Increase of Reliability of Transfer of Blocks the Digital Information on the Hydroacoustic Communication Channel

Boris I. Filippov* and Gennadiy A. Chernetsky
Novosibirsk State Technical University
20 Karl Marx, Novosibirsk, 630073, Russia

Received 09.03.2016, received in revised form 13.03.2016, accepted 09.04.2016

The In work it is shown that the hydroacoustic channels of impulse noise or short-term interruptions for improving the quality of data transmission can be applied different variants of convolutional and cyclic codes. Convolutional codes at a rate of $R \leq 3/4$ in conjunction with broadband signals (BBS) or convolutional codes $R \leq 2/3$ with code interleaving algorithm can reduce the probability of an error at the output channel for the known error statistics. Taking into account the energy gains from the computational complexity of encoding and interleaving of code is more favorable option “code + BBS” to 4÷5 interlaces. Given the multi-bit optimal filter BBS, its implementation is always more difficult than implementing a threshold decoder trellis.

Keywords: hydroacoustic channel autocorrelation function (FAC) and the cross-correlation (FCC), noise-resistant codes, broadband signals (BBS), M-sequence.

Повышение достоверности передачи блоков цифровой информации по гидроакустическому каналу связи

Б.И. Филиппов, Г.А. Чернецкий
Новосибирский государственный технический университет
Россия, 630073, Новосибирск, пр. Карла Маркса, 20

В статье показано, что в гидроакустических каналах с импульскими помехами или кратковременными перерывами связи для повышения качества передачи данных могут быть применены различные варианты сверточных и циклических кодов. Уменьшить вероятность ошибки на выходе канала для известной статистики ошибок позволяют сверточные коды со скоростью R ≤ 3/4 совместно с широкополосными сигналами (ШПС) или сверточные коды R ≤ 2/3 с алгоритмом перемежения кода. С учетом энергетического выигрыша от кодирования и вычислительной сложности перемежения кода выгоднее вариант "код + ШПС" до 4÷5 перемежений. С учетом многоразрядности оптимального фильтра ШПС его реализация всегда сложнее, чем реализация порогового декодера сверточного кода.

Ключевые слова: гидроакустический канал, функции автокорреляции (ФАК) и взаимной корреляции (ФЗК), помехоустойчивые коды, широкополосные сигналы (ШПС), M–последовательности.

1. Introduction

The transfer of a final set of code words known on the reception party (these words may contain from 4th to 128 symbols, number of words 16 ÷ 128 [1]), is possible by use of some code words of any block code from total number of $N_B = q^n - 1$ (where $q$ – the code basis, and $n$-number of symbols in the word) with the subsequent correlation processing on the reception party. Thus code words, known on the reception party, are used as basic signals of correlators at coherent processing. Also coherent or incoherent processing of such code sequences by means of optimum filters is possible, each of which is coordinated in a form with a form of code sequence. However to increase probability of the correct reception of code words, it is necessary to reduce probability of transition of $p(A_i/A_j)$ for $i \neq j$, where $A_i$, $A_j$ respectively the accepted and transferred code words [2]. For this purpose it is necessary to transfer such code words which have good autocorrelated (FAC) and cross correlation (FCC) functions. Good in the sense that they have to have a narrow main petal and, whenever possible, small values of side petals.

Such set of code words is formed by so-called correlation codes [3]. Usually these codes have big redundancy and they are called as also broadband or noise-type signals (NTS). In foreign literature [4] such methods of formation of signals are called as methods of an expanded range (spread-spectrum: ss). The basic purpose of correlation codes consists in compensation of the distorting influence of noise, impulse and deliberate hindrances.

All set of correlation codes conditionally shares on temporary codes and the time-and-frequency codes (TAFC). Binary codes in the main strip of frequencies, binary phase-modulated (PM) codes, multilevel codes in the main strip of frequencies, not binary PM codes are distinguished from the first. The codes TAFC are divided on the basis of simultaneity of transfer of one or more than one frequency element.
Codes in the main strip of frequencies apply regardless of a modulation method, in the basic, with post-detection processing. PM process signals, as a rule, to the detector.

