

ERROR DETECTION WITH REAL-NUMBER CODES BASED ON RANDOM MATRICES

Vieira, José M. N., Santos, Dorabella M. S., Ferreira, Paulo J. S. G.

Departamento de Electrónica, Telecomunicações e Informática / IEETA
Universidade de Aveiro
Aveiro Portugal

ABSTRACT

Some well-known real-number codes are DFT codes. Since these codes are cyclic, they can be used to correct erasures (errors at known positions) and detect errors, using the locator polynomial via the syndrome, with efficient algorithms. The stability of such codes are, however, very poor for burst error patterns. In such conditions, the stability of the system of equations to be solved is very poor. This amplifies the rounding errors inherent to the real number field. In order to improve the stability of real-number error-correcting codes, other types of coding matrices were considered, namely random orthogonal matrices. These type of codes have proven to be very stable, when compared to DFT codes. However, the problem of detecting errors (when the positions of these errors are not known) with random codes was not addressed. Such codes do not possess any specific structure which could be exploited to create an efficient algorithm. In this paper, we present an efficient method to locate errors with codes based on random orthogonal matrices.

Index Terms— Error correction, random matrices, real number codes, sparse solutions

1. INTRODUCTION

Conventional error correcting codes are defined over finite fields. However, real-number codes can also be employed when floating point issues become important. A finite field can be embedded in a real or complex field and several authors studied the properties of real-number codes [1, 2, 3].

Some such codes include the DFT and DCT codes. These particular codes are cyclic, and, hence, can be used to detect and correct errors using the so-called locator polynomial via the syndrome, with efficient algorithms. Unfortunately, due to their structure, the stability of these codes is very poor for burst error patterns. Shannon showed in his seminal paper [4] that most of the codes can achieve channel capacity. The structure imposed on the codes, is only intended for practical algorithms to code and decode.

Surprisingly enough, if the matrix involved does not have any particular structure, the code obtained performs quite well independently of the error pattern. These codes which are

based on random matrices are dubbed *random codes*. They have been shown to have a good stability in correcting erasures (errors in known positions) [5]. However, the problem of correcting errors (detecting and correcting errors) was not addressed by the authors. This problem presents itself as a combinatorial problem, but that can be tackled as a linear programming problem, under certain conditions.

2. CODES AND STRUCTURE

In the particular case of DFT codes, to circumvent the poor stability of the code when facing burst erasure patterns, a parallel concatenated code (PCC) is used, which consists of a two-channel structure, where the first channel employs a DFT code and the second channel employs additionally an interleaver (Figure 1).

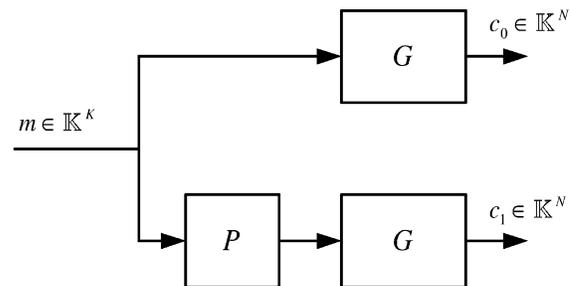


Fig. 1. Two channel coder with $K < N$. The interleaver is denoted by P .

These two-channel codes outperform their single-channel counterparts, specially for occurrences of bursty losses. Their condition number can be several orders of magnitude lower than the single channel DFT codes, which makes the two-channel structure very stable, even when bursts of losses occur. The improvement in stability has to do with the randomness introduced by the interleaver [6, 7], although it has not yet been possible to demonstrate this mathematically.

3. RANDOM CODES

However, stable single channel real-number codes even under bursty erasure patterns have been proposed [5]. These codes are based on random gaussian matrices and, hence, have no specific structure.

