APPLICATION OF DETERMINISTIC CHAOS IN GENERATION OF ERROR-CORRECTION BLOCK CODES

Dejan Djonić and Lazo Manojlović
Mihajlo Pupin Institute, Mirijevski Bulevar 2
11050 Belgrade, Yugoslavia
++381 11 789 591, ml01996p@kiklop.etf.bg.ac.yu

ABSTRACT
In this paper, we present a new method for constructing error-correction block codes which is based on theory of deterministic chaos. The method is naturally rooted on non-linear iterative mappings and property of sensitive dependence on initial conditions. We describe the coding process for binary block codes and block codes with continuous amplitude. To justify the applicability of the new method to problem of error-correction, these codes are compared to maximum length binary codes and a class of asymptotically good codes. The results are encouraging: estimated coding gain for binary codes with respect to the union coding bound of the maximum length codes is significant.

I. INTRODUCTION
Diverse mathematical tools and techniques have been used to construct error-correction codes. Among these techniques most widely spread are algebraic techniques that are proved to be most useful in theory of block codes. Block codes, as well as convolutional codes, are used in variety of practical applications that are vital in modern world. However it should be noticed that since new to the knowledge of authors there has not been found a practically obtainable coding scheme that satisfied the famous Shannon second theorem (This theorem states that for a given arbitrarily small probability of error, there can be found a block code of sufficiently long code length, with a code rate smaller than channel capacity, such that exhibits smaller error probability rate than that fixed probability.). This theorem has been proved using the concept of random coding and states that a randomly chosen code should have specified performance. This paper presents a new method for obtaining amplytudally continuous and binary error-correcting codes using techniques and tools of deterministic chaos. Such codes can be interpreted as deterministic and controlled way of generating random codes.

The reason why deterministic chaos is used lies in sensitive dependence on initial conditions [1]. This property, introduced by E. Lorenz, states that chaotic mappings and differential equations have exponential separation of initial adjacent points. A specific class of chaotic mappings is used in this paper in order to obtain very separated code words. Another reason is in the need of constructing codes with low degree of symmetry among code words of a code. J.M. Landau [2] found that block codes with continuous amplitude with low probability of error transmission should not have high degree of symmetry. Deterministic chaos surely ensures this lack of symmetry.

Proposed paper presents first step in utilising deterministic chaos in error-correcting code theory. For this reason, the authors named these codes as Chaotical Codes. Possible next steps could be in using some other mappings and tools of deterministic chaos as well as more precise determination of its parameters. Promising possibility is also in using laws of deterministic chaos in constructing realisable decoding schemes.

II. FUNCTION ITERATION AND CHAOS
Chaos is ubiquitous and robust phenomenon that can occur in almost any man-made or natural systems where nonlinearity is present. We shall consider systems whose time dependence is deterministic i.e. there exists a prescription, either in terms of differential or difference equation for calculating their future behaviour from given initial conditions. Deterministic chaos denotes the irregular or chaotic motion which is generated by nonlinear systems whose dynamical laws uniquely determine the time evolution of a state of system from a knowledge of its previous history.

In this brief retrospective we shall bound ourselves on chaos generated by differential equations that shall be used in next sections. For complete and rigorous analysis of deterministic chaos reader is referred to an excellent text by Schuster [1].

If a real-valued function f maps the unit interval [0,1] (or any other interval) into itself, the sequence of iterates \( x_n = f(x_{n-1}) \), for \( n=0,1,\ldots \) will always stay in that interval. The sequence of points \( \{x_n\} \) is called the orbit of the point \( x_0 \).

In this paper we shall introduce logistic map.

Logistic map, the first thoroughly examined map that leads to deterministic chaos, is defined as:
\( f_r(x) = rx(1-x) \)  

(1)

where \( 1<r<4 \). The behaviour of its iterates depends on parameter \( r \) and shows large qualitative changes for different ranges of \( r \). For \( r = 4 \) function \( f \) becomes most sensitive on initial conditions and we shall later consider that case.

