The Hong Kong Polytechnic University
香港理工大學

Classical error correction using the [7,4,3] Hamming code

recovering from bit errors using parity checks

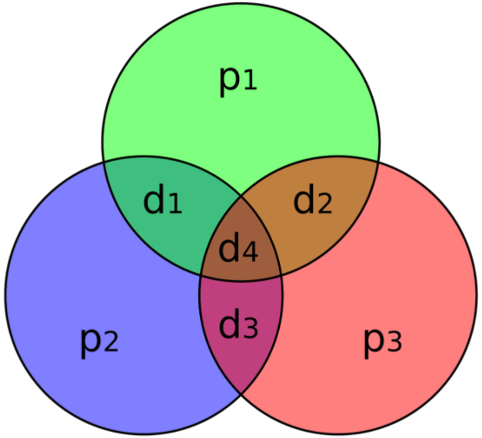
Quantum Computing

Presenter: Eric XI

July 28, 2025

Contents

- Background
- A visually appealing representation
- Classical error correction
  - Linear vector spaces
  - Classical coding theory
- Parity check
  - Venn diagram
  - Matrix



Background

- Classical communication can be considered to consist of the transmission of binary digits (message, binary word, binary vector). A noisy communication channel will corrupt the message, change the message **u** to **u'**. The difference **e** = **u'** − **u** is called the error vector. Error correction consists in deducing **u** from **u'** (1).

- Error correction code (ECC) is a tool for error detection and correction in information transmission.

- Richard Hamming pioneered this field in the 1940s and invented the first error-correcting code in 1950: the [7,4,3] Hamming code.

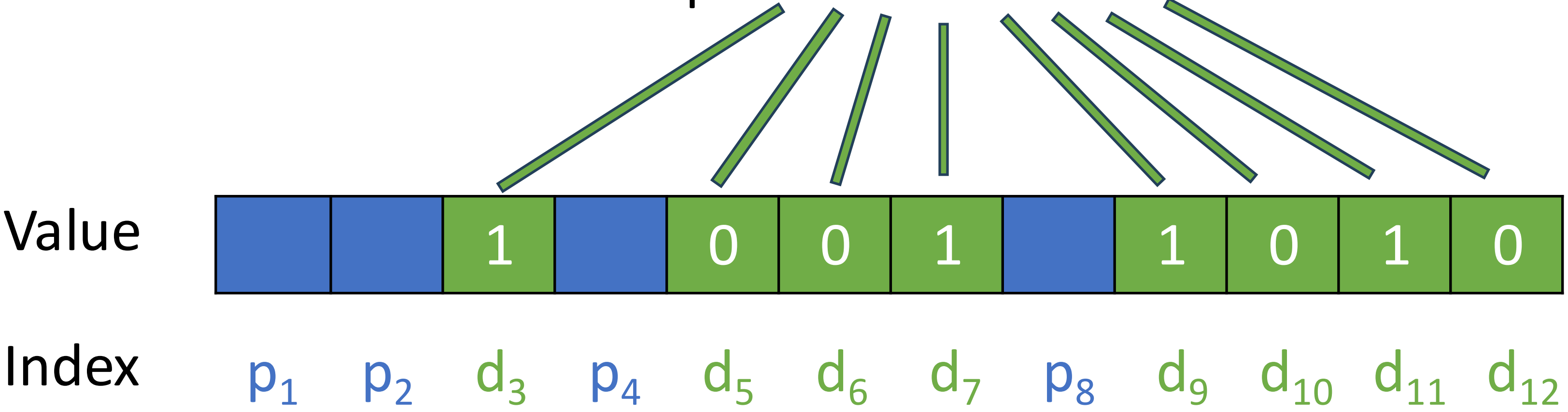
- In quantum error correction, the [7,4,3] Hamming code is used as the base for the Steane code (2).

