



به نام خداوند مهربان

Low-Density Parity-Check Codes Construction and Combinatorial Designs

M.H. Tadayon
tadayon@itrc.ac.ir

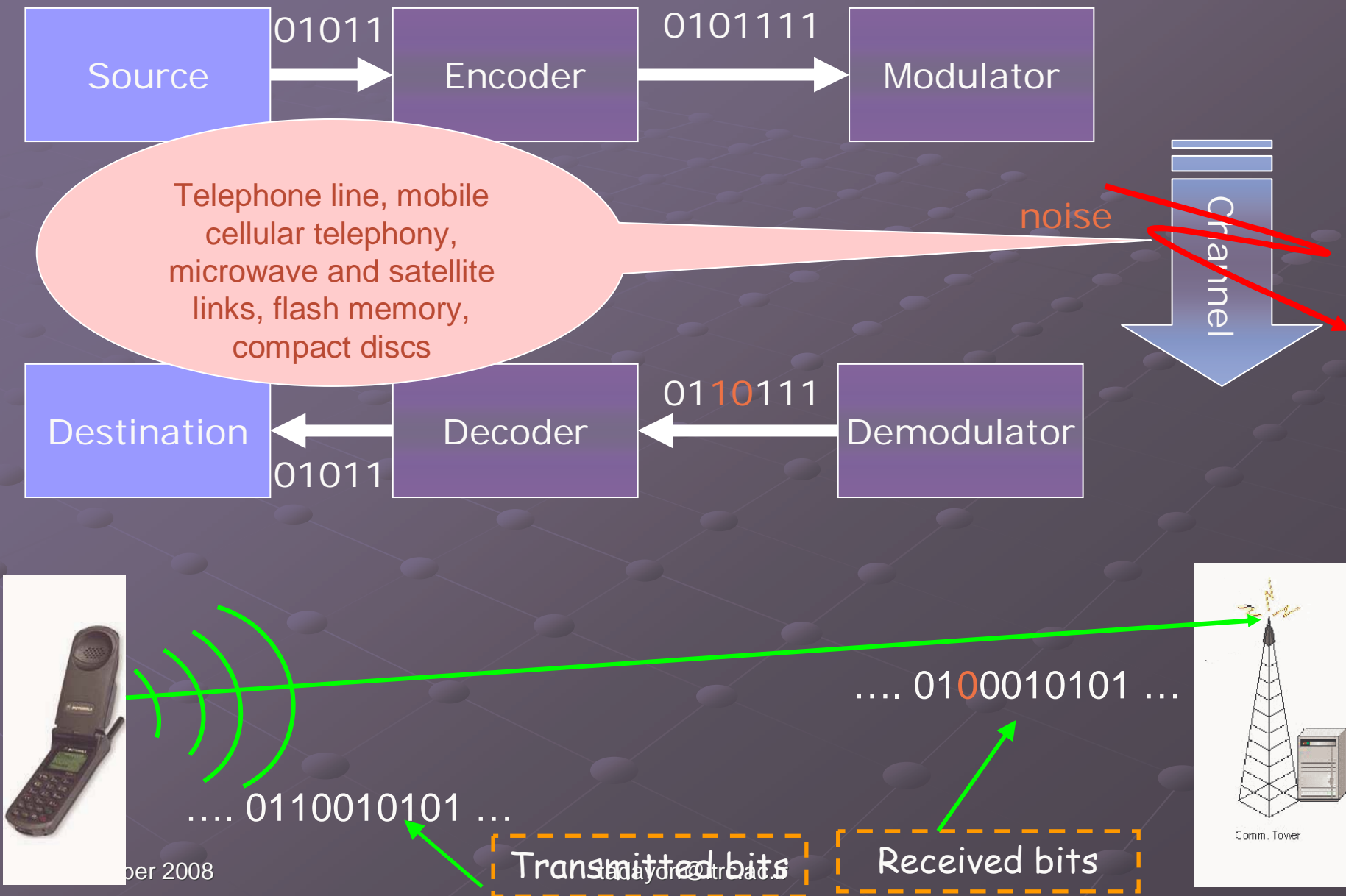
Iran Telecommunication Research Center (ITRC)

Oct. 2008

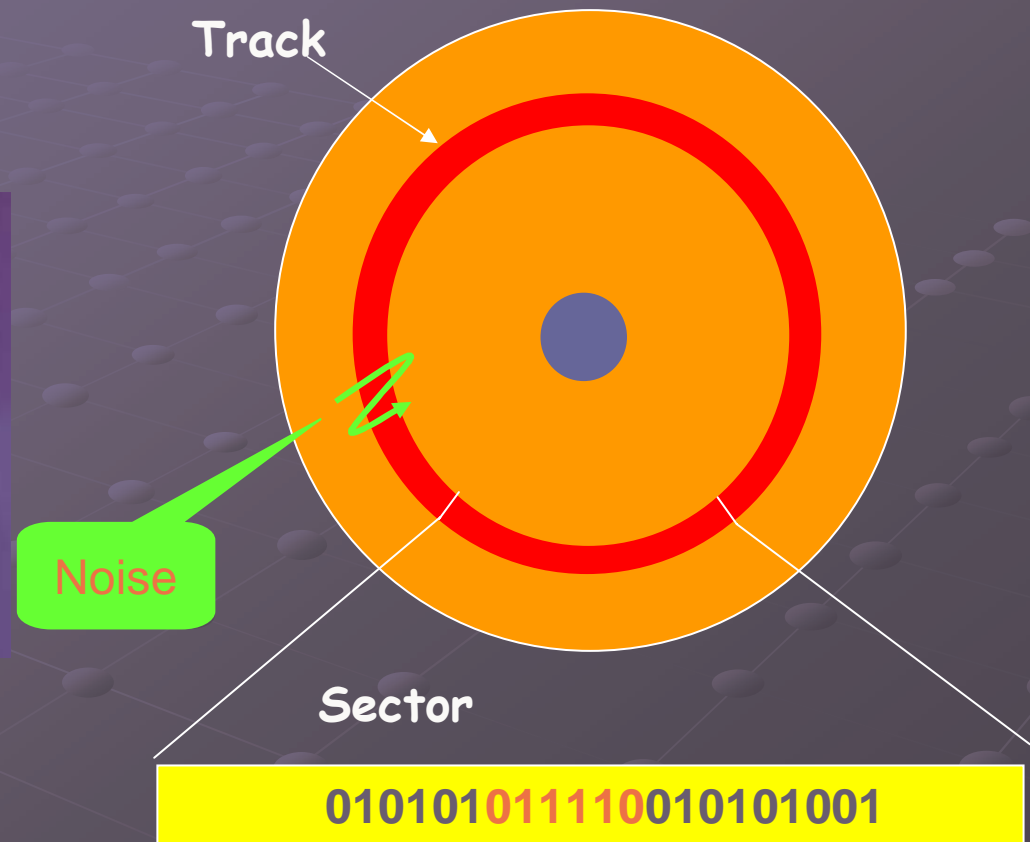
Outline

- Block Codes
- Noisy Channel Coding Theorem (Shannon Theorem)
- Low-Density Parity-Check (LDPC) Codes
- Combinatorial Designs and LDPC Codes
- Some properties

A Communication model



Cont.



