Lower Bounds on the Minimum Pseudo-Weight of Linear Codes

Pascal O. Vontobel and Ralf Koetter[1]
Coordinated Science Laboratory and Dept. of ECE
University of Illinois at Urbana-Champaign
e-mail: `vontobel@ifp.uiuc.edu`, `koetter@uiuc.edu`

Abstract — **We discuss two techniques for obtaining lower bounds on the (AWGN channel) pseudo-weight of binary linear codes. Whereas the first bound is based on the largest and second-largest eigenvalues of a matrix associated with the parity-check matrix of a code, the second bound is given by the solution to a linear program.**

The fundamental polytope/cone [1] turns up in a variety of contexts: when characterizing the valid configurations of graph-covers of factor graphs, when formulating the linear programming decoder, or when looking at the beliefs that are possible for the Bethe free energy associated to a factor graph.

It is probably fair to say that one of the most important parameters that characterize the fundamental polytope/cone is the minimum pseudo-weight of all the pseudo-codewords that lie in the fundamental polytope/cone. The AWGNC pseudo-weight [2, 1] of a pseudo-codeword $\mathbf{x}$ is defined to be $w_{\mathrm{p}}(\mathbf{x}) \triangleq w_{\mathrm{p}}^{\mathrm{AWGNC}}(\mathbf{x}) \triangleq \frac{||\mathbf{x}||_1^2}{||\mathbf{x}||_2^2}$. In the following, $w_{\mathrm{p}}^{\mathrm{min}}(\mathbf{H})$ will denote the minimum AWGNC pseudo-weight of a linear code C defined by the parity-check matrix $\mathbf{H}$ and $w_{\mathrm{H}}^{\mathrm{min}}(\mathsf{C})$ will denote the minimum Hamming weight of a linear code C. (Given a code, note that the minimum Hamming weight is a function of the code whereas the minimum pseudo-weight is a function of the parity-check matrix describing the code.) In [1] we discussed two ways of obtaining *upper* bounds on the minimum AWGNC pseudo-weight: one of them was based on searching for low-weight pseudo-codewords in the fundamental cone, the other was based on the so-called canonical completion. In this paper we now introduce two techniques for obtaining *lower* bounds.

The first one (Th. 1) is a purely algebraic eigenvalue-based bound that turns out to have the same form as the bit-oriented lower bound given by Tanner [3] for the minimum Hamming weight of a binary code. (Therefore, parity-check matrices that lead there to a non-trivial bound give also here a non-trivial bound.)

The second bound (Claim 3) is a linear-programming-based bound which was originally very much inspired by the linear programming lower bound on the minimum Hamming weight as presented by Tanner [3]. But finally, its form is quite different. Actually, the present form of the linear program reminds much more of the "lift and project" technique in [4, Sec. 5.4.2] which was used to obtain a modification of the linear programming decoder. But the approach in [4] is used to constrain the fundamental polytope whereas we are interested in relaxing the fundamental polytope. Note moreover that in [3] and in [4] an important ingredient is the relation $x_i = x_i^2$ (which holds because the components of the vector $\mathbf{x}$ were desired to be 0 or 1), but this does not hold anymore for components of pseudo-codewords.

Theorem 1 *Let C be a (j,k)-regular code of length n defined by the parity-check matrix $\mathbf{H}$ and let the corresponding Tanner graph have one component. Let $\mathbf{L} \triangleq \mathbf{H}^{\mathsf{T}}\mathbf{H}$ and let μ_1 and μ_2 be the largest and second-largest eigenvalue, respectively, of $\mathbf{L}$. Then the minimum Hamming weight and the minimum AWGNC pseudo-weight are lower bounded by*

$$w_{\mathrm{H}}^{\mathrm{min}}(\mathsf{C}) \geq w_{\mathrm{p}}^{\mathrm{min}}(\mathbf{H}) \geq n \cdot \frac{2j-\mu_2}{\mu_1-\mu_2}.$$

Corollary 2 *Consider a binary code of length n whose automorphism group is two-transitive on the bits and whose dual code has minimum Hamming weight $w_{\mathrm{H}}^{\mathrm{min}\perp}(\mathsf{C})$. Let $\mathbf{H}$ be the matrix consisting of all vectors in the dual code whose Hamming weight equals $w_{\mathrm{H}}^{\mathrm{min}\perp}(\mathsf{C})$. Then,*

$$w_{\mathrm{H}}^{\mathrm{min}}(\mathsf{C}) \geq w_{\mathrm{p}}^{\mathrm{min}}(\mathbf{H}) \geq \frac{n-1}{w_{\mathrm{H}}^{\mathrm{min}\perp}(\mathsf{C})-1} + 1.$$

(We assume that the above parity-check matrix $\mathbf{H}$ spans indeed the whole dual code; if not, then the lower bound is for an even larger code.)

Claim 3 *Let C be a code of length n with parity-check matrix $\mathbf{H}$. Then, the minimum Hamming weight and the minimum AWGN pseudo-weight can be lower bounded by*

$$w_{\mathrm{H}}^{\mathrm{min}}(\mathsf{C}) \geq w_{\mathrm{p}}^{\mathrm{min}}(\mathbf{H}) \geq \frac{1}{\max_{\mathbf{y}\in\mathcal{K}_1'(\mathbf{H})} f'(\mathbf{y})}.$$

Here, $f'(\,\cdot\,)$ is a linear function and $\mathcal{K}_1'(\mathbf{H})$ is a certain convex polytope in $\mathbb{R}^{n^2}$ derived from $\mathbf{H}$, therefore the denominator represents a linear program. Note that any feasible point of the dual linear program also yields a lower bound.

For the details of Claim 3 we refer to [5] where we also discuss different variations of the bound and how to use the automorphism group of the parity-check matrix $\mathbf{H}$ to reduce the size of the linear program.

References

[1] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *Proc. 3rd Intern. Conf. on Turbo Codes and Related Topics*, (Brest, France), pp. 75–82, Sept. 1–5 2003.

[2] N. Wiberg, *Codes and Decoding on General Graphs.* PhD thesis, Linköping University, Sweden, 1996.

[3] R. M. Tanner, "Minimum-distance bounds by graph analysis," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 808–821, 2001.

[4] J. Feldman, *Decoding Error-Correcting Codes via Linear Programming.* PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 2003.

[5] Preprint at `http://www.ifp.uiuc.edu/~vontobel`.

[1] Both authors were supported by NSF Grants CCR 99-84515 and CCR 01-05719.