At big bases of a signal of \( B=TF > 10^2 \cdot 10^4 \) apply also discrete compound frequency (DCF) signals. Sometimes they are called cascade codes. In DCF signals each element of a signal of BBS is a difficult signal, that is represents a set of simpler signals. Thus elements of primary sequence can represent code elements of a noise-proof code. Then it is about combined use of the codes correcting mistakes and BBS [5, 6].

2. Binary correlation codes

Phase-modulated PM signals represent sequence of radio impulses which initial phases change under the set law. Usually the phase of a binary signal accepts values 0 or \( \Pi \) (opposite signals). FM signal can be multiphase.

Video (duration \( T \)) consisting of the positive and negative impulse of duration of \( \tau_0 < T \) corresponds to the PM radio frequency signal. The base of a signal \( B=TF= T/\tau_0 =N \) is in number equal to number of impulses in a signal.

Discrete frequency signals represent sequence of radio impulses of duration of \( \tau_0 \) which bearing frequencies change under the set law. The base of such signal is equal

\[
B=TF =NF_0N \ \tau_0= N^2 F_0, \tau_0=N^2,
\]

where \( F_0 = 1/\tau_0 \) – width of a range of one impulse.

Above definition of DCF signals was given. For example, DCF – PM signal is a discrete compound frequency signal with phase modulation of positive and negative impulses. There is base \( B=N_0 N^2 \), where \( N_0 = F_0 \tau_0 \) – number of impulses of PM of a signal in one DCF frequency element of a signal.

Also signals of DCF – FM can be used (with code frequency modulation and frequency manipulation).

The type of the BBS correlation functions depends on correlation properties of sequence of the modulating symbols

\[
A = (a_1, a_2, a_3, \ldots, a_i, \ldots, a_N) \ \text{or} \ \{a_n\}_N^n.
\]

As the modulating sequences in signals of BBS pseudorandom sequences (PRS) are used, as a rule: Barker's codes, sequences Golda, M-sequences, sub-codes of noise-proof codes and so forth.

M-sequences and sub-codes of noise-proof codes are of special interest as the number of necessary PSP can be big.

3. Correlation codes on the basis of M-sequences

M – sequences represent periodic sequences of impulses which properties are close to properties of casual sequences. The main properties of M-sequences are as follows.

1. M-sequences are periodic with the period \( N= q^m -1 \), where \( q = 2, 3, 5 \) etc. – the code basis (as a rule, it is the whole prime numbers), \( m \) – number of categories of the register of the shift used for generation of sequence. Side petals of periodic FAC are equal \( (1/N) \), and at FCC they don’t exceed size of \( (1/\sqrt{N}) \).
2. The M-sequence can be generally made of several types of impulses (for example, impulses can differ in initial phases, the bearing frequencies and so forth). Impulses of various look meet on sequence length approximately identical number of times.

3. M-sequences are formed by means of linear schemes on the basis of the shifting registers and the making polynomials. The demanded number of categories of the register of shift is defined from a ratio

\[ m = \log(N + 1)/\log(q). \]

4. M-sequences are called usually pseudorandom sequences or sequences of the maximum length of the register of shift.

Regular methods of formation of M-sequences on the basis of differential sets and the making polynomials are known. In Tabl. 1 [6] of the making polynomials for \( M \leq 11 \) are provided.

Couple of mutually inverse M-sequences possesses good FCC. However the greatest interest for communication systems and management ensembles of M-sequences represent, NB which power \( N_B > 2 \). In process of reduction of dimensions and consumption of power supply of the coordinated filters and correlators there is possible a realization of reception of the ensembles containing tens and hundreds of signals of PRS.

Power of ensemble is defined by expression \([4]\) \( N_B = \phi(N)/m \), where \( \phi(N) \) – Euler’s function (number of coprimes among \( 1, 2, \ldots, N-1 \)). If \( N \) prime number, \( \phi(N) = N - 1 \).

