of two or more radar stations in the common view zone under the stationary active noise [2]. The existence of the direct and reverse channels in the classical MS requires to meet the condition $k_o(T_{pr} + T_{rr}) < T_{mc}$, where $k_o > 0$ is a coefficient determining the overall data delay while processing in the codec. In the simplest case $k_o$ is a number of data repeats in the reliability increasing algorithms. Parameters $T_{pr}$ and $T_{rr}$ represent the time of control information processing in the direct and reverse channel respectively. The data processing and decision (in managed and managing objects as well) on MS take the time $\Delta = T_{mc} - T_{v0}$, where $T_{v0} = k_o(T_{pr} + T_{rr})$ and commonly $\Delta \gg 0$. The parameters above may multiple with the collection and processing of information in hierarchic IMC [2, 3].

Considering inequality $T_{v0} < T_{mc}$ the parameter $P$ becomes actual in $F(\ast)$ with the given $V$ and $U$, because IMC can accept to processing only reliable data [2]. During the development of the telecommunication system one needs to consider a number of different factors, which may in a varying degree affect the efficiency of its operation under the real conditions. Naturally, at the design stage, there is no usually the complete information about the place of application, purpose of communication and the ability of environment to influence its operation. It is reasonable to give the antagonistic (conflicting) properties to unknown conditions for the purpose to achieve the guaranteed performance of the communication system and IMC in general. Performance (P1) of permissible (possible defined only by limit values) conditions from $U$ and selected (or strictly specified) elements from $V$ are estimated by the set of real numbers $\{R\}$. The procedure of finding $V$ with conditions $U$ for reaching $F(\ast)$ and their interpretation $F: V \times U \rightarrow R$ constitute the conceptual and semantic side of the model of researched systems. The formal side of the model is the further application of these structures for formulating and solving mathematical problems of the system synthesis [2].

In the case of specified conditions $\{u_{0\ast}, u_1, \ldots, u_n, \ldots\} = U_{0\ast}$, where $U_{0\ast} \in U$, the operation of the synthesized system becomes the classic optimization (generally multi-critical) in sense of reaching the extremal values of $T_{e\ast \in R}$ (or)

$$P_{e\ast \in R} \rightarrow F(\ast) \left\{V, U_{0\ast}\right\} \rightarrow \max, \quad \forall F \in V$$

The solutions of (1) is the set $\{V_{e\ast}(V, U_{0\ast})$ of so-called
\( \varepsilon \)-optimal systems \( \tilde{V}_\varepsilon (\varepsilon \geq 0) \) defined by the expression
\[ \tilde{V}_\varepsilon \in V_\varepsilon (V, U_0, T, P) \leftrightarrow F \{ V, U, T, P \} \leq F \{ \tilde{V}_\varepsilon, U_0, T, P \} + \varepsilon. \] (2)

for any \( \tilde{V} \in V \).

Thus, for selected \( \tilde{V} \) and specified conditions \( U_0 \) the operation indicators of \( \varepsilon \)-optimal system cannot be improved. And if \( \varepsilon > 0 \), there is still the reason to search the ways to reduce computational costs. When \( \varepsilon = 0 \) the optimal elements of the system are not available \( V_\varepsilon (V, U_0, T, P) = \{ \} \), but
\[ F \{ \tilde{V}_\varepsilon, U \} \geq \sup_{\tilde{V}_\varepsilon \in V_\varepsilon} F \{ \tilde{V}_\varepsilon, U_0, T, P \} - \varepsilon \text{ at } \tilde{V} \in V. \]

In [2] it was shown, that considering the general approach to telecommunication system synthesis (TSS), it is reasonable to regard the set of operation conditions as two subsets. First is \( U_p \in U \), where the operation conditions of the system are defined a priori. And second is the subset \( U_{np} \in U \), where the conditions of its realization are unknown until the real application in the system. From the sets \( U_{np} \) occur with a high probability in TSS intended for use in game situations with antagonistic interests, during the abnormal phenomena and emergency situations. The subset \( U_{np} \) is applied to the solution of problems of digital data protection from noise while the transmission. This is determined by the high a priori uncertainty of the channel as of an element of any telecommunication system, especially in case of application of radio interface.

The design of the system with uncertainty supposes the incomplete knowledge of operation conditions. In fact, in this case, a whole class of environments (for example, set \( U_{np} \)), in which the system may be applied is determined. However, in order to formulate the mathematical problem we use anyway the additional knowledge about the appliance conditions which lead to different approaches to the system synthesis. The important property of the conditions class \( U_{np} \), leading to specific synthesis tasks, is their conflictness.

