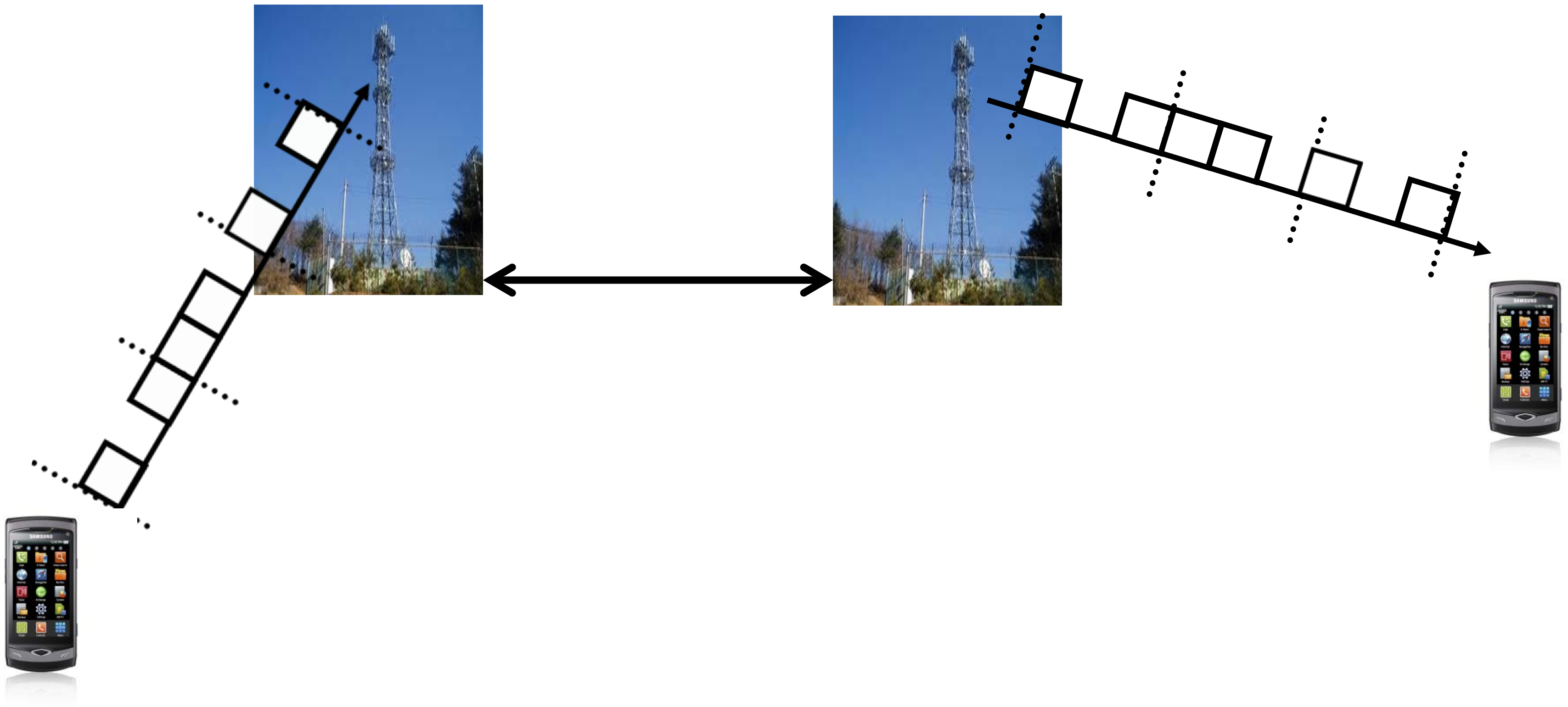
Hamming Codes

Heung-No Lee

2020-11-08

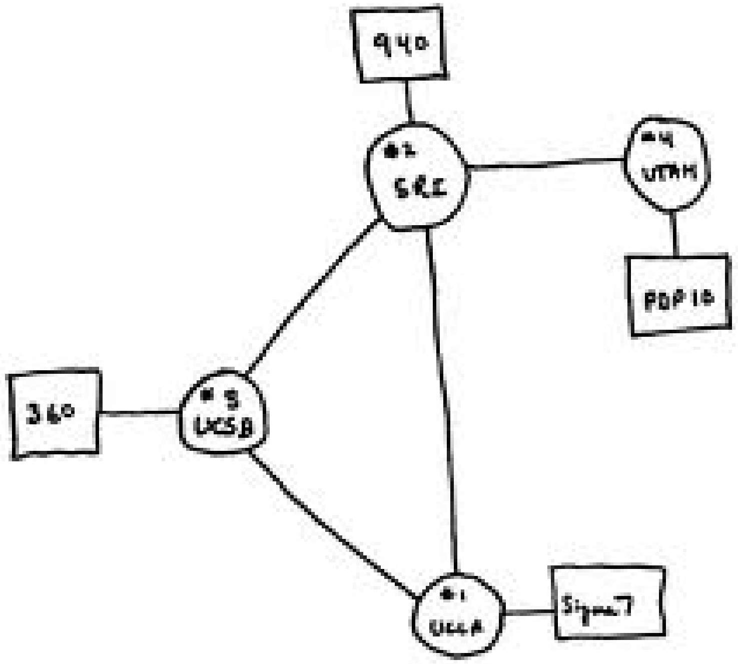
Binary Waves Carry Your Voice

- Sound waves → Analog Digital Conversion → Bit stream
- Electro magnetic waves are used to present a bit.
- The most simple one is ON-OFF communications.
- Bit Flip Errors occur during transmission and reception process.



Internet Channel ~ erasures occur!

- Idea inception, 1960s, USA.
  - ARPANET
- Researchers @UCLA, UCSB, SRI, U-UTAH
  - 1969, 4 computers