Block Codes

❖ [n, k]-code:

A k dimensional subspace of F_q^n

❖ $M=n-k=$ **Redundancy**

Code Rate

$$R = \text{Code rate} = \frac{\text{Dimension}}{\text{Code length}} = \frac{k}{n}$$

$$0 < R < 1$$

Generator & Parity-Check Matrix

❖ **G**: $k \times n$ **generator matrix**, which $\mathbf{c} = \mathbf{m}G \in F_q^n$

$$C : (m_1, m_2, \dots, m_k) \mapsto (c_1, c_2, \dots, c_n)$$

$$(c_1, c_2, \dots, c_n) = (m_1, m_2, \dots, m_k) \times \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ g_{21} & g_{22} & \dots & g_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{pmatrix}$$

❖ **H**: $(n-k) \times n$ **parity-check matrix**, such that $GH^T = \mathbf{0}$ in F_q

Example : [7, 4]-Hamming code

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

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

$$y \in C \quad \text{iff} \quad yH^T = 0$$

$$GH^T = 0$$

Minimum Distance

❖ **d**: Minimum distance (the minimum weight of codewords)

Theorem: Let d_{min} be the minimum distance of a code C . Then C is a t -error-correcting code if and only if $d_{min} \geq 2t + 1$.

Higher minimum distance = Stronger code

Finding minimum distance:
NP hard

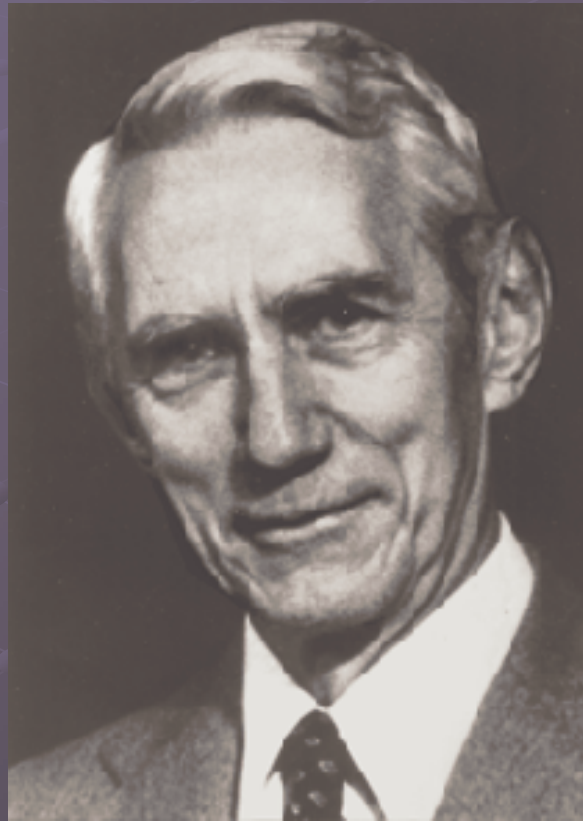
Linear Block Codes

- ❖ There are many practical linear block codes:
 - Hamming codes
 - Cyclic codes
 - Reed-Solomon codes
 - BCH codes
 - ...

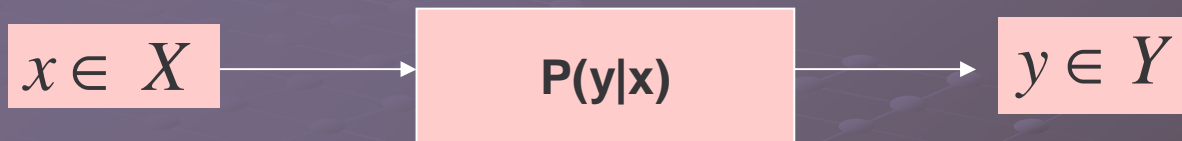
But ...

Shannon's Channel Coding Theorem

- In 1948, Claude Shannon published the paper: “A Mathematical Theory of Communications” which laid the foundations of Information Theory.



Noisy Channel Coding Theorem (Shannon Theorem)



$$\text{Mutual Information } I(X;Y) = \sum_{x,y} P(x,y) \log \frac{P(x|y)}{P(x)}$$

$$\text{Channel Capacity } C = \max_{P(x)} I(X;Y) \text{ bits/channel use}$$

$\forall \epsilon, \delta > 0, R : 0 < C - R < \epsilon,$
a large length n code of rate R with $P_e < \delta$

Error Control Coding

- good codes

- Low-complexity encoding and decoding
- Can approach channel capacity with low probability of error decoding

Low-Density Parity-Check (LDPC) Codes

● Gallager 1963, Tanner 1984, MacKay 1996

- Linear block codes with **sparse** (small fraction of ones) parity-check matrices
- Have simple representation in terms of **bipartite graphs**
- Simple and efficient iterative decoding in the form of belief propagation
- A class of channel capacity (Shannon limit) approaching codes

Graphical Representation

Example :

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

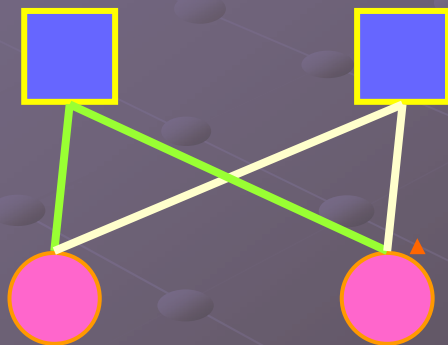
$$\mathbf{c}H^T = \mathbf{0}$$

$$c_1 + c_2 + c_4 = 0$$

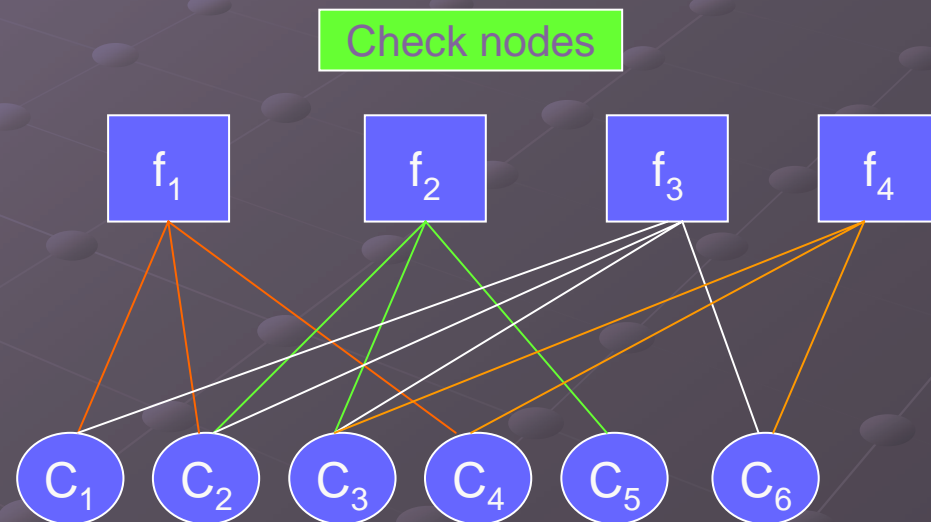
$$c_2 + c_3 + c_5 = 0$$

$$c_1 + c_2 + c_3 + c_6 = 0$$

$$c_3 + c_4 + c_6 = 0$$



cycle of
length 4



LDPC codes construction types

● Random-like codes

- Gallager (Low-density parity-check codes)
- Mackay (Near Shannon limit performance of LDPC codes)
- . . .

