Low-Density Parity-Check (LDPC) Codes

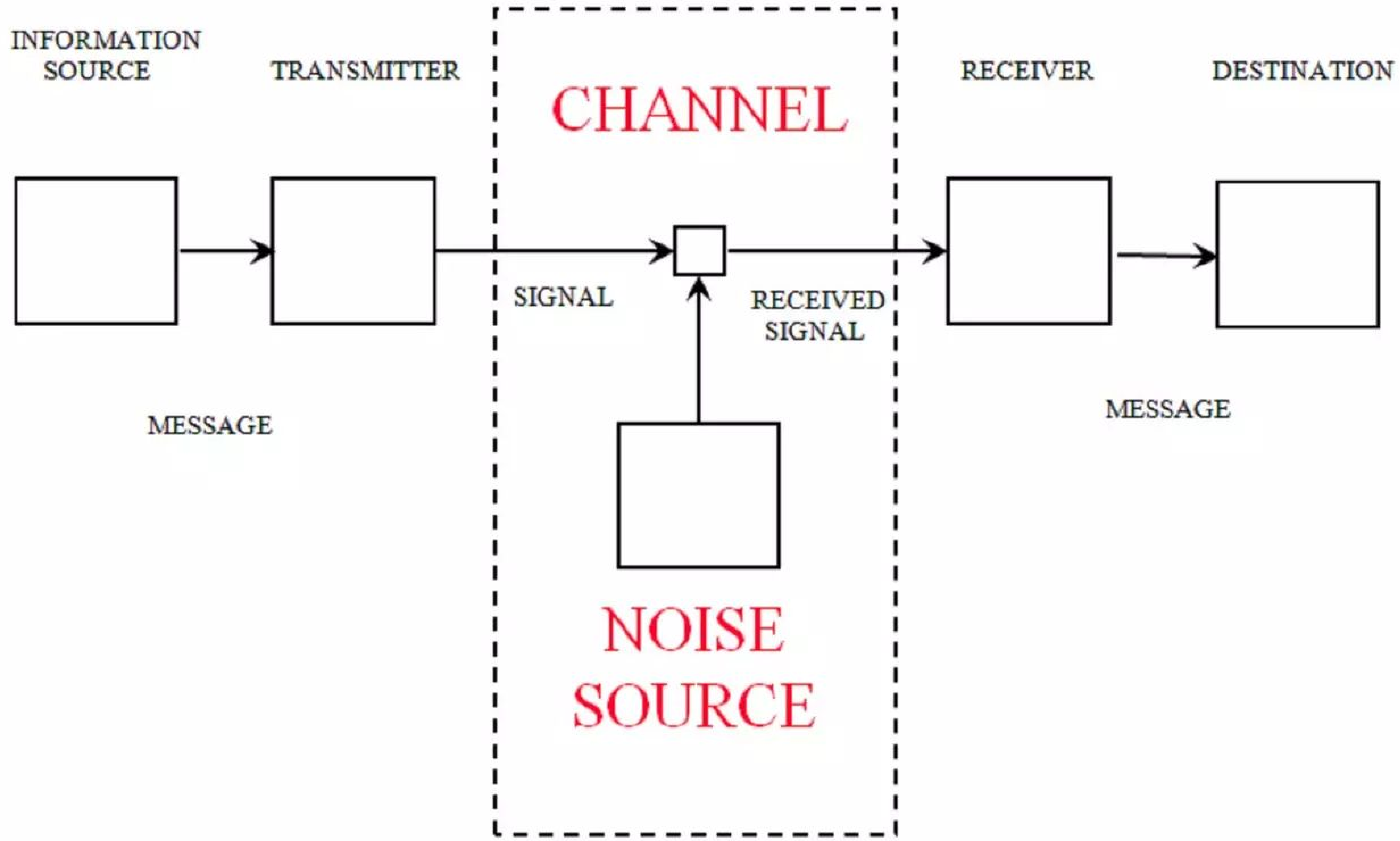
Sahar Foroughi Farsani

saharforoughi@gmail.com
Islamic Azad University of Najafabad
May, 2014

Contents

Contents

A Noisy Communication System



Shannon’s Coding Theorem

- In 1948, Claude Shannon, generally regarded as the father of the Information Age, published the paper: “A Mathematical Theory of Communications” whish laid the foundations of Information Theory.