  - The 1st remote login success (UCLA Professor Kleinrock)
  - Information packets are used.
  - Packets may be dropped, if congested.



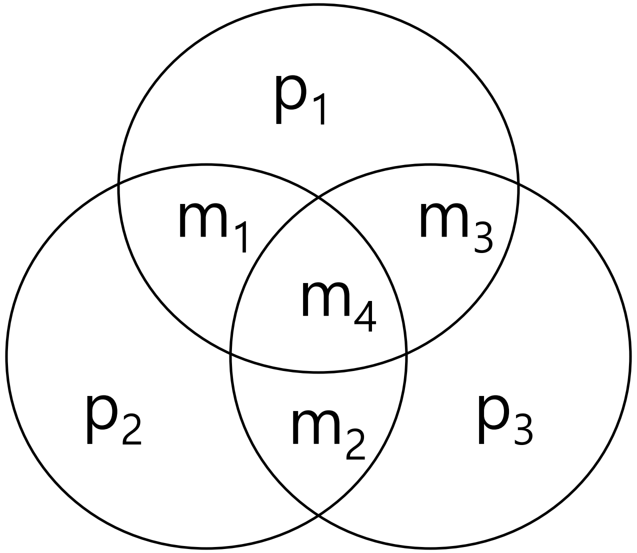
Early Internet 1969

Hamming Codes (1950)

- Length 7 Bit Pattern

m_1	m_2	m_3	m_4	p_1	p_2	p_3

- Four bits are *information* bits
- Three bits are *check* bits
- Together is a codeword.



- Check bits are added to correct errors!
- **How**: make codeword bits related with each other!
- **Relation**: All numbers inside a circle should sum up to zero.