● Structured codes

- Shu lin and . . . (Low-density parity-check codes based on finite geometries . . .)
- S. Johnson and . . . (Codes for iterative decoding from partial geometries)
- Fossorier (Quasi-cyclic low-density parity-check codes . . .)
- Vasic and . . . (Combinatorial constructions of LDPC codes. . .)
- Honary and . . . (Construction of LDPC codes based on BIBDs)
- . . .

Complexities Comparison

Code	Encoding	Decoding
Random Linear Code	$O(n^2)$	$O(2^n)$
LDPC Quasi-cyclic LDPC	$O(n^2)$ $O(n)$	$O(n)$ (Sum-Product Algorithm)

Decoding of linear codes:
NP hard

Gallager Codes

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_{\omega_c} \end{bmatrix}_{\mu\omega_c \times \mu\omega_r}$$

Where for $i=1,2,\dots,\mu$, the i -th row of submatrix H_1 contains of w_r 1's in columns $(i-1)w_r + 1$ to iw_r and other submatrices are simply column permutation of H_1 .

Example: $w_c=3$, $w_r=4$

$H =$

$w_r=4$	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0
	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0
	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
	0	0	0	1	0	0	0	0	0	0	0	0	1	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
$w_c=3$	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0
	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0
	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0
	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1

Drawback

- length-4 cycles in H
- encoding complexity

Mackay Codes

- **H is created randomly**

- generating weight- w_c columns and (as near as possible) uniform row weight
- generating weight- w_c columns, while ensuring weight- w_r rows, and no two columns having overlap greater than one(avoid cycle of length 4)

- **Drawback: lack sufficient structure to enable low-complexity encoding**

Example: $w_c=3$, $n=20$, $n-k=10$

H=

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

$w_r=7$

as near as possible uniform row weight

$w_r=6$

$w_r=5$

$w_c=3$

Combinatorial Designs and LDPC Codes

STS (v) & LDPC Mackay and S. Johnson Codes

Example: STS(7) or 2- (7, 3, 1)

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$$

$$B_1 = \{x_1, x_2, x_4\}$$

$$B_2 = \{x_2, x_3, x_5\}$$

$$B_3 = \{x_3, x_4, x_6\}$$

$$B_4 = \{x_4, x_5, x_7\}$$

$$B_5 = \{x_1, x_5, x_6\}$$

$$B_6 = \{x_2, x_6, x_7\}$$

$$B_7 = \{x_1, x_3, x_7\}$$

Drawback

- length and rate
- generating several family of codes

x_1
 x_2
 x_4
 x_5
 x_7

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

Euclidian Geometries & LDPC

Shu lin and . . .

- Let p be a prime. Given two integers $m \geq 2$ and $s \geq 1$, the m -dimensional **Euclidian geometry** $EG(m, p^s)$ over $GF(p^s)$ consists of points, lines and hyperplanes (μ -flats).
 - A μ -flat is a μ -dimensional, $0 \leq \mu \leq m$, subspace of the points of $EG(m, p^s)$ over $GF(p^s)$.
 - A μ -flat has $p^{\mu s}$ points.
 - A point is a 0-flat and a line is a 1-flat.
 - A line contains p^s points
 - In $EG(m, p^s)$ there are $p^{(m-1)s}(p^{ms}-1)/(p^s-1)$ lines and every point is the intersection of $(p^{ms}-1)/(p^s-1)$ lines
 - The set of points and lines of $EG(m, p^s)$ form a $2-(p^{ms}, p^s, 1)$ BIBD

Example:

- Consider the 2-dimensional Euclidean geometry $EG(2, 2^2)$. Let α be a primitive element of $F_{2^{2 \times 2}}$. The incident vector for the line $L = \{\alpha^7, \alpha^8, \alpha^{10}, \alpha^{14}\}$ is $(0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1)$. The vector and its 14 cyclic shifts form the parity check matrix H .

$H =$

Cyclic LDPC
Low-complexity
encoding

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

Cycle shifts
of
The first row

Affine planes & LDPC

Shu lin and . . .

- Any 2 -(n^2 , n , 1) design is called an **affine plane** of order n , denoted $\text{Aff}(n)$.
 - One line contains n points;
 - One point belongs to exactly $n+1$ lines;
 - Every line contains n points;
 - There are exactly n^2 points in $\text{Aff}(n)$;
 - There are exactly n^2+n lines in $\text{Aff}(n)$;
- For any prime power q there exists an affine plane of order q .

Example: Aff(n=3)

$$\mathbf{H}_{Aff} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{9 \times 12}$$

Projective planes

Shu lin and . . .

- A $2-(n^2+n+1, n+1, 1)$ design is called a **projective plane** of order n , denoted by $\text{Pr}(n)$.
 - One line contains $n+1$ points;
 - One point belongs to exactly $n+1$ lines;
 - Every line contains $n+1$ points;
 - There are exactly n^2+n+1 points in $\text{Pr}(n)$;
 - There are exactly n^2+n+1 lines in $\text{Pr}(n)$;

Example: $\text{Pr}(n=3)$.

$$H_{\text{Proj}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{13 \times 13}$$

