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:

\[ cH^T = 0 \quad , \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} . \]
Tanner graph for Abelian group block codes:

- Without loss of generality, we consider a subgroup \(L\) of the alphabet sequence space \(G = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}\).

- The character group \(\hat{G}\) of \(G\) is the group of all homomorphisms \(\psi : G \rightarrow \mathbb{R}_{[0,1]}\) under the operation defined by
  \[(\psi_1 \circ \psi_2)(a) = \psi_1(a) + \psi_2(a), \forall a \in G.\]

- The inner product \(\langle \cdot, \cdot \rangle : \hat{G} \times G \rightarrow \mathbb{R}_{[0,1]}\) is defined for every pair \((\psi, a)\) by \(\langle \psi, a \rangle = \psi(a)\).

- Elements \(\psi \in \hat{G}\) and \(a \in G\) are called orthogonal if \(\langle \psi, a \rangle = 0\).

- \(\hat{G} \cong G\).

- For any isomorphism \(\Phi\) between \(\hat{G}\) and \(G\), we define a pairing \((\cdot, \cdot)_\Phi : G \times G \rightarrow \mathbb{R}_{[0,1]}\) by \((c, a)_\Phi = \langle \Phi(c), a \rangle\).

- Then
  \[(c, a)_\Phi = \frac{c_{a_1} i_1}{g_1} + \frac{c_{a_2} i_2}{g_2} + \cdots + \frac{c_{a_n} i_n}{g_n} \mod 1
  \]
  \(\triangleq (c, a)_{(i_1, \ldots, i_n)}\).

- 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:

\[
\begin{align*}
(x, y)_{(1,1)} &= \frac{x_1 y_1}{3} + \frac{x_2 y_2}{3} \\
(x, y)_{(1,2)} &= \frac{x_1 y_1}{3} + \frac{2x_2 y_2}{3} \\
(x, y)_{(2,1)} &= \frac{2x_1 y_1}{3} + \frac{x_2 y_2}{3} \\
(x, y)_{(2,2)} &= \frac{2x_1 y_1}{3} + \frac{2x_2 y_2}{3}.
\end{align*}
\]

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 \( C^* = \{c^*_1, \ldots, c^*_r\} \) be a generating set for \( L^*_\Phi \). Then

\[
(c_i^*, c)_{\Phi} = 0, \ i = 1, \ldots, r,
\]

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 $(\cdot, \cdot)_{(1, \ldots, 1)} : G \times G \rightarrow \mathbb{R}_{[0,1]}$, and the corresponding dual $L^*_{(1, \ldots, 1)} \subset G$ 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
\[
L^* = L^*_{(1, \ldots, 1)} = \{ c^* \in G : \sum_{i=1}^{n} c_i^* c_i / g_i = 0 \mod 1, \forall c \in L \}.
\]

$L$ is fully described by
\[
\sum_{i=1}^{n} c_k^* c_i / g_i = 0 \mod 1, \; k = 1, \ldots, r,
\]

or equivalently by
\[
c \diag \left( \frac{1}{g_1}, \ldots, \frac{1}{g_n} \right) (C^*)^T = 0 \mod 1,
\]

where $c = (c_1, \ldots, c_n) \in L$, and $C^* = \{ c_1^*, \ldots, c_r^* \}$ 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 

\[ L = \{ 0000, 0031, 0220, 0251, 0440, 0411, 1300, 1331, 1520, 1551, 1140, 1111 \}. \]

Then, 

\[ L^* = \{ 0000, 0240, 0420, 1511, 1151, 0031, 1300, 1331, 0451, 1540, 1120, 0211 \}. \]

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

Finding a simple TG for $L$ \rightarrow 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 $\Lambda \subset \mathbb{R}^m$.

![Tanner graph for lattices]

  - **Dual lattice:**

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

  - **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 $G = \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$ under component-wise addition.

  - $L(\Lambda)$ represents the dynamical structure of $\Lambda$ with respect to $\Lambda'$.
• Generalized construction A (GCA):
  
  – Let \( L \subset \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n} \). We construct
    \[
    \Lambda = \Lambda' + L \operatorname{diag}(\frac{a_1}{g_1}, \ldots, \frac{a_n}{g_n}),
    \]
    where
    \[
    \Lambda' = a_1 \mathbb{Z} \oplus \cdots \oplus a_n \mathbb{Z}.
    \]
  – The construction reduces to “construction A” if \( g_i = a_i = 2, \ \forall i \).
  – \( L \) is the label code of \( \Lambda \).
  – Example 2 For \( L = \{00, 11\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2 \), maximizing the coding gain of \( \text{GCA}(L) \) 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 \( \{1, 1/\sqrt{3}\} \).

  \textit{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 \( L^* \) is developed.

\[
L \xrightarrow{\text{GCA}} \Lambda \xrightarrow{B^* = (B^{-1})^T} \Lambda^* \xrightarrow{\Phi^*} L^*
\]

\( a_i = g_i, \ \forall i \)

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

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

We then have:

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

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

\[
\Phi\quad \Phi^*\quad \text{GCA}\quad \text{GCA}\quad \Lambda\quad \Lambda^*
\]

\[
\text{Duality}\quad a_i d_i = g_i, \ \forall i\quad \text{Duality}
\]

(11)
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
  
  \[ L^* = \left\{ 0000, \ 0240, \ 0420, \ 1511, \ 1151, \ 0031, \ 1300, \ 1331, \ 0451, \ 1540, \ 1120, \ 0211 \right\}. \]

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

\[
\begin{array}{cccc}
\odot \in \mathbb{Z}_2 & c_2 \in \mathbb{Z}_6 & c_3 \in \mathbb{Z}_6 & (c_4) \in \mathbb{Z}_2 \\
\end{array}
\]

\[ 3c_1 + c_2 + 2c_3 = 0 \text{ mod. 6} \quad c_3 + c_4 = 0 \text{ mod. 2} \]
**Lattices:**

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

- Measure of label code complexity:
  \[ |G| = \prod_{i=1}^{n} g_i = |L||L^*| \]

- **Theorem 3** For any lattice \( \Lambda \), and in any graph coordinate system,
  \[ g_i \geq \left\lceil \gamma(\Lambda)^{1/2}\gamma(\Lambda^*)^{1/2} \right\rceil, \quad i = 1, \ldots, n \]
  \[ |G| \geq \left\lceil \gamma(\Lambda)^{1/2}\gamma(\Lambda^*)^{1/2} \right\rceil^n \]

- 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 \( E_7, E_8 \).
– For many other important lattices, the bounds are improved:

<table>
<thead>
<tr>
<th>$\Lambda$</th>
<th>$BW_n, n = 2^m, m$ even</th>
<th>$K_{12}$</th>
<th>$E_6, E_6^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_i \geq [(\gamma \gamma^*)^{1/2}]$</td>
<td>$\sqrt{n/2}$</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Improved bound</td>
<td>$\sqrt{n}$</td>
<td>4</td>
<td>${2^4, 4^2}$</td>
</tr>
<tr>
<td>$</td>
<td>G</td>
<td>\geq [(\gamma \gamma^*)^{1/2}]^n$</td>
<td>$(n/2)^n/2$</td>
</tr>
<tr>
<td>Improved bound</td>
<td>$n^{n/2}$</td>
<td>$4^{12}$</td>
<td>256</td>
</tr>
</tbody>
</table>

– 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”.

(14)
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 be cycle-free Tanner graphs.
  - Construction of dense lattices with low iterative decoding complexity in high dimensions.