Correlation codes of big length on the basis of M-sequences can contain in the coder some registers with feedback with logical association of releases of these registers.

Depending on methods of construction and power correlation codes are divided on:
- a ensembles of M-sequences;
- Gold’s ensembles;
- Kassami’s ensembles.

Gold’s ensembles use information and basic registers and, respectively, two the making polynomial of \( g_a(x) \) and \( g_b(x) \).

Table 1. Power of M-sequences

<table>
<thead>
<tr>
<th>M</th>
<th>( N_B )</th>
<th>При</th>
<th>q</th>
<th>M</th>
<th>( N_B )</th>
<th>При</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>10</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>11</td>
<td>176</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>4</td>
<td>20</td>
<td>48</td>
<td>176</td>
<td>12</td>
<td>144</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>8</td>
<td>48</td>
<td>160</td>
<td>960</td>
<td>13</td>
<td>630</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>22</td>
<td>304</td>
<td>1120</td>
<td>14</td>
<td>156</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>48</td>
<td>720</td>
<td>15</td>
<td>1800</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>18</td>
<td>150</td>
<td>16</td>
<td>2048</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>320</td>
<td>17</td>
<td>7710</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td>1008</td>
<td>18</td>
<td>7776</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
More powerful Kassami’s codes for even \( M \) use bigger number of registers, and degrees of the making polynomials are connected by a ratio \( \deg g_1(x) = M; \deg g_2(x) = M/2; \deg g_3(x) = M \).

Then

\[
N_B = \begin{cases} 
2^{m/2}(2^m+1), & \text{for } m=2 \text{ mod } 4 \\
2^{m/2}(2^m+1)-1, & \text{for } m=0 \text{ mod } 4 
\end{cases}
\]

4. Correlation codes on the basis of noise-proof codes

Considering that correlation codes are a subset of noise-proof codes, already known cyclic codes can be used for receiving a correlation code of power of \( N_B \) with satisfactory properties.

It is known that cyclic codes contain to \((2^k-1)/n\) cycles of \( n \) volume. If to take one code floor from each cycle, it is possible to receive a correlation code of power of \( N_B \approx (2^k-1)/n \). For example, Goley’s code \((23,12), d=7\) allows to receive a correlation code of the power \( N_B=178 \) at which the FCC level reaches 52% of the main petal of FAC.

Value of FCC depends on code distance which at not binary codes at equal with binary to length and speed is more. Respectively, correlation properties of not binary codes it is better. However in all cases it is necessary to check the received correlation code for lack of the quasicycles giving coincidence of symbols at shifts on some number of positions.

It is necessary to notice that correlation codes on the basis of cyclic codes have, as a rule, big power with an identical length in comparison with M-sequences.

Cyclic codes, as we know, are generated by cyclic shifts in Galois’s fields [7]. Using Galois’s fields, additive and the multiplicative groups, it is possible to construct other permutable codes, including nonlinear which can be used for receiving ensembles of DCF. Various groups of shifts are known, in which for creation of noiseproof codes various shifts are used: symmetric, sign-variable, Mathieu’s, affine, and also cyclic.

For example, for many years in systems of team communication and at data transmission full codes with a constant weight (CCW) are widely applied. Now the regular algorithms allowing to realize practically CCW with a length of \( n > 30 \) are developed. The geometrical algorithm of [3] creation of CCW from a full binary code is focused on realization of formation and coherent reception by means of ROM. This algorithm is based on use of treelike structure of codes and a choice of such tops of a tree which provide a subset of code words with necessary properties.

Optimum reception of block correlation codes of power of \( N_B \) in the presence of cyclic synchronization assumes use of \( N_B \) of correlators and the scheme of the decision choosing the code word with the greatest level of a signal (the greatest FCC). If speed of correlators at the set speed of transfer allows to use the multiplex mode, there can be enough one or several correlators with the reconstructed structure. Otherwise quasi-optimum methods of reception which, at some loss in a noise stability, allow to simplify the scheme of the decoder are used.

