Conditionally Cycle-Free Generalized Tanner Graphs: Theory and Application to High-Rate Serially Concatenated Codes

Thomas R. Halford and Keith M. Chugg
Communication Sciences Institute
Department of Electrical Engineering - Systems
University of Southern California
Los Angeles, CA 90089-2565
Email: {halford,chugg}@usc.edu

Abstract—Generalized Tanner graphs have been implicitly studied by a number of authors under the rubric of generalized parity-check matrices. This work considers the conditioning of binary hidden variables in such models in order to break all cycles and thus derive optimal soft-in soft-out (SISO) decoding algorithms. Conditionally cycle-free generalized Tanner graphs are shown to imply optimal SISO decoding algorithms for the first order Reed-Muller codes and their duals - the extended Hamming codes - which are substantially less complex than conventional bit-level trellis decoding. The study of low-complexity optimal SISO decoding algorithms for the family of extended Hamming codes is practically motivated. Specifically, it is shown that extended Hamming codes offer an attractive alternative to high-rate convolutional codes in terms of both performance and complexity for use in very high-rate, very low-floor, serially concatenated coding schemes.

I. INTRODUCTION

Very high-rate codes are of great interest for a number of practical applications including data storage and high-speed fiber links. The design of modern error-correcting codes which simultaneously have very low error floors (e.g. $< 10^{-10}$ bit error rate) and very high rates (e.g. $> 0.9$) is a particularly challenging problem of practical interest. Due to the inherent difficulty of simulating the performance of codes in the very low floor region, the design of such codes relies on the principles of uniform interleaver analysis (cf. [1] and the references therein). To review, on the additive white Gaussian noise (AWGN) channel with binary antipodal signaling, the bit error rate ($P_b$) and codeword error rate ($P_{cw}$) of a large class of modern codes vary asymptotically with block size as

$$P_b \sim N^{\alpha_{\text{max}}} \quad P_{cw} \sim N^{\alpha_{\text{max}} + 1}$$

where $N$ is the interleaver size and $\alpha_{\text{max}}$ is the maximum exponent of $N$ in an asymptotic union bound approximation. Note that $\alpha_{\text{max}}$ depends on both the specific code construction and constituent codes used. If the bit (codeword) error rate decays with $N$, then the code is said to exhibit interleaver gain in bit (codeword) error rate. Designs for codes with low floors require interleaver gain in both bit and codeword error rates thus require $\alpha_{\text{max}} \leq -2$.

Serially concatenated code (SCC) constructions (i.e. codes composed of an inner code and outer code separated by a random-like interleaver) are well-suited to low-floor design because, provided the inner code is recursive, the maximum exponent of $N$ is [1]

$$\alpha_{\text{max}} = - \left\lfloor \frac{d_{\text{min,o}} + 1}{2} \right\rfloor$$

where $d_{\text{min,o}}$ is the minimum distance of the outer code. Since the rate of an SCC is equal to the product of the rates of its constituent codes, the design of a high-rate, low-floor SCC requires a high-rate outer code satisfying $d_{\text{min,o}} \geq 3$. However, it is very challenging to find such outer codes for which there exist low-complexity optimal SISO decoding algorithms. To this end, Graell i Amat et al. introduced a class of high-rate convolutional codes with optimal SISO decoding algorithms of moderate complexity based on their dual codes [2], [3].

An alternative approach to the design of high-rate low-floor codes are the systematic with serially concatenated parity (S-SCP) codes proposed in [4], of which Jin et al.’s generalized repeat accumulate (GRA) codes [5] are an example. The S-SCP code structure can be viewed as a systematic code with a parity generating concatenated system that resembles an SCC. It was demonstrated in [4] that S-SCP codes have the same maximum error exponent and design rules as SCCs: codes constructed with a parity generating system composed of a recursive inner parity generator and an outer code satisfying $d_{\text{min,o}} \geq 3$ achieve interleaver gain in both bit and codeword error rates. In contrast to SCCs, good S-SCPs can be constructed with inner parity generators that have rate greater than 1 so that the rate of outer code can be lower than the overall code rate thus alleviating the aforementioned challenge of finding high-rate, $d_{\text{min,o}} \geq 3$ outer codes with low-complexity SISO decoding algorithms.

The design of good high-rate, low-floor codes has thus been largely solved for the AWGN channel. However, the S-SCP design philosophy is not directly applicable to the large class of systems which have recursive channels. The term recursive channel is introduced to describe systems in which
the aggregate of the modulation and (possible) precoding with the channel is recursive. Continuous phase modulations over AWGN and fading channels as well as certain models for precoded magnetic recording channels (e.g. EPR4 [6]) are examples of recursive channels.

