Dual Soft Decoding of Linear Block Codes using Ant Colony Optimization

Ahmed Azouaoui, Hicham Bouzkraoui and Youssef Hadi

Department of Computer Science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco.

MISC Laboratory, Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco.

Abstract

In this paper we introduce a novel and efficient soft decoding algorithm for linear block codes. It is known that this decoding is a NP-hard problem where exhaustive search methods become almost impossible in large problem space. After the emergence of metaheuristic approaches, several algorithms were proposed based on these technics and show good performance results comparing to computational resources cost. In this context we present a new soft decoding decision algorithm, based on Ant Colony Optimization, this approach has proven its efficiency in optimization problems. In contrast to existing decoders, the proposed Dual Ant Colony Optimization Soft Decoder (DACOSD) operates on the dual code instead of the code itself. Hence we can optimize our decoder for codes with high rates. This algorithm was simulated over an AWGN channel, then we proceed by tuning of our algorithm parameters, after that, we compare the obtained performances with competitor decoding algorithms. In fact, the proposed decoder is on the top of the most recent soft decoders such DDGA, CGAD-M and CGAD-HSP algorithms. Besides, we discussed the complexity of the proposed algorithm compared to the most known decoders.

Keywords: Ant Colony Optimization, Soft Decoding, Error Correcting Codes, Linear Codes, Dual Code, BCH, QR, RS

INTRODUCTION

Coding theory is interested in finding the best way to transmit information accurately from a source to a destination over different kinds of channels. In real world, the channel is generally perturbed by a noise dependent on environment conditions, hence information reliability is lost. Trying to slightly improve communication performance using classical approaches either by extending hardware capacity or using better material quality, is highly expensive. However, contrary to what was generally believed, Shannon proved in 1948, that there exist a coding scheme which permits transmission that nearly the channel capacity with arbitrarily small errors [1]. Thus, software optimization can reduce such cost, actually several algorithms were proposed to enhance communication reliability, with remarkable performance in order to achieve Shannon limit.

To simplify the study, scientists use the model in Fig.1, which depicts different transmission chain components. In fact spotlight was put on decoder part where significant efforts were made in order to find coding/decoding models that approach channel capacity, especially using AWGN channel model. Decoding schemes are classified into two classes, hard and soft decision algorithms. The first approach makes hard decision on the received digital message, thus works only on binary vectors. While Soft-decoding algorithms use digital signal information received directly from demodulation and use real numbers associated with each codeword symbol. Therefore this decoding is capable of correcting more errors.

Soft-decoding is classified as a NP-hard problem [2], where classical algorithms search would not be effective and almost impossible. To tackle this problem, several works were proposed; G.Forney designed a soft decoding algorithm, called “Generalized Minimum Distance Decoding” GMD [3]. OSD Algorithm was also used to implement a soft decision decoder [4]. Nowadays, Artificial Intelligence (AI) and metaheuristic methods were introduced in this field, after their success on optimization problems, several researches were published of decoders based on neural networks and Genetic Algorithms (GA). In fact Maini et al. was the first to introduce a GA decoder [5], and then several GA-Based Decision Soft decoders came after [6-10]. In other side, other algorithms were proposed using dual code [11-13], then recently also Maini was extended to DDGA decoder[14] and two dual soft decoders based on compact GA were proposed in 2017 [15]. Using dual code for high rate codes, seems to reduce considerably the execution time, thus, taking advantage from this simple idea we propose in this paper, a novel soft decoder based on Ant Colony Optimization (DACOSD), as far as we know, this approach has not been previously used to decode linear codes. The remainder of this article will be organized as follow: in section2, we will describe the Ant Colony Optimization method, then in section3 we will explain our DACOSD algorithm. In the section 4 we will discuss the parameter tuning of our decoder then use some famous codes samples base to compare with competitor decoders. Finally we finish our paper by summary of this work and the future trends.

![Figure 1. Communication system model](image-url)
ANT COLONY OPTIMIZATION (ACO)

Ant Colony Optimization algorithms were inspired from ant’s behavior when searching food near the nest, they are considered among metaheuristic methods. Dorigo et al. were the first to propose an algorithm using this technique to find the shortest path within a given graph [16]. In fact, biologists have discovered that ants use a chemical substance called pheromone, these ants drop the pheromone on their way, when arriving to some junction, the ants make a probabilistic choice based on pheromone quantity on each possible path, therefore after several walks, the concentration of pheromone grows on some optimal path. However this mechanism alone can glorify sub optimal or blocked ways, that’s why the evaporation of the pheromone trails, takes place by weakening the “nasty paths”.