Quasi Cyclic LDPC codes

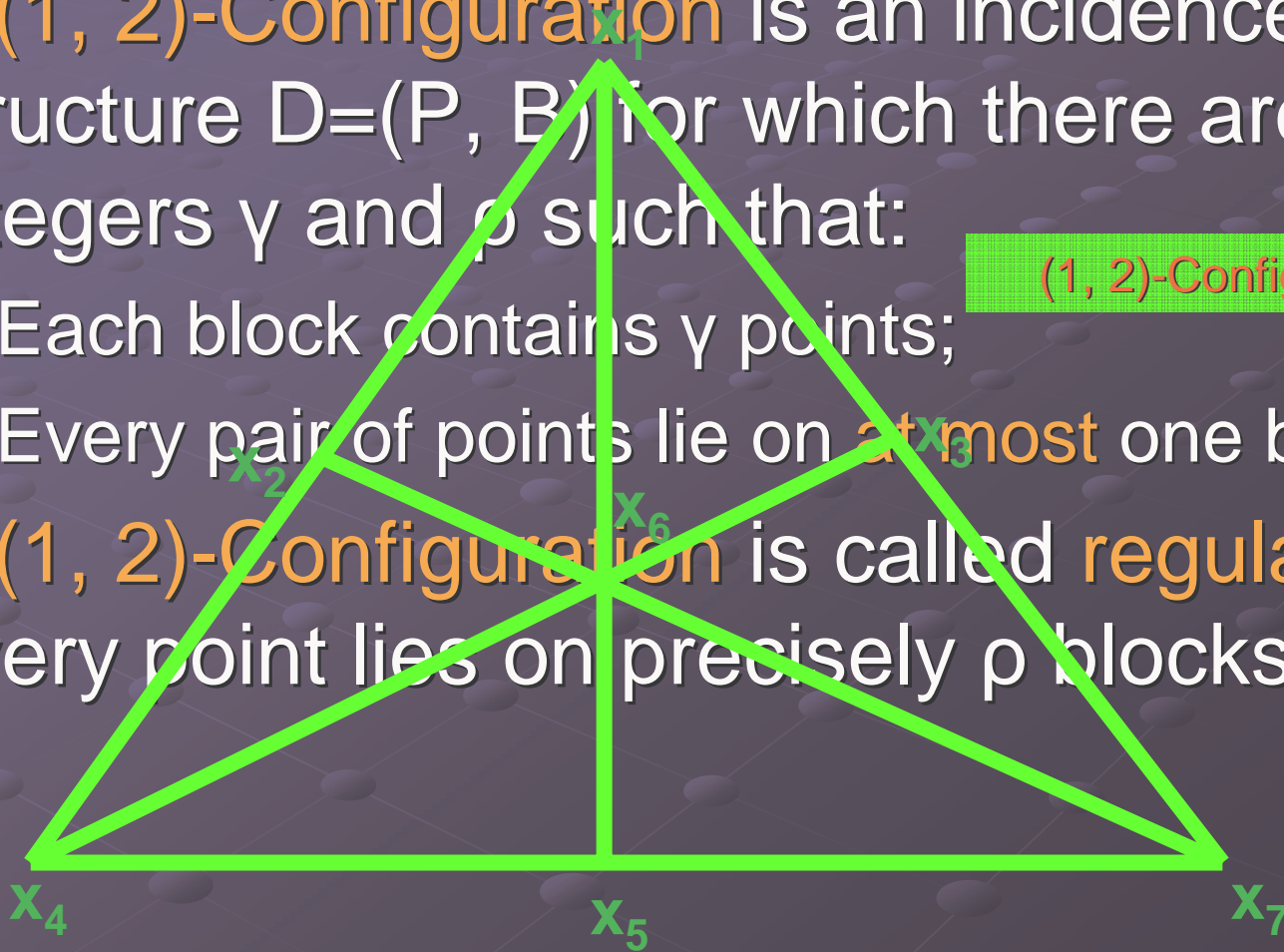
- A $m \times n$ sparse bipartite graph representing a Quasi Cyclic LDPC code. The graph consists of two sets of nodes: variable nodes (circles) and check nodes (squares). The edges between them are represented by various symbols (circles, triangles, crosses, etc.) indicating the connections. Some symbols are highlighted in yellow.

$$\mathbf{H}_A = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \dots & \mathbf{I} \\ \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{q-1} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{I} & \mathbf{P}^{\gamma-1} & \dots & \mathbf{P}^{(\gamma-1)(q-1)} \end{bmatrix}$$

(1, 2)-Configuration & LDPC

- A **(1, 2)-Configuration** is an incidence structure $D=(P, B)$ for which there are two integers γ and p such that:
 - Each block contains γ points;
 - Every pair of points lie on **at most** one block
- A **(1, 2)-Configuration** is called **regular** if every point lies on precisely p blocks.

(1, 2)-Configuration



Why (1, 2)-configuration?

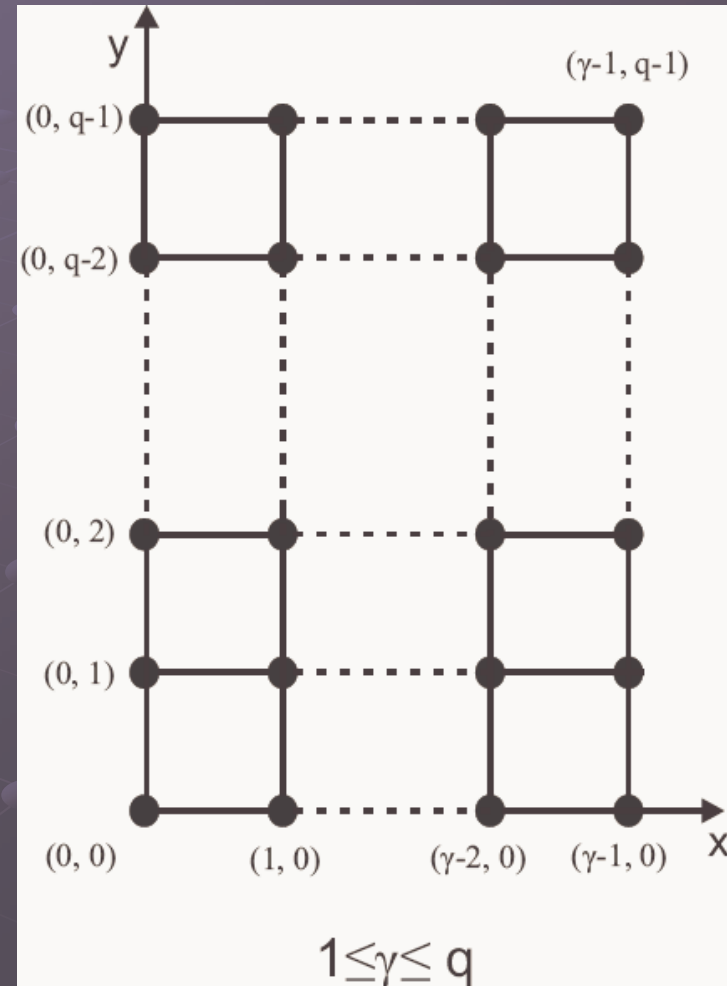
- Constructed LDPC codes have **girth at least 6**.
- **Minimum distance** of constructed LDPC codes is **at least $\gamma+1$** .
- Constructed LDPC codes have a good structure and can be represented as a **cyclic or quasi-cyclic code**

Integer Lattices

Vasic and . . .

Integer lattices:

$L(\gamma \times q) = \{(x, y) : 0 \leq x \leq \gamma - 1, 0 \leq y \leq q - 1\}$, $\gamma \leq q$ and γ, q are nonnegative integers.