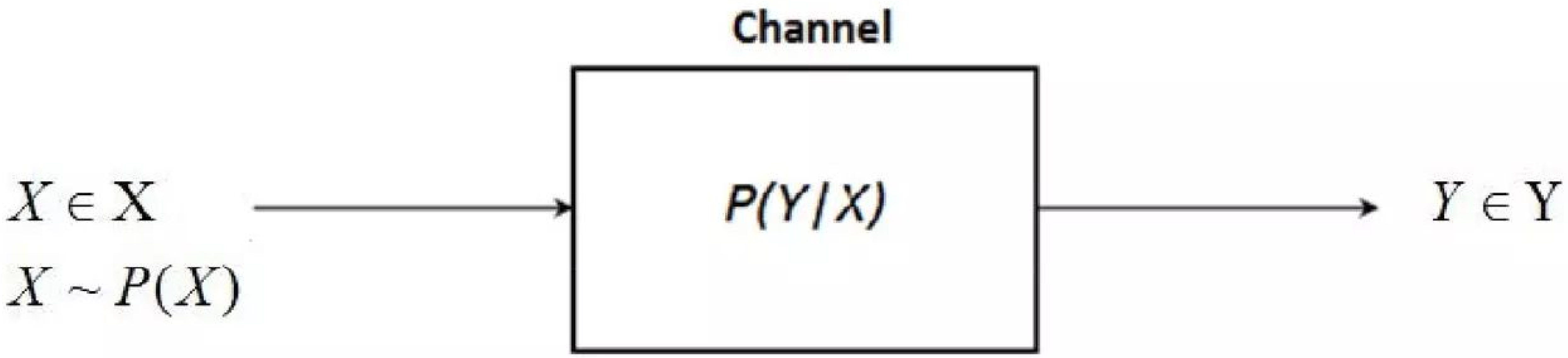
Claude Elwood Shannon
1916 - 2001

✓ Every communication channel is characterized by a single number C, called the channel capacity.

✓ It is possible to transmit information over this channel reliably (with probability of error → 0) if and only if:

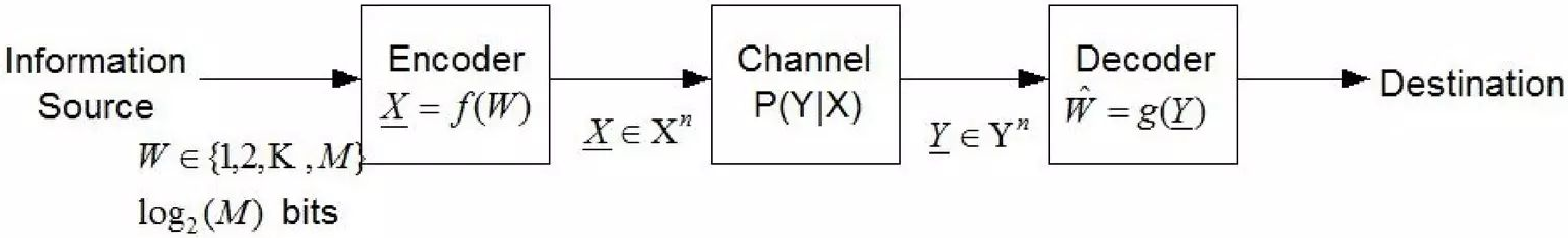
$$R \overset{def}{=} \frac{\#\,\text{information bits}}{\text{channel use}} < C$$

Discrete Memoryless Channel:



$$C = \max_{P(X)} I(X;Y) = \max_{P(X)} \sum_{X,Y} P(X)P(Y|X)\log_2\left(\frac{P(Y|X)}{\sum_X P(X)P(Y|X)}\right) \qquad \frac{bits}{channel\ use}$$

- Shannon introduced the concept of codes as ensembles of vectors that are to be transmitted.
- To achieve reliable communication, it is thus imperative to send input elements that are correlated. This leads to the concept of a code, defined as a (finite) set of vectors over the input alphabet.
- The code has a rate of k/n bits per channel use, or k/n bpc ($k=\log_2 M$).



