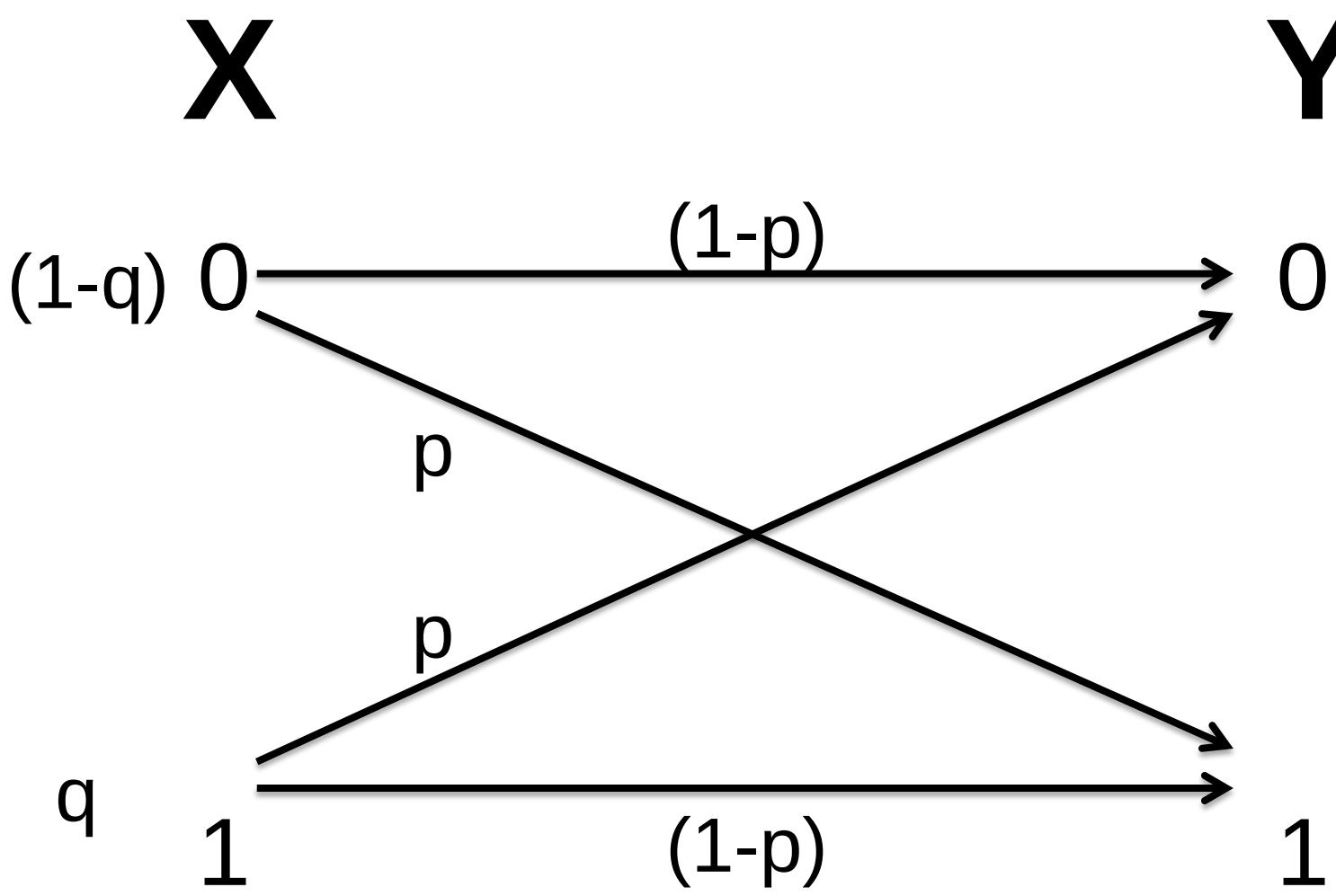
ELE32
Introdução a Comunicações
Codificação de Canal