In light of the above discussion, high-rate, low-floor codes for use in systems with recursive channels can be constructed via the serial concatenation of a high-rate code and the channel (where the recursive channel is treated like an inner code). The outer high-rate code can be a modern (e.g. SCC or S-SCP) code or a classical (e.g. algebraic or convolutional) code. Classical outer codes are more attractive, however, for application in practical systems. Specifically, the use of a classical outer code for which there exists a simple non-iterative SISO decoding algorithm offers reductions in decoding complexity, decoding latency, and required memory with respect to a modern, iteratively decoded outer code. As with the design of SCCs for the AWGN channel, the design of such codes requires a high-rate, $d_{min} \geq 3$ outer classical code for which there exists a low-complexity optimal SISO decoding algorithm.

To this end, the present work introduces novel low-complexity SISO decoding algorithms for the family of first-order Reed-Muller codes (and hence their duals, the extended Hamming codes [7]) in Section III based on variable conditioning in generalized Tanner graphs (GTGs), which are defined in Section II. It is shown in Section IV that extended Hamming codes offer an attractive alternative to the high-rate convolutional codes studied in [2], [3] for use as outer codes in serial concatenation with recursive inner channels. Concluding remarks are given in Section V.

II. CONDITIONALLY CYCLE-FREE GTGS

A. Generalized Code Extensions

Let $C$ be an $[n, k, d]$ binary linear block code and let

$$ I \subseteq \{1, 2, \ldots, n\} $$

be some subset of the coordinate index set of $C$. A generalized extension of $C$, $\tilde{C}$, is formed by adding a parity-check on the bits corresponding to the index set $I$ to $C$ (i.e. a partial parity-check). Note that if $I = \{1, 2, \ldots, n\}$ then $\tilde{C}$ is simply a classically defined extended code [7]. The generalized extended code $\tilde{C}$ has length $n + 1$, dimension $k$ and minimum distance either $d$ or $d + 1$ depending on the choice of $I$. More generally, a degree-$g$ generalized extension of $C$ is formed by adding $g$ partial parity bits to $\tilde{C}$. Note that the $j^{th}$ partial parity bit, $e_{n+j}$, in such an extension forms a partial parity on any of the bits $c_i$ for $i \in \{1, \ldots, n+j-1\}$.

B. Generalized Tanner Graphs

This work introduces the term generalized Tanner graph (GTG) to denote the Tanner graph [8] corresponding to the parity-check matrix of a generalized code extension. Specifically, let $\tilde{C}$ be a degree-$g$ generalized extension of the $[n, k, d]$ binary linear block code $C$ and let $H = [h_{ij}]$ be an $(n - k + g) \times (n + g)$ parity-check matrix for $\tilde{C}$. The GTG associated with $H$ is the bipartite graph $G_H = (U \cup W, E)$ with disjoint vertex classes:

$$ U = \{u_j\}_{j=1}^{n+g} \quad \text{and} \quad W = \{w_i\}_{i=1}^{n-k+g} $$

corresponding to the columns and rows of $H$, respectively. An edge connects $u_j$ and $w_i$ in $G_H$ if and only if $h_{ij} = 1$. Note that a number of authors have previously considered such graphical representations of binary codes under the rubric of generalized parity-check matrices (cf. [9]).

As an example, consider the $[8, 4, 4]$ first-order Reed-Muller code $C_{RM(1,3)}$, any codeword of which can be decomposed via the squaring construction [7] as

$$ c = (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) = (u_1, u_2, u_3, u_4, u_1 + v_1, u_2 + v_2, u_3 + v_3, u_4 + v_4) \quad \text{(5)} $$

where $u$ is drawn from the $[4, 3, 2]$ single parity-check code and $v$ is drawn from the $[4, 1, 4]$ repetition code. A degree-1 generalized extension $\tilde{C}_{RM(1,3)}$ can be formed by adding the partial parity bit $c_4 + c_8 = v_4$ to $C_{RM(1,3)}$. A parity-check matrix for $\tilde{C}_{RM(1,3)}$ is

$$ \tilde{H}_{RM(1,3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}. \quad \text{(6)} $$

Figure 1 illustrates the GTG corresponding to $\tilde{H}_{RM(1,3)}$.