The conflictness of operation conditions significantly affects the principles of formulating and solving the problems of system synthesis. The TSS element synthesized for conflictable conditions must be resistant to a class of outside impact. The impact can be selected to be optimal (optimized at least) in some sense. The selection is made from a class limited by the energy, technical, economical and intellectual resources of antagonistic system.

The essence of the conflict environment is that the concretion of the element \( U_{np} \in U \) for the given system \( \tilde{V} \) may be performed by the natural stochastic factors or by the antagonistic party. The target of antagonist is to solve the opposite problem up to a fatal failure in IMC operation. For example, it can optimize in terms of energy the impact on the TSS in order to minimize the value of EFF \( F^\bullet \).

If the TS from the IMC uses the error-correcting code

\[ C_{p,k,d'} \text{ where } n \text{ is the codeword length, } k \text{ – the number of information bits, and } d \text{ – Hamming metric, it is sufficient to make } t \geq (d+1)/2 \text{ errors to disrupt the codec work or put TS in the repetition mode and increase the parameter } T_{\varepsilon}. \]

The reason to solve the synthesis problem in this case is the practical necessity of the system which is supposed to operate under the antagonistic pressure.

As stated above, the \( \varepsilon \)-optimal system is able to provide the sub-optimal modes of decoder operation. For example, by using a soft data processing and correcting the erasures instead of just the error correction mode [2].

In the new conditions the decoder produces the maximum possible number of erased positions in order to minimize the decoding errors (the decoding beyond the constructive possibilities of the code). Usually the similar algorithms of the algebraic decoding use the information about the weight structure of the code.

Suppose in the erasure procedure \( \bar{P}_{\Delta S} \) is the probability of erroneous decoding of one codeword averaged by the set of code combinations, where \( \Delta \) is the non-specified number
\[ (\Delta = 0, d - 1) S. \] Apparently:
\[ \bar{P}_{\Delta S} = \sum_{i=0}^{\Delta} P_{i} \cdot P_{i} + \sum_{i=\Delta+1}^{d} P_{i}. \] (3)

where \( P_{i} \) is the error probability at the registration in combination of \( i \) erasures, and \( P_{i} \) – the error probability in the same codeword.

Let’s set another rule, when the receiver processor forms the soft decision for the symbols (SDS) on the result of signal demodulation. The same solutions can be applied to the non-binary symbols as well.

Let the new algorithm, on the results of receiving the whole combination, provides a purposeful selection of SDS with the lowest reliability and let it, on the results of such a selection, always forms the greatest possible number of erasures in a codeword. Denote the probability of erroneous combination decoding under these conditions as \( P_{s} \).

The formal inequality is
\[ P_{s} \sum_{i=0}^{\Delta} P_{i} + \sum_{i=\Delta+1}^{d} P_{i} > P_{s} \sum_{i=0}^{\Delta} P_{i} + P_{s} \sum_{i=\Delta+1}^{d} P_{i}. \] (4)

After transformation of the right side of (4), we obtain:
\[ P_{s} \sum_{i=0}^{\Delta} P_{i} + \sum_{i=\Delta+1}^{d} P_{i} > P_{s} \text{ since} \]
\[ \sum_{i=0}^{\Delta} P_{i} + \sum_{i=\Delta+1}^{d} P_{i} = 1. \]

Then \[ P_{s} \sum_{i=0}^{\Delta} P_{i} < \sum_{i=0}^{\Delta} P_{i} \cdot P_{i}. \]

Reinforcing this inequality, we obtain
\[ P_s \sum_{i=0}^{\Delta} P_{es} P_{er} + \sum_{i=\Delta+1}^{d} P_{er} > P_s. \] (Hence, \( P_{\Delta s} > P_{C_s} \) [2].

It follows, that in the optimal system while decoding of the redundant code combinations among the received symbols of a single combination, using the values of the SDS, it is reasonable to allocate (directly or variatively) exactly \( d - 1 \) erasures and correct the erased positions, minimizing the erroneous decisions for the non-erasure positions by the correct forming of SDS indices [4, 5].

Without considering the antagonistic system details, it should be noted that elements of the set \( U_{np} \) in the system designed for the conditions \( U_p \) may occur as massive equipment failure in cases of abrupt change of the parameters of IMC channel. If for the operating under the conditions defined by class \( U_p \), there is developed and implemented the system \( V \in V \), then solution of the counteraction optimization problem is reduced to following situation:

\[ F\{\hat{V}, U_{np}, T, P\} \rightarrow \min_{U_{np} \in U} . \] (5)

For example, by reservation, adaptation or intentional failure to perform the rule of synchronization will be specified by the interaction protocol.