ITA

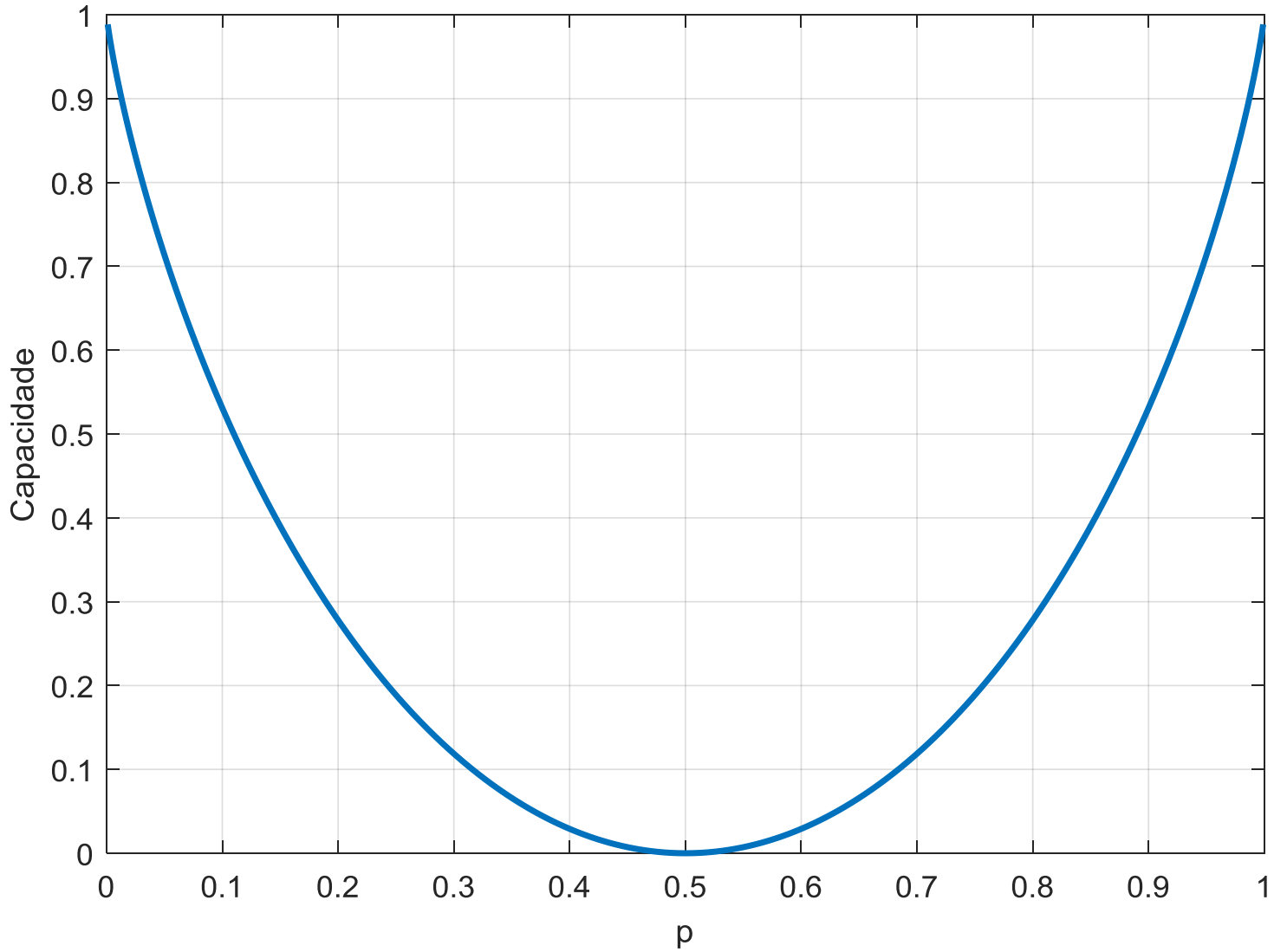
2º. Semestre de 2018

manish@ita.br

Canal causa erros de transmissão



Capacidade do Canal BSC



Como proteger informação contra erros de transmissão?

