

# Tanner Graphs for Group Block Codes and Lattices: Construction and Complexity

by

Amir H. Banihashemi  
Department of Systems and Computer Engineering  
Carleton University  
Ottawa, Ontario, Canada K1S 5B6

(This has been a joint work with Professor Frank Kschischang)

# Table of Contents

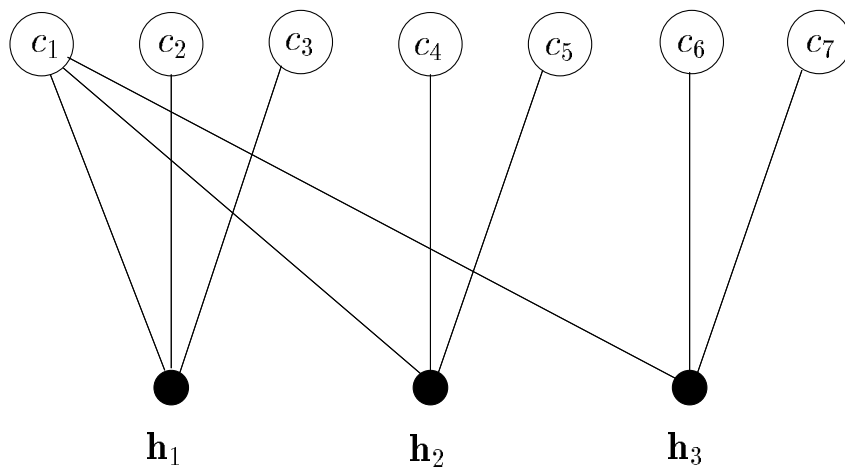
- **Introduction**
- **Tanner graph (TG) construction**
- **Generalized construction A**
- **TG complexity of codes and lattices**
- **Concluding remarks**

## Introduction

- **Tanner (1981) generalized Gallager's LDPC codes (1962) to codes defined by general bipartite graphs.**
- **Tanner also devised efficient decoding algorithms.**
- **Wiberg, Loeliger and Kötter (1996) extended Tanner graphs to include *hidden nodes*, and thus to cover trellis diagrams as a special case.**
- **Many well-known decoding algorithms in communications such as VA, BCJR, SOVA, and the decoding algorithm for turbo codes can now be considered as special cases of Tanner's algorithms applied to a trellis.**

• **Tanner graph for a linear block code:**

$$\mathbf{c}H^T = \mathbf{0} \quad , \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} .$$



• **Tanner graph for Abelian group block codes:**

- Without loss of generality, we consider a subgroup  $L$  of the alphabet sequence space  $\mathbf{G} = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$ .
- The character group  $\hat{\mathbf{G}}$  of  $\mathbf{G}$  is the group of all homomorphisms  $\psi : \mathbf{G} \rightarrow \mathbb{R}_{[0,1]}$  under the operation defined by  $(\psi_1 \circ \psi_2)(\mathbf{a}) = \psi_1(\mathbf{a}) + \psi_2(\mathbf{a}), \forall \mathbf{a} \in \mathbf{G}$ .
- The inner product  $\langle \cdot, \cdot \rangle : \hat{\mathbf{G}} \times \mathbf{G} \rightarrow \mathbb{R}_{[0,1]}$  is defined for every pair  $(\psi, \mathbf{a})$  by  $\langle \psi, \mathbf{a} \rangle = \psi(\mathbf{a})$ .
- Elements  $\psi \in \hat{\mathbf{G}}$  and  $\mathbf{a} \in \mathbf{G}$  are called orthogonal if  $\langle \psi, \mathbf{a} \rangle = 0$ .
- $\hat{\mathbf{G}} \cong \mathbf{G}$ .
- For any isomorphism  $\Phi$  between  $\hat{\mathbf{G}}$  and  $\mathbf{G}$ , we define a pairing  $(\cdot, \cdot)_{\Phi} : \mathbf{G} \times \mathbf{G} \rightarrow \mathbb{R}_{[0,1]}$  by  $(\mathbf{c}, \mathbf{a})_{\Phi} = \langle \Phi(\mathbf{c}), \mathbf{a} \rangle$ .
- Then
 
$$\begin{aligned} (\mathbf{c}, \mathbf{a})_{\Phi} &= \frac{c_1 a_1 i_1}{g_1} + \frac{c_2 a_2 i_2}{g_2} + \cdots + \frac{c_n a_n i_n}{g_n} \pmod{1} \\ &\stackrel{\Delta}{=} (\mathbf{c}, \mathbf{a})_{(i_1, \dots, i_n)}. \end{aligned}$$
- Both the pairing and the notion of orthogonality (dual code) depend on  $\Phi$ .