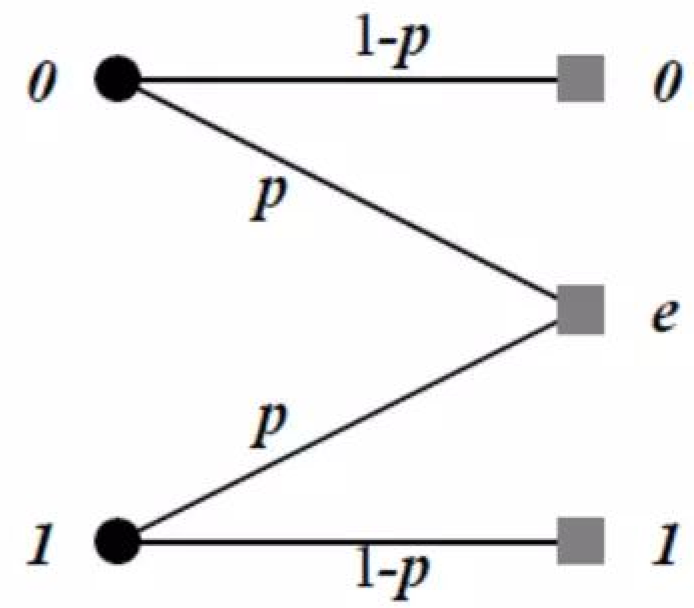
code rate:

$$R = \frac{\log_2(M)}{n} \quad \frac{\text{bits}}{\text{channel use}}$$

reliable transmission is possible if $R < C$

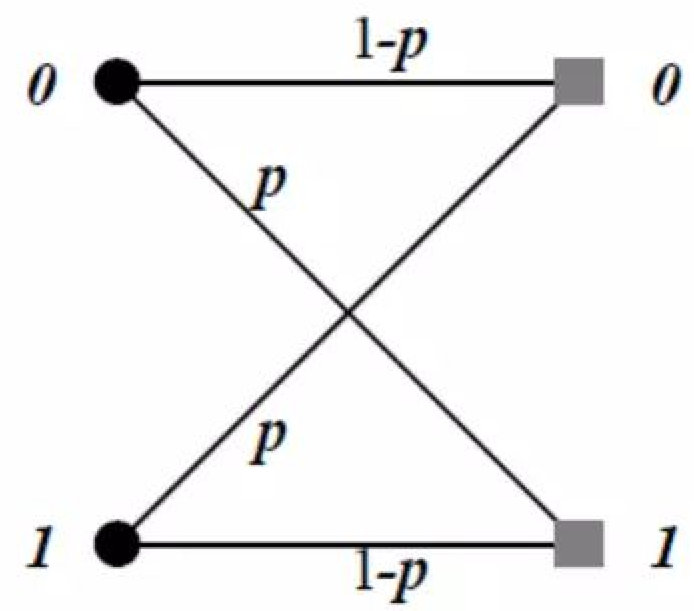
Common Channels

- Binary Erasure Channel (BEC)