1The term Tanner graph has been used to describe different classes of graphical models by different authors. In this work, the term Tanner graph is used in its most restricted sense. That is to say, there is a bijection between the set of Tanner graphs for an $[n, k, d]$ binary linear code $C$ and the set of $n - k \times n$ parity check matrices for that code.
C. Conditionally Cycle-Free Generalized Tanner Graphs

Hidden variable conditioning in graphical models is well-understood in the context of tail-biting trellises (cf. [10]). If a tail-biting trellis contains a hidden (state) variable, $V$, with alphabet size $2^m$ then optimal SISO decoding can be performed on this trellis by decoding on $2^m$ cycle-free conditional trellises (one per possible value of $V$) and then appropriately marginalizing over the results of the decoding rounds. This work applies hidden variable conditioning to generalized Tanner graphs in order to obtain cycle-free graphical models and thus optimal SISO decoding algorithms.

As an example, consider again the GTG for $C_{RM(1,3)}$ illustrated in Figure 1 and suppose that the partial parity variable $c_4 + c_8$ is not considered unknown but fixed to be either a 0 or a 1. This conditional GTG is illustrated in Figure 2. Note that the conditional variable $c_4 + c_8$ is now treated as a visible, deterministic variable as indicated by the half-edges labeled by ‘0’/’1’ in Figure 2. The GTG illustrated in Figure 2 is cycle-free; optimal SISO decoding of a code with such a model can be accomplished by decoding twice on the conditionally cycle-free model (once with $c_4 + c_8 = 0$ and once with $c_4 + c_8 = 1$) and then appropriately marginalizing over the results of the two decoding rounds [11].

More generally, a degree-$f$ conditionally cycle-free generalized Tanner graph contains $f$ variables which can be fixed to remove all cycles. Optimal SISO decoding can be achieved by decoding $2^f$ times on a degree-$f$ conditionally cycle-free GTG (and appropriately marginalizing over the results).

III. CONDITIONALLY CYCLE-FREE GTGS FOR FIRST-ORDER REED-MULLER CODES

Let $C_{RM(r,m)}$ denote the Reed-Muller code with parameters

$$n = 2^m, \quad k = \sum_{j=0}^{r} \binom{m}{j}, \quad d = 2^{m-r}. \quad (7)$$

**Theorem 1:** There exists a degree-$(m-2)$ conditionally cycle-free generalized Tanner graph for $C_{RM(1,m)}$, $m \geq 3$.

**Proof:** By induction on $m$. The $m = 3$ case was shown by construction in Section III. Suppose that there exists a degree-$(m-3)$ conditionally cycle-free graphical model for $C_{RM(1,m-1)}$. There exists a squaring construction for $C_{RM(1,m)}$ such that if $c \in C_{RM(1,m)}$ then

$$c = (u, u + v) \quad (8)$$

where $u \in C_{RM(1,m-1)}$ and $v \in C_{RM(0,m-1)}$ [7]. A GTG for this code is illustrated in Figure 3. The code vertex labeled $C_{RM(1,m-1)}$ corresponds to a GTG for that code.

By the induction hypothesis, a degree-$(m-2)$ conditionally cycle-free GTG is formed by conditioning on the repetition constraint $C_{RM(0,m-1)}$ and on $m-3$ variables in the model corresponding to $C_{RM(1,m-1)}$. \hfill \Box

It is well-known that a symbol-wise optimal SISO decoding algorithm for a code $C$ implies a symbol-wise optimal SISO decoding algorithm for its dual $C^\perp$ [12], [13]. The conditionally cycle-free GTGs for first-order Reed-Muller codes described above thus imply optimal SISO decoding algorithms for the family of Reed-Muller codes with parameters $[2^m, 2^m - m - 1, 4]$; the extended Hamming codes.

Let $A_m$ and $C_m$ denote the number of addition and comparison operations required by the optimal SISO decoding algorithm implied by the conditionally cycle-free GTG for $C_{RM(1,m)}$ described above. Counting operations in the binary graphical model illustrated in Figure 3 yields the following recursion for $A_m$ and $C_m$:

$$A_m = 3 \cdot 2^m + 2A_{m-1}, \quad C_m = 2^m + 2C_{m-1}. \quad (9)$$

Note that these formulae include the comparisons required for marginalizing over the results of the individual decoding rounds. It is clear that the complexity of SISO decoding using the proposed conditionally acyclic binary graphical models

\*Note that min-sum or min*-sum processing is assumed throughout this work so that $C_m$ counts the number of min or min* operations.
thus grows as $O(n \log n)$. Ashikhim and Litsyn proposed a MAP decoding algorithm for the family of $C_{RM(1,m)}$ codes with similar asymptotic complexity based on fast Hadamard transforms [14]. Note that the complexity of bit-level trellis decoding of this code family grows as $O(n^2)$.