Background

- [7,4,3] Hamming code: A linear error-correcting code that encodes 4 bits of data into 7 bits by adding 3 parity bits.
    - The notation [n, k, d] (7,4,3) means that the codewords are n bits long, there are 2^k of them (k dimension of the vector space specified by Generator matrix G), and they all differ from each other in at least d digits (minimum Hamming distance).
    - This algorithm can detect and correct any single-bit error, or detect two-bit errors.
    - Perfect codes, have optimal error correction efficiency (Codes that attain the Hamming bound).

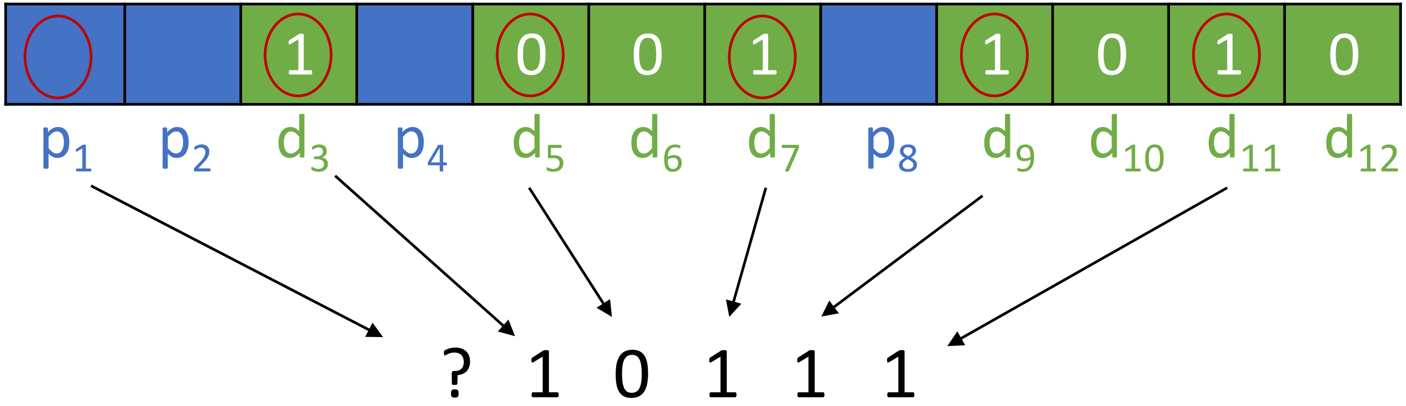
A visually appealing representation

- Example: 1 0 0 1 1 0 1 0



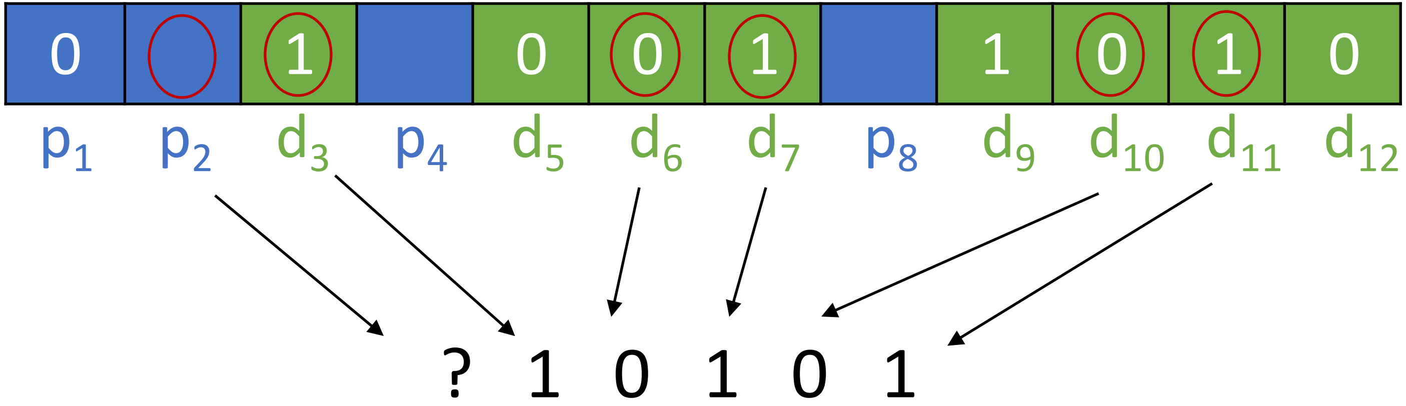
A visually appealing representation

- Example: 1 0 0 1 1 0 1 0



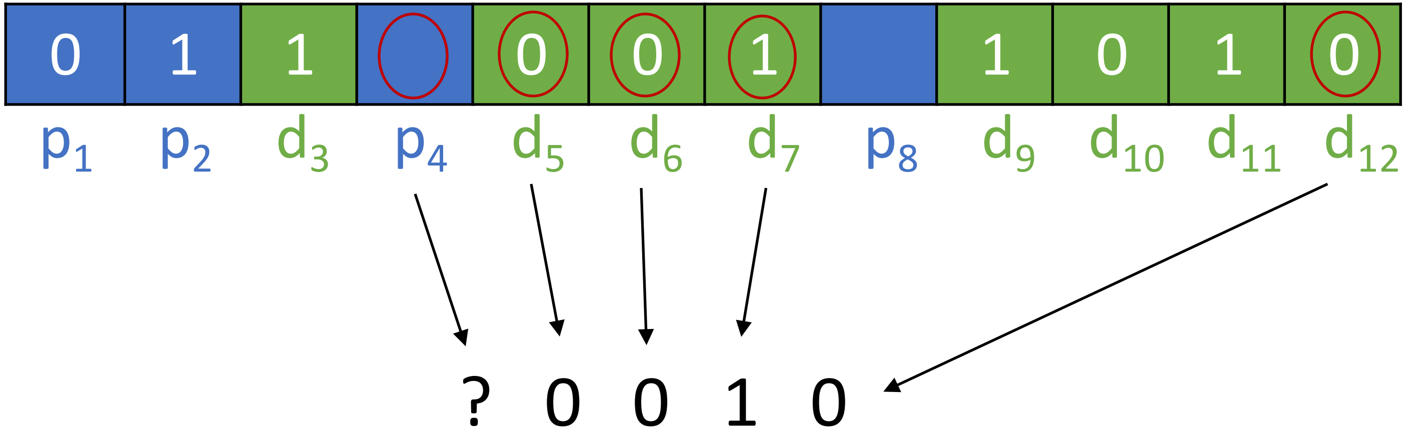
A visually appealing representation

- Example: 1 0 0 1 1 0 1 0