$$C = 1 - p$$

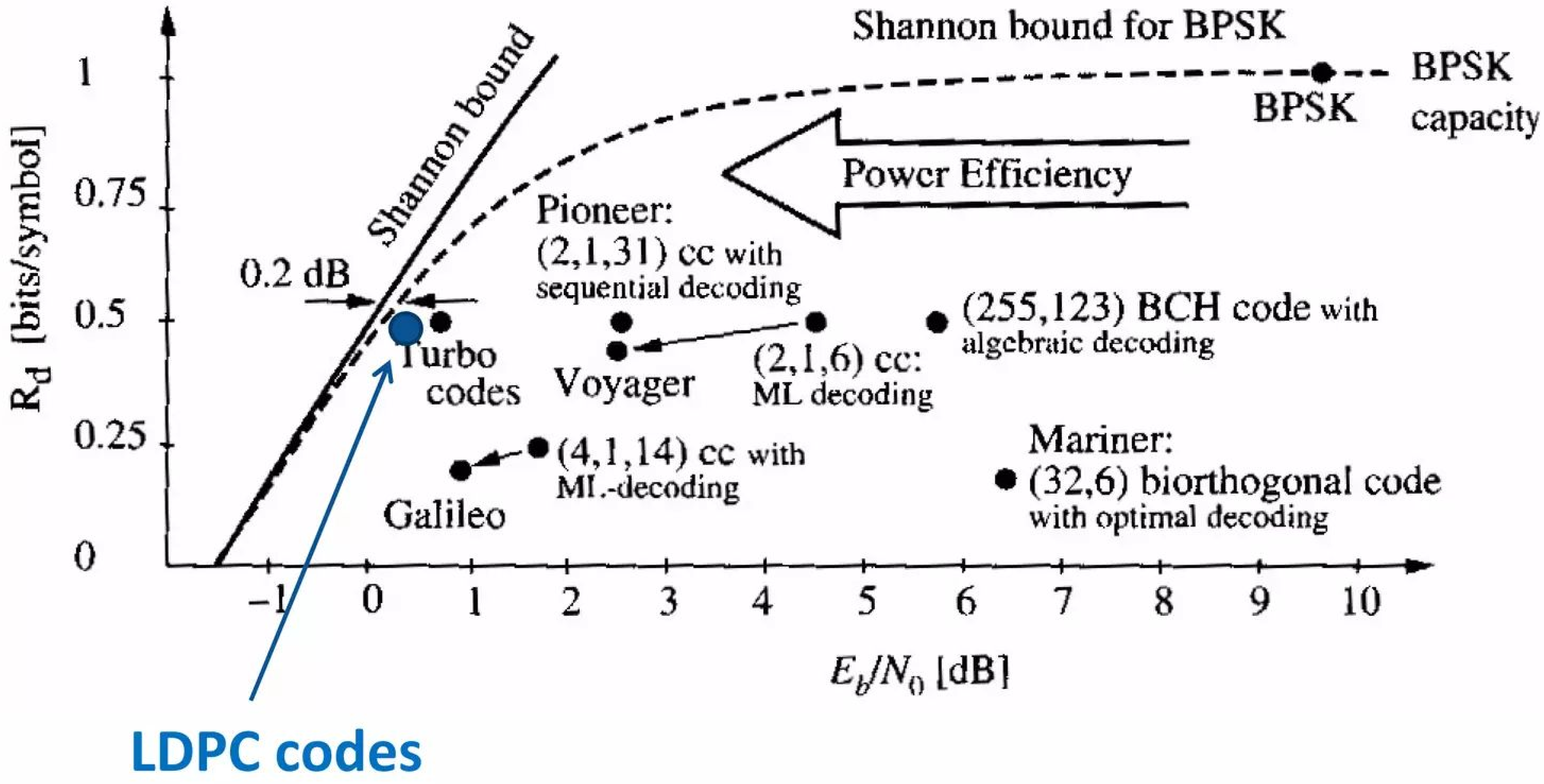
- binary symmetric channel (BSC)



$$C = 1 - H_2(p) \quad ,$$

$$H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$$

Evolution of Coding Technology



from Trellis and Turbo Coding, Schlegel and Perez, IEEE Press, 2004

Contents

Low-Density Parity-Check (LDPC) Codes
Brief History

- Invented by Gallager in his PhD thesis at MIT in 1963.
- Analyzed by Zyablov-Pinsker, Margulis in 70’s.
- Generalized in 1981 by Tanner.
- Re-discovered in 1995 by MacKay, Neal.
- Re-discovered and generalized by Sipser, Spielman, Luby, Shokrollahi, Richardson, Urbanke, etc.
- LDPC codes “dormant” for 35 years:

“A bit of 21st –century coding that happened to fall in the 20th century”.

Main Features

- Near Shannon limit performance
- Simple decoding algorithms – message-passing decoding
- Low decoding complexity
- Allow parallel implementation
- Flexibility in choice of parameters
- Amenable to rigorous analysis

Definition

- Any linear block code can be defined by its parity-check matrix. If this matrix is sparse, i.e. it contains only a small number of 1s per row or column, then the code is called a low-density parity-check code.