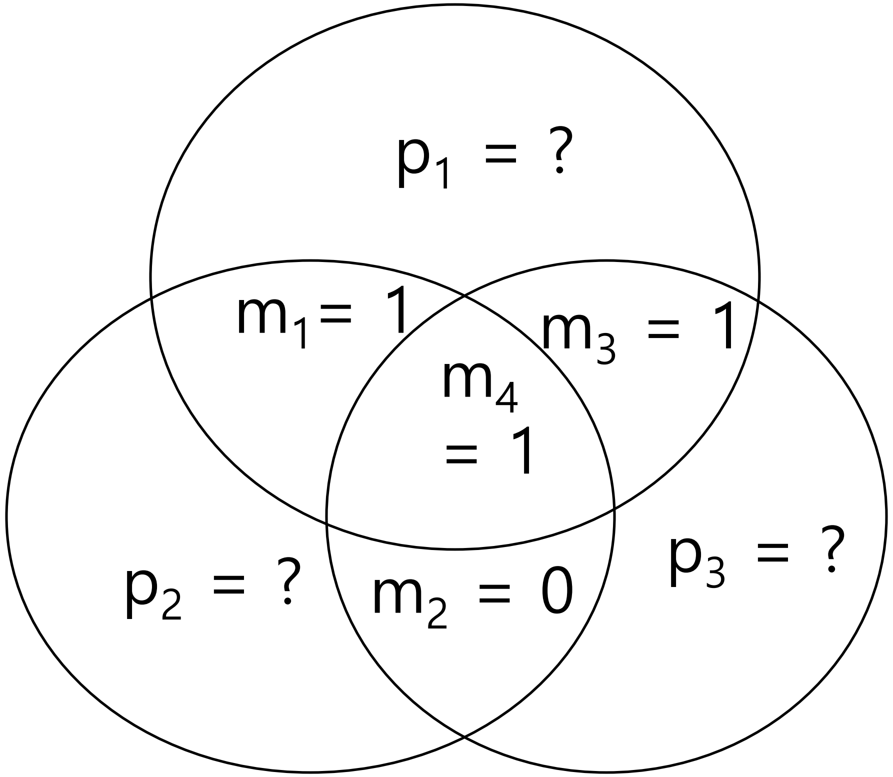
Channel Coding

- Message
- Encoding: tx message → codeword
- Channel: codeword → Received codeword
- Decoding: received codeword → decoded codeword → decoded message
- Decoding error: tx message is not equal to dec message.

Hamming Codes (1950) : Encoding Ex 1

- Info bits are
  (1, 0, 1, 1)
- What is the codeword?
- (1, 0, 1, 1, p_1, p_2, p_3)?
  - p_1 = ?
  - p_2 = ?
  - p_3 = ?

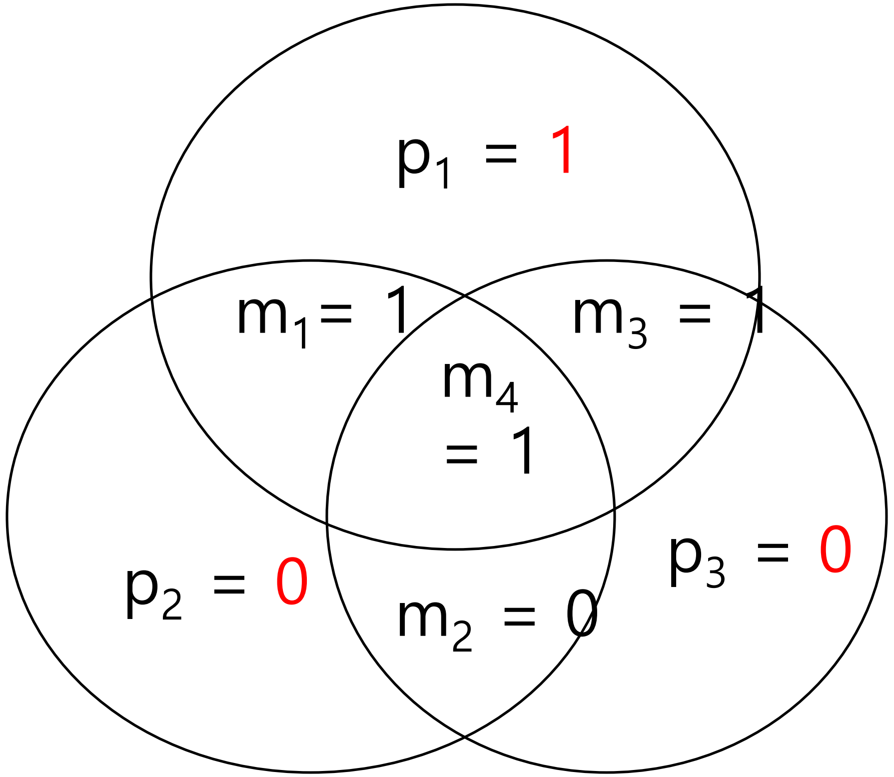
m_1	m_2	m_3	m_4	p_1	p_2	p_3
1	0	1	1	?	?	?



