On Tanner Graphs of Lattices and Codes

Amir H. Banihashemi, Frank R. Kschischang, and P. Glenn Gulak
Dept. of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 1A4
Email: ahashemi,frank@comm.toronto.edu, gulak@eecg.toronto.edu

Abstract — **The problem of finding a low-complexity Tanner graph for a general lattice Λ is studied. The problem is divided into two subproblems: 1) Finding an orthogonal sublattice Λ' of Λ which minimizes the complexity of the label code of the quotient group Λ/Λ'. 2) Constructing a simple Tanner graph for the label code obtained in part 1. The proposed approach for solving subproblem 2 can also be applied to any abelian group block code with arbitrary finite alphabets at different coordinates. The results of this work are useful in finding low-complexity graph representation of lattices and codes, which consequently results in efficient graph-based decoding algorithms.**

I. Summary of Results

The graph representation of codes and the corresponding decoding algorithms, initiated by the work of Gallager on low-density parity-check codes [2] and later generalized by Tanner [3] to codes defined by general bipartite graphs, have continued to be an active area of research particularly in the past few years (see, e.g., [6] and the references therein). The construction of Tanner graphs for linear block codes is well-known and is based on using a parity-check matrix of the code [3]. A Tanner graph construction for lattices, using a method different from the one discussed in this paper, was briefly sketched in [5]. In this work, we develop Tanner graph constructions for abelian group block codes, an important application of which is to represent the label code of a lattice [1] in a given coordinate system. Our study shows that to obtain a low-complexity Tanner graph for an n-dimensional (n-D) lattice Λ, it is reasonable to divide the problem into two subproblems: **1)** finding a set of 1-D orthogonal subspaces $\{W_i\}_{i=1}^n$, called graph coordinate system, which minimizes the sizes g_i of the label groups $G_i = P_{W_i}(\Lambda)/\Lambda_{W_i}$, where $P_{W_i}(\Lambda)$ and Λ_{W_i} denote the projection and cross section of Λ on W_i, **2)** deriving a simple Tanner graph for the corresponding label code of Λ/Λ', where Λ' is the orthogonal sublattice of Λ in $\{W_i\}_{i=1}^n$. In the following, we first address subproblem 2.

To simplify the presentation of the label code, we consider its isomorphic group defined over the alphabet $\mathcal{A} = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$, where $\mathbb{Z}_{g_i} = \{0, 1, \ldots, g_i - 1\}$. This is denoted by $\mathbf{G}(\Lambda)$. The dual $\mathbf{G}^*$ of $\mathbf{G}$ is also defined over $\mathcal{A}$. It consists of those codewords $\mathbf{c}^* = (c_1^*, \ldots, c_n^*) \in \mathcal{A}$ such that $\sum_{i=1}^n c_i^* c_i / g_i \in \mathbb{Z}$, $\forall \mathbf{c} = (c_1, \ldots, c_n) \in \mathbf{G}$, where multiplications and divisions are performed in the field of real numbers. It can be seen that $\mathbf{G}^*$ is also an abelian group with order $|\mathbf{G}^*| = |\mathcal{A}|/|\mathbf{G}|$. The label code $\mathbf{G}$ is therefore fully described by the following set of check equations:

$$\sum_{i=1}^n b_{ji} c_i / g_i \in \mathbb{Z}, \; j = 1, \ldots, r, \tag{1}$$

where $\mathbf{b}_1, \ldots, \mathbf{b}_r$ form a set of generators for $\mathbf{G}^*$. The problem of finding a simple Tanner graph for $\mathbf{G}$ is thus reduced to the problem of finding an appropriate set of generators for $\mathbf{G}^*$. A good criterion could be to find a minimal set of generators with minimum number of nonzero coordinates. This in turn, minimizes the number of check equations and the number of edges in the Tanner graph, respectively.

Regarding subproblem 1, we consider $|\mathcal{A}| = \prod_{i=1}^n g_i = |\mathbf{G}||\mathbf{G}^*|$ as the measure of complexity for the label code. Note that g_i, which is the alphabet size at position i of $\mathbf{G}$, plays an important role in the graph-based decoding complexity of $\mathbf{G}$.

Theorem 1 *Let a lattice Λ have a label code $\mathbf{G}$ in the graph coordinate system $\mathcal{S}$. Then $\mathbf{G}^*$ is the label code of the dual lattice Λ^* in $\mathcal{S}$.*

Theorem 2 *For any lattice Λ, and in any graph coordinate system,*

$$g_i \geq [\gamma(\Lambda)\gamma(\Lambda^*)]^{1/2}, \; i = 1, \ldots, n, \tag{2}$$

where γ denotes the coding gain. For each i, the bound is achieved iff both Λ and Λ^* have a vector of minimum length along the graph coordinate i.

The lower bound of (2) results in $\sum_{i=1}^n g_i/n \geq [\gamma(\Lambda)\gamma(\Lambda^*)]^{1/2}$ which for many interesting lattices, improves over the previously known result of $\sum_{i=1}^n g_i/n \geq \gamma(\Lambda)^{1/2}$, [4]. In particular, for iso-dual lattices, we obtain $\sum_{i=1}^n g_i/n \geq \gamma(\Lambda)$.

Corollary 1 *For any lattice Λ, and in any graph coordinate system,*

$$|\mathcal{A}| \geq [\gamma(\Lambda)\gamma(\Lambda^*)]^{n/2}, \tag{3}$$

where the bound is achieved iff both Λ and Λ^* have n mutually orthogonal vectors of minimum length along the graph coordinates.

For self-dual lattices, Theorem 1 implies that $\mathbf{G}$ is self-dual, and thus minimizing $|\mathcal{A}|$ results in the minimum value for $|\mathbf{G}| = |\mathbf{G}^*| = |\mathcal{A}|^{1/2}$. Based on the results of [1], it can be seen that for many self-dual lattices, such as the Leech lattice and the Barnes-Wall lattices BW_n, $n = 2^m$, m odd, the lower bounds (2) and (3) are achieved.

References

[1] A. H. Banihashemi and I. F. Blake, "Trellis complexity and minimal trellis diagrams of lattices," to appear in *IEEE Trans. Inform. Theory*, Sept. 1998.

[2] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. 8, pp. 21-28, Jan. 1962.

[3] R. M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533-547, Sept. 1981.

[4] V. Tarokh and I. F. Blake, "Trellis complexity versus the coding gain of lattices I," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1796-1807, Nov. 1996.

[5] V. Tarokh, "Minimal Tanner graphs for block codes and lattices," *Proc. 5th Can. Workshop on Inform. Theory*, 1997.

[6] "Special issue on concatenated coding techniques and iterative decoding: sailing toward channel capacity," *IEEE JSAC*, vol. 16, Feb. 1998.

0-7803-5000-6/98/$10.00