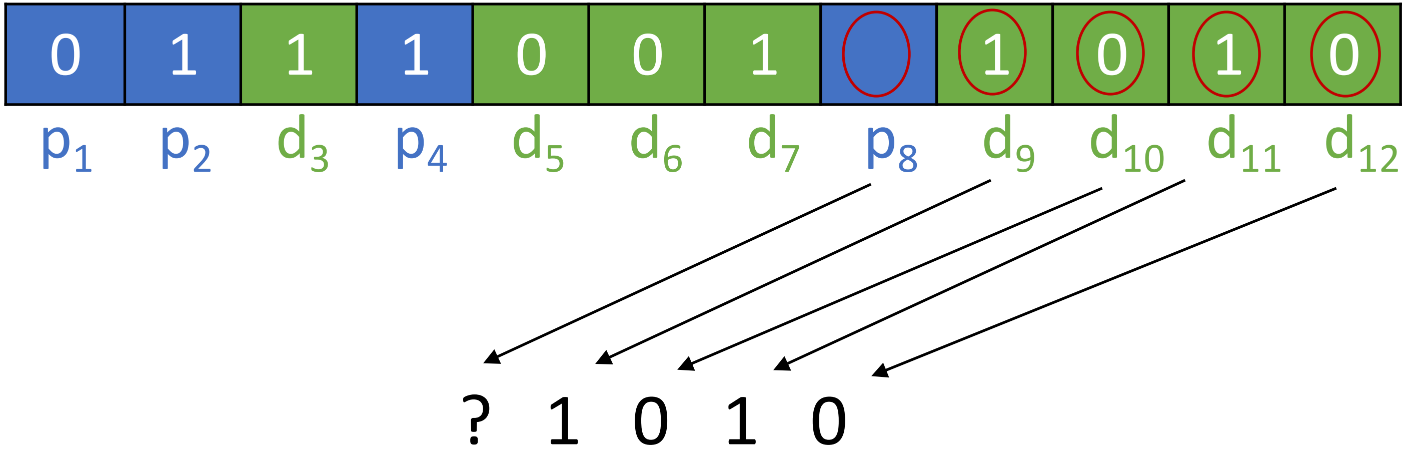
A visually appealing representation

- Example: 1 0 0 1 1 0 1 0



A visually appealing representation

- Example: 1 0 0 1 1 0 1 0



A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

  Error detection

0	1	1	1	0	0	1	0	1	0	1	0
p_1	p_2	d_3	p_4	d_5	d_6	d_7	p_8	d_9	d_{10}	d_{11}	d_{12}

0	1	1	1	0	0	1	0	1	1	1	0
p_1	p_2	d_3	p_4	d_5	d_6	d_7	p_8	d_9	d_{10}	d_{11}	d_{12}

A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