Hamming Codes (1950) : Codeword

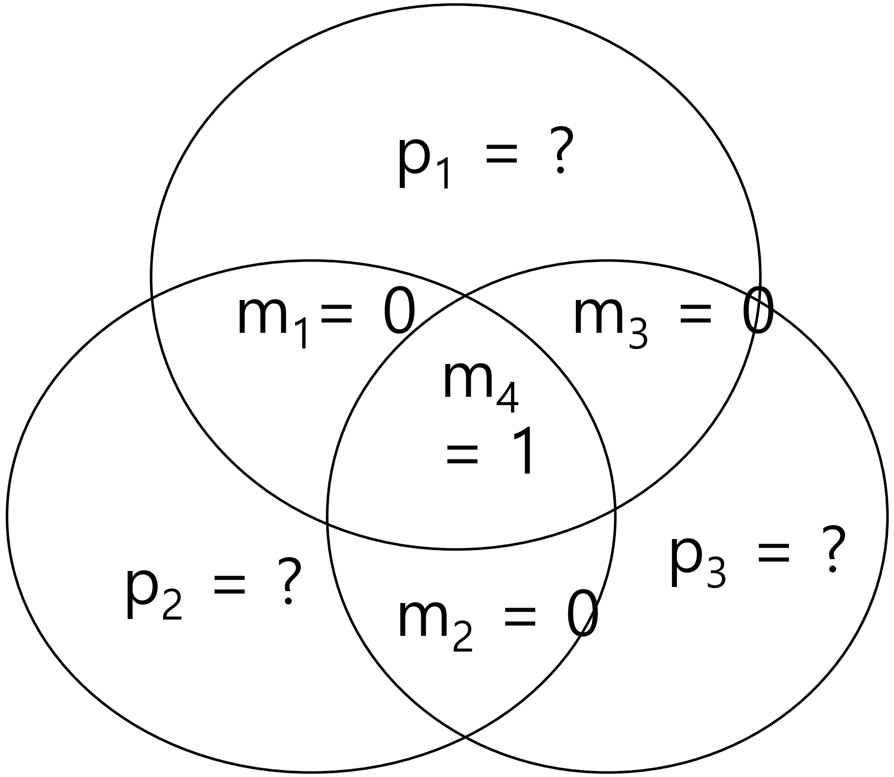
- Info bits are (1, 0, 1, 1)
- What is the codeword?
- (1, 0, 1, 1, p_1, p_2, p_3)?
  - p_1 = 1
  - p_2 = 0
  - p_3 = 0

m_1	m_2	m_3	m_4	p_1	p_2	p_3
1	0	1	1	1	0	0



Hamming Codes (1950) : Encoding Ex 2

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	1	?	?	?