Example of multiplex processing is the decoder having ROM in which all code words of the used code are written down. The decoder consistently for \( N_B \) of steps reads out all mere verbiage and calculates their FCC with the accepted word, number of a step with the greatest value of FCC is issued for an exit of the decoder. At the power of code of 128 and modern element base such way of processing of a signal can provide rather low speed of transfer of symbols of a code (some tens of thousands of
orthogonality of signals of S. Therefore at a weak background of fluctuation hindrances existence of the filter exit. Emissions of FVK can both increase, and to reduce a resultant signal due to nonideal coordinated with the accepted BBS signal responses to the accepted signal and to a hindrance the smaller relation signal/noise even taking in to account redundancy of a code. As noise-proof range hindrances. Application of a noise-proof code allows receiving necessary quality of transfer at disturbing BBS can be carried out by increase in spectral density of fluctuation noise according to the filter (1) decreases and the probability of a mistake increases.

5. BBS noise stability

BBS noise stability usually is considered concerning the fluctuation, impulse, concentrated hindrances and the disturbing influence of other BBS from the used ensemble.

1. Action of fluctuation hindrances at big base of a signal of BBS irrespective of the power of a correlation code is considered similar to detection of a single signal of BBS against fluctuation hindrances. Thus the relation signal/noise at the exit of the optimum filter is defined by expression

\[ h^2 = \frac{E}{N_0}, \]

where \( E \) – energy of a signal, \( N_0 \) – the spectral density of power of a hindrance. Therefore it is possible to consider that BBS doesn’t change a signal noise stability concerning this type of hindrances.

However, if BBS signals is not absolutely orthogonal, that coefficient of correlation \( R_{ij} \neq 0 \), and when determining probability of a mistake \( p_{o\text{uw}} \) it is necessary to consider the following equality

\[ p_{o\text{uw}}(h, R_{ij}) = p_{o\text{uw}}(h \cdot \sqrt{1-R_{ij}}, 0), \]

from which follows that systems not of absolutely orthogonal signals are equivalent to system of orthogonal signals, if energy of these signals to increase in \( \sqrt{1-R_{ij}} \) time.

2. Action of impulse hindrances on a signal of BBS depends on intensity of a hindrance. We will consider a filter response in the form of the multiby-pass line of a delay with the detector. It will be defined the bending-around FCC BBS and an impulse of a hindrance, and instead of an impulse of a hindrance of duration of \( T_h \) (approximately equal duration of the BBS element) at the exit of the filter there will be a response lasting \( 2T \), and its size is equal to \( S_n \).

Then the relation signal/noise at the exit of the filter will be equal

\[ h^2 = \left( \frac{P}{P_n} \right) \cdot B^2. \] (1)

Therefore, the impulse hindrance is weakened at the filter exit in \( B^2 \) of times.

At intensive impulse hindrances it is necessary to close the channel for the period of action of a powerful impulse of a hindrance. For this purpose the scheme of reception turns on the limiter. When passing through it of BBS and fluctuation hindrance the relation signal/noise decreases by 2 dB, but the level of hindrances is fixed. If the power of a impulse hindrance is much more signal power, at the exit of the limiter is the response determined only by restriction level. Therefore, the average power of a impulse hindrance of any power at the exit of the limiter will have identical power. A impulse hindrance influencing a signal, excludes from consideration the struck parts BBS signals. On the other hand the signal becomes not quite coordinated with the BBS filter. Thus the response of the filter decreases by size \( \frac{T - T_h}{T} \). Respectively the relation signal/noise at the exit of the filter (1) decreases and the probability of a mistake increases.
3. Action of the hindrances concentrated on a range having spectral density in a signal strip 

\[ N_{\text{cf}} = P_{\text{cn}} / F \]

is defined by the relation signal/noise of a look

\[ h_{\text{cf}} = \frac{P_{\text{cn}}}{P_{\text{c}}} \cdot B. \]

Therefore, the concentrated hindrance is weakened in \( B \) time.