The first ACO algorithm called Ant System (AS) was designed to solve the famous Travelling Salesman Problem (TSP) [16]. The problem is to find the shortest path visiting n cities, each city must be visited only once. This mechanism is modelled by a graph G where the cities are the vertices and the edges are formed by paths between cities. In the AS algorithm there is a set of iterations (1 ≤ y ≤ y_max), every ant x (1 ≤ x ≤ m), scans the graph and build a complete path of n cities, for each ant the relative path between city i and city j depends on several conditions:

1) The set of cities already visited by ant x which is on city i, noted by \( F^x_i \)
2) \( \eta_{ij} \) The visibility of city j to i, it is a measure which let the ants to choose the near city rather than the far ones. Often \( \eta_{ij} \) is a decreasing function of the \( d_{ij} \) the distance between city i and city j (for example \( \eta_{ij} = \frac{1}{d_{ij}} \)).
3) The pheromone quantity dropped on the path between 2 cities i and j at iteration y, called intensity and noted \( \tau_{ij}(y) \) which define the global attractiveness of parts of the whole path and continually updated by the ants.

Arriving to city i the ant x makes a choice based on the following formula which defines the probability to walk to city j:

\[
P^x_i(y) = \left( \frac{(\tau_{ij}(y))^{\alpha} (\eta_{ij})^{\beta}}{\sum_{k \in F^x_i} (\tau_{ik}(y))^{\alpha} (\eta_{ik})^{\beta}} \right) j \in F^x_i
\]

\( \alpha \) and \( \beta \) are 2 parameters which control the relative role of the intensity \( \tau_{ij}(y) \) of pheromone and the visibility \( \eta_{ij} \), a tradeoff should be done on diversification and intensification of the algorithm behavior.

After each iteration \( y \) every ant x drops a quantity of pheromone over the walked path, depending on solution quality

\[
\Delta \tau^x_{ij}(y) = \begin{cases} 
\rho \frac{Q}{L^x(y)} (i, j) \in T^x(y) \\
0, \text{ otherwise}
\end{cases}
\]

For each iteration \( y = 1 \ldots y_{\text{max}} \)
For each ant \( x = 1 \ldots m \)
Select randomly a city \( i_0 \)
For each non visited city \( i \)
Select a city \( j \) from \( \text{J} \) using equation (1)
End For
Deposit pheromone \( \Delta \tau^x_{ij}(y) \) on the path \( T^x(y) \) using equation (2)
End For
Vaporization of the paths using equation (3)
End For

The Algorithm can be briefly summarized in the next pseudo code:

DACOSD Algorithm

We note \( C(n, k, d) \) a linear code of length n, dimension k and minimum distance d over the field \( F_2 \). This code can be described by a \( k \times n \) matrix \( G \) called Generator matrix, a message \( m = \{ m_i \}_n \) can be then encoded to a codeword \( c = \{ c_i \}_n \) using the equation:

\[
c = mG
\]

We define also a parity check \( n-k \times n \) matrix noted \( H \) which satisfies the following property:

\[
\forall v \in F_2^n, v \text{ is codeword } \implies Hv^t = 0
\]

Suppose we transmit the codeword \( c = \{ c_i \}_n \) using BPSK modulation and let \( z = \{ z_i \}_n \) be the modulated signal over a Gaussian channel with noise \( n = \{ n_i \}_n \), where \( z = \{ z_i \}_n \) and \( n = \{ n_i \}_n \) are independent sequences, \( n_i \sim N(0, \frac{N_0}{2}) \) and \( N_0 \) is the noise power spectral density.

The received signal \( r = \{ r_i \}_n \) is such that \( r = z + n \).

We note \( v = \{ v_i \}_n \) the hard decision of \( r \) as \( r = \{ r_i \}_n \), the error syndrome \( s = \{ s_i \}_{n-k} \) could be then expressed as follows:

\[
s = \nu H^t
\]

When the syndrome \( s \) is zero, that means, the hard decision is a codeword and there was no error in transmission. But when we have an error in transmission, our decoder tries to find the codeword \( \hat{c} \) which maximizes the probability \( p(c|r) \) over the code space, known as maximum likelihood decoding (MLD).

Using the noise distribution and Bayes theorem, the MLD is equivalent to the following equation:
We form the complete error $\mathbf{e} = (e_l, e_j)$ using equation (11).