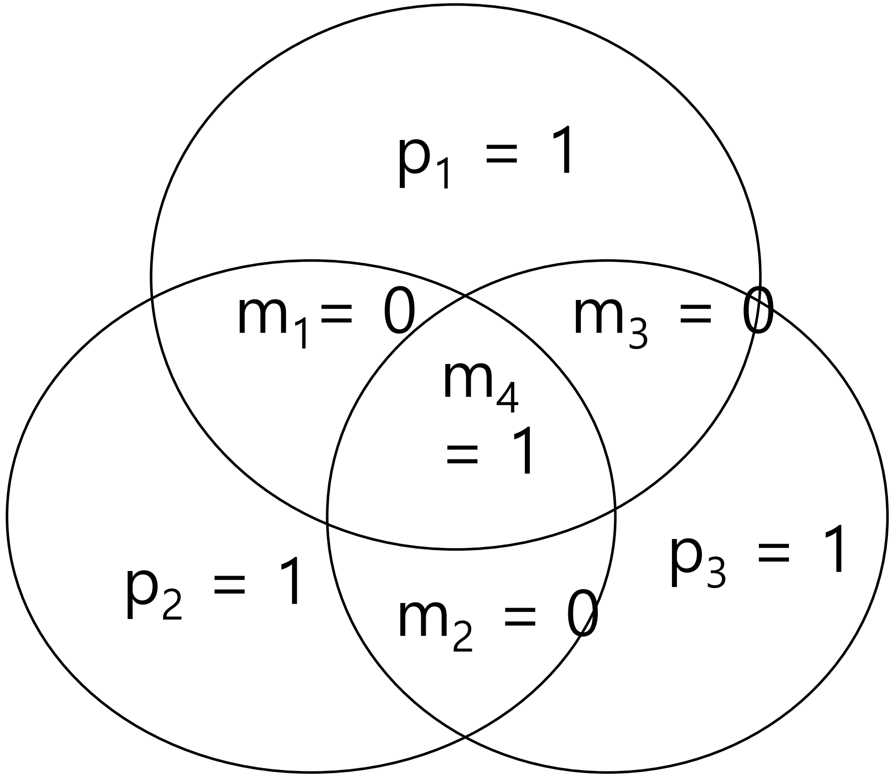


Hamming Codes (1950) : Codeword

(0, 0, 0, 1, p_1, p_2, p_3)?

- p_1 = 1
- p_2 = 1
- p_3 = 1

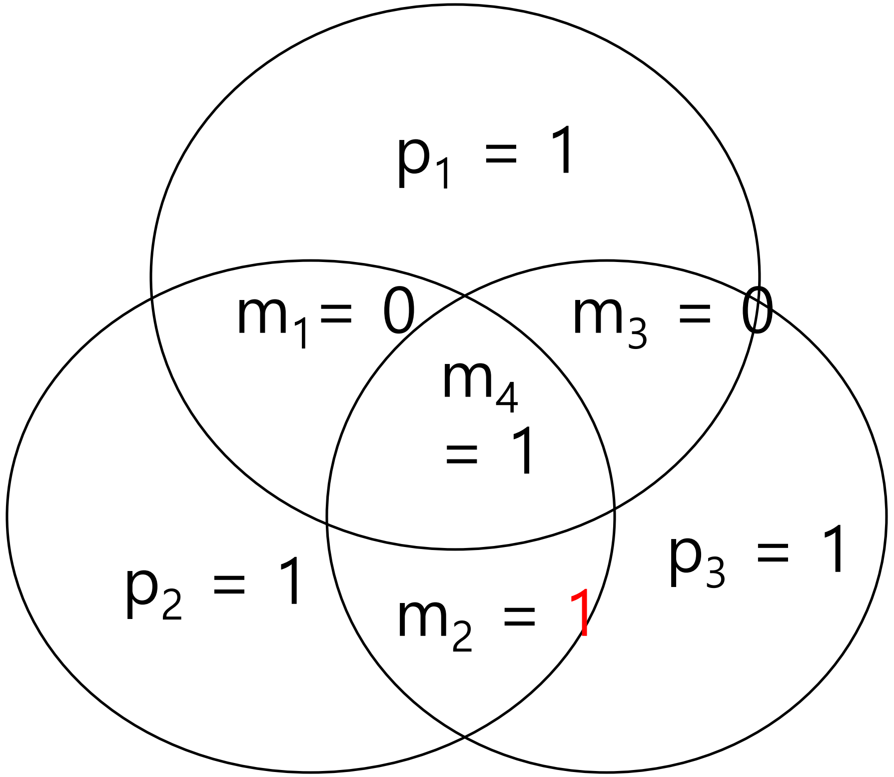
m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	1	1	1	1



