Teoria da Informação

Códigos de Hamming

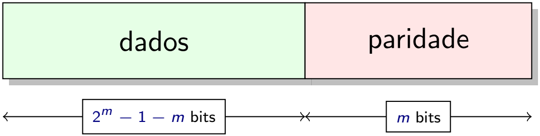
Miguel Barão

ESCOLA DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE INFORMÁTICA

Conhecimentos necessários:

- Aritmética módulo 2.
- Espaços vectoriais.
- Rank de uma transformação linear.
- Espaço nulo (kernel) de uma transformação linear.

O código de Hamming permite corrigir até 1 erro numa palavra de código.
Seleccionando o número pretendido de bits de paridade $m \geq 2$, as palavras de código têm comprimento $2^m - 1$, das quais m são bits de paridade e $2^m - 1 - m$ são dados.



Exemplo:

$$\underbrace{1111}_{\text{dados}}\ \underbrace{111}_{\text{paridade}}$$

Código de Hamming

- Define-se a matriz de Hamming onde cada coluna contém um número em binário de 1 a 7:

$$\mathbf{H} \triangleq \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- As palavras de código válidas são todas as que satisfazem a equação $\mathbf{Hc} = 0$. Isto é,

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

A tabela seguinte mostra todas as 16 palavras de código que satisfazem $\mathbf{Hc} = \mathbf{0}$:

0	0000000	8	1000011
1	0001111	9	1001100
2	0010110	10	1010101
3	0011001	11	1011010
4	0100101	12	1100110
5	0101010	13	1101001
6	0110011	14	1110000
7	0111100	15	1111111

- Suponha-se que ocorreu um erro na transmissão de uma palavra de código.
- A troca de um bit (devido ao erro) pode ser simulada fazendo um XOR bit-a-bit entre a palavra de código transmitida e um vector de zeros onde o bit onde ocorre o erro é colocado a um:

$$1010101$$

$$\oplus$$

$$0001000$$

$$=$$

$$1011101$$

- Ou seja, é recebida a palavra $\mathbf{r} = \mathbf{c} \oplus \mathbf{e}$.

- Como se viu anteriormente, uma palavra de código satisfaz $\mathbf{Hc} = \mathbf{0}$. O descodificador usa esta equação para detectar erros: $\mathbf{Hc} \neq \mathbf{0} \Rightarrow$ erro.
- Caso não ocorram erros na transmissão, a palavra recebida é igual à transmitida, $\mathbf{r} = \mathbf{c}$, e portanto $\mathbf{Hr} = \mathbf{0}$.
- No caso de ocorrer um erro na transmissão, a palavra recebida é $\mathbf{r} = \mathbf{c} \oplus \mathbf{e}$. Neste caso obtém-se

$$\begin{aligned}\mathbf{Hr} &= \mathbf{H}(\mathbf{c} \oplus \mathbf{e}) \\ &= \mathbf{Hc} \oplus \mathbf{He} \\ &= \mathbf{0} \oplus \mathbf{He} \\ &= \mathbf{He}\end{aligned}$$

- Qual o resultado de $\mathbf{He}$?

- Qual o resultado de **He**?
- Usando o exemplo anterior, $e = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}^T$, obtém-se

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

O resultado indica a posição onde ocorreu o erro!

Supondo que o código de Hamming (7,4) é aplicado num canal binário simétrico, qual a probabilidade de erro na descodificação?
Resposta: Como o código permite corrigir até um bit errado, então a transmissão ocorre sem erros nas seguintes situações:

- Não houve bits trocados.
- Houve um bit trocado.

A probabilidade de a transmissão ocorrer sem erros é então:

Supondo que o código de Hamming (7,4) é aplicado num canal binário simétrico, qual a probabilidade de erro na descodificação?
Resposta: Como o código permite corrigir até um bit errado, então a transmissão ocorre sem erros nas seguintes situações:

- Não houve bits trocados.
- Houve um bit trocado.

A probabilidade de a transmissão ocorrer sem erros é então:

$$\Pr\{\text{não ocorrerem erros}\} = (1 - p_e)^7 + 7(1 - p_e)^6 p_e.$$