Error detection

0	1	1	1	0	0	1	0	1	1	1	0
p_1	p_2	d_3	p_4	d_5	d_6	d_7	p_8	d_9	d_{10}	d_{11}	d_{12}

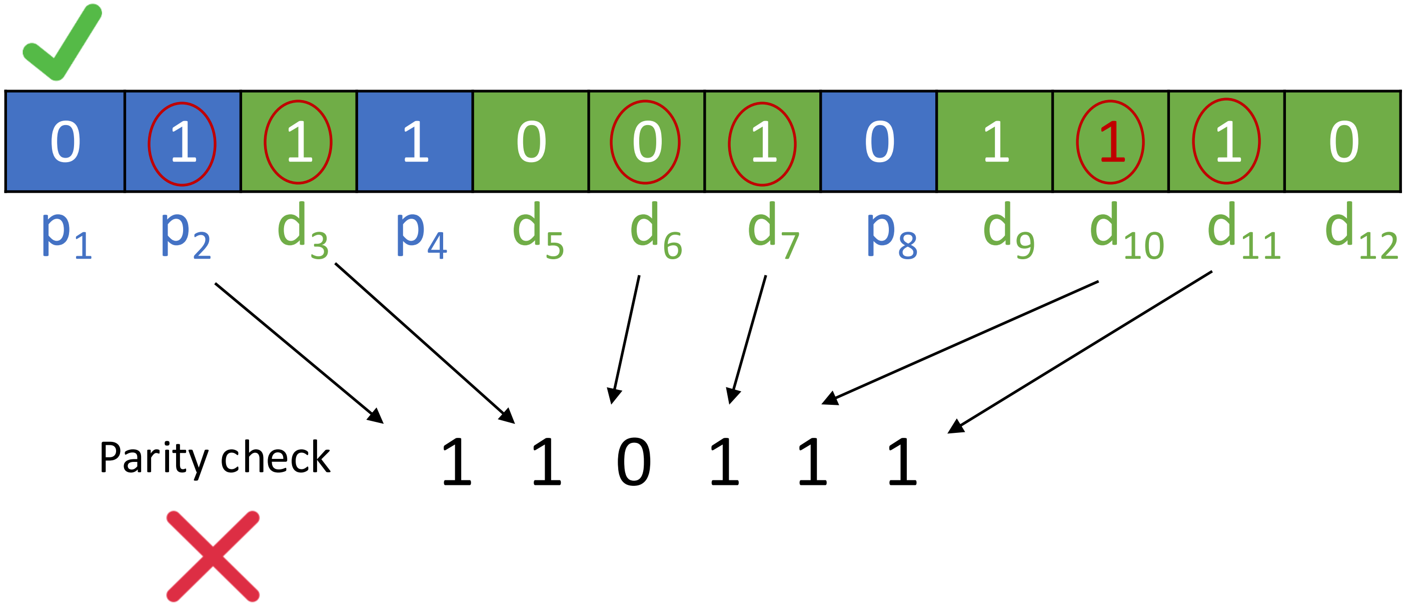
Parity check 0 1 0 1 1 1

✔

A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

Error detection



A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

Error detection

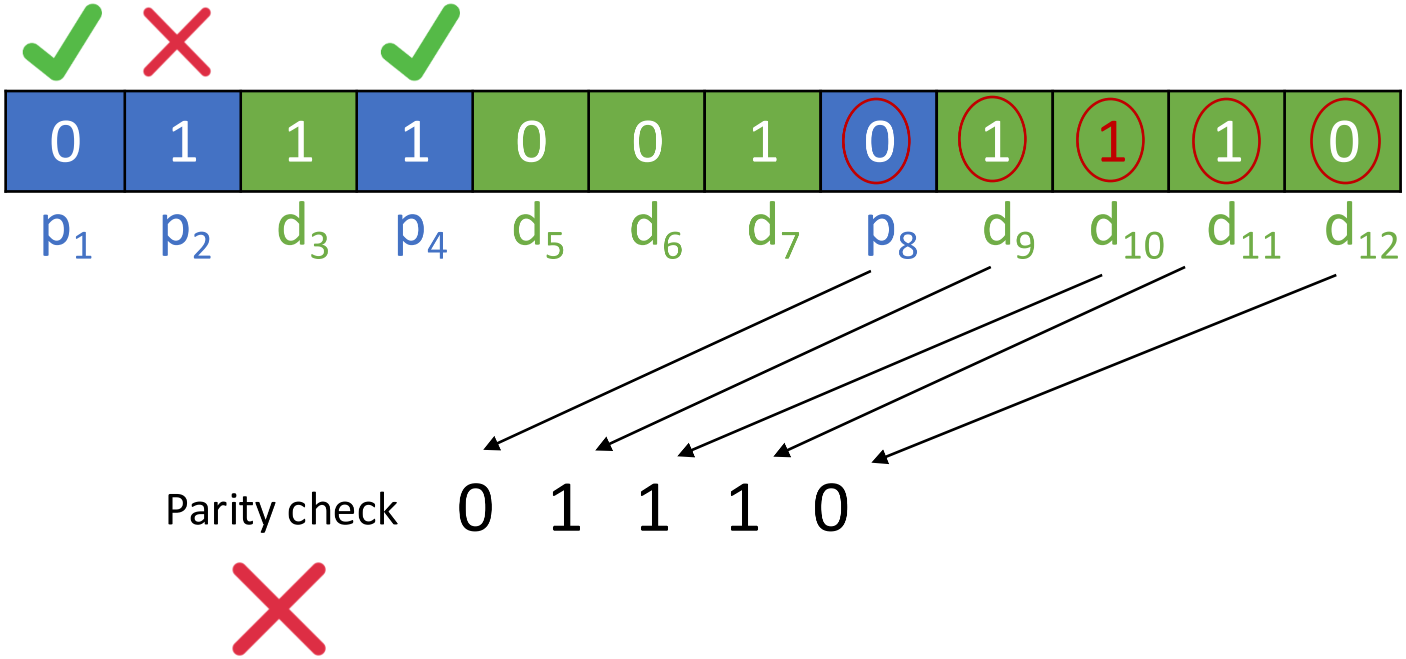
0	1	1	1	0	0	1	0	1	1	1	0
p_1	p_2	d_3	p_4	d_5	d_6	d_7	p_8	d_9	d_{10}	d_{11}	d_{12}