Decoding Ex 1

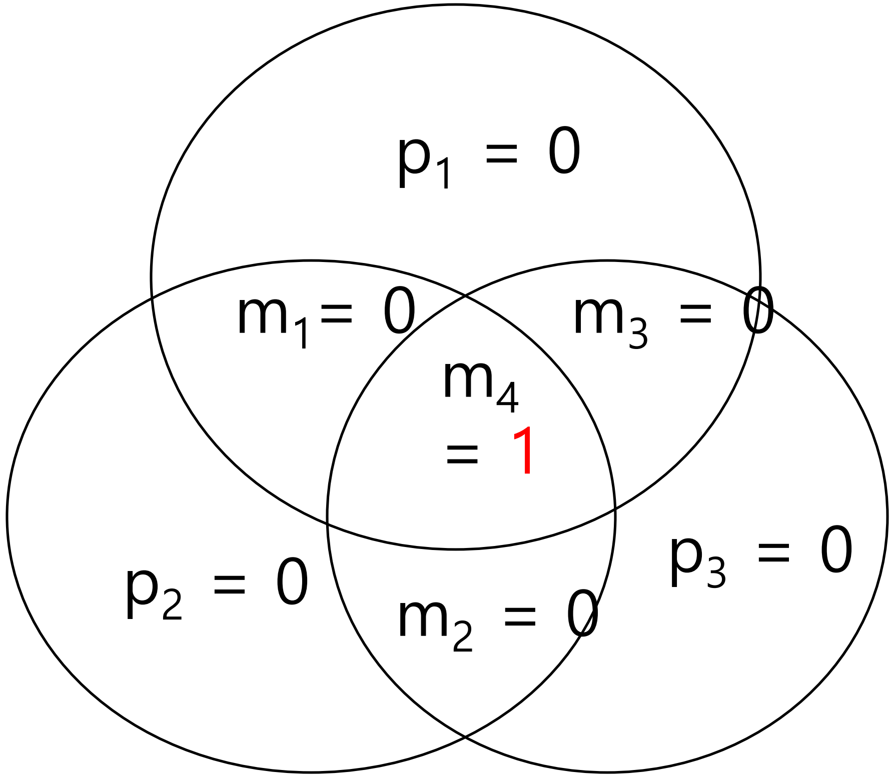
- Suppose the transmitted word is
  (0, 0, 0, 1, 1, 1, 1)
- Suppose the 2nd bit is flipped.
- Namely, received is (0, 1, 0, 1, 1, 1, 1).
- Let's write the results into the diagram and try to decode it.
- 1st circle is O.K.
- 2nd, 3rd circles are NG.
- Note m2 = 0 makes both OK.
- Error corrected!