- Basically there are two different possibilities to represent LDPC codes:
  - Matrix Representation
  - Graphical Representation

- **Parity-Check Matrix:**

(with dimension n ×m for a (8, 4) code)

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

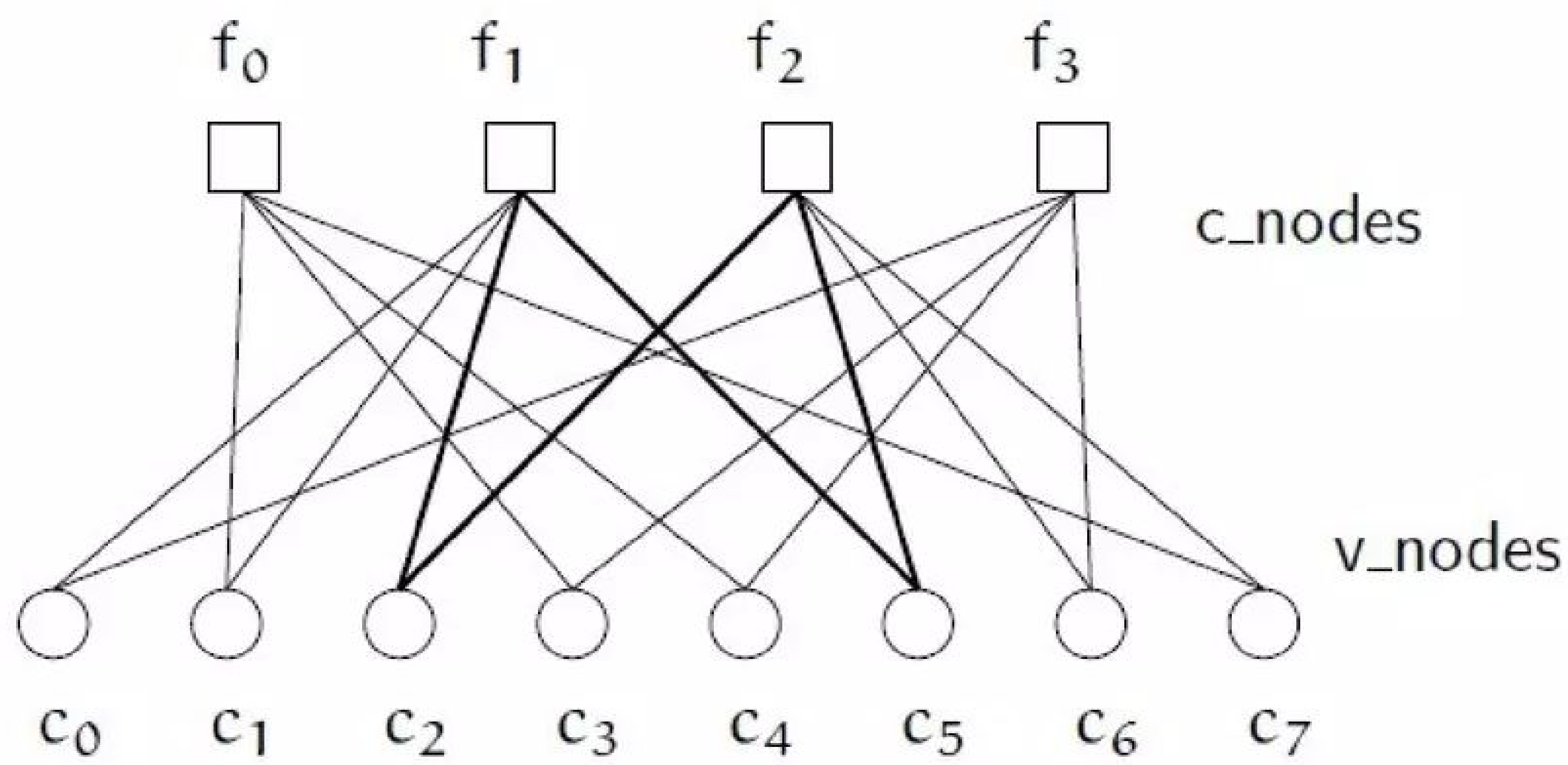
  - ρ = the number of 1's in each row
  - γ = the number of 1's in each column

For a matrix to be called low-density the two conditions $\gamma \ll n$, $\rho \ll m$ must be satisfied.