In this case, the original signal $m \in \mathbb{R}^K$ is coded as

$$c = Gm \quad (1)$$

with $c \in \mathbb{R}^N$ where G is an $N \times K$ submatrix of an $N \times N$ gaussian matrix ($K < N$). Defining the set of the index of the lost samples (erasures) by $J \subset \{1, \dots, N\}$ with at most $N - K$ samples, and \bar{J} as its complement, then we can define $G(\bar{J})$ as the matrix with the known rows of G . To get the message m from the known samples of c it suffices to solve the system of equations (1) with the known rows of G

$$\hat{m} = G(\bar{J})^+ c(\bar{J}),$$

where $G(\bar{J})^+$ stands for the pseudo-inverse of $G(\bar{J})$. It has been shown in [5] that with high probability, such codes are very stable even under bursty losses.

As a comparison between random codes and a structured real-number code, Figure 2 shows the condition number of a DFT code, its PCC counterpart and a random code, with $N = 256$ (128 in each channel for the PCC) and $K = 21$, as the number of bursty losses increases. It can be seen that for the random code, the condition number never exceeds 10, while for the DFT code the condition number explodes quickly. The PCC, in turn, is much more stable than the DFT code (by six orders of magnitude for many losses), but the random code outperforms the two-channel code.

The connection between randomness and stability is again highlighted: the more structure, the worse the performance. A question arises, however: since it is not possible to take advantage of the structure of random matrices, can detection of errors be carried out with these new codes?

4. ERROR CORRECTION WITH RANDOM CODES

In the previous section we presented a method to recover the error amplitudes solving an overdetermined system of equations minimizing the ℓ_2 norm. In this section we show how to construct a real number code in order to correct errors in the received vector, finding their positions and amplitudes. Consider the random matrix $F \in \mathbb{R}^{N \times N}$ with elements following a normal distribution and the following partition

$$F = \begin{bmatrix} G & \vdots & H \\ N \times K & & N \times (N-K) \end{bmatrix},$$

where $G \in \mathbb{R}^{N \times K}$ is the coding matrix and $H \in \mathbb{R}^{N \times (N-K)}$ the parity check matrix. The matrix F can be orthogonalized

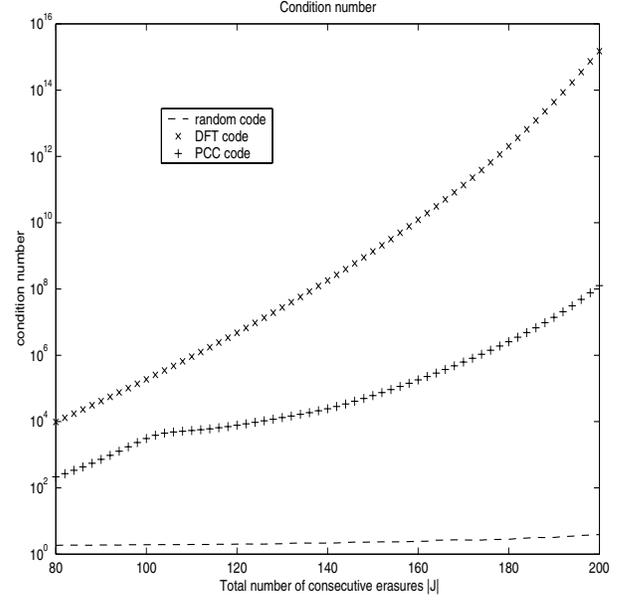


Fig. 2. Log plot of the condition number versus the total number of consecutive missing samples for the DFT code ($N = 256$), the two-channel counterpart ($N = 128$ and $|J|/2$ missing samples per channel) and a random code ($N = 256$), with $K=21$.