- Sinais recebidos são diferentes dos transmitidos
- Modificação pode causar erro de bit
- Adição de mecanismos de proteção permite aumentar confiança no valor do bit transmitido
- Como proteger os bits de informação?

Mecanismo 1: Repetição

- Repetir um mesmo bit N vezes exige mais do que N/2 erros de transmissão para se errar o bit

Bloco transmitido		Bloco recebido:
00000	→	0**11**00
11111		1**00**11

- Problema: taxa de bits de informação cai para 1/N (um bit de informação para cada N bits transmitidos.

Mecanismo 2: Paridade

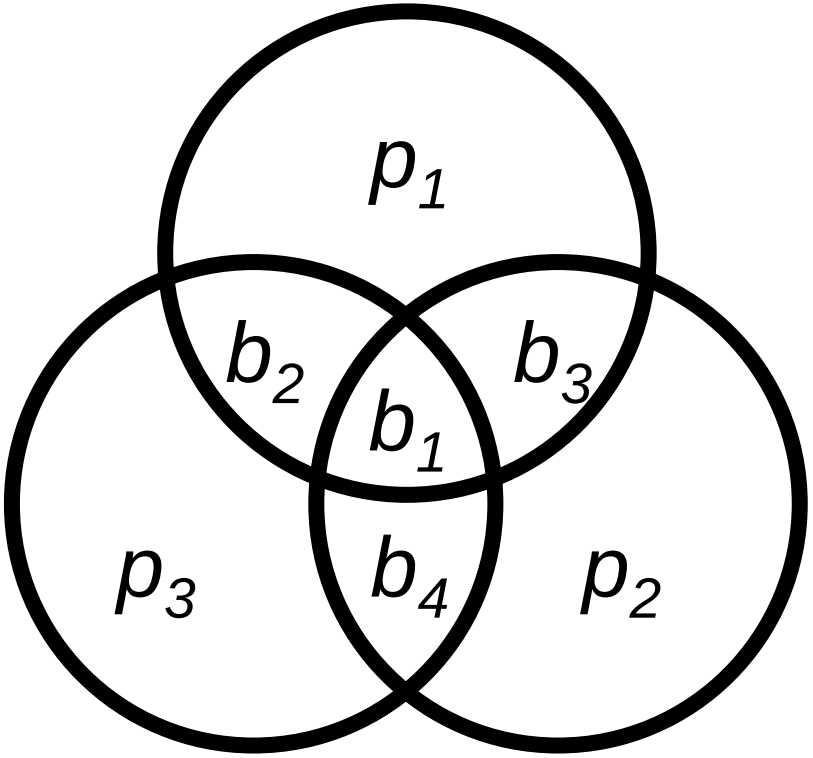
- Adição de um bit gerado pela soma módulo 2 dos bits de informação permite taxa de (N-1)/N

Bloco transmitido		Bloco recebido:
01001	→	01001
10010		11010 ✗

- Problema: não é possível identificar qual bit está errado.

Mecanismo 3: Código de bloco

- Bloco transmitido pode ser gerado com regras mais elaboradas:



Bloco transmitido

$b_1 b_2 b_3 b_4 p_1 p_2 p_3$

Ex: **0110011**

Método permite identificar e corrigir até um erro de transmissão. Taxa de 4/7

Código de bloco

- Um código de bloco binário é um conjunto de vetores binários, todos com tamanho N.
- Entretanto, nem todas as 2^N possibilidades de vetores binários são parte do código. Somente 2^K vetores binários são parte do código. Os vetores que fazem parte do código são chamados palavra-código.
- O código de Hamming é um código de bloco.

