Constructing Low-Density Parity-Check Codes with Circulant Matrices

J. W. Bond, S. Hui†, and H. Schmidt‡

Science Applications International Corp, 4105 Hancock St, San Diego, CA, 92110, e-mail: bond_jw@marlin.nosc.mil
† Department of Mathematics, San Diego State University, San Diego, CA 92182, e-mail: hui@saturn.sdsu.edu
‡ Technology Service Corporation, 962 Wayne Ave, Suite 800, Silver Spring, MD 20910, e-mail: hschmidt@tscwo.com

Abstract — **This is a report on our ongoing effort to implement Low-Density Parity-Check codes with Iterative Belief Propagation decoding in a communication system. The system requires the codes to have block lengths from 1000 to 2000 bits. We describe two different methods of constructing the codes using: (1) a combination of random and circulant matrices, and (2) random and circulant matrices with constraints to control the number of low weight codewords. We illustrate the performances of the different constructions with simulations.**

I. Introduction

Sparse matrix parity-check code was introduced by Gallager [4] and has attracted much attention recently; see, for example, MacKay [6], Luby *et al* [5], and Bond [1].

The most common method of implementing the sparse matrix method is to randomly construct a $m \times (n+m)$ parity-check matrix

$$H = \begin{bmatrix} R & C \end{bmatrix},$$

where R is $m \times n$ and C is $m \times m$ with certain desired properties and then put it into systematic form

$$\begin{bmatrix} C^{-1}R & I \end{bmatrix}.$$

The most common condition to impose on the parity-check matrix H is that the locations of 1's of any two different rows be different with at most one exception. The generator matrix is then

$$\begin{bmatrix} I \\ C^{-1}R \end{bmatrix}.$$

Of course, there is no guarantee that the matrix C is invertible. Indeed, it is quite likely for C to be non-invertible. Note that C is not invertible in $\mathbb{F}_2$ if its base 10 determinant is even.

II. Construction using Circulant Matrices

In our implementation, we use a circulant matrix C. Recall that a square matrix is circulant if each row of the matrix is the cyclic shift of the previous row. An example of a circulant matrix is

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

It is easy to see that the inverse of a circulant matrix is again circulant. The use of a circulant matrix allows us to guarantee invertibility and to control the number of cycles. Another advantage of a circulant matrix is that it is automatically regular. The most important reason for using a circulant matrix is the following mathematical fact.

Let C be a circulant matrix with first row $\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \end{bmatrix}$. We showed in Bond [3] that if $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ is primitive in $\mathbb{F}_2[x]$, then each row of the inverse of C has asymptotically the same number of zeros and ones in each row. Using this fact on the inverse of primitive circulant matrices, it is not hard to see that the average weight of the check-bits is about $m/2$ (see Bond [2]), where n is the number of check-bits. This guarantees good performance on the average when circulant matrices corresponding to primitive polynomials are used in the construction.

III. Random and Circulant Construction with Constraints

By using a circulant matrix that corresponds to a primitive polynomial in the construction of the parity-check matrix, we can guarantee that the average weight of the codewords is at least $m/2$. However, it is possible to have low weight codewords. We attempt to eliminate the low weight codewords by carefully choosing the random part of the parity-check matrix.

The codewords are vectors of the form

$$w = \begin{bmatrix} I \\ C^{-1}R \end{bmatrix} b,$$

where $b \in \mathbb{F}_2^n$. For w to be a low weight codeword, b and $a = C^{-1}Rb$ must have low weights. So to have low weight codewords, the equation $Rb = Ca$ must be solvable by low weight vectors b, a. We choose R carefully so that $Rb = Ca$ has few or no solutions with low weight a's and b's.

IV. Conclusions

Low-density parity-check codes with excellent average distance properties can be constructed by using parity-check matrices that are concatenations of circulant matrices and random matrices. However, these codes may have low minimum weights and this can give block error rates that are unacceptable for many important applications. In this talk we present the block error rate for codes constructed using circulant matrices and codes that are obtained by carefully choosing the circulant matrix and random matrix to ensure that the resulting codes have few or no low weight codewords.

References

[1] Bond, J. W., Hui, S. and Schmidt, H. (1997) Low density parity check codes based on sparse matrices with no small cycles, Proceedings of the IMA.

[2] Bond, J. W., Hui, S. and Schmidt, H. (1999) Sparse matrix parity-check codes and circulant matrices, In preparation.

[3] Bond, J. W., Hui, S. and Schmidt, H. (1999) The Euclidean algorithm and primitive polynomials over finite fields, submitted.

[4] Gallager, R. G. (1963) *Low Density Parity-Check Codes*, MIT Press.

[5] Luby, M., Mitzenmacher, M., Shokrollahi, M. A., Spielman, D. (1998) Analysis of Low Density Codes and Improved Designs using Irregular Graphs, Preprint.

[6] MacKay, D. J. C. (1998) Good error-correcting codes based on very sparse matrices, Preprint.