In the following text we introduce the Lyapunov exponent and invariant measure as quantitative measures which characterise a chaotic system which is generated by one-dimensional map. These quantitative measures are very useful in choosing chaotic maps and their parameters in generation of chaotical codes.

The Lyapunov exponent \( \lambda(x_0) \) measures exponential separation of adjacent points under the action of a map which leads to chaotic motion. Given the initial point \( x_0 \) Lyapunov exponent is defined as [1]

\[
\lambda(x_0) = \lim_{N \to \infty} \lim_{\varepsilon \to 0} \frac{1}{N} \ln \left[ \frac{f^N(x_0 + \varepsilon) - f^N(x_0)}{\varepsilon} \right]
\]

(3)

If \( \lambda > 0 \), given map exhibits sensitive dependence on initial conditions and chaos arise in the system. For larger values of \( \lambda \) system will have larger average of separation of nearby orbits. For \( \lambda \leq 0 \) the system exhibits a regular motion Logistic map has the largest Lyapunov exponent for \( r=4 \) and this fact will be used later.

The invariant measure \( p(x) \) determines the density of the iterates of a unimodular map [1] over the unit interval and is defined via

\[
p(x) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \delta \left[ x - f^n(x_0) \right].
\]

(4)

This function should be understood as probability density function of iterates after certain number of iterations. It can be shown however that \( p(x) \) is stationary i.e. it does not change with time under the action of the map \( f(x) \) and that it can be determined as unique solution of the so-called Frobenious-Perron integral equation [1]

\[
p(x) = \int \delta(y - f(x)) p(x) dx.
\]

(5)

Using somewhat complicated topological transformations it can be shown that the invariant measure for the logistic map for \( r = 4 \) is

\[
p_{f_4}(x) = \frac{1}{\pi} \frac{1}{\sqrt{1-x}}.
\]

(6)

This result shows that the invariant density of a purely chaotic map needs not always a dull constant. Note that for \( r = 4 \) logistic map become ergodic.

III. REALISATION OF CHAOTICAL CODES

Theory of Deterministic Chaos and Chaotical mappings is well suited to generate block codes with good performances. We make this assertion for several reasons:

- Orbits of adjacent initial points generated by a chaotical map are distant because of the sensitive dependence on initial points of chaotical systems. If we understand these orbits as code words we should have distant code words in a certain sense which is very favourable.

- It was shown [2] that codes with good performance must have very low degree of symmetry-chaotical codes indeed have very low symmetry.

- Chaotical maps are deterministic and therefore introduce determinicity in code words. We can expect that this deterministic property can be used to construct appropriate decoding scheme for chaotical codes. Certain results on classification of chaotical signals have already been reported [3].

- Some novel engineering application of chaos in synthesis of chaotic signals and spread-spectrum communications have been successfully reported in literature [4].

Block codes can be divided in two classes according to nature of their code words:

1. Binary block codes—code symbols of these codes can be only 0 or 1.

2. Block codes with continuous amplitude.

We will present here possible application of chaotical logistic map in generation of both classes of codes.

A. Binary Codes

Coder for binary error-correction code \((n,k)\) can be realized as presented in Fig. 1.

![Fig. 1. Coder for binary codes](image_url)

Here function \( f \) is any nonlinear map whose iterates, under certain choice of parameters of function \( f \), behave chaotically. Multilevel coding is introduced to achieve greater distance between orbits. Parameter \( K \) determines number of iterations per each step, while \( N \) determines number of steps. We will briefly describe functions of D/A and A/D converters.
- D/A converter converts input k-bit information code words in \(2^k\) values in neighborhood of initial point \(x_0\) so that code word \(u_i\) is being mapped in analogue value \(x_i^{(0)} = x_0 + \delta\) (\(\delta\) is a small constant).
- A/D converter in step j converts values from interval [0,1] in binary values with step equal to \(2^{-n}\) \((\sum_{k=0}^{n} a_k = n)\). Notice that if switch A is closed systematic code is generated.