4. The disturbing influence of other BBS of ensemble is shown that at the exit of the filter coordinated with the accepted BBS signal responses to the accepted signal and to a hindrance linearly interact. Extent of influence is defined by FAC and FCC. In the presence of synchronization the disturbing signal has impact only at the time of counting of the main signal at the filter exit. Emissions of FVK can both increase, and to reduce a resultant signal due to nonideal orthogonality of signals of \( S \). Therefore at a weak background of fluctuation hindrances existence of the disturbing BBS can be neglected. At essential influence of fluctuation noise taking note of the disturbing BBS can be carried out by increase in spectral density of fluctuation noise according to expression

\[ N_{\text{cf}} = N_{\text{f}} + P_{\text{cn}} / 2F, \]

where \( P_{\text{cn}} \) – the power of the disturbing signal.

6. Combined use of BBS and noise-proof codes

At combined use of BBS and noise-proof codes with correction of mistakes symbols of code words of a noise-proof code are transferred by signals of BBS of a parallel or consecutive look.

Application of parallel BBS leads to expansion of a range of a signal as each symbol of a code of duration of \( T \) includes \( N \) elements of a signal of BBS. For transfer of symbols of a binary code in this case enough only two signals of BBS that is the advantage of this way of transfer. Thus BBS provides the relation necessary signal/noise \( h_{\text{c}} = \frac{P_{\text{c}}}{P_{\text{n}}} \) for a noise-proof code at which the code provides effective correction of mistakes, and also resistance to the impulse and concentrated on range hindrances. Application of a noise-proof code allows receiving necessary quality of transfer at the smaller relation signal/noise even taking into account redundancy of a code. As noise-proof codes both block and convolutional codes can be applied to the considered purposes. A lack of such method of application of BBS of a hydroacoustic communication channel is expansion of a range of a signal or reduction of speed of transfer in \( N \) times.

To avoid expansion of a range, it is possible to apply consecutive BBS when the signal of BBS is formed of elementary signals which duration is equal to duration of code symbols [5]. In this case expansion of a range doesn’t happen, but the general signal gets difficult structure as elements \( N \) of signals of BBS are at the same time transferred in the channel. In this case the peak factor of a total signal exceeds 1 that at nonlinear strengthening will lead to distortions and emergence of combinational frequencies. This phenomenon can be avoided if to use some parallel amplifiers of the transmitted signal.
Combined use of consecutive BBS and noise-suppressing code can be more preferable to a hydroacoustic communication channel in which width of a range of a signal is practically limited to a pass-band of hydroacoustic antennas and value of the bearing frequencies.

Questions of a noise stability of combined use of consecutive BBS and the codes correcting mistakes were considered in works [7, 8]. The main results of these works briefly consist in the following.

Application of consecutive BBS allows to receive a power prize in discrete communication channels with packages of mistakes at the expense of a decorrelation of mistakes. In channels with impulse hindrances even at the big power of a signal there can be mistakes whereas application of BBS or the correcting codes it is possible to achieve their correction. It doesn’t mean that the power prize is infinitely great; in this case it is about a certain equivalent of EVK. Analyzing operation of the discrete channel with BBS at action of the impulse hindrances (PH) which in work [9] are considered as short-term breaks (STP) of communication (this term is used further), it is possible to draw a conclusion that for ensuring identical probability of a mistake, in comparison with usual signals, BBS give an equivalent prize in the relation signal/noise in \((N-l_{in})/l_{in}\) times, and the power prize from transition to BBS will make

\[
EVP = 10 \cdot \log ((N-l_{in})/l_{in}) FT, \tag{2}
\]

where \(l_{in}\) – number of mistakes in the corrected STP communication.

Using (2), can estimate EVK of the correcting code used together with BBS in relation to the channel with BBS without coding

\[
EVK = 10 \cdot \log \left( \frac{(N-l_{in}^{1})/l_{in}^{1} \cdot k}{(N-l_{in}^{2})/l_{in}^{2} \cdot n} \right),
\]

Respectively, the general prize (EVKP) is defined by the sum

\[
EVKP = EVP + EVK.
\]

Considering that EVK increases with reduction of number of mistakes within code restriction, it is possible to expect that EVKP will be significantly more, than the simple sum of power prizes only from a code or only from BBS.

