

Lecture 11: Graph codes

Course instructor: Alexey Frolov

`al.frolov@skoltech.ru`

Teaching Assistant: Stanislav Kruglik

`stanislav.kruglik@skolkovotech.ru`

February 28, 2017

- 1 LDPC codes
- 2 Expander graphs and expander codes

- 1 LDPC codes
- 2 Expander graphs and expander codes

- LDPC codes were invented by Robert G. Gallager in the 1960s and forgotten for three decades.
- After Turbo codes were invented 1993, LDPC codes found new attention



Robert G. Gallager

- LDPC codes are defined with use of *sparse* parity-check matrix, i.e. the percentage of 1s in the parity check matrix for a LDPC code is low.
- A regular LDPC code has the property that:
 - every code digit is contained in the same number of equations,
 - each equation contains the same number of code symbols.
- An irregular LDPC code relaxes these conditions.

Definition by parity-check matrix

Definition by parity-check matrix: [Gallager, '62]

$$H = \begin{array}{cccccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}$$

15 × 20

Code: $\{\mathbf{v} \mid \mathbf{v}\mathbf{H}^T = \mathbf{0}\}$
(null space of a **sparse**
parity-check matrix \mathbf{H})

Definition by parity-check matrix

Definition by parity-check matrix: [Gallager, '62]

$H =$

0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	1
0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0
0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0
1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0
0	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1

15 × 20

Code: $\{\mathbf{v} \mid \mathbf{v}\mathbf{H}^T = \mathbf{0}\}$
(null space of a **sparse** parity-check matrix \mathbf{H})

Regular LDPC code:

Column weight: $J = 3$

Row weight: $K = 4$

$$R \geq 1 - \frac{J}{K}$$

Definition by parity-check matrix

Definition by parity-check matrix: [Gallager, '62]

$H =$

0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	1
0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0
0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	1	0	0
1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
0	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1

15 × 20

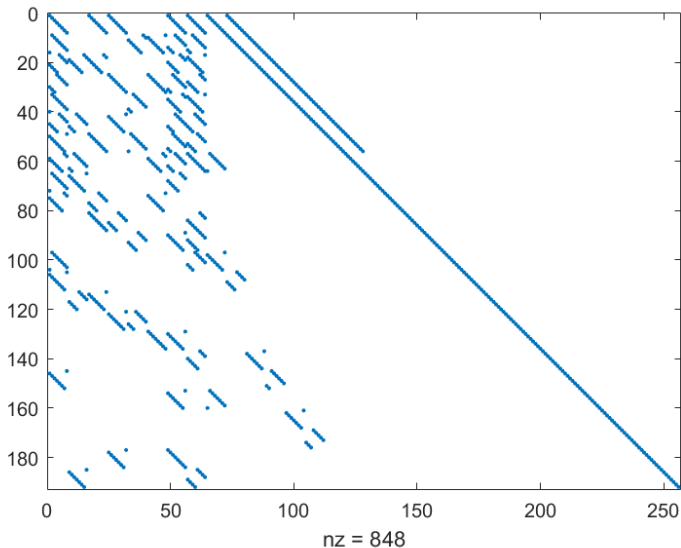
Code: $\{\mathbf{v} \mid \mathbf{v}\mathbf{H}^T = \mathbf{0}\}$
(null space of a **sparse**
parity-check matrix \mathbf{H})

Regular LDPC code:
Column weight: $J = 3$
Row weight: $K = 4$

$$R \geq 1 - \frac{J}{K}$$

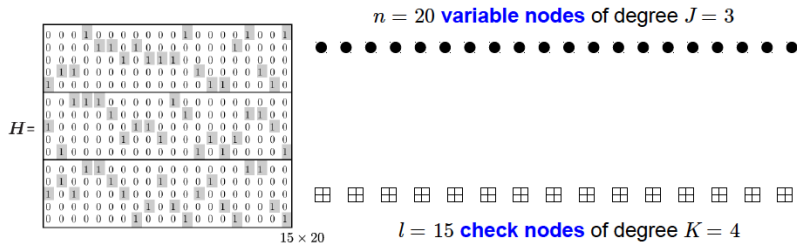
- If the row and column weights J and K are not constant, then the LDPC code is **irregular** (more later)