- Consider  $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ . There are only 4 pairings:

$$\begin{aligned}(\mathbf{x}, \mathbf{y})_{(1,1)} &= \frac{x_1 y_1}{3} + \frac{x_2 y_2}{3} \\(\mathbf{x}, \mathbf{y})_{(1,2)} &= \frac{x_1 y_1}{3} + \frac{2x_2 y_2}{3} \\(\mathbf{x}, \mathbf{y})_{(2,1)} &= \frac{2x_1 y_1}{3} + \frac{x_2 y_2}{3} \\(\mathbf{x}, \mathbf{y})_{(2,2)} &= \frac{2x_1 y_1}{3} + \frac{2x_2 y_2}{3} .\end{aligned}$$

**We have  $(11, 12)_{(1,1)} = 0$ , while  $(11, 12)_{(1,2)} \neq 0$ .**

**Also for the subgroup  $L = \{00, 11, 22\}$  of  $G$ ,**

**$L_{(1,1)}^* = L_{(2,2)}^* = \{00, 12, 21\}$ , and  $L_{(1,2)}^* = L_{(2,1)}^* = \{00, 11, 22\}$ .**

- Let  $C^* = \{c_1^*, \dots, c_r^*\}$  be a generating set for  $L_{\Phi}^*$ . Then

$$(c_i^*, c)_{\Phi} = 0, \quad i = 1, \dots, r,$$

**fully describes  $c \in L$ , and can be used to construct a Tanner graph for  $L$ .**

- **Does the choice of the pairing, or equivalently, the choice of the dual code, influence the Tanner graph in any way?**

- **Theorem 1** *The TG complexity for a group code*  
 $L \subset G = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$  *is independent of the choice of the pairing.*
- **We choose the pairing**  $(, )_{(1, \dots, 1)} : G \times G \longrightarrow \mathbb{R}_{[0,1]}$ , **and the corresponding dual**  $L^*_{(1, \dots, 1)} \subset G$  **to construct a TG for L.**
- **For**  $L \subset G = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$ , **the dual group  $L^* \subset G$  is defined by**

$$L^* = L^*_{(1, \dots, 1)} = \{c^* \in G : \sum_{i=1}^n c_i^* c_i / g_i = 0 \pmod{1}, \forall c \in L\} .$$

- **L is fully described by**

$$\sum_{i=1}^n c_{ki}^* c_i / g_i = 0 \pmod{1}, \quad k = 1, \dots, r, \quad (1)$$

**or equivalently by**

$$c \operatorname{diag}\left(\frac{1}{g_1}, \dots, \frac{1}{g_n}\right) (C^*)^T = 0 \pmod{1}, \quad (2)$$

**where**  $c = (c_1, \dots, c_n) \in L$ , **and**  $C^* = \{c_1^*, \dots, c_r^*\}$  **is a generator for**  $L^*$ .

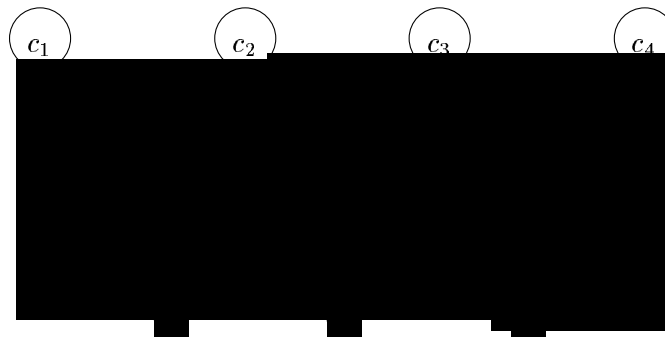
– **Example 1** Let  $G = \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2$ , and

$$L = \left\{ \begin{array}{l} 0000, 0031, 0220, 0251, 0440, 0411, \\ 1300, 1331, 1520, 1551, 1140, 1111 \end{array} \right\}.$$

*Then,*

$$L^* = \left\{ \begin{array}{l} 0000, 0240, 0420, 1511, 1151, 0031, \\ 1300, 1331, 0451, 1540, 1120, 0211 \end{array} \right\}.$$