- **Bipartite Graph (so-called *Tanner graph*):**

That means that the nodes of the graph are separated into two distinctive sets: variable nodes (v-nodes) and check nodes (c-nodes).

  - m check nodes
    (the number of parity bits)
  - n variable nodes
    (the number of bits in a codeword)



Regular and irregular LDPC codes

- A regular LDPC matrix is an $n \times m$ binary matrix having exactly γ ones in each column and exactly ρ ones in each row, where $\gamma < \rho$ and both are small compared to m.

- If H is low-density but the numbers of 1's in each row or column aren't constant the code is called a irregular LDPC code.

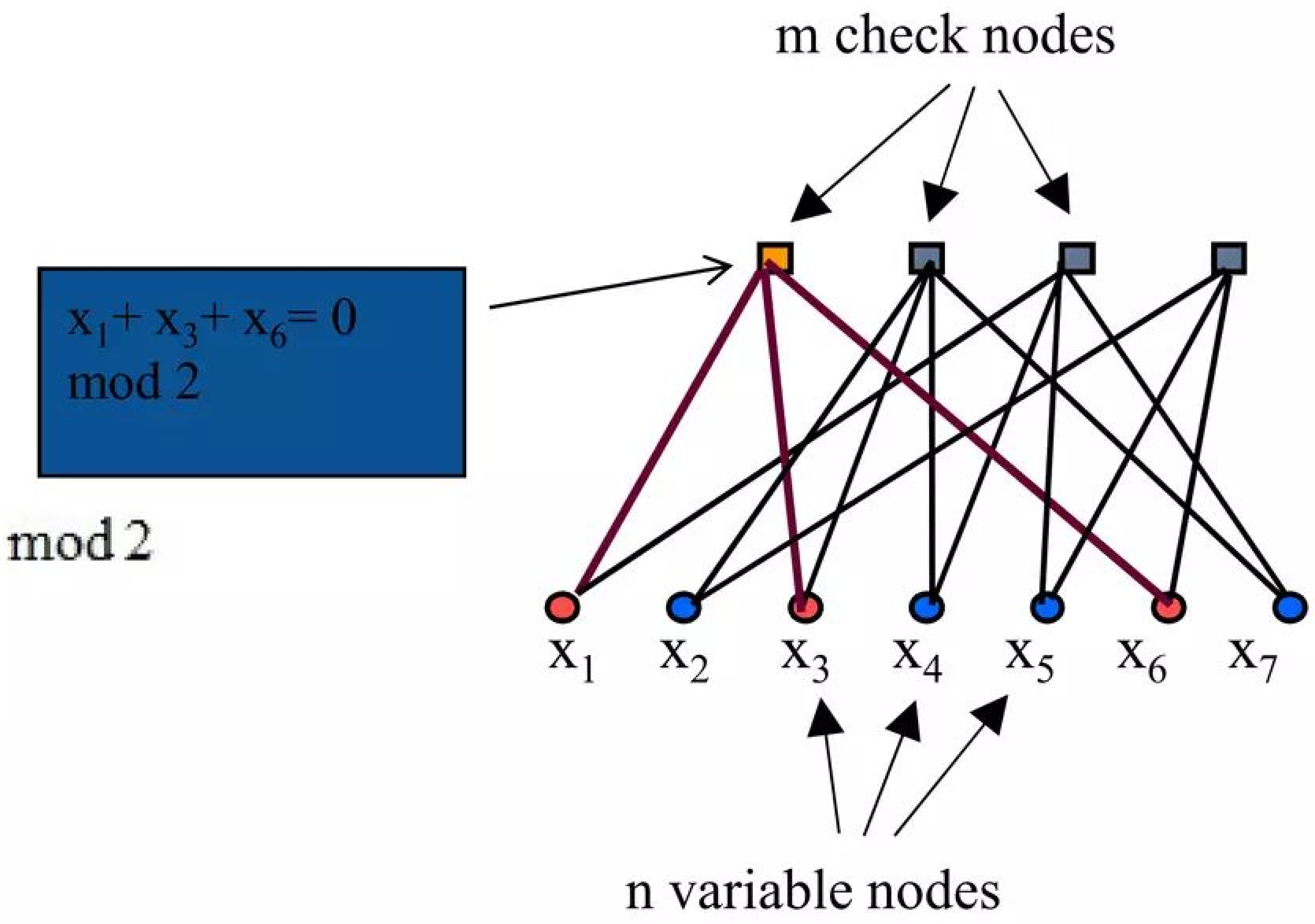
- It's also possible to see the regularity of this codes while looking at the graphical representation. There is the same number of incoming edges for every v-node and also for all the c-nodes.