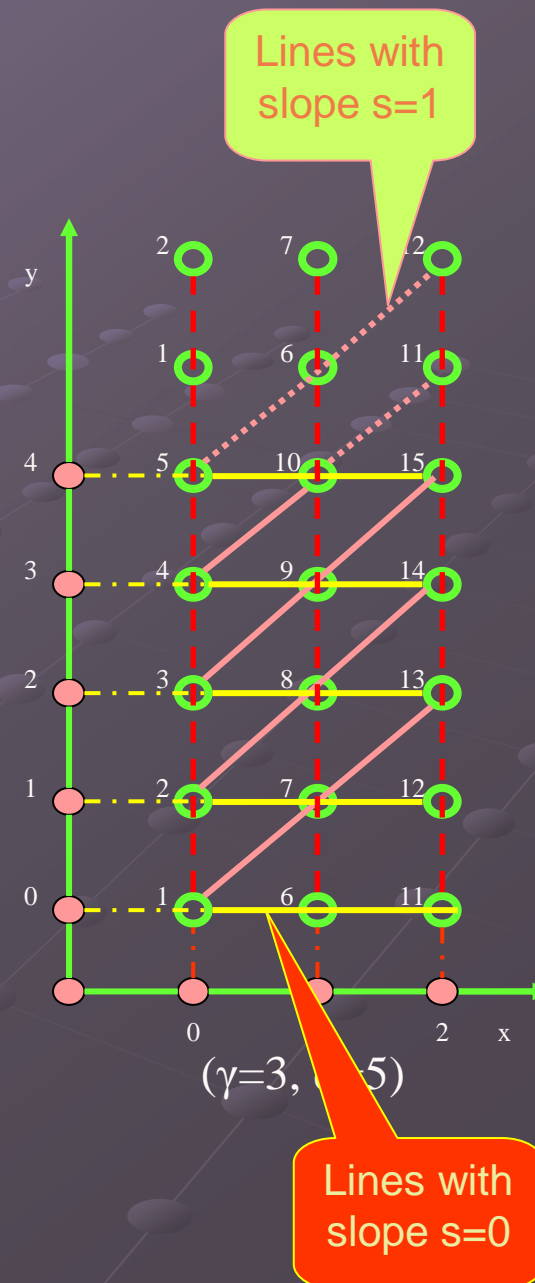
Integer Lattice designs

- The line $\ell_s(a)$ with slope $0 \leq s \leq q-1$ and passing through the point $(0, a)$ is defined by:

$$\ell_s(a) = \{(x, sx+a \pmod{q}), : 0 \leq x \leq \gamma-1\}$$

$L(\gamma, q)$

- γq points
- q^2 lines
- any line contains γ points
- each point is in the intersection of q lines
- $(1, 2)$ -configuration

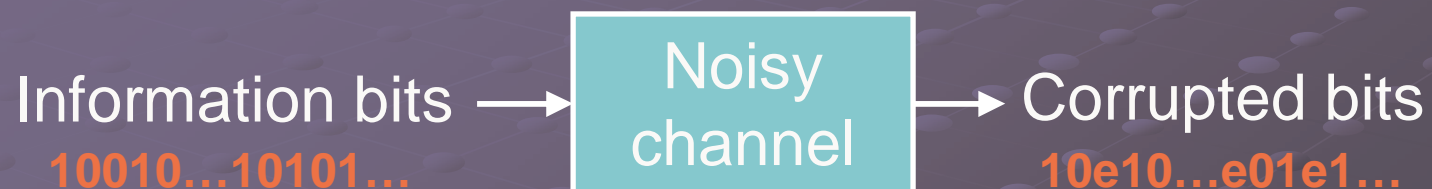


● Example: Lattice $L(3,5) \equiv \text{Array } (\gamma=3, q=5)$

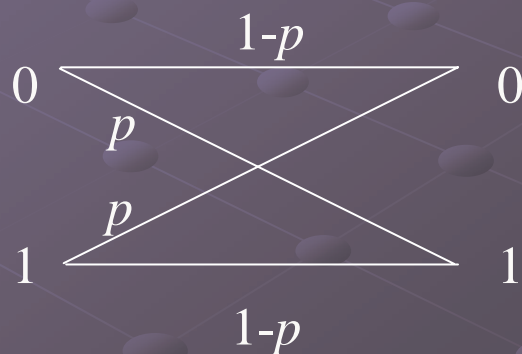
$$\mathbf{P} = \mathbf{P}^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\mathbf{H}_{Latt(3,5)} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P} & \mathbf{P}^2 & \mathbf{P}^3 & \mathbf{P}^4 \\ \mathbf{I} & \mathbf{P}^2 & \mathbf{P}^4 & \mathbf{P}^6 & \mathbf{P}^8 \end{bmatrix}$$

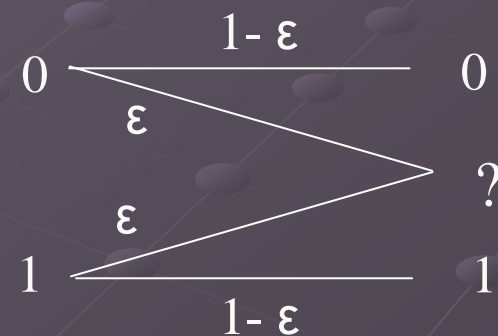
Noisy Channels



Binary symmetric channel BSC (p)



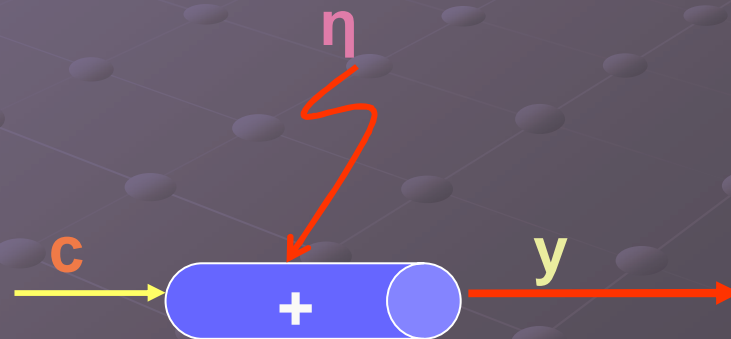
• Binary erasure channel BEC (ϵ)



AWGN (Additive White Gaussian Noise) channel

- \mathbf{c} a codeword, $\boldsymbol{\eta} \sim \text{normal}(\mu=0, \sigma^2)$, \mathbf{y} received word

$$\mathbf{y} = \mathbf{c} + \boldsymbol{\eta}$$



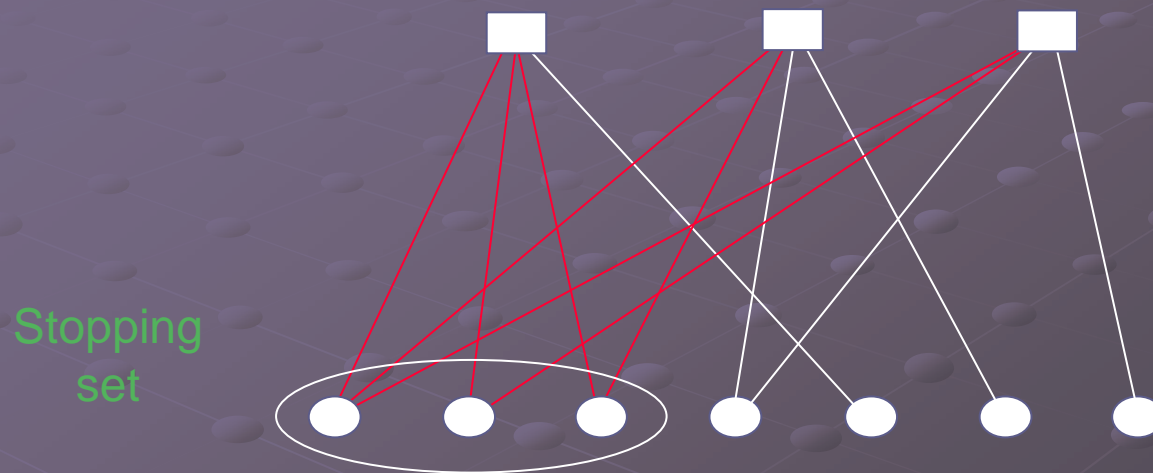
Stopping Sets

(a problem in binary erasure channels)