At optimum coherent processing of signals the probability of the wrong decoding of BBS when \(q\) of the BBS elements is distorted, depends on length of BBS, a way of transfer (a type of modulation) and a way of reception of signals

\[
P_{\text{err}} (N,q) = 0.5 \left[ 1 - \Phi \left( \sqrt{FT_0 \frac{N-q}{kq}} \right) \right],
\]

where \(k=1; 0.5; 0.25\) for signals of AM, a FM, PM, respectively.

Results of calculations and pilot studies of correction of packages of impulse hindrances of \(l_{in}\) for the convolutional code \(R=1/2, n=404\) and BBS of various length are given in Fig. 1.

With an identical length of \(N = n\) convolutional code corrects packages of mistakes better BBS, BBS with a length of 1024 has the correcting ability, approximately identical with a code. If STP of considerable length appear not often, BBS and the decoder in each timepoint contains only one package of mistakes.
Any convolutional code \((n, k)\), the correcting \(t_i\) of mistakes, can correct a package of errors of \(l_{pi} = t_i\) or more (for example, in the iterative decoder). The convolutional code for correction of longer packages of mistakes can be received by interleaving of symbols at the exits of \(i\) of coders of the same code [5]. Then \([in, ik]\) a code which decoding requires \(i\) of identical decoders though in single-processor computers it can be done serially and in one decoder turns out \([\ldots]\). Naturally, thus big memory and in \(i\) of times big computing complexity is required in \(i\) of times. As such codes can correct and independent errors, they it is more preferable than the codes which are specially intended for correction of packages of mistakes (for example, Ivadare’s codes). It is obvious that interleaving of a code technically simpler task, than lengthening of BBS several times.

Dependence \(l_{pi} = f(N)\) allows to choose a necessary combination of the BBS parameters and a code.

The analysis of results of calculations of a power prize (Fig. 2) doesn’t allow answering a question that it is better to use for correction of STP unambiguously: only BBS, only a code or BBS together with a code. Application of BBS \((N = 1024)\) allows to correct STP from 35÷40 of binary symbols, and taking into account change of speed of transfer in the channel without convolutional code \((R=1/2)\) it is equivalent 70÷80 to symbols; the convolutional code taking into account signal statistics at \(n=404\) \((R=1/2)\) corrects STP with a length of 85÷90 symbols long, that is approximately as much, but with much smaller length of a code (or code restriction), than when sharing the same BBS and the codes with \(l_{pi} = 190÷200\). In the same time of the same STP it is possible to correct a convolutional code at \(n = 1024\) without BBS.

Expediency of this or that decision can be defined after an assessment of computing complexity and complexity of realization of BBS processing devices and decoders the convolutional codes, and also statistical tests of these devices for channel models taking into account real statistics of STP.

**Conclusions**

In channels with impulse hindrances or short-term breaks of communication various options of use the convolutional and cyclic codes can be applied to improvement of quality of data transmission. Thus for receiving positive and energetically favorable option it is necessary to consider the following:

- length of code restriction of a code and length of additional algorithm of a decorrelation of mistakes has to be less average value of an interval between packages of impulse hindrances;

![Fig. 1. Dependence of \(l_{pi}\) on duration BBS](image-url)
convolutional codes with a speed of $R \leq \frac{3}{4}$ together with BBS or the convolutional $R \leq \frac{2}{3}$ codes with algorithm of interleaving of a code allow to reduce probability of a mistake at the channel exit for known statistics of mistakes;

- taking into account EVK and computing complexity interleaving of a code is more favorable than "code + BBS" option to $4\div5$ of interleaving;

- considering multiword length of the BBS optimum filter, its realization is always more difficult, than realization of the threshold decoder of a convolutional code.

**References**


