MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Sparse Factor Graph Representations of Reed-Solomon and Related Codes

Jonathan S. Yedidia

TR2004-097 June 2004

Abstract

We present sparse factor graph representations of Reed-Solomon codes based on a fast Fourier transform. These representations can be used to create encoders, or message-passing decoders that use soft input information. We discuss various simplications and transformations of the factor graph representations that may be useful. Finally, we show that other interesting codes can be represented using sparse fast transform factor graphs.

ISIT 2004

1. Published in the Proceedings of the International Symposium on Information Theory, 2004, p. 260. Please see TR2003-135 for a longer version.

Sparse Factor Graph Representations of Reed-Solomon and Related Codes

Jonathan S. Yedidia
MERL, 201 Broadway, 8th floor
Cambridge, MA 02139
e-mail: yedidia@merl.com

Abstract — **We present sparse factor graph representations of Reed-Solomon codes based on a fast Fourier transform. These representations can be used to create encoders, or message-passing decoders that use soft input information. We discuss various simplifications and transformations of the factor graph representations that may be useful. Finally, we show that other interesting codes can be represented using sparse fast transform factor graphs.**

I. Introduction

We present a family of Forney factor graph (FFG) representations for Reed-Solomon (RS) codes, based on the fast Fourier transform (FFT), similar to those introduced by Forney [1] for Reed-Muller (RM) codes.

The basic building block in our FFG representations is called a butterfly factor node (BFN). A BFN relates, by a set of linear constraints defined over $GF(q)$, an equal number of "input" variables on the left and "output" variables on the right. The linear constraints are denoted by marking the square representing the BFN; see figure 1 for an example.

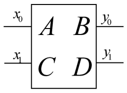

Figure 1: A BFN representing the constraints $y_0 = Ax_0 + Bx_1$ and $y_1 = Cx_0 + Dx_1$.

RS codewords can be obtained from a discrete Fourier transform (DFT) over $GF(q)$, where the first k "frequency" components are given by the information symbols, and the other $N - k$ frequency components are fixed to zero [2]. Using BFN's, we can build an FFT representation of RS codes, at least for convenient values of N and q (see Figure 2).

II. Other Codes and Representations

Extended RS codes where both N and q are a power of 2 can also be constructed using transforms (which are *not* FFT's) constructed using BFN's. Other excellent codes, including the ternary extended Golay code, can be represented in a similar way [3]. Carlach and Otmani [4] have shown that a variety of excellent self-dual binary codes, including the binary extended Golay code, can also be constructed in a similar manner, using factor nodes that enforce the constraints of the extended Hamming code.

One potential problem with the representations considered above is that the variables in internal layers do not receive any channel evidence. It may be worthwhile to consider codes obtained from lengthening the above codes by connecting channel evidence to the internal variables.

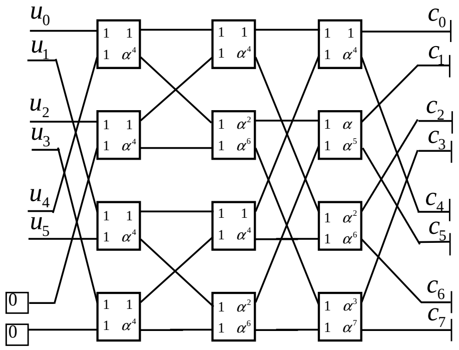

Figure 2: An FFG representation of an $[N = 8, k = 6]_{q=9}$ RS code. u_i are the information symbols, c_i are the codeword symbols, and α is a primitive element of $GF(q)$.

These representations can be simplified using reduction rules similar to those introduced by Forney [1] for RM codes. It is also easy to make redundant versions of these representations, by exploiting the symmetries of the codes, or the fact that alternative FFT constructions exist for a given DFT.

III. Encoders and Decoders

The representations discussed here can be used to make efficient encoders, and they can also be used as the basis of message-passing decoders. For such decoders, it is important to use a form of belief propagation that simultaneously enforces all the constraints in a BFN.

The appropriate message-update rules can be considered a simple form of generalized belief propagation (GBP) [5]. In the context of an application that uses an ordinary real-valued FFT, Storkey demonstrates the advantages of GBP compared to a BP approach that treats the constraints in each butterfly separately [6].

References

[1] G.D. Forney, Jr., "Codes on Graphs: Normal Realizations," *IEEE Trans. on Information Theory*, vol. 47, pp. 520-548, Feb. 2001.

[2] See, e.g., R. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003.

[3] J.S. Yedidia, http://www.merl.com/papers/TR2003-135/.

[4] J.-C. Carlach and A. Otmani, "A Systematic Construction of Self-Dual Codes," *IEEE Trans. on Information Theory*, vol. 49, pp. 3005-3009, Nov. 2003.

[5] J.S. Yedidia, W.T. Freeman, and Y. Weiss, http://www.merl.com/papers/TR2002-35/.

[6] A. Storkey, "Generalised Propagation for Fast Fourier Transforms with Partial or Missing Data," *Advances in Neural Information Processing Systems*, vol. 16, 2004.