7. The code $\mathbf{c}' = \mathbf{v} + (e_l, e_j)$ is related to the $H'$ matrix, thus our estimated transmitted codeword is then

$$\hat{\mathbf{c}} = \pi^{-1}(\mathbf{c}')$$

The ACO algorithm is modeled by the following graph (in case of $n=7$ and $k=4$):

![Graph of linear code (n=7,k=4)](image)

The search space will be the field $F_{2}^{n-k}$ represented by the above graph in case of $n=7$ and $k=4$.

For ant $x$ at iteration $y$ the probability of setting the bit-i to 1 is defined as follows:

$$P_{ij}^y = \frac{(\tau_{ij}(y))^\alpha (\eta_{ij})^\beta}{\sum_{ij}(\tau_{ij}(y))^\alpha(\eta_{ij})^\beta}$$

The parameters $\alpha$, $\beta$, and $\eta_{ij}$ are ACO parameters adapted based on simulation results. At the end of ant $x$ walk all bits $e_i$ are set and the path is the constructed error $\mathbf{e}_j = (e_i)_{n-k}^1$. After that the solution fitness is measured by euclidean distance of $\mathbf{z}' = (\mathbf{z}_{1})_{k}^1$ from $\mathbf{r}' = (\mathbf{r}_{1})_{n-k}^1$, thus we define the pheromone to be dropped by ant $x$ at iteration $y$ as follow:

$$\Delta \tau_{ij}^y(y) = \frac{q}{\sum_{ij} (\mathbf{r}_{ij}-\mathbf{z}_{ij})^2}$$

Where the bit-i $(k+1 \leq i \leq n)$ is set to $j \in \{0,1\}$ by the ant $x$, and $Q$ is a parameter defined by parameter tuning results. The algorithm could be then summarized as below:

Set ACO parameters $\alpha$, $\beta$, $\rho$, $m$, $Q$, $y_{\text{max}}$

Initialize pheromone intensity $\tau_{ij}(0)$ and visibility $\eta_{ij}$

For each iteration $y=1 \ldots y_{\text{max}}$

For each ant $x=1 \ldots m$

Set randomly the bit-(k+1) to “0” or “1”

For each bit-i $i=k+2 \ldots n$

Set the bit-i using equation (13)

End For

Form the error codeword $\mathbf{e}$ using equation (11)

Compute $d_{\text{euc}} = \sum_{i=1}^{n}(r_i' - z_i')^2$

Update the most probable error $e$ based on best $d_{\text{euc}}$

Deposit pheromone $\Delta \tau_{ij}^y(y)$ on the path $T^x(y)$ using equation (14)

End For

Vaporization of the paths using equation (3)

End For

RESULTS AND DISCUSSION

1. ACO PARAMETERS SETTINGS

We run several simulations of performance (BER) expressed as function of SNR (Signal to Noise Ratio), with different ACO parameters values in order to find the most suitable set to
our decoder. For every parameter tuning we fix the other parameters. The remaining parameters were set by default according to the below table:

<table>
<thead>
<tr>
<th>Table I: Parameters Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Default code</td>
</tr>
<tr>
<td>Channel</td>
</tr>
<tr>
<td>Modulation</td>
</tr>
<tr>
<td>Minimum number of bit error</td>
</tr>
<tr>
<td>Minimum number of blocs</td>
</tr>
</tbody>
</table>

Figure 3, shows, that the best performance is achieved when $\alpha=0.1$. We can suppose also that the best range for $\alpha$ parameter is [0-1]. Intuitively large values of $\alpha$ tends to amplify the initial paths choosed by ants.

From figure 4, $\beta=2.5$, is almost the best choice, we can also use the range [1-3] as the best set of $\beta$ values, which is confirmed by the recommendation [17].

The performance is quite similar as seen in figure 5, we find $\rho=0.5$ is the most suitable value, which is recommended [17].

From the graph in figure 6, there is no visible best value, by taking the average over all SNR values, it shows that $m=50$ is the best choice, several simulations prove that it is useless to consider $m>k$, it is recommended to set $m \approx k$ [17].

In figure 7, The simulations shows that the parameter Q has slight impact on performance, taking into account the average over all SNR values, we may set Q=100.

From theoretic view, the ACO algorithm converges when $y_{\text{max}}$ is sufficiently large. However, simulations in figure 8 shows that for $y_{\text{max}} > 500$ iterations, there is no visible improvement of performance, therefore we could set $y_{\text{max}} = 500$. 

- Figure 3. Impact of parameter $\alpha$ variation on BER.
- Figure 4. Impact of parameter $\beta$ variation on BER.
- Figure 5. Impact of parameter $\rho$ variation on BER.
2. BENCHMARKING

a) BER Performance

In this subsection, we will show the effectiveness of our dual ACO soft decoder with the some concurrent decoders.
The figure 9, shows that our algorithm performs better than OSD-1, SIHO [8] and AutDAG [10], but over performs DDGA [14] and Maini [5] only for medium and low noise level. From the figure 11, our decoder performs better than CGAD [11], actually we can have a gain of 1.5 dB at 10^{-4}, besides, it is slightly better than Maini and DDGA.