**The Concept of Splitting the Code Space into Clusters**

Note as \( GF(2^k) \) the field, where \( k \in N \) is a number of bits in nonredundant code combination. If the information source work over this field then after it passes the channel encoder containing generator matrix \( G_{k \times n} \) it forms the sequences of length \( n > k \). This operation sets the group code \( C_{n,k} \) over the field \( GF(2^n) \). Considering the nesting of binary fields with extension degree less than or equal to \( n \), the combinations of any \( C_{n,k} \) code can be split into clusters with unique numbers \( w_i \), and, consequently, they can be lexicographically ordered. Here \( 1 \leq w \leq k \) is the sum of the number of bits defining the cluster number, \( s = \) the used numeral system [2].

Then \( C_{n,k} = \{\{c_0\}, \ldots, \{c_{2^n-1}\}\} \), where \( \{c_i\} \) is the set of \( C_{n,k} \) combinations belonging to the cluster with number \( w_i = i \), where \( i = 0, 2^n - 1 \). Under the new conditions all code combinations contain three parts non intersecting among themselves by symbols of the code vector: \( \langle w \rangle \) – the combination of any randomly selected bits of cluster number; \( \langle k - w \rangle \) – bits of indicator of equivalence code; \( \langle n - k \rangle \) – other bits, not used and not necessarily redundant. In the group \( C_{n,k} \) all the clusters \( \{c_i\} \) can be attributed to two types. The first type is the unique cluster containing the identity element of the additive Abelian group \( \{c_{i=0}\} = \{0, c_{0,2^k}, \ldots, c_{0,2^k-w}\} \). In this cluster all the elements belonging to the group \( \langle w \rangle \) are equal to zero.

The second type includes clusters with numbers \( i \neq 0 \). Cluster \( \{c_{i-0}\} \) is the basic one. The change of the number of bits for \( w \) within specified limits leads to the same expansion or reduction of cluster combinations list \( \{c_{i-0}\} \) or \( \{c_{i \neq 0}\} \). For example, if \( w = k \) then \( \{c_{i \neq 0}\} = 1 \) and, consequently, the base cluster consists only of the one zero code combination (the lower bound by the combinations number in cluster, and then each combination code is independent cluster). If \( w = 1 \), then \( \{c_{i \neq 0}\} = C_{n,k}/2 \), and the base cluster contains half of code combinations set (the upper bound). The choice of symbols for cluster number \( \langle w_i = i \rangle \) can be arbitrary.

Based on the properties of an algebraic group, this lexicographical ordered number repeats in the code \( 2^n \) times [6]. Symbols from the part \( \langle k - w \rangle \), represented as the vectors, should form field elements from \( GF(2^{k-w}) \). The failure of this condition leads to a linear dependence of combinations and unsatisfactory result in the cluster forming system. According to research, the properties of the base cluster are reproduced in any other cluster \( \{c_{i \neq 0}\} \), therefore the combinations from \( \{c_{i \neq 0}\} \) cumulatively represent the information about all clusters. It can be easily proved by properties of shortened systematic codes. As an example the Table 1 shows three clusters (from four possible) for the code combination space \( (7, 4, 3) \). This illustrates the properties that are valid for all other classes of block codes in table 1.

**Property 1.** For the set of combinations of the same value \( w_i = i \), vectors in positions \( \langle k - w \rangle \) form the field elements of \( GF(2^{k-w}) \). This follows from the binary Galois fields nesting property and leads to the possibility of construction of an equivalent code only in the presence of the elements of the identity matrix \( I_{(n - w) \times (n - w)} \) among \( \langle k - w \rangle \) selected items. For non-binary codes Property 1 always perform.

**Property 2.** Any cluster with number \( w_i = i \neq 0 \) contains itself, the combination of any randomly selected bits of cluster number; \( \langle k - w \rangle \) – bits of indicator of equivalence code; \( \langle n - k \rangle \) – other bits, not used and not necessarily redundant. In the group \( C_{n,k} \) all the clusters \( \{c_i\} \) can be attributed to two types. The first type is the unique cluster containing the identity element of the additive Abelian group \( \{c_{i=0}\} = \{0, c_{0,2^k}, \ldots, c_{0,2^k-w}\} \). In this cluster all the elements belonging to the group \( \langle w \rangle \) are equal to zero.