by a QR factorization using a Gram-Smith orthogonalization and in this case we have

$$H^T G = 0.$$

Consider a vector $m \in \mathbb{R}^K$ and the coding operation

$$c = Gm,$$

that results in the codeword $c \in \mathbb{R}^N$ where $N > K$. Consider that the vector c is corrupted in L samples with index given by the set $J \subset \{1, \dots, N\}$ and we can write the corrupted vector y as

$$y = c + e,$$

with e a sparse error vector with L samples different from zero at positions given by J . If we multiply the vector y by H^T we have

$$s = H^T y = H^T (c + e) = H^T Gm + H^T e = H^T e.$$

The vector s is known as the syndrome [8] and because the columns of H are orthogonal to the columns of G , the syndrome is a function of only the error vector e . From the received signal y it is possible to calculate the syndrome s , and the error vector e can be recovered by solving the underdetermined system of equations

$$H^T e = s. \quad (2)$$

This system has many solutions and we want the sparsest one. This is a combinatorial problem very hard to solve and can be stated as

$$(P_0) \quad \min \|e\|_0 \quad \text{subject to} \quad H^T e = s$$

with $\|e\|_0 = \#\{i \in 1, \dots, N : e_i \neq 0\}$ the ℓ_0 -norm (pseudo-norm). This problem has a unique solution if the vector e is sufficiently sparse. The following theorem states this property.

Theorem 1 *If $\|e\|_0 = L$, then e is the unique solution of (P_0) if and only if*

$$L < \frac{K(H^T) + 1}{2}.$$

The function $K(H^T)$ is the ambiguity index of H^T , and is defined as the largest number such that any set of $K(H^T)$ columns of H^T is linearly independent. This bound is well known in the coding theory as the Singleton bound [9]. If $H \in R^{N \times (N-K)}$, then $K(H^T) \leq N - K$ and we have $L < (N - K + 1)/2$. Note that to construct a code capable of correcting t errors we have to add two new samples to the message vector m or have $N - K = 2t$.

The system of equations of (2) can be expanded to

$$\begin{bmatrix} | & | & & | \\ h_1 & h_2 & \cdots & h_N \\ | & | & & | \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_N \end{bmatrix} = s$$

and it is easy to see that the syndrome s can be written as a linear combination of the vectors h_i

$$s = \sum_{i \in J} h_i e_i.$$

4.1. Obtaining sparse solutions with ℓ_1 norm

Donoho and Elad [10, 11], showed that in certain conditions the (P_0) can be solved by the more tractable problem

$$(P_1) \quad \min \|e\|_1 \quad \text{subject to} \quad H^T e = s$$

with $\|e\|_1 = \sum_i |e_i|$ the ℓ_1 -norm. This is a linear programming problem and can be solved using the simplex or an interior point algorithm [12, 13, 14]. The following theorem states in which conditions the two problems are equivalent [10, 11].

Theorem 2 *If $\|e\|_0 = L$ and*

$$L < \frac{1 + 1/M(H^T)}{2} = ebp,$$

then (P_0) is equivalent to (P_1) and solving the latter problem leads to the same sparse solution obtained by solving (P_0) .

The mutual incoherence $M(H^T) = \max_{i \neq j} |h_i^T h_j|$ (assume H^T normalized with $\|h_i\|_2 = 1$) gives a measure of the distribution of the frame vectors of H^T . If $M(H^T)$ is high it means that certain vectors of H^T are almost collinear. The ebp stands for equivalence break point and gives the number of errors that is guaranteed the code to correct. Note that if the $L < ebp$ the equivalence between (P_0) and (P_1) is guaranteed, but if $L \geq ebp$ the equivalence may be broken. It is well known [15] that if we assume $K(H^T) = N - K$ (not without significance, since we are dealing with random matrices) that the following holds for the mutual incoherence

$$M(H^T) \geq \sqrt{\frac{K}{(N-K)(N-1)}} = M_{opt}.$$

$M(H^T)$ measures how spread-out the columns of H^T are and due to the Schwartz inequality we have $0 \leq M(H^T) \leq 1$. Note that for a square matrix A we have $M(A) = 0$ if A has orthogonal columns.