- A stopping set is a **subset S of the variable nodes** in Tanner graph of code C such that **all the neighbors of S are connected to S at least twice.**
- The size of the **smallest non-empty stopping sets of code C** is called the **stopping distance**

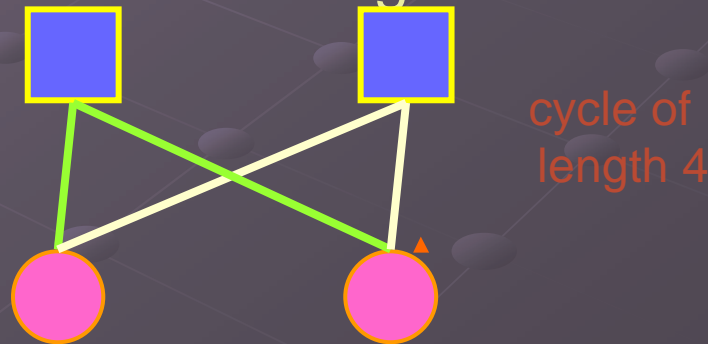
Finding stopping distance:
NP hard

Example: $[7,4]$ -Hamming code

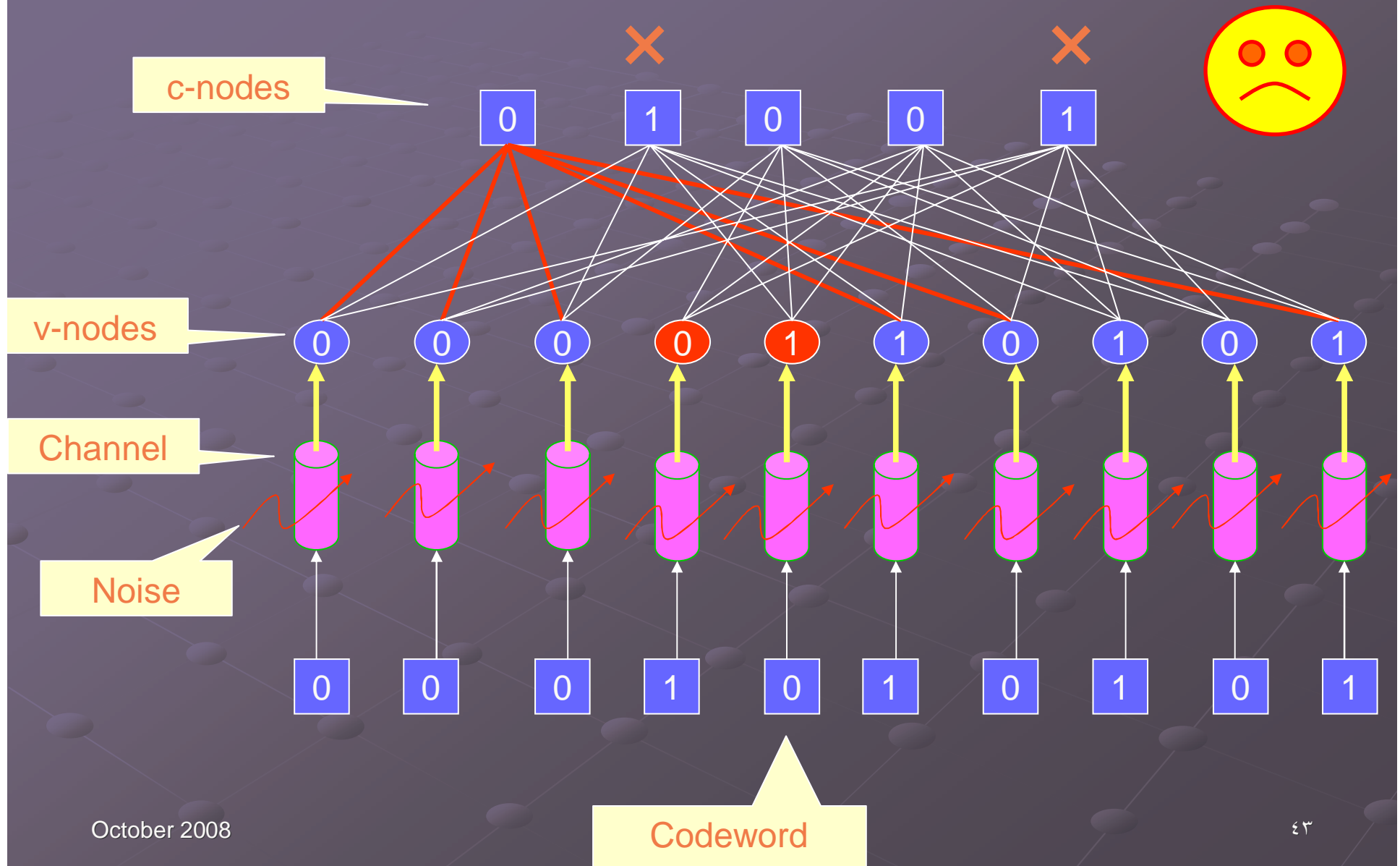


Iterative Decoding

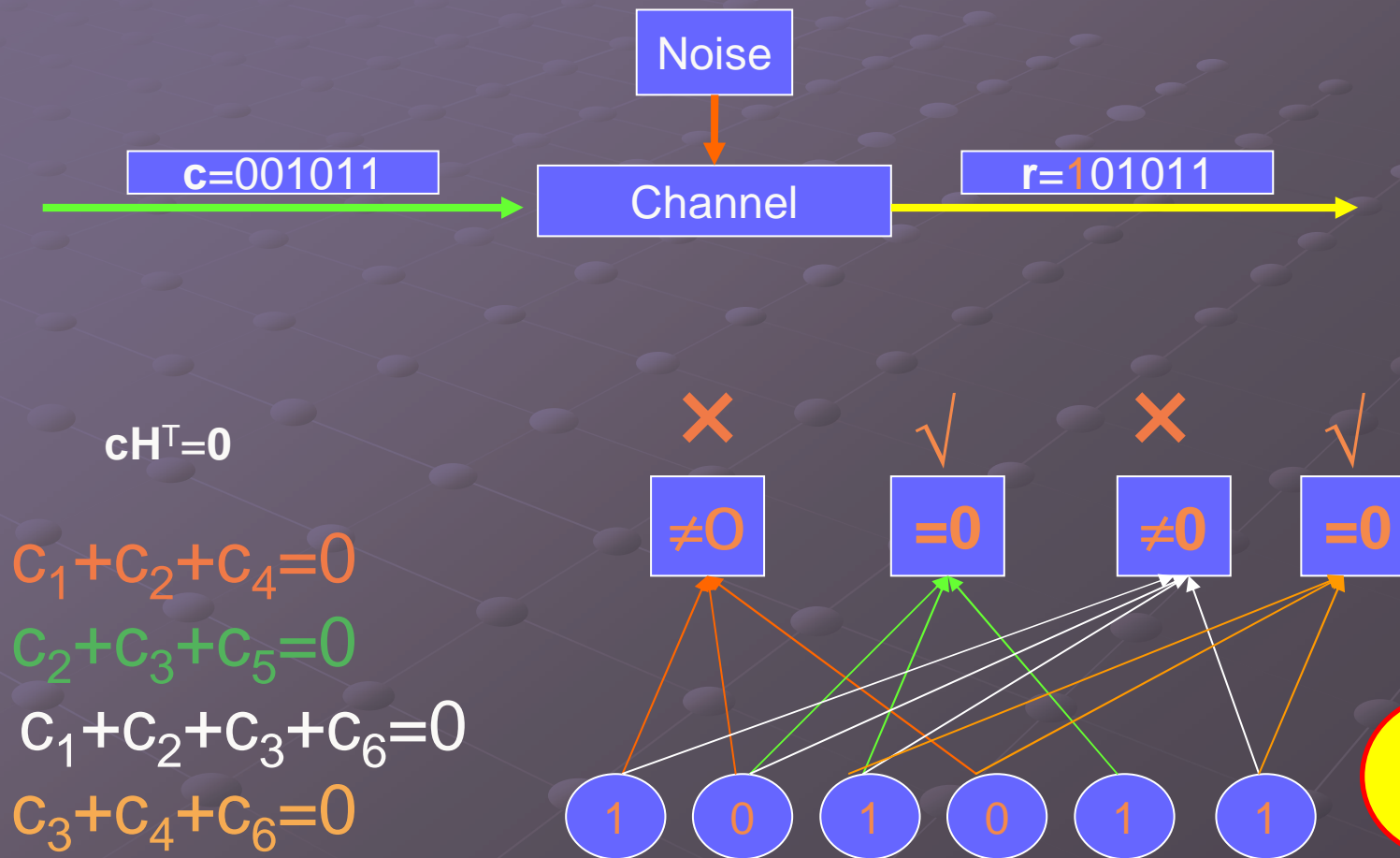
- **Hard Decision** (passing of messages between **variable nodes** and **check nodes** are 0 or 1)
 - Bit-Flipping Algorithm (BFA)