- The LDPC codes as invented by Gallager were regular codes.

- The LDPC code defined by the graph is the set of vectors $C = (c_1,\ldots,c_n)$ such that $H.c^T = 0.$

- Example:

$$H\,x^t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \mod 2$$



Code Construction

- An LDPC code ensemble is presented by variable node and check node degrees distribution.

- More precisely, we define (n, γ, ρ)*-code as a linear code of length n, with* parity-check matrix containing the columns of weight γ *and the rows of weight* ρ.

- The parity-check matrix H contains:

$$r = n\gamma/\rho$$

rows, and therefore, the code rate is lower-limited as

$$R \geq 1 - \gamma/\rho$$

- Weights distributions can be defined by means of generating functions *λ(x) and ρ(x):*

$$\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}$$

$$\rho(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1}$$

- λ_i *:* the ratio of parity-check columns with weight *i,*
- ρ_i *:* the ratio of rows in H with weight *i,*
- d_v *,* d_c *:* the maximum weights of columns and rows.

Now define: $\sum_{i \geq 2} \lambda_i / i = \int_0^1 \lambda(x)\, dx$, so:

$$r = n \frac{\int_0^1 \rho(x)\, dx}{\int_0^1 \lambda(x)\, dx}$$

$$R \geq 1 - \frac{\int_0^1 \rho(x)\, dx}{\int_0^1 \lambda(x)\, dx}$$

Applications

- LDPC codes have already been adopted in satellite-based digital video broadcasting and long-haul optical communication standards, are highly likely to be adopted in the IEEE wireless local area network standard, and are under consideration for the long-term evolution of third generation mobile telephony.

- LDPC is also used for 10GBase-T Ethernet, which sends data at 10 gigabits per second over twisted-pair cables.

- As of 2009, LDPC codes are also part of the Wi-Fi 802.11 standard as an optional part of 802.11n and 802.11ac, in the High Throughput (HT) PHY specification.

Conclusion

- LDPC codes are one of the hottest topics in coding theory. Unlike many other classes of codes LDPC codes are already equipped with very fast (probabilistic) encoding and decoding algorithms. LDPC codes are not only attractive from a theoretical point of view, but also perfect for practical applications.

- LDPC codes are becoming the mainstream in coding technology.
  - Already implemented in 3G and LAN standards

- Many important researches are still open!

References

1. Andr´e Neubauer and Jurgen Freudenberger and Volker Kuhn, "*Coding Theory Algorithms, Architectures, and Applications*", Wiley Press, ISBN 978-0-470-02861-2.
2. Evgenii Krouk and Sergei Semenov, "*Modulation and coding techniques in wireless communications*", Wiley Press, ISBN 978-0-470-74505-2.
3. Amin Shokrollahi, "*LDPC Codes: An Introduction*", Digital Fountain, Inc, April 2003.
4. Bernhard M.J. Leiner, "*LDPC Codes – a brief Tutorial*", April 2005.
5. John R. Barry, "*Low-Density Parity-Check Codes*", Georgia Institute of Technology.
6. Thomas J. Richardson and Rüdiger L. Urbanke, "The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding", IEEE Transactions on Information Theory, February 2001.

Thank You!