In order to specifically demonstrate that conditionally cycle-free generalized Tanner graphs (CCF-GTGs) can imply substantially less complex optimal SISO decoding algorithms than bit-level trellises, the number of addition and comparison operations for each SISO decoding algorithm is tabulated in Table I for a number of first-order Reed-Muller codes. The trellis complexity was evaluated by considering the total number of addition and comparison operations required to perform the full SISO BCJR algorithm [15] (rather that soft-in hard-out Viterbi decoding) on bit-level trellises with minimal state complexities as given by Lu and Huang in [16].

![Complexity of trellis decoding vs. the proposed optimal SISO decoding algorithm.](image)

**IV. APPLICATION: HIGH-RATE SCCS**

In [3], Graell i Amat et al. studied a serially concatenated coding scheme consisting of a high-rate convolutional outer code and a recursive rate-1 inner code corresponding to a simplified discrete-time model of a precoded EPR4 magnetic recording channel. Specifically, the recursive channel model comprises a $1/1 \oplus D^2$ precoder followed by a digital recording channel subject to intersymbol interference (ISI) with partial response polynomial $1 + D - D^2 - D^3$ followed finally by an AWGN channel. Note that the precoder and ISI can be jointly decoded on an 8-state trellis.

In this section, the performance of this scheme is compared to one which replaces the high-rate convolutional codes with extended Hamming codes. Specifically, 4 convolutional outer codes with input block size 4000 bits and respective rates 8/9, 9/10, 11/12, and 16/17 are compared to four algebraic outer codes composed of the following mixtures of extended Hamming codes:

- The mixture of 3 $C_{RM(3,5)}$ and 69 $C_{RM(4,6)}$ codewords resulting in a code with input block size 4011 bits and rate $4011/4512 = 0.8890 \approx 8/9$.
- The mixture of 56 $C_{RM(4,6)}$ and 7 $C_{RM(5,7)}$ codewords resulting in a code with input block size 4032 bits and rate $4032/4480 = 9/10$.
- The mixture of 30 $C_{RM(4,6)}$ and 19 $C_{RM(5,7)}$ codewords resulting in a code with input block size 3990 bits and rate $3990/4352 = 0.9168 \approx 11/12$.
- The mixture of 2 $C_{RM(4,6)}$, 26 $C_{RM(5,7)}$, and 3 $C_{RM(6,8)}$ codewords resulting in a code with input block size 3975 bits and rate 3975/4224 = 0.9411 $\approx 16/17$.

As reported in [3], the SCCs using convolutional codes utilize $s$-random interleavers [17]. The codes using mixed extended Hamming outer codes utilize high sum-spread pseudo-random interleavers that were generated using the real-relaxation optimization method described in [18].

Figure 4 compares the performance of the respective rate 8/9 and 11/12 codes while Figure 5 compares the performance of the respective rate 10/11 and 16/17 codes. Note that the performance of the serially concatenated codes with convolutional outer codes is reported for 10 decoding iterations while the performance of the codes with mixed extended Hamming outer codes is reported for 10 and 20 decoding iterations. All curves correspond to min$^+$-sum processing (or its dual-domain equivalent [13]).

![Bit error rate performance of the respective rate 8/9 and 11/12 serially concatenated codes.](image)

Observe in Figures 4 and 5 that the codes constructed with mixed extended Hamming outer codes compare favorably in terms of performance to those with convolutional outer codes of similar rates and input block sizes. The mixed extended Hamming codes compare favorably to their high-rate convolutional code counterparts in terms of complexity also. Table II tabulates the average number of add and comparison operations per input bit, per decoding iteration, required for optimal SISO decoding (using the CCF-GTG algorithm) for each of the mixed extended Hamming codes. The rate $k/k+1$ convolutional outer-codes in [3] were decoded on the 16- (for $k = 8, 9, 10$) and 32- (for $k = 16$) state trellises corresponding to their respective rate $1/1 + k$ duals. Optimal SISO decoding on a rate $1/1 + k$, $16- (32-)$ state trellis requires at least 96 (192) additions and 64 (128) comparisons per input bit, per decoding iteration. Thus, if one assumes that an addition and...
V. Conclusion

Motivated by the search for optimal SISO decoding algorithms with complexity less than that of trellis decoding, this work studied conditionally cycle-free generalized Tanner graphs. It was shown that such models exist for the family of first-order Reed-Muller codes and that these models imply low-complexity SISO decoding algorithms for these codes and their duals: the extended Hamming codes. It was shown that the proposed low-complexity SISO decoding algorithms for the family of extended Hamming codes are particularly useful in the context of high-rate serially concatenated codes.