Irregular LDPC example, PCM with $R = 1/4$



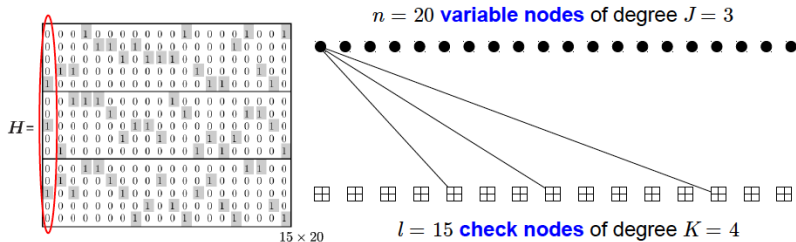
Tanner graph

Representation by bi-partite graph: [Tanner, '81]



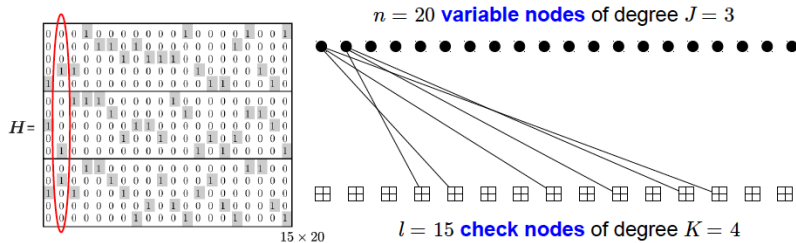
Tanner graph

Representation by bi-partite graph: [Tanner, '81]



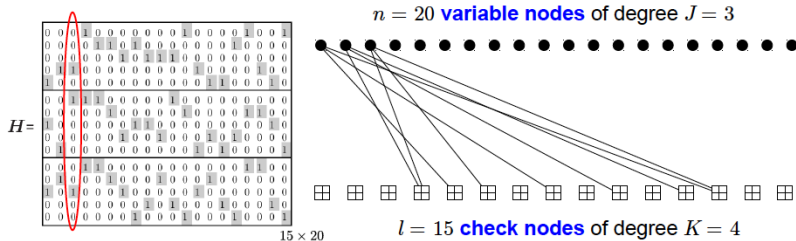
Tanner graph

Representation by bi-partite graph: [Tanner, '81]



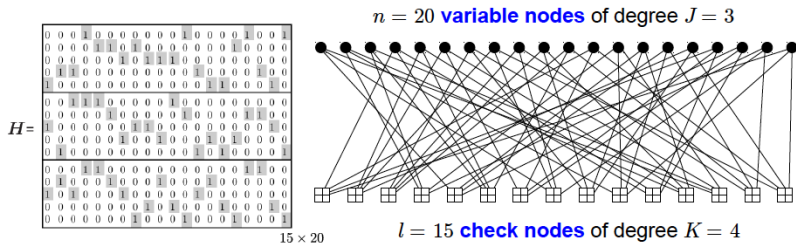
Tanner graph

Representation by bi-partite graph: [Tanner, '81]



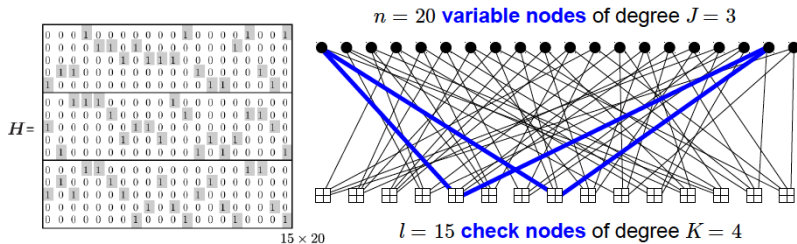
Tanner graph

Representation by bi-partite graph: [Tanner, '81]



Tanner graph

Representation by bi-partite graph: [Tanner, '81]