Relação entre palavras-código de palavras de informação

- Logo, as palavras-código estão contidas no espaço binário com dimensão N
- Logo, é possível associar a cada vetor binário do código um vetor binário com tamanho K. Este vetor de tamanho K é chamado de palavra de informação.
- A relação entre palavra de informação e palavra-código é feita através do codificador. Um mesmo código pode ter vários codificadores.
- A taxa do código de bloco é a razão entre o número de bits de informação e o tamanho (em bits) da palavra-código transmitida

Operações com palavras código

- Se $\mathbf{v}_1$ e $\mathbf{v}_2$ são palavras-código, definimos $\mathbf{v}_3 = \mathbf{v}_1+\mathbf{v}_2$ como sendo o vetor obtido pela soma módulo 2 (XOR) dimensão a dimensão dos vetores originais.
- Um código é linear se, para qualquer par de palavras-código $\mathbf{v}_1$ e $\mathbf{v}_2$, $\mathbf{v}_3 = \mathbf{v}_1+\mathbf{v}_2$ também é uma palavra código.
- Neste caso as palavras-código formam um sub-espaço do espaço de Hamming N dimensional.

0010010 + 0010001 = 0000011

Peso e distância de Hamming

- O peso de Hamming de um vetor é o número de 1's que ele tem. Por exemplo, o vetor [0**1**0**11**0**1**0**11**] tem peso de Hamming 6
- A distância de Hamming entre dois vetores é o número de posições em que eles diferem.
- A distância de Hamming entre dois vetores também pode ser vista como o peso de Hamming da soma módulo-2 dos dois vetores.

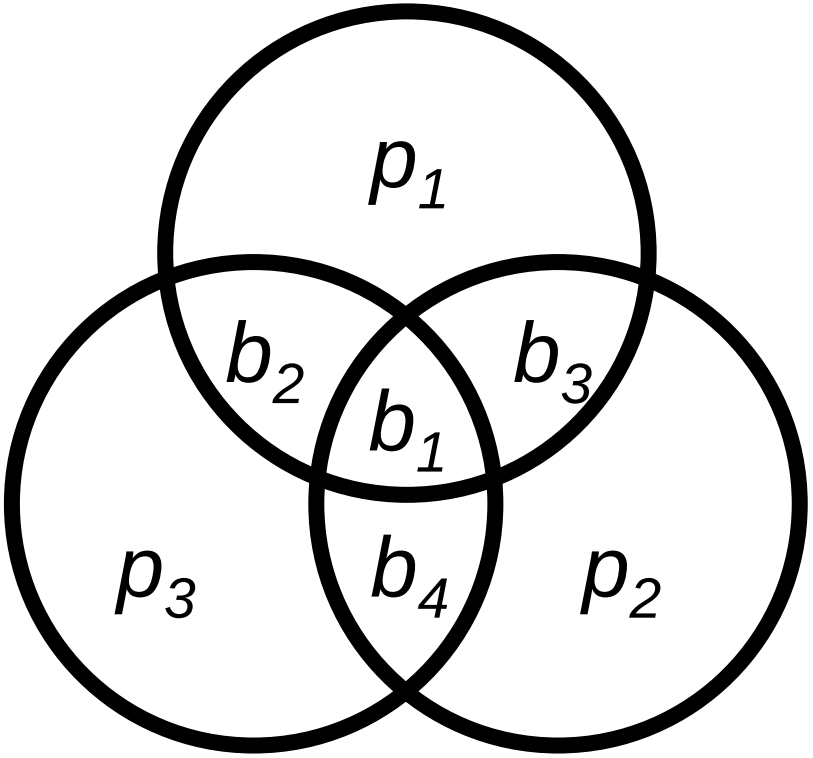
0010010 + 0010001 = 0000011

Recepção

- A palavra recebida pode ser diferente da palavra-código transmitida se houver erros de transmissão. O melhor que podemos fazer é encontrar a palavra-código mais próxima da recebida (critério MV), ou seja, a palavra-código que tem a menor distância de Hamming da palavra recebida.
- Estes códigos funcionam pela adição de redundância: para transmitir K bits de informação, utilizamos N>K bits da palavra-código.