Parity check 1 0 0 1 0

A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

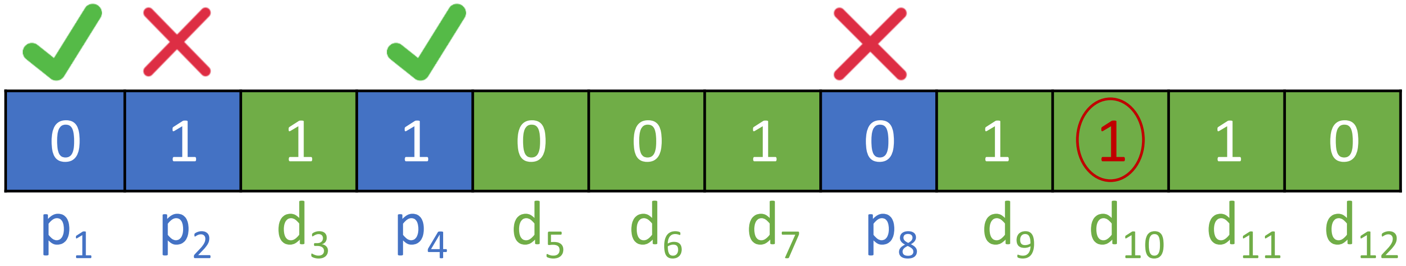
Error detection



A visually appealing representation

- Example: 1 0 0 1 1 0 1 0

Error detection



Here P_2 and P_8 are incorrect, so 2+8=10th bit is the bad bit

Preliminary

- A string of n bits is considered to be a vector of n components
  - E.g. 011 is the vector (0,1,1).

- Vector addition: equivalent to the exclusive-or operation $\oplus$ carried out bitwise between the binary strings
  - E.g. (0,1,1) + (1,0,1) = (0 + 1,1 + 0,1 + 1) = (1,1,0)

- Inner product (also called parity check or check sum)
  - E.g. (1,1,0,1) · (1,0,0,1) = 1 + 0 + 0 + 1 = 0
  - To satisfy a parity check **u**, $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}\mathbf{v}^T = 0$

- Linear vector space $\longrightarrow$ Hamming space, completely specified by its generator matrix G
  - E.g. $G = \begin{pmatrix} 0011 \\ 1100 \end{pmatrix} = \begin{pmatrix} 0011 \\ 1111 \end{pmatrix}$ 2^2 vectors

Preliminary

- Weight (or Hamming weight) of a binary vector **u** is the number of non-zero components, written wt(u).
  - E.g. wt(0001101) = 3

- The minimum distance d of a linear space is equal to the smallest weight of a non-zero vector of the space.

- Parity check matrix H
  - $HG^T = \mathbf{0}$

Preliminary

- For [7, 4, 3] Hamming code:
  - The generator matrix is

$$G = \begin{pmatrix} 1010101 \\ 0110011 \\ 0001111 \\ 1110000 \end{pmatrix} \tag{1}$$

  - So the sixteen members of the space are

$$\begin{array}{cccc} 0000000 & 1010101 & 0110011 & 1100110 \\ 0001111 & 1011010 & 0111100 & 1101001 \\ 1110000 & 0100101 & 1000011 & 0010110 \\ 1111111 & 0101010 & 1001100 & 0011001 \end{array} \tag{2}$$

  - The parity check matrix is

$$H = \begin{pmatrix} 1010101 \\ 0110011 \\ 0001111 \end{pmatrix} \tag{3}$$

Preliminary

- For [7, 4, 3] Hamming code:

$$\begin{array}{cccc} 0000000 & 1010101 & 0110011 & 1100110 \\ 0001111 & 1011010 & 0111100 & 1101001 \\ 1110000 & 0100101 & 1000011 & 0010110 \\ 1111111 & 0101010 & 1001100 & 0011001 \end{array}$$

The minimum distance is 3 since the smallest weight of vectors is 3.

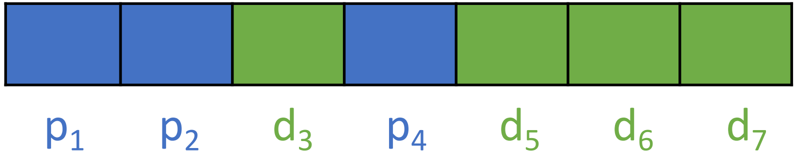
- A code with minimum Hamming distance d between its codewords can detect at most d-1 errors and can correct $\lfloor(d-1)/2\rfloor$ errors (3).