*A generator for  $L^*$  is  $\{1151, 0240, 0031\}$ .*

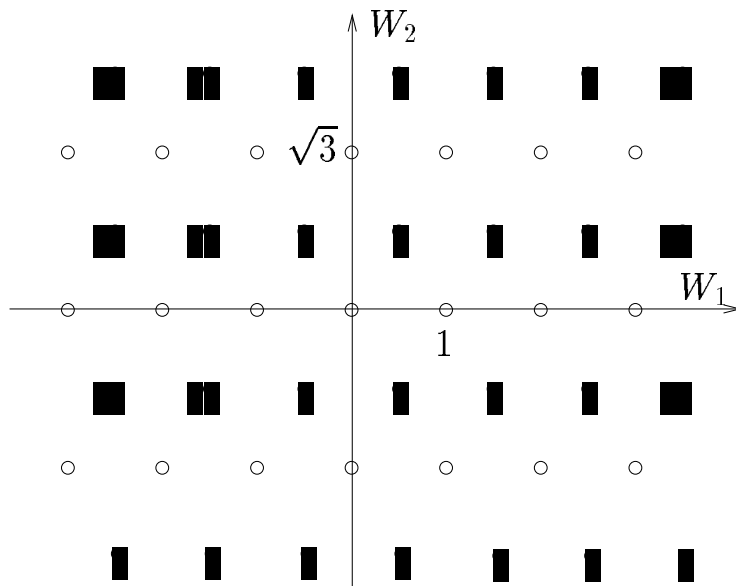


$$3c_1 + c_2 + 5c_3 + 3c_4 \in 6\mathbb{Z} \quad c_2 + 2c_3 \in 3\mathbb{Z} \quad c_3 + c_4 \in 2\mathbb{Z}$$

- **Finding a simple TG for  $L$   $\longrightarrow$  Finding an appropriate generator for  $L^*$ .**
- **Given  $L$ , finding a generator for  $L^*$  using exhaustive search is computationally infeasible!**

- **Tanner graph for lattices:**

- A lattice is a discrete, additive subgroup  $\Lambda \subset \mathbb{R}^m$ .



- Dual lattice:

$$\Lambda^* = \{ \mathbf{x} \in \text{span}(\Lambda) \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{y} \in \Lambda \} .$$

- Label code of  $\Lambda$ ,  $L(\Lambda)$ , is isomorphic to  $\Lambda/\Lambda'$ , where  $\Lambda'$  is a rectangular sublattice of  $\Lambda$ , and is defined as a subgroup of  $\mathbf{G} = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \dots \times \mathbb{Z}_{g_n}$  under component-wise addition.
- $L(\Lambda)$  represents the dynamical structure of  $\Lambda$  with respect to  $\Lambda'$ .

- **Generalized construction A (GCA):**

- Let  $\mathbf{L} \subset \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ . We construct

$$\Lambda = \Lambda' + \mathbf{L} \operatorname{diag}\left(\frac{a_1}{g_1}, \dots, \frac{a_n}{g_n}\right),$$

where  $\Lambda' = a_1\mathbb{Z} \oplus \cdots \oplus a_n\mathbb{Z}$ .

- The construction reduces to “construction A” if  $g_i = a_i = 2, \forall i$ .
- $\mathbf{L}$  is the label code of  $\Lambda$ .
- **Example 2** For  $\mathbf{L} = \{00, 11\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2$ , maximizing the coding gain of  $GCA(\mathbf{L})$  with respect to  $a_1, a_2$  results in the hexagonal lattice with coding gain  $2/\sqrt{3}$ . This is achieved for  $\{a_1, a_2\} = \{1, \sqrt{3}\}$  or  $\{1, 1/\sqrt{3}\}$ .

*For the same code, construction A results in a lattice with unit coding gain.*

- **Theorem 2**  $[L(\Lambda)]^* = L(\Lambda^*)$ .

- An efficient algorithm for finding a generator for  $\mathbf{L}^*$  is developed.

$$\mathbf{L} \xrightarrow[\substack{\text{GCA} \\ a_i = g_i, \forall i}]{\phantom{\text{GCA}}} \Lambda \xrightarrow{B^* = (B^{-1})^T} \Lambda^* \xrightarrow{\Phi^*} \mathbf{L}^*$$

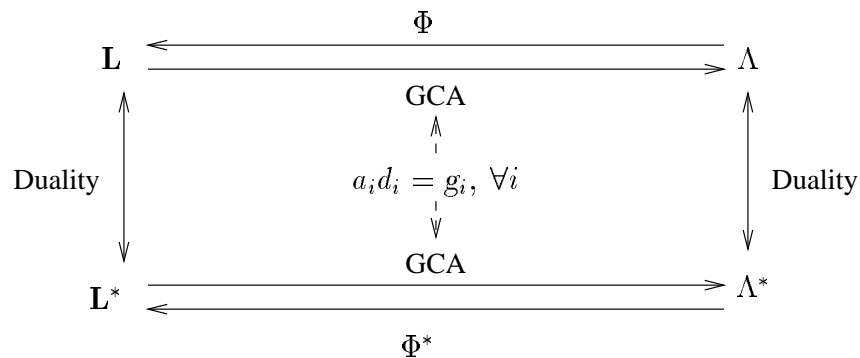
- **Example 1 (Cont.)** We obtain the following matrices as a basis for  $\Lambda$  and a generator for  $\mathbf{L}$ :