The second type includes clusters with numbers \( i \neq 0 \). Cluster \( \{c_{i-0}\} \) is the basic one. The change of the number of bits for \( w \) within specified limits leads to the same expansion or reduction of cluster combinations list \( \{c_{i-0}\} \) or \( \{c_{i \neq 0}\} \). For example, if \( w = k \) then \( \{c_{i \neq 0}\} = 1 \) and, consequently, the base cluster consists only of the one zero code combination (the lower bound by the combinations number in cluster, and then each combination code is independent cluster). If \( w = 1 \), then \( \{c_{i \neq 0}\} = C_{n,k}/2 \), and the base cluster contains half of code combinations set (the upper bound). The choice of symbols for cluster number \( \langle w_i = i \rangle \) can be arbitrary.

Based on the properties of an algebraic group, this lexicographical ordered number repeats in the code \( 2^n \) times [6]. Symbols from the part \( \langle k - w \rangle \), represented as the vectors, should form field elements from \( GF(2^{k-w}) \). The failure of this condition leads to a linear dependence of combinations and unsatisfactory result in the cluster forming system. According to research, the properties of the base cluster are reproduced in any other cluster \( \{c_{i \neq 0}\} \), therefore the combinations from \( \{c_{i \neq 0}\} \) cumulatively represent the information about all clusters. It can be easily proved by properties of shortened systematic codes. As an example the Table 1 shows three clusters (from four possible) for the code combination space \( (7, 4, 3) \). This illustrates the properties that are valid for all other classes of block codes in table 1.

**Property 1.** For the set of combinations of the same value \( w_i = i \), vectors in positions \( \langle k - w \rangle \) form the field elements of \( GF(2^{k-w}) \). This follows from the binary Galois fields nesting property and leads to the possibility of construction of an equivalent code only in the presence of the elements of the identity matrix \( I_{(n - w) \times (n - w)} \) among \( \langle k - w \rangle \) selected items. For non-binary codes Property 1 always perform.

**Property 2.** Any cluster with number \( w_i = i \neq 0 \) contains itself, the combination of any randomly selected bits of cluster number; \( \langle k - w \rangle \) – bits of indicator of equivalence code; \( \langle n - k \rangle \) – other bits, not used and not necessarily redundant. In the group \( C_{n,k} \) all the clusters \( \{c_i\} \) can be attributed to two types. The first type is the unique cluster containing the identity element of the additive Abelian group \( \{c_{i=0}\} = \{0, c_{0,2^k}, \ldots, c_{0,2^k-w}\} \). In this cluster all the elements belonging to the group \( \langle w \rangle \) are equal to zero.
the key combination $c_{i,kli}$ with the additive identity in the field $GF(2^{k-w})$ on selected $(k-w)$ positions. According to Property 1 the selected vectors on $(k-w)$ positions of any cluster form binary field with degree of the extension equal $(k-w)$ and, consequently, among them should be the additive identity. This allows the receiver to generate the combinations $c_{i,kli}$ by using elements from $(w)$. For the non-binary codes Property 2 is valid as well.

**Property 3.** The summation of vector $c_{i,kli}$ with any other vector of this cluster produces a vector, belonging to the cluster $i = 0$. This means, that zero cluster can be the only one list, which is processed by the list decoder, and all the other vectors can always be conversed by suitable $c_{i,kli}$ to zero cluster vectors. Indeed, $\{c_{i,\neq0}\} \oplus c_{i,kli} = \{0,\ldots, c_{0,2^{k-w}}\}$.

Since $\langle w_{\neq0} \rangle \in \{c\}$ and $c_{i,kli} \in \{c\}$, then after the summation in the binary field (or in the field of elements from $GF(2^k)$ for non-binary codes) position $\langle w \rangle \equiv 0$, which means the conversion of the combination to the base cluster with the number $i = 0$. This clustering property allows decoder to process always only one list. Key combinations of the clusters can be stored in the decoder memory or be formed by multiplying of vector $\langle w_{\neq0} \rangle \langle k-w \rangle = 0$ on $G_{k,n}$. Property 3 is valid for non-binary codes.

**Property 4.** In case of cyclic codes and soft data processing, any reliable configuration of symbols that determine values $\langle w \rangle$ allows calculating the cluster number depending on number of steps of cyclic data shifts. Property 4 is valid for non-binary codes, such as Reed-Solomon code (RS).

Application of the listed clustering properties of code vector space allows to converse any vector of $C_{n,k}$ to the vector system of base cluster.