From the figure 11, our decoder performs better than CGAD [11], actually we can have a gain of 1.5 dB at 10^{-4}, besides, it is slightly better than Maini and DDGA.

In figure 10, we can see the superiority of the DACOSD over the Chase-2 [18], SDGA [9], cGA-HSP and cGA-M [15]. The gain is 1dB comparing to Chase-2 almost for all BER, at 10^{-4} BER the gain is about 0.7dB over the cGA-M.

In figure 12, the DACOSD has better performance than Chase-2 and SIHO. In fact at 10^{-5} BER we have a gain of 1dB comparing to Chase-2.

From the figure 13, DACOSD perform better than slightly Chase-2, DSGA [12], the gain is about 0.5dB.
Figure 14. Performance of Maini, DDGA, OSD-1, and DACOSD decoders on BCH (63, 57, 3)

The figure 14, show that DACOSD has the same performance as Maini, DDGA and OSD-1.

Figure 15. Performance of Chase-2, CGAD, SDGA, cGA-HSP, cGA-M and DACOSD decoders on RS (15, 7, 9)

The above figures 15 and 16, shows that the for RS code, DACOSD is indeed better than Chase-2, CGAD, SDGA and the most up to date decoders cGA-HSP, cGA-M. M. For LDPC code DACOSD is more effective than GAMD [7], we can gain about 0.7 dB at 10^{-3} BER.

b) Complexity Analysis

The below table summarize algorithm complexity of different competitor’s decoders:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chase-2</td>
<td>$O(2^{[d-1]/2}n^2\log_2n)$</td>
</tr>
<tr>
<td>Maini</td>
<td>$O(N_iN_g[Kn + \log N_i])$</td>
</tr>
<tr>
<td>DDGA</td>
<td>$O(N_iN_g[k(n-k) + \log N_i])$</td>
</tr>
<tr>
<td>OSD-1</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>SDGA</td>
<td>$O(2^{[N_iN_g[kn^2 + kn + \log(N_i)]})$</td>
</tr>
<tr>
<td>CGAD</td>
<td>$O(T_c, k(n-k))$</td>
</tr>
<tr>
<td>DACOSD</td>
<td>$O(m_{\text{max}}(n-k)n)$</td>
</tr>
</tbody>
</table>

$t=\lfloor d-1\rfloor/2$, the error correcting capability

$N_i$, parameter used is Genetic Algorithm, called population size.

$N_g$, parameter used is Genetic Algorithm, called number of generations.

$T_c$, parameter used is CGAD algorithm, called average number of generations.

For codes with high rates ($k\sim n$), DDGA, CGAD and DACOSD have linear complexity with $n$, while Chase-2, Maini, OSD-1 and SDGA have worst complexity, about $O(n^2)$.
Using simulations setting, for codes with high rates \( \left( \frac{k}{n} \geq 90\% \right) \), the complexity might be upper bounded for DDG\(\text{A}, \text{CGAD and DACOSD as follows}

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Parameters Setting</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDG(\text{A}</td>
<td>N_l = 300, N_p = 100</td>
<td>(O(300k\text{kn}))</td>
</tr>
<tr>
<td>CGAD</td>
<td>( T_e = 1000 )</td>
<td>(O(100\text{kn}))</td>
</tr>
<tr>
<td>DACOSD</td>
<td>( m \approx k, y_{\max} = 500 )</td>
<td>(O(50\text{kn}))</td>
</tr>
</tbody>
</table>

From the above table, we can see that for \( k<200 \) our algorithm has the lowest complexity comparing to its concurrent decoders for high rate codes.

**CONCLUSION**

This paper has made original contribution in the area of soft decoding algorithms by introducing Ant Colony Optimization metaheuristic approach, using dual code instead of the code itself and taking advantage of the reliability information of the received signal, to provide larger coding gain and less algorithmic complexity. The performance of this decoder was investigated with different codes over an AWGN channel, the obtained results confirm that it performs better than its competitors. We focus also on algorithm parameter tuning to enhance the performance. The proposed algorithm can be used for non-cyclic and non-binary codes and on different kind channel models, with low implementation changes.

Although we tested our algorithm on linear block codes, there is no reason why not use it for convolutional codes and combine this approach with different metaheuristic methods to enhance performance.

**REFERENCES**