### B. Block Codes With Continuous Amplitude

Block codes with continuous amplitude \(S(N,M)\) is defined as mapping of \(M\) discrete information words \(u_i\) \((i = 1,2,...,M)\) to a set of \(M\) points \(S_i = (s_{i1}, s_{i2}, ..., s_{in})\) in \(N\)-dimensional space. These codes are usually studied by their geometric interpretation. We now define Euclidean distance \(d_{ij}\) between two code words \(S_i\) and \(S_j\) that is essentially important for evaluating performances of codes with continuous amplitude

\[
d_{ij} = d(S_i, S_j) = \sqrt{\sum_{k=1}^{n} (s_{ik} - s_{jk})^2}. \tag{7}
\]

For a specific code we can find its distance matrix \(D = (d_{ij})\) which has dimensions \(M\) by \(M\).

The most important parameter for comparing code performances is certainly its probability of error. Average probability of error \(P_e\) represents the degree of false decisions made by decoder. The precise expression for \(P_e\) in case of block codes with continuous amplitude is complicated and therefore not well suited for practical evaluations. Instead of this expression many forms of upper and lower boundaries were found and used extensively in literature. The most common upper limit for \(P_e\) is uniform coding bound. In this paper uniform coding bound will be used as an approximation for exact expression for \(P_e\) in case of discrete memoryless channel with additive gaussian noise. We will conjecture that information words have the same probability and that the code words are decoded by the maximum likelihood criterion. Uniform coding bound for this case is

\[
P_{ume} = \frac{1}{2M} \sum_{i=1}^{M} \sum_{j=1}^{M} \text{erfc} \left( \frac{d_{ij}}{2\sqrt{2\sigma^2}} \right). \tag{8}
\]

For substantial signal to noise ratios uniform coding bound gives similar results as the exact formula. We can, therefore, knowing only the distance matrix \(D\) of a certain code evaluate its performance.

Coder for these codes is very similar to coder for binary codes shown in Fig. 1. For sake of brevity we will describe the function of coder for codes with continuous amplitude using Fig. 1. The only alteration needed for this case is that coder does not have A/D converters that are shown in grey in Fig.1. Parameter \(N\) determines number of coding steps as well as dimensionality of code words while parameter \(K\) represents number of iterations per single coding step. Switch A is always open in this case or in fact it actually does not have to exist.

### IV. SIMULATION RESULTS

Chaotic codes presented in this paper were generated and analysed using the program Mathematica [5]. Performances of binary codes were determined by simulation of decoding process in presence of additive noise. As for codes with continuous amplitude their performances were calculated using uniform coding bound (8) and presented in Slepian diagrams.

#### A. Binary Codes

In this paper chaotic binary codes are compared with maximum length codes (ML codes). Performances of chaotic codes with same parameters \(n\) and \(k\) as those of ML codes are compared with their union coding bound that are known. ML code of degree \(m\) is a \((2^m-1,m)\) code.

Binary chaotic codes (BCC3, BCC4, and BCC5) that are simulated in this paper are compared with ML codes of degree 3, 4 and 5. For all simulated codes parameters are fixed as \(K=30, x_0=0.3\) and \(\delta=10^{-4}\). Evaluation of bit error rate is obtained on set of 100,000 information bits. Soft decision decoding was applied. Results gained by simulation are compared with union coding bound of ML codes [6]

\[
P_e = (2^m -1) \text{erfc} \left( \sqrt{\frac{2^m R E_b}{N_0}} \right) \tag{9}
\]

where \(m\) is code degree, \(R=m/(2^m-1)\) code rate and \(E_b/N_0\) signal to noise ration. Noise variance is calculated as \(\sigma^2 = N_0/2\).