Voltando ao exemplo

- Bloco transmitido pode ser gerado com regras mais elaboradas:



Bloco transmitido

$b_1 b_2 b_3 b_4 p_1 p_2 p_3$

Ex: **0110011**

Método permite identificar e corrigir até um erro de transmissão. Taxa de 4/7

Descrição via matriz geradora

- **v** = **uG** onde:

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

- Interpretação: as palavras código são combinações lineares das linhas de **G**, que são linearmente independentes

Descrição via matriz de verificação de paridade

- $\mathbf{vH}^T = \mathbf{0}$, onde:
- Interpretação: as palavras código são ortogonais aos vetores (coluna) de $\mathbf{H}^T$

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

Decodificação

- Decodificar é escolher os bits de informação a partir do vetor recebido.
- O problema é que o canal pode fazer com que o vetor recebido seja diferente do vetor transmitido
- Modelo útil: **r** = **v**+**e**, onde
  - **v** é o vetor transmitido → 0000000
  - **e** é o padrão de erro → 0000010
  - **r** é o vetor recebido → 0000010

Detecção por síndrome (1/2)

1. Transmitimos a palavra-código **v**
2. Há erros de transmissão de forma que recebemos **r** = **v**+**e**, onde a soma é modulo 2 e **e** é um vetor binário que vale 1 onde há erros de transmissão.
3. Ao testar a palavra recebida, obtemos:

$$\mathbf{s} = \mathbf{r}\,\mathbf{H}^T = (\mathbf{v}+\mathbf{e})\mathbf{H}^T = \mathbf{v}\mathbf{H}^T+\mathbf{e}\mathbf{H}^T = \mathbf{0} + \mathbf{e}\mathbf{H}^T.$$

4. Como $\mathbf{H}^T$ tem dimensão (K)X(N-K), há (N-K) vetores **s** distintos. Os valores de **s** são chamados de síndrome.

Detecção por síndrome (2/2)

5. Associamos para cada vetor **s** um padrão de erro **e'**. Há vários valores de **e** que geram o mesmo **s**. Entre todos os possíveis, selecionamos o valor de **e'** com o menor peso de Hamming, pois este é o mais provável.
6. Tentamos corrigir os erros de transmissão decidindo que a palavra-código transmitida foi **r**+**e'**.
7. Caso **e** = **e'**, decidiríamos corretamente por **r**+**e'** = **v**+**e**+**e'** = **v**+**e**+**e** = **v**
8. Caso **e** $\neq$ **e'**, decidiríamos erroneamente por **r**+**e'** $\neq$**v**. Neste caso teríamos erros de transmissão de informação.
9. Extraímos os bits de informação da palavra-código **r**+**e'**