4.2. Grassmannian Frames

A code with a parity check matrix H that attains an optimal mutual incoherence $M(H^T)$, is expected to achieve good results. Such matrices exist and are known as Grassmannian frames [16, 17]. This type of frames has applications in coding with real numbers and they guarantee that the mutual incoherence is maximum $M(H^T) = M_{opt}$ and the vectors h_i are distributed in an optimal way in order to maximize the relative angle defined by $|h_i^T h_j|$ with $i \neq j$ and $\|h_i\|_2 = 1$. For this type of frames the equivalence break point is optimized

$$ebp_{opt} = \frac{1 + 1/M_{opt}}{2},$$

and it would be expected that they perform much better than the random case. However, that is not true, and simulation results showed that in most cases the random frames perform better. Note that the mutual incoherence does not give all the information about the frame subspace. We also have to consider the angle between each vector h_i and the subspaces formed by all the possible sets of two and more vectors h_j .

Assuming normalized vectors h_i , we can calculate the Gram matrix of H^T which has all the possible dot products $|h_i^T h_j|$ with $i \neq j$. The mutual incoherence gives only the worst case, and we can get more insight on the distribution of the angles if we evaluate the histogram of the off diagonal elements of the Gram matrix. In the figure 3 we can compare the histograms for a random generated matrix and a Grassmannian matrix. Notice the normal distribution of the frame angles for the random matrix and the maximum dot product of 0.25 for the Grassmannian matrix.

In order to validate the error correction with random matrices we have implemented error correction algorithms that generates a syndrome for a positive valued error pattern and

gets the sparse solution by solving (P_1) using a linear programming method of interior point. For each number of errors we tested 10^5 error patterns and counted the number correctly recovered. In the figure 4 we can see that for this simulation the random code performed slightly better than the Grassmannian code. We can also see that both methods correct most of the error patterns well above the ebp threshold.

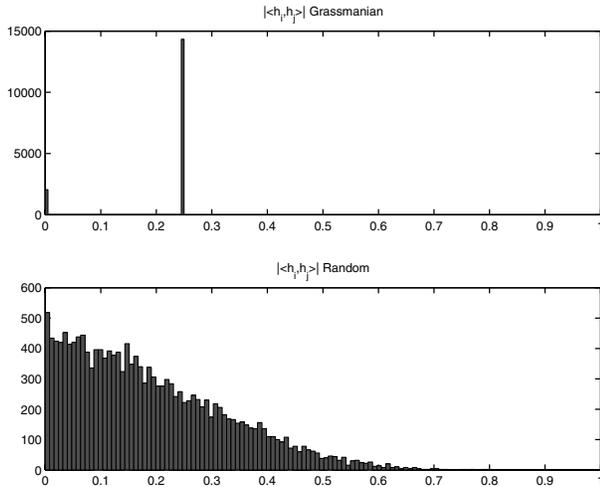


Fig. 3. Histograms of all possible angles between any two frame vectors. The top plot is for the Grassmannian matrix and the bottom one for the random one.

One of the problems in solving (P_1) directly with a linear programming algorithm, is that all the errors should be positive. To circumvent this limitation, we define for any error vector e the two variables e^+ and e^- as $e_i^+ = \max\{e_i, 0\}$ and $e_i^- = \max\{-e_i, 0\}$ from which e can be recovered as $e = e^+ - e^-$. Solving the following problem with $\hat{e} = [e^+ \ e^-]^T$,

$$\min \|\hat{e}\|_1 \quad \text{subject to} \quad [H^T \quad -H^T] \hat{e} = s \quad \text{and} \quad \hat{e} \geq 0,$$

we can correct positive and negative error amplitudes.

5. CONCLUSIONS

A method for correcting errors in real-number codes was proposed. Instead of solving the hard combinatorial problem it was shown that it is possible to obtain the same solution by solving a linear programming problem. We also showed that the optimal Grassmannian matrices do not always perform better than a simple random code. This observation makes clear that the mutual incoherence is not enough to characterize the code capacity. In Figure 4 we can see that the ebp (\circ) measured for the random code is much more conservative than the ebp (∇) for the Grassmannian code. We also proposed a different measure to characterize a code, but it is not practical because of the combinatorics.