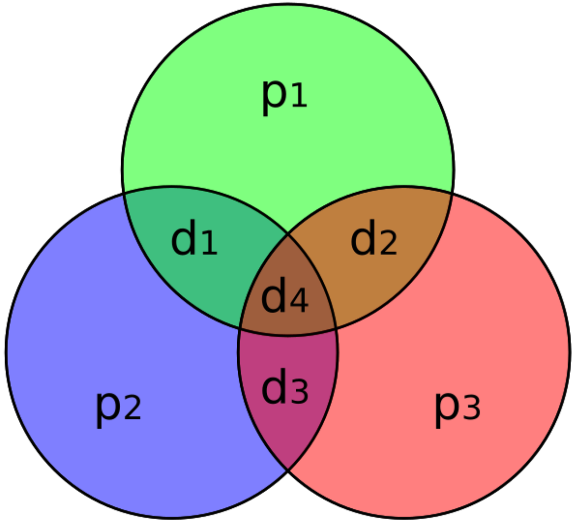
- Hamming bound: For a Hamming space, the number of code vectors is limited by the Hamming bound

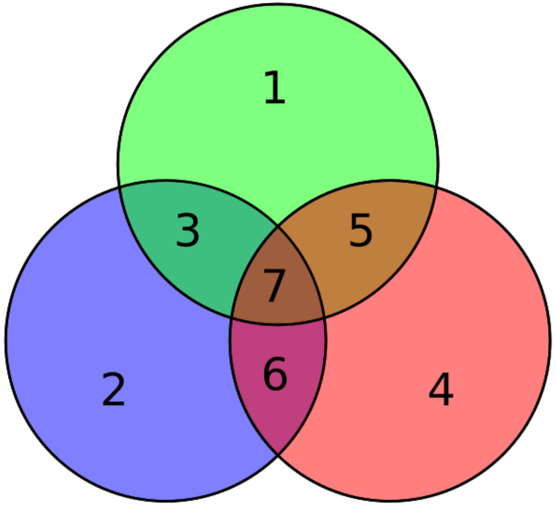
$$2^7/(C(7,0) + C(7,1)) = 2^7/(1 + 7) = 2^4 \qquad (4)$$

Parity check by Venn diagram

- For [7, 4, 3] Hamming code:



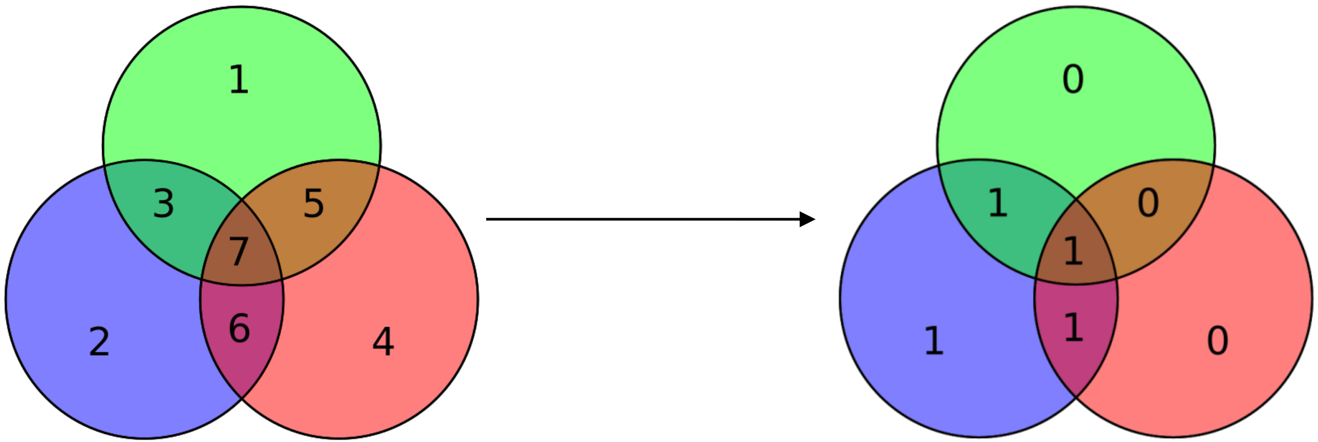




Parity check by Venn diagram

- For [7, 4, 3] Hamming code:

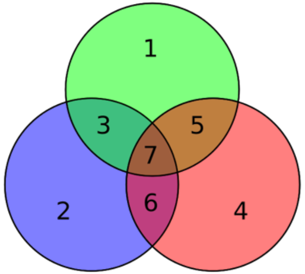
0	1	1	0	0	1	1
p_1	p_2	d_3	p_4	d_5	d_6	d_7

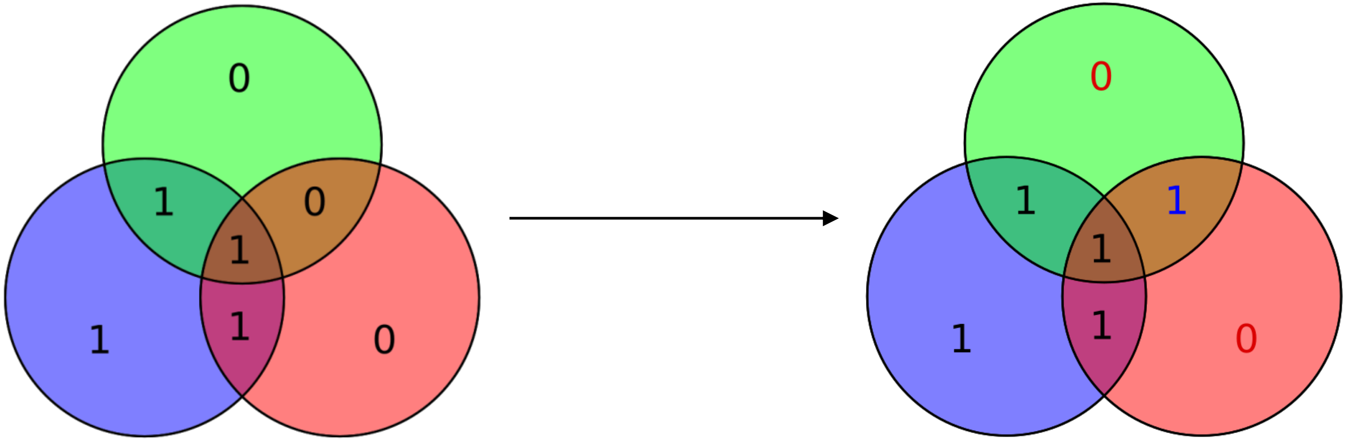


Parity check by Venn diagram

- For [7, 4, 3] Hamming code:

p_1	p_2	d_3	p_4	d_5	d_6	d_7
0	1	1	0	1	1	1





Parity check by Matrix

- For [7, 4, 3] Hamming code:

$$\mathbf{p} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{5}$$

$$\mathbf{x} = \mathbf{G}^{\mathrm{T}}\mathbf{p} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \\ 2 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{6}$$

$$\mathbf{z} = \mathbf{H}\mathbf{r} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \tag{7}$$

Parity check by Matrix

- For [7, 4, 3] Hamming code:

$$\mathbf{r} = \mathbf{x} + \mathbf{e}_5 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \tag{8}$$

$$\mathbf{z} = \mathbf{H}\mathbf{r} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \tag{9}$$

$$\mathbf{r}_{\text{corrected}} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ \overline{1} \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{10}$$

References

(1) Atkins AB, Dyl EA. Price reversals, Bid-Ask spreads, and market efficiency. Journal of Financial and Quantitative Analysis [Internet]. 1990 Dec 1;25(4):535. Available from: https://doi.org/10.2307/2331015

(2) Steane AM. Error correcting codes in quantum theory. Physical Review Letters [Internet]. 1996 Jul 29;77(5):793–7. Available from: https://doi.org/10.1103/physrevlett.77.793

(3) Robinson DJS. An introduction to abstract algebra. Walter de Gruyter; 2008.

(4) Wikipedia contributors. Hamming(7,4) [Internet]. Wikipedia. 2025. Available from: https://en.wikipedia.org/wiki/Hamming(7,4)