- Tanner graphs typically contain **cycles** (length 4 cycle highlighted above)
- The **girth** of a Tanner graph is the length of the shortest cycle (4 in this example)

Gallager's ensemble of LDPC codes

Ensemble $\mathcal{E}(N, K, J)$

$$\mathbf{H} = \begin{pmatrix} \pi_1(\mathbf{H}_b) \\ \pi_2(\mathbf{H}_b) \\ \vdots \\ \pi_J(\mathbf{H}_b) \end{pmatrix}_{\ell b \times bn_0}$$

where

$$\mathbf{H}_b = \begin{pmatrix} 11\dots 1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & 11\dots 1 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & 11\dots 1 \end{pmatrix}_{b \times bK}$$

Theorem (Gallager'62)

For any $J > 2$ there exists $\delta^(K, J) > 0$ such that:*

- there are codes in the ensemble $\mathcal{E}(N, K, J)$ for which the following inequality holds*

$$d(\mathcal{C}) \geq (\delta^* - \varepsilon)N \quad (1)$$

- the number of such codes ($G(N, K, J)$) satisfy the following relation*

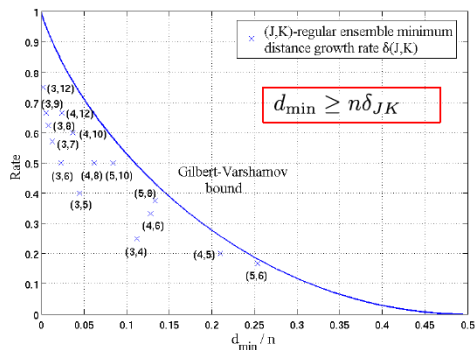
$$\lim_{N \rightarrow \infty} \frac{G(N, K, J)}{|\mathcal{E}(N, K, J)|} = 1.$$

The value δ^ is the smallest positive root of equation*

$$(J-1)h(\delta) + J \max_{s>0} \left(\delta \log \delta - \frac{1}{K} g_0(s, K) \right) = 0.$$

Lower bound on the minimum distance

- δ_{JK} is called the **typical minimum distance ratio**, or **minimum distance growth rate**, of a code ensemble



Upper bound on the minimum distance

$$\mathbf{H} = \begin{array}{|c|c|} \hline & \begin{array}{c} \xleftarrow{N} \qquad \qquad \qquad \xrightarrow{tN} \\ \hline \end{array} \\ \hline \mathbf{H}_1 & \mathbf{0} \\ \hline \mathbf{A} & \mathbf{H}_2 \\ \hline \end{array}$$

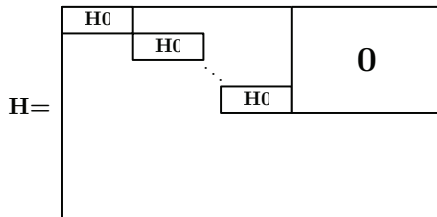
Lemma

Let the parity-check matrix \mathbf{H} of the code \mathcal{C} has a special form shown above, then

$$R(\mathcal{C}) \leq R(\mathcal{C}_1)(1 - \tau) + R(\mathcal{C}_2)\tau,$$

where the codes \mathcal{C}_1 and \mathcal{C}_2 correspond to parity-check matrices \mathbf{H}_1 and \mathbf{H}_2 .

Upper bound on the minimum distance



Theorem

Let \mathcal{C} be a generalized LDPC code of length N , rate R , minimum distance δN , with constituent $[n_0, R_0, d_0]$ code \mathcal{C}_0 . Then for sufficiently large N the following inequality holds

$$R(\mathcal{C}) \leq \min_{\frac{q}{q-1}\delta \leq \tau \leq 1} \left\{ R_0(1 - \tau) + R^*\left(\frac{\delta}{\tau}\right)\tau \right\} + o(1),$$

where $R^*(\delta)$ is any upper bound on the code rate.

Bit-flipping decoding algorithm

- If there exists a variable node, such that the number of unsatisfied check nodes is bigger than the number of satisfied check nodes \Rightarrow flip the bit.
- Continue until such variable nodes exist.