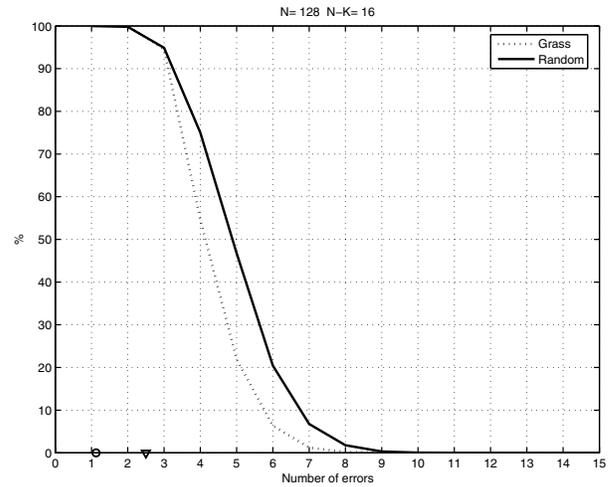


Fig. 4. Percentage of corrected error patterns for several number of errors (horizontal axis). Unexpectedly, the random code outperformed the Grassmannian code. \circ and ∇ represents the ebp of the random and Grassmannian codes respectively.

6. REFERENCES

- [1] T. G. Marshall Jr., "Methods for error correction with digital signal processors," in *Proceedings 25th Midwest Symposium on Circuits and Systems*. IEEE, 1982, pp. 1–5.
- [2] T. G. Marshall Jr., "Coding of real-number sequences for error correction: A digital signal processing problem," *IEEE Journal on Selected Areas of Communication*, vol. 2, no. 2, pp. 381–391, 1984.
- [3] Gagan Rath and Christine Guillemot, "Subspace based error and erasure correction with dft codes for wireless channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 11, pp. 3241–3252, 2004.
- [4] C. E. Shannon, "A mathematical theory of communication," *Bell Systems Technical Journal*, vol. 27, pp. 379–423, 1948.
- [5] Zizhong Chen and Jack Dongarra, "Numerically stable real-number codes based on random matrices," in *ITW2004*, San Antonio, Texas, 2004, IEEE, pp. 24–29.
- [6] Paulo J. S. G. Ferreira and José M. N. Vieira, "Stable dft codes and frames," *IEEE Signal Processing Letters*, vol. 10, no. 2, pp. 50–53, 2003.
- [7] José Vieira, "Stability analysis of non-recursive parallel concatenated real number codes," in *2nd Signal Processing Education Workshop*, Callaway Gardens, Pine Mountain, Georgia, USA, 2002, IEEE.

- [8] Richard E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, NY, 1983.
- [9] Richard E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, Cambridge, 2002.
- [10] David Donoho and Xiaoming Huo, “Uncertainty principles and ideal atomic decomposition,” *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2845–2862, 2001.
- [11] Michael Elad and Alfred M. Bruckstein, “A generalized uncertainty principle and sparse representation in pairs of bases,” *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2558–2567, 2002.
- [12] Margaret H. Wright, “The interior-point revolution in constrained optimization,” Tech. Rep. 98, Bell Laboratories.
- [13] Stephen Boyd and Lieven Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, UK, 2004.
- [14] Edwin K. P. Chong and Stanislaw H. Zak, *An Introduction to Optimization*, John Wiley & Sons. Inc., USA, 1996.
- [15] L. R. Welch, “Lower bounds on the maximum cross correlation of signals,” *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 397–399, 1974.
- [16] Thomas Strohmer and Robert W. Heath Jr., “Grassmannian frames with applications to coding and communication,” *Applied and Computational Harmonic Analysis*, vol. 14, no. 3, pp. 257–275, 2003.
- [17] Hardin Ronald H. Conway, John H. and Neil J. A. Sloane, “Packing lines, planes, etc.: Packings in grassmannian spaces,” *Experimental Mathematics*, vol. 5, no. 2, pp. 139–159, 1996.