![Fig. 2](image.png)

**Fig. 2.** Results of simulation for BCC3, BCC4, and BCC5. Dashed curve represents performances without coding.
B. Block Codes With Continuous Amplitude

Block codes with continuous amplitude that are generated in this paper are chosen such as to have same transmission rate $R_N = \text{ld}M/N$ and dimensions as asymptotically good codes presented in [7]. These codes are chosen because they present a class of best block codes with continuous amplitude with substantially better characteristics than algebraic codes such as permutational codes. As in the case of binary codes this was done to allow easy comparison and evaluation of performances of chaotic codes.

For concrete code and fixed parameters $N$ and $M$ other parameters ($r$, $K$, $\sigma_0$ and $\delta x$) that determine the code are chosen as follows. Parameter $r$ that governs the logistic map is chosen as $r = 4$ because Lyapunov exponent than has the largest value. Number of successive iterations $K$ as well as initial condition $\sigma_0$ are determined using simple optimisation procedure. This procedure represents way for obtaining the best code using the criterion of minimal needed signal to noise ratio $A$ to acquire fixed probability of error. Parameter $A$ can be calculated in terms of average energy per dimension of block code $E_0$ and noise variance $\sigma$

$$A = \frac{E_0}{\sigma^2}.$$  \hspace{1cm} (10)

Values of parameter $A$ were calculated by numerical solving of equation (8) in terms of noise variance. This calculation uses substantial computational time. For this reason parameter $\delta x$ was excluded from optimisation procedure and fixed on $\delta x = 10^4$. Results obtained by optimisation procedure are presented in standard Slepian efficiency diagram in which specific codes are presented as dots. The diagram represents signal to noise ratio above ideal $A_{\text{ideal}}$ in terms of transmission rate $R_N$. $A_{\text{ideal}}$ is a minimal signal to noise ratio for which is possible to construct optimal code according to fundamental theorem of information theory.

Results of simulation are presented in Fig. 3, for $P_e = 10^{-5}$. Lower bound of positions of optimal block codes for $N=5$ are presented with bold line [8]. Simulated codes are numerated from 1 to 16. Their dimensions and results of optimisation procedure for $x_0$ and $K$ are presented in Table 1. Detailed description of whole procedure and results is given in [9].

**CONCLUSION**

In this paper we have presented a new possible method for constructing binary block codes and block codes with continuous amplitude. Using the computer we have simulated these codes and determined their performances. Specifically, simulated binary block codes showed substantial improvement above union coding bound of ML codes (9). For example, code BCC4 for probability of error $10^{-5}$ gives the coding gain of 4dB, while code BCC3 gives the coding gain of 2.5dB. It should be noticed that codes with lower coding rates have better characteristics. This property of chaotic binary codes can be explained by the fact that presented method of coding does not depend on number of code words.

<table>
<thead>
<tr>
<th>No</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>9</td>
<td>3</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>M</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>12</td>
<td>22</td>
<td>4</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td>K</td>
<td>60</td>
<td>40</td>
<td>20</td>
<td>40</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>40</td>
</tr>
</tbody>
</table>

Table 1. Codes numerated from 1 to 8.

<table>
<thead>
<tr>
<th>No</th>
<th>9</th>
<th>19</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>7</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>M</td>
<td>25</td>
<td>5</td>
<td>13</td>
<td>23</td>
<td>11</td>
<td>19</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>K</td>
<td>31</td>
<td>50</td>
<td>30</td>
<td>100</td>
<td>63</td>
<td>20</td>
<td>20</td>
<td>63</td>
</tr>
</tbody>
</table>

Table 1. (continuation) Codes numerated from 9 to 16.

As for codes with continuous amplitude, simulation showed that signal to noise ratios needed to acquire given probability of error are 0.5 – 1dB higher than respective codes from the class of asymptotically good codes. These codes have the similar property that their characteristics degrade with increase of transmission rate.

We hope that this paper may be inspiration for research issues on utilising of properties of deterministic chaos in decoding process of presented chaotic codes.

![Fig. 3. Diagram of efficiency for $P_e = 10^{-5}$ with positions of simulated chaotic codes from Table 1.](image-url)
REFERENCES