- **Soft Decision** (passing of messages between **variable nodes** and **check nodes** are probabilistic)
 - Sum-Product Algorithm (SPA)
- Iterative decoding is optimal only if the code graph has no cycles
 - Want: to make **girth** (smallest cycle length) as large as possible;
 - Number of cycles of short length as small as possible;



A graph representation of error detection

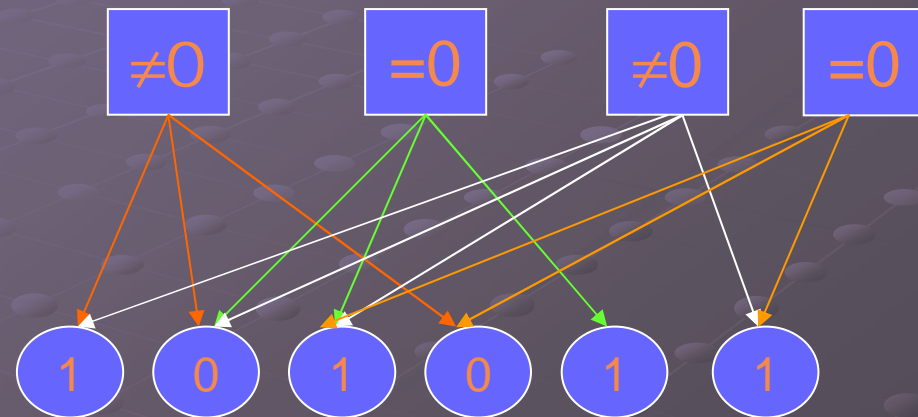


An example of Check and Variable nodes update (BFA)

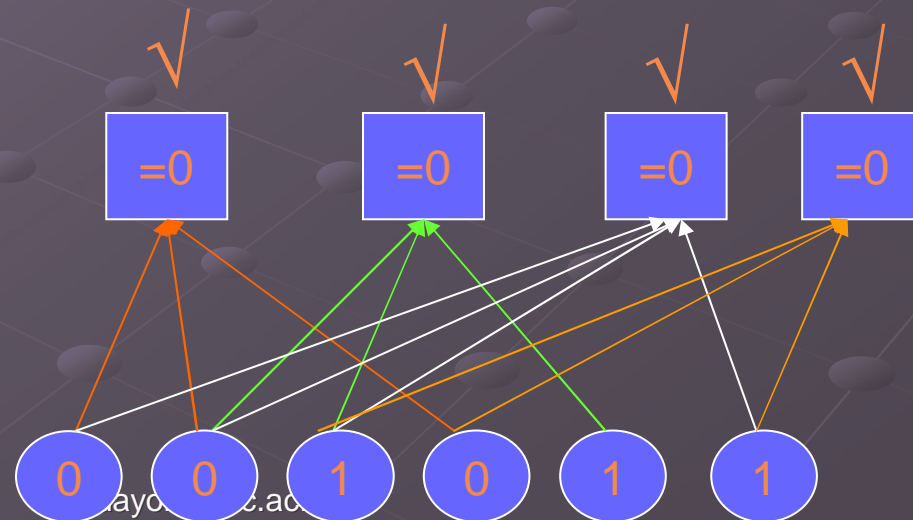


An example of Check and Variable nodes update (BFA)