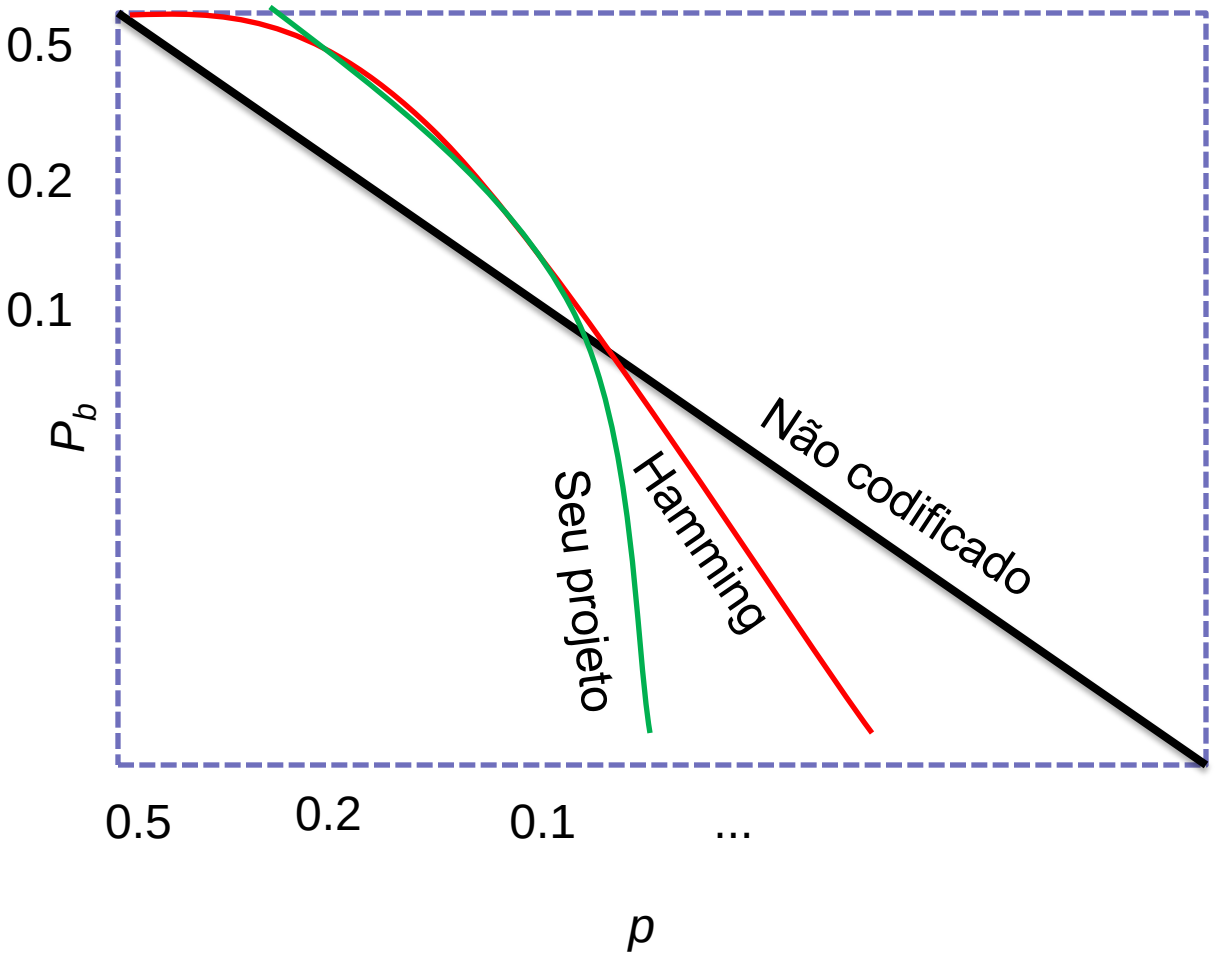
Exemplo

- Transmitimos 0000000
- Recebemos 00**1**0000
- Síndrome calculada = [0010000]H = [110]
- Padrões de erro que causam esta síndrome:
  - **0010000**, 1000001, 0101000, 0000110, ...
- É mais provável que tenha havido um erro de transmissão do que dois erros. Logo, **e**’ quando s = [110] vale 0010000
- Valor corrigido = 0010000+0010000 = 0000000
- O sistema corrigiu este erro
- De fato, este código é capaz de corrigir corretamente todas as situações em que há exatamente um erro de transmissão no bloco

Atividades

- Implemente o canal BSC com parâmetro *p* qualquer
- Implemente o codificador e decodificador de Hamming como descrito aqui
- Projete e implemente um codificador e decodificador com taxa 4/7 mas com tamanho de palavra-código maior do que o código de Hamming
- Obtenha via simulação as curvas de probabilidade de erro de bit de informação para os dois sistemas: o de Hamming e o seu projeto. Detalhes no roteiro

Resultado esperado



Visão alternativa: grafo