

An Analysis of the Relationships between Pseudocodewords

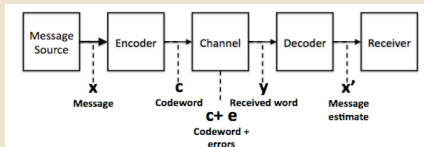
Katherine Morrison
University of Nebraska—Lincoln

Email: s-kmorri11@math.unl.edu

This is joint work with:
Nathan Axivig, Deanna Dreher, Eric Psota, Lance C. Pérez, and Judy L. Walker¹

What is Channel Coding?

The goal of channel coding is to allow the transmission of information over a noisy channel in such a way that the receiver can recover the original information. This is done by adding redundancy to the information before transmission.



Example: If the message $\mathbf{x} = x_1 x_2 x_3 x_4$ is encoded as $\mathbf{c} = c_1 c_2 c_3 c_4 c_5 c_6 c_7$, with $c_i = x_i$ for $i=1 \dots 4$, $c_5 = x_2 + x_3 + x_4$, $c_6 = x_1 + x_3 + x_4$, and $c_7 = x_1 + x_2 + x_4$, then the codewords in \mathbb{F}_2^7 form the [7,4,3] Hamming code.

Shannon's Theorem

The tradeoff between information and redundancy in a code is measured by the **rate**, which equals the length of the messages divided by the length of the codewords. In 1948 Shannon proved that every noisy channel has a **capacity** R_0 such that for any $R < R_0$ there exist codes of rate R that provide arbitrarily reliable communication over the channel. This existence proof led to the search for capacity-achieving codes.

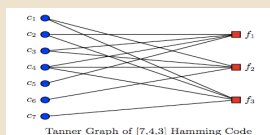
Low-Density Parity-Check Codes

One class of near-capacity-achieving codes is the set of **low-density parity-check (LDPC) codes**. These codes are the nullspaces of 0-1 parity-check matrices that are sparse. The [7,4,3] Hamming code is an example. LDPC codes have minimal tradeoff between information and redundancy while maintaining good error-correcting capabilities, and they come equipped with low-complexity **iterative message-passing decoders (IMPDs)**. These codes are used in a number of practical applications such as deep space communication, local area networks, and fourth generation wireless communication.

Tanner Graphs of LDPC Codes

LDPC codes may be represented in terms of a bipartite graph, known as the **Tanner graph**. The parity-check matrix of a code is the incidence matrix of the Tanner graph.

Example: Tanner graph of the [7,4,3] Hamming code:



The codeword variable nodes are represented by c_1, \dots, c_7 while f_1, \dots, f_3 , known as check nodes, represent the relations modulo 2 that the variable node values must satisfy.

Overview of Iterative Message-Passing Decoders

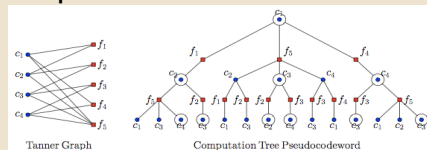
Based on the received word \mathbf{y} , IMPDs calculate an assignment of 0 or 1 for each variable node plus a measure of reliability for that estimate. These estimates are broadcast to the neighboring check nodes. The check nodes make further estimates based on what they receive and broadcast these new values back to the neighboring variable nodes. This message-passing process is repeated until some stopping criterion is met.

Given the practical value of LDPC codes, it has become essential to understand the associated IMPDs. It is particularly important to understand when IMPDs fail, i.e. what causes them to produce noncodeword outputs.

Computation Tree Pseudocodewords

By tracing back through the paths of the messages passed by an IMPD to compute the value of a particular variable node, we derive a computation tree rooted at that variable node. IMPDs can be precisely modeled using computation trees.² Furthermore, one can consider configurations on computation trees: assignments of 0s and 1s to the variable nodes such that the sum of values at each check node is zero mod 2; these configurations are known as **computation tree pseudocodewords**.

Example:



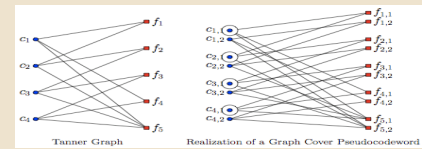
Wiberg shows that the computation tree pseudocodewords that do not correspond to codewords are the precise cause of noncodeword outputs with IMPDs. The set of computation tree pseudocodewords often grows exponentially with the depth of the tree making this set difficult for theoretical analysis.

An Alternative Approach: Graph Cover Pseudocodewords

Because the computations done by IMPDs depend solely on the neighborhoods of nodes in the Tanner graph, IMPDs cannot distinguish between the Tanner graph and any cover of this graph. This intuition led Vontobel and Koetter to explore **graph covers**.³ Any assignment of 0s and 1s to the variable nodes of a graph cover that satisfies the local check constraints is a realization of a **graph cover pseudocodeword**. By calculating the average number of 1s assigned to each variable node, one can find a corresponding vector that has the same length as the original code, known as the **normalized graph cover pseudocodeword**.

Graph Covers Cont'd

Example:



Vontobel and Koetter give a compact characterization of this set of pseudocodewords: they are the set of rational points within the **fundamental polytope** of the code. The vertices of this polytope are the possible outputs of the **linear programming (LP) decoder**.

Unifying Computation Tree and Graph Cover Pseudocodewords

The goal of this work is to apply the theoretical findings on graph cover pseudocodewords to an analysis of computation tree pseudocodewords, the known cause of errors with IMPDs. Specifically, we investigate when a particular graph cover pseudocodeword gives rise to a computation tree pseudocodeword since this correspondence may allow for a compact description of the set of computation tree pseudocodewords. Since computation trees are necessarily connected, it is clear that only realizations of graph cover pseudocodewords that occur on connected covers, i.e. **connected realizations** of normalized graph cover pseudocodewords, can induce computation tree pseudocodewords.

Theorem: Let T be a Tanner graph with corresponding fundamental polytope P and suppose ω is a vertex of P . Then every graph cover realization of ω is either connected or the disjoint union of connected graph cover realizations of ω .

Theorem: Let T be a Tanner graph with average variable node degree a_c and average check node degree a_f . Suppose either

$$a_c \geq 3 \text{ and } a_f \geq 3, \text{ or} \\ a_c \geq 4 \text{ and } a_f \geq 2.$$

Then any rational point in the fundamental polytope, i.e. any normalized graph cover pseudocodeword of T , can be realized on a connected cover.

References

[1] N. Axivig, D. Dreher, K. Morrison, E. Psota, L.C. Pérez, and J.L. Walker. Analysis of connections between pseudocodewords. To appear in *IEEE Transactions on Information Theory*.

[2] N. Wiberg. Codes and decoding on general graphs. PhD thesis, Linköping University, Linköping, Sweden, 1996.

[3] P. Vontobel and R. Koetter. Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes. To appear in *IEEE Transactions on Information Theory*.