- 1 LDPC codes
- 2 Expander graphs and expander codes

Let $G = (V, E)$ be a graph with n vertices. Let us denote by

$$\Gamma(v) = \{u : (u, v) \in E\}$$

the neighbors of the vertex v and by

$$\Gamma(S) = \bigcup_{v \in S} \Gamma(v)$$

the neighbors of the vertex set S .

Definition

A graph G is called an (ω, α) -expander, if

$$\forall S \subset V, |S| \leq \omega n \Rightarrow \Gamma(S) > \alpha |S|.$$

In what follows we consider the following graph types:

- G – bipartite ($V = V_L \sqcup V_R$) (J, K) –regular,
 $\deg(v) = J, v \in V_L$ $\deg(v) = K, v \in V_R$.
- G – Δ –regular, $\deg(v) = \Delta$;

Lemma

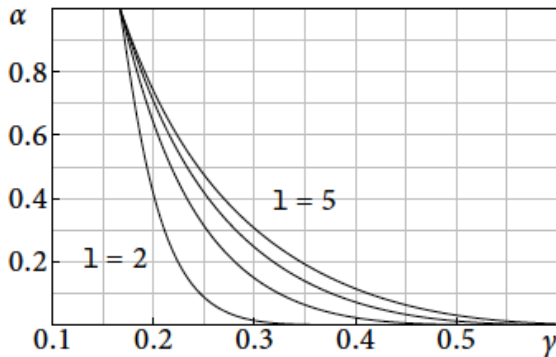
Let G be a graph chosen uniformly from the ensemble of (J, K) -regular bipartite graphs and let $n \rightarrow \infty$. For a given $\gamma \in [\frac{1}{K}, 1 - \frac{1}{J})$ let δ be the positive solution of the equation

$$\begin{aligned} \frac{J-1}{J}h(\delta) - \frac{1}{K}h(\delta\gamma K) \\ - \delta\gamma K h\left(\frac{1}{\gamma K}\right) = 0. \end{aligned}$$

Then for $0 < \delta' < \delta$ and $\beta = J(1 - \gamma) - 1$

$$\Pr(\{G \text{ is an } (J, K, \delta', J\gamma) \text{ expander}\}) \geq 1 - O(n^{-\beta}).$$

Expansion of random graph



Theorem

Let G be (J, K) regular bipartite graph, which is also $(\omega, \alpha = 3J/4)$ -expander. The algorithm is able to correct up to $\omega/2N$ errors.

Consider a regular graph. Associate check codes with vertexes and codeword bits with edges.

Lemma

Let $G = (V, E)$ be a Δ -regular graph with n vertexes and the second largest eigenvalue λ . Let $S \subset V$, then

$$e(S) \leq \frac{|S|}{2} \Delta \frac{|S|}{n} + \lambda \left(1 - \frac{|S|}{n} \right).$$

Consider \mathbf{f} :

$$\mathbf{f}(i) = -\frac{1}{|S|}, \quad i \in S$$

$$\mathbf{f}(i) = \frac{1}{n - |S|},$$

$$|(Af, f)| \leq \lambda(f, f).$$

$$(Af, f) = 2 \sum_{(i,j) \in E} f(i)f(j) = n_0 \sum_{i=1}^n f^2(i) - \sum_{(i,j) \in E} (f(i) - f(j))^2.$$

$$\sum_{i=1}^n f^2(i) = 1/|S| + 1/(n - |S|).$$

$$\sum_{(i,j) \in E} (f(i) - f(j))^2 = e(S, \bar{S})(1/|S| + 1/(n - |S|))^2.$$

$$2e(S) + e(S, \bar{S}) = n_0|S|.$$

Theorem

$$\delta(\mathcal{C}) \geq \left(\frac{\delta_0 + \frac{\lambda}{\Delta}}{1 - \frac{\lambda}{\Delta}} \right) \delta_0.$$

Choose underlying regular graph to be bipartite.

Thank you for your attention!