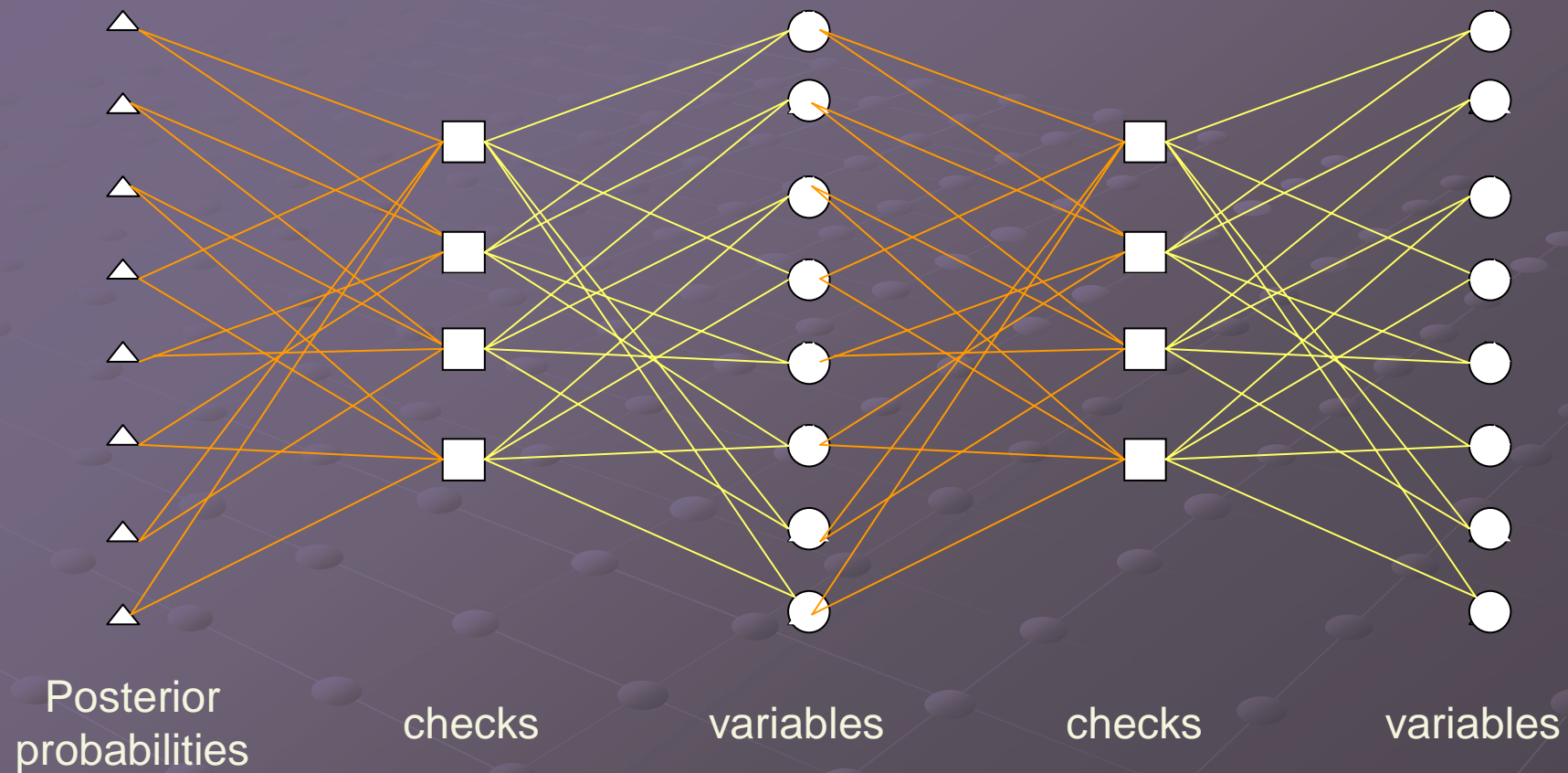
● Variable update



● Parity update

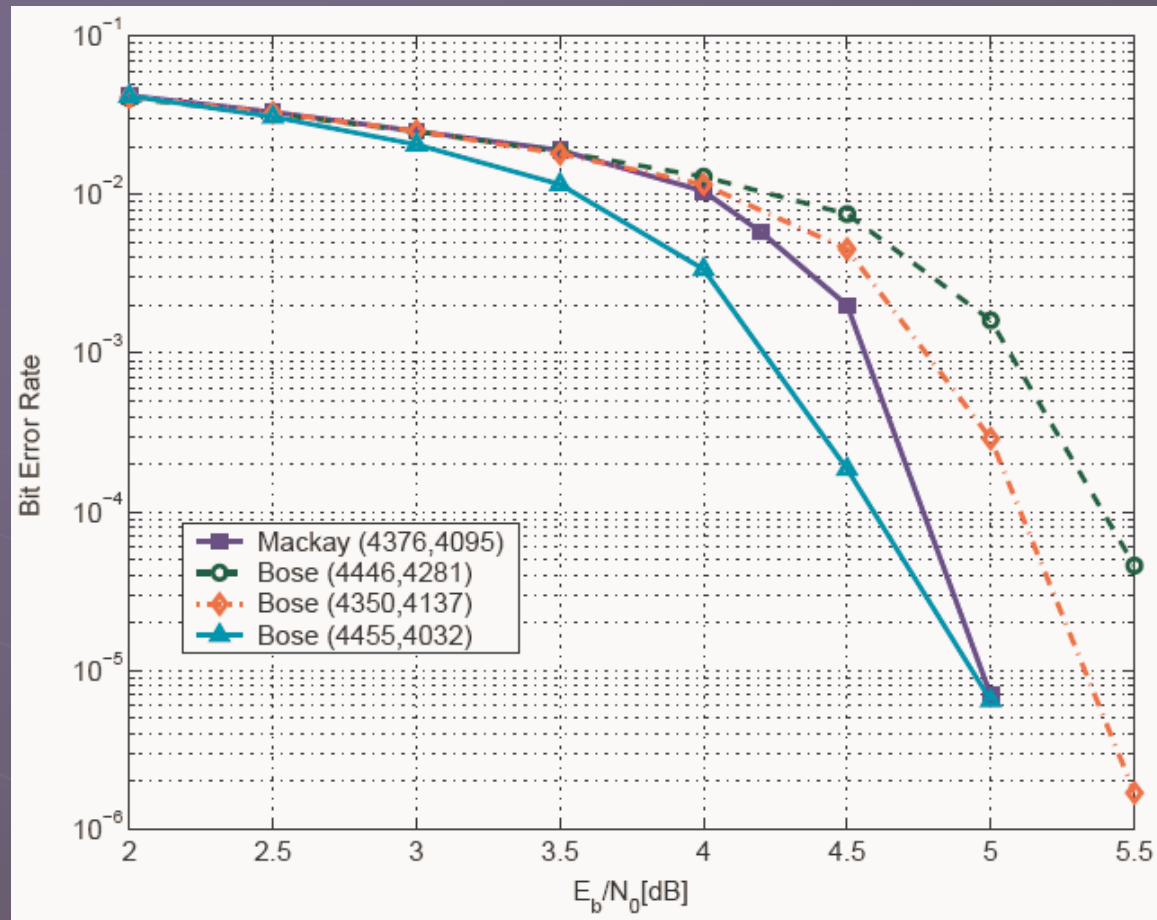


More Decoding



Processing

Performance



References

- H. Pishro-Nik, “Modern Coding Theory: LDPC Codes”.
- O. Milenkovic, “On The Analysis And Application Of LDPC Codes”.
- A. Gomilko, “Turbo Codes overview”.
- . . .



Thank You