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 4 & -2 & 0 \\ 0 & 0 & 3 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 0 & 3 & 1 \end{pmatrix}.$$

We then have:

$$B^* = \begin{pmatrix} \frac{1}{2} & -\frac{1}{6} & -\frac{1}{3} & 1 \\ 0 & \frac{1}{3} & \frac{2}{3} & -2 \\ 0 & 0 & -\frac{1}{2} & \frac{3}{2} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad C^* = \begin{pmatrix} 1 & 5 & 4 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & 3 & 1 \end{pmatrix}.$$

- Relationships among a group code, its GCA lattice, and their duals:



# Tanner graph complexity

- **Group codes:**

- A TG is called **minimal** if it minimizes both the number of check nodes and the number of edges.

- **Example 1 (Cont.)** We have

$$\mathbf{L}^* = \left\{ \begin{array}{l} 0000, 0240, 0420, 1511, 1151, 0031, \\ 1300, 1331, 0451, 1540, 1120, 0211 \end{array} \right\}.$$

$\mathbf{L}^*$  is not cyclic. An optimal generator is  $\{1120, 0031\}$ .

$$\begin{array}{cccc} \textcircled{c_1} \in \mathbb{Z}_2 & \textcircled{c_2} \in \mathbb{Z}_6 & \textcircled{c_3} \in \mathbb{Z}_6 & \textcircled{c_4} \in \mathbb{Z}_2 \end{array}$$



$$3c_1 + c_2 + 2c_3 = 0 \text{ mod. } 6 \quad c_3 + c_4 = 0 \text{ mod. } 2$$

• **Lattices:**

– **Low-complexity TG:**

1. **low-complexity label code**
2. **low-complexity TG for the code of part 1**

– **Measure of label code complexity:**

$$|\mathbf{G}| = \prod_{i=1}^n g_i = |\mathbf{L}||\mathbf{L}^*|.$$

– **Theorem 3** *For any lattice  $\Lambda$ , and in any graph coordinate system,*

$$g_i \geq \lceil \gamma(\Lambda)^{1/2} \gamma(\Lambda^*)^{1/2} \rceil, \quad i = 1, \dots, n,$$
$$|\mathbf{G}| \geq \lceil \gamma(\Lambda)^{1/2} \gamma(\Lambda^*)^{1/2} \rceil^n.$$

– **The bounds are achieved for many well-known lattices such as the Leech lattice, the Barnes-Wall lattices  $BW_n$ ,  $n = 2^m$ ,  $m$  odd,  $D_n, D_n^*$ ,  $n \geq 3$ , and  $E_7, E_7^*$ .**

- For many other important lattices, the bounds are improved:

$\Lambda$	$BW_n, n = 2^m, m \text{ even}$	$K_{12}$	$E_6, E_6^*$
$g_i \geq \lceil (\gamma\gamma^*)^{1/2} \rceil$	$\sqrt{n/2}$	3	2
<b>Improved bound</b>	$\sqrt{n}$	4	$\{2^4, 4^2\}$
$ \mathbf{G}  \geq (\lceil (\gamma\gamma^*)^{1/2} \rceil)^n$	$(n/2)^{n/2}$	$3^{12}$	64
<b>Improved bound</b>	$n^{n/2}$	$4^{12}$	256

- Strictly optimal coordinate systems, in which the bounds are achieved, are found.
- Tanner graph structure of many important lattices in (strictly) optimal coordinate systems is studied.
- It is shown that for many important lattices, such as  $BW_n, n = 2^m, m \geq 3$ , and  $E_n, E_n^*, n = 6, 7, 8$ , the optimal label codes cannot be supported by cycle-free Tanner graphs.
- This supports the conjecture that “good lattices cannot be represented by cycle-free TGs”.

## Concluding remarks

- **Construction and complexity of Tanner graphs for Abelian group block codes and lattices were discussed.**
- **“Generalized construction A” for lattices was introduced, and was used to develop an efficient algorithm for finding a generator for the dual of an arbitrary group code.**
- **Tight lower bounds on the label code complexity of lattices were derived.**
- **For many important lattices, the minimal label codes, which achieve the lower bounds, cannot be supported by cycle-free Tanner graphs.**
- **Future research:**
  - **Which Tanner graphs are good for decoding purposes?**
  - **Conjecture: Good lattices cannot be supported by cycle-free Tanner graphs.**
  - **Construction of dense lattices with low iterative decoding complexity in high dimensions.**