Property 1 improves the computing efficiency by the exclusion from the procedure of permutation decoding the calculation of inverse matrix during the determining of the obtained codes equivalence. Receiver processor works with a single list, without expending time on searching for the most probable combinations from a whole set $C_{n,k}$. Therefore, the list decoding procedure becomes regular unlike the stochastic model of list making. The method is of particular importance in non-binary codes processing, as it allows avoiding the procedure of searching for the polynomial error locator, for example, using the Berlekamp-Massey algorithm (BMA) [7].

### Decoding non-binary codes

Non-binary codes Reed Solomon found wide application in data protection systems for data storage and recovery in communication systems in the conditions of formation of burst errors, in the systems of concatenated coding or systems of generalized concatenated coding [6, 7]. One of the major drawbacks of such codes is a need for the organization of the computational process in extended Galois fields, thus execution addition operation substantially differs from the multiplication operation. Application of cluster partition of code vectors RS code into clusters reduces the complexity of the computing process by complete exclusion of multiplication operations. The main difference of non-binary code from the binary codes RS is the property of their maximum decodability. This means, that in the Option 2 is exclude conditional operator (step 4), which making this algorithm is attractive in terms of implementation. Consider code RS (7,3,5) in $GF(2^6)$.

Generator polynomial code –

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)$$

where $\alpha'$ – primitive element of the field. Let coder formed $V_{np} = \alpha^0 \alpha^3 \alpha^6 \alpha^5 \alpha^3 \alpha^5$ and let in transmission of its error vector had the appearance of $V_{er} = 0000 \alpha^3 \alpha^3 \alpha^2$. The receiver receives vector $V_{np} = \alpha^a \alpha^2 \alpha^3 \alpha^4 \alpha^6 \alpha^2$, in which at the results of the analysis of the quantized soft decisions (QSD) installed reliability of the first three characters $\alpha^0 \alpha^3 \alpha^5$. Then the receiver by encoding form combinations $\alpha^0 \alpha^3 \alpha^5$ forms a cluster of key combination $c_{\alpha^0 \alpha^3 \alpha^5,kli} = \alpha^0 \alpha^3 \alpha^5 \alpha^3 \alpha^5$. By performing $V_{np} \oplus c_{\alpha^0 \alpha^3 \alpha^5,kli} = 0000 \alpha^3 \alpha^3 \alpha^2 \alpha^2$ and encoding vector of zero cluster $0 \alpha^2$, get $c_{0,\alpha^2} = 000 \alpha^3 \alpha^2 \alpha^3 \alpha^2$. It is easy to check, that the validity of $V_{np} \oplus c_{\alpha^0 \alpha^3 \alpha^5,kli} \oplus c_{0,\alpha^2} = V_{er}$. The complexity of the implementation of the decoder with considering performing of addition operations and multiplication in the field $GF(2^m)$ at the traditional use of ABM and procedures Chen estimated as $O_{BMA} = 2t(16t + 4) + 2t(q^m - 1)$, where $t$ – the multiplicity of correctable error code. The complexity implementation of the proposed algorithm is with the use of QSD estimated simpler expression $O_{MKP} = tk + 3n$. at this $O_{BMA} > O_{MKP}$ Numerical method established, that at $m = 5$ and ratio $R = k/n = 0.8$ complexity of implementation decoder when using the described method is reduced by 4.5 times. With increasing multiplicities of parameter $t$ and using parameter $t R = 0.5$ winnings increases to 7.4.

### Conclusions

Synthesis of modern exchange of digital information systems is largely associated with the development and implementation of soft-error-correcting codes decoding methods. This provides improvement energy efficiency of data exchange systems in the limits of 2-3 dB, but inevitably increases the complexity of realization decoders. The last circumstance in the conditions of intensive development of radio electronics means considered insurmountable and therefore in modern systems of self-organizing network structures soft decoding techniques are increasingly being...
applied. Considered that decoding by list represents the most simple realization of decoders redundant codes even under the application stochastic methods of listing. The article shows the systematic algebraic structure of binary and non-binary correcting codes allowing to apply the method preparation of a single list which accumulates itself only combination of the zero (basic) cluster. The developed method for transferring combinations of any cluster into the combinations system of basic cluster represents the innovative approach to the organization system of list decoding using a single deterministic list.

СПИСОК ЛИТЕРАТУРЫ
1. Лычагин, Н. И., С. А. Агеев С. А., Гладких А. А., Васильев А. В. Неалгебраическое декодирование групповых кодов в стирающем канале связи // Системы и средства связи телевидения и радиовещания. – 2006. – № 1, 2. – С. 49–55.

REFERENCES