A number of interesting directions for future work are motivated by the present work. It would be interesting to search for more codes for which conditionally cycle-free generalized Tanner graphs offer complexity savings over trellis decoding.

It would also be interesting to study the performance of the sub-optimal, iterative, SISO decoding algorithms implied by GTGs in which only a subset of hidden variables required to break all cycles are conditioned. Specifically, a study of codes with known algebraic decompositions may lead to novel low-complexity SISO decoding algorithms. There are also a number of interesting avenues of study concerning the application of the optimal SISO decoder for extended Hamming codes. Specifically, the algorithm presented in this work has a natural tree structure which can lead to particularly efficient implementations in hardware [19].

REFERENCES

[1] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, “Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding,” IEEE Trans. Information Theory, vol. 44, no. 3, pp. 909–926, May 1998.

[2] A. G. i Amat, S. Benedetto, and G. Montorsi, “Optimal high-rate convolutional codes for partial response channels,” in Proc. Globecom Conf., vol. 2, Taipei, Taiwan, November 2002, pp. 1031–1036.

[3] A. G. i Amat, G. Montorsi, and S. Benedetto, “New high-rate convolutional codes for concatenated schemes,” in Proc. International Conf. Communications, vol. 3, New York, NY, May 2002, pp. 1661–1666.

[4] K. M. Chugg, P. Thiennviboon, G. D. Dimou, P. Gray, and J. Melzer, “A new class of turbo-like codes with universally good performance and high-speed decoding,” in Proc. IEEE Military Comm. Conf., Atlantic City, NJ, October 2005.

[5] H. Jin, A. Khandekar, and R. McEliece, “Irregular-repeat-accumulate codes,” in Turbo Code Conf., Brest, France, 2000.

[6] J. Li, K. R. Narayanan, E. Kurtas, and C. N. Georghiades, “On the performance of high-rate TPC/SPC codes and LDPC codes over partial response channels,” IEEE Trans. Communications, vol. 50, no. 5, pp. 723–734, May 2002.

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. North-Holland, 1978.

[8] R. M. Tanner, “A recursive approach to low complexity codes,” IEEE Trans. Information Theory, vol. IT-27, pp. 533–547, September 1981.

[9] J. S. Yedidia, J. Chen, and M. C. Fossorier, “Generating code representations suitable for belief propagation decoding,” in Proc. Allerton Conf. Commun., Control, Comp., Monticello, IL, October 2002.

[10] S. M. Aji, G. B. Horn, and R. J. McEliece, “Iterative decoding on graphs with a single cycle,” in Proc. IEEE International Symp. on Information Theory, Cambridge, MA, August 1998, p. 276.

[11] J. Heo and K. M. Chugg, “Constrained iterative decoding: Performance and convergence analysis,” in Proc. Asilomar Conf. Signals, Systems, Comp., Pacific Grove, CA, November 2001, pp. 275–279.

[12] C. R. P. Hartmann and L. D. Rudolph, “An optimum symbol-by-symbol decoding rule for linear codes,” IEEE Trans. Information Theory, vol. IT-22, no. 5, pp. 514–517, September 1976.

[13] G. Montorsi and S. Benedetto, “An additive version of the SISO algorithm for the dual code,” in Proc. IEEE International Symp. on Information Theory, Washington, DC, June 2001.

[14] A. Ashikhmin and S. Litsyn, “Simple MAP decoding of first-order Reed-Muller and Hamming codes,” IEEE Trans. Information Theory, vol. 50, no. 8, pp. 1812–1818, August 2004.

[15] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, “Optimal decoding of linear codes for minimizing symbol error rate,” IEEE Trans. Information Theory, vol. IT-20, pp. 284–287, March 1974.

[16] C.-C. Hu and S.-H. Huang, “On bit-level trellis complexity of Reed-Muller codes,” IEEE Trans. Information Theory, vol. 41, no. 6, pp. 2061–2064, November 1995.

[17] D. Divsalar and F. Pollara, “Turbo codes for PCS applications,” in Proc. International Conf. Communications, Seattle, WA, 1995, p. 5459.

[18] S. Crozier, “New high-speed high-distance interleavers for turbo-codes,” in Proc. 20th Biennial Symp. Comm., Kingston, ON, Canada, 2000, pp. 3–7.

[19] P. A. Beerel and K. M. Chugg, “A low latency SISO with application to broadband turbo decoding,” IEEE J. Select. Areas Commun., vol. 19, no. 5, pp. 860–870, May 2001.