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	1	0	1	1	1	1



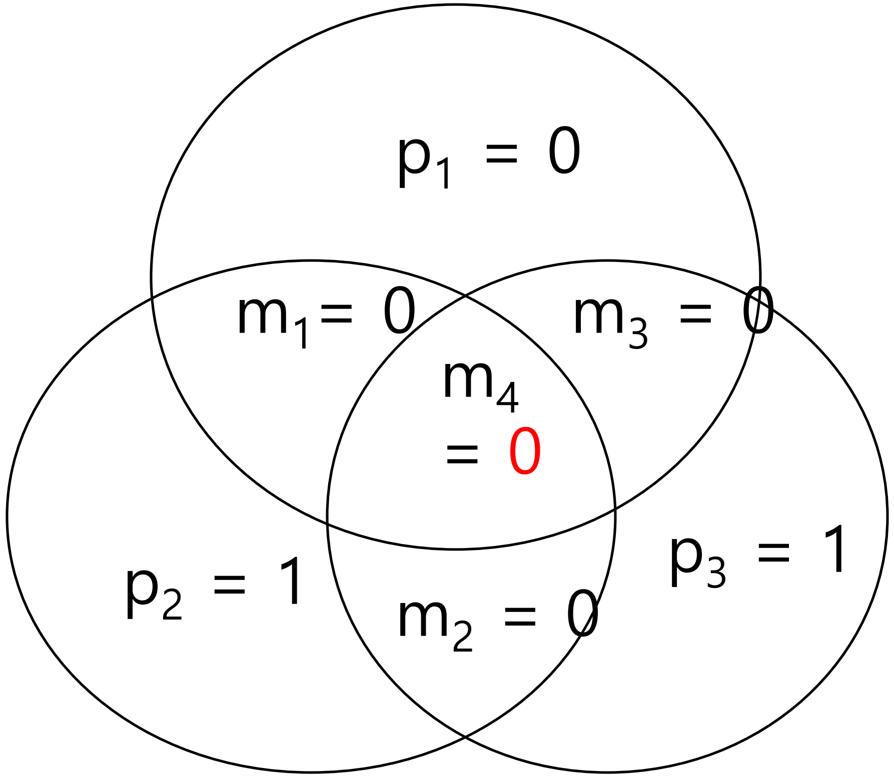
Decoding Exercise 2:

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	1	0	0	0



Decoding Exercise 2:

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	0	0	0	0



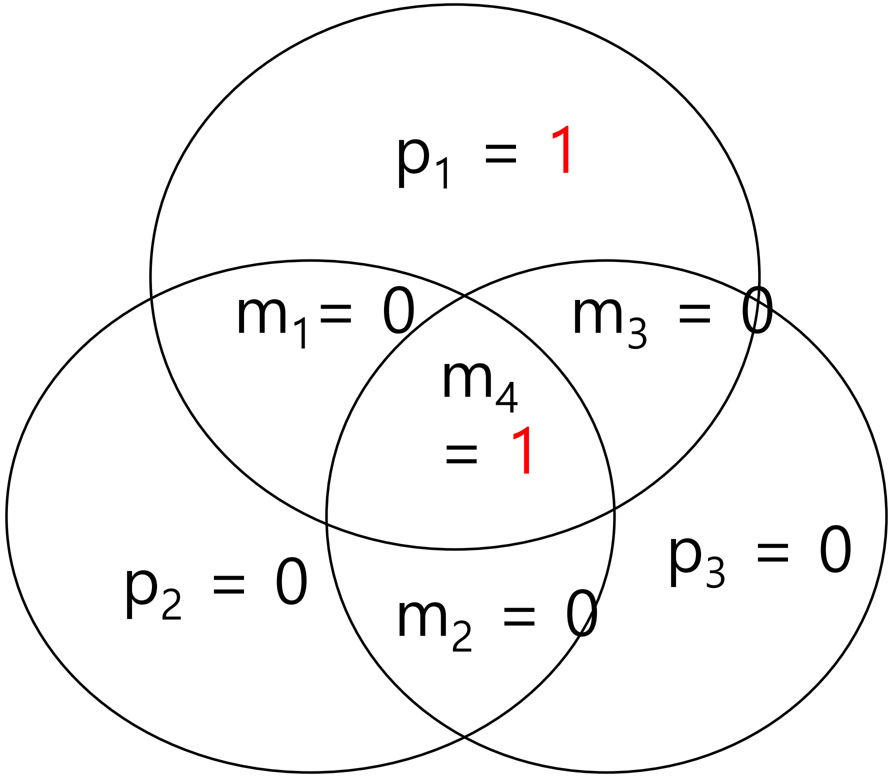
Decoding Exercise 3:

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	1	1	0	0

Correctable?

One bit correction → No

Two bit correction →
(0 0 0 0 0 0 0)
(1 0 1 1 1 0 0)
… not unique



Erasure Error Correction Ex 1

- Let Tx codeword be

(0, 0, 0, 1, 1, 1, 1)

- 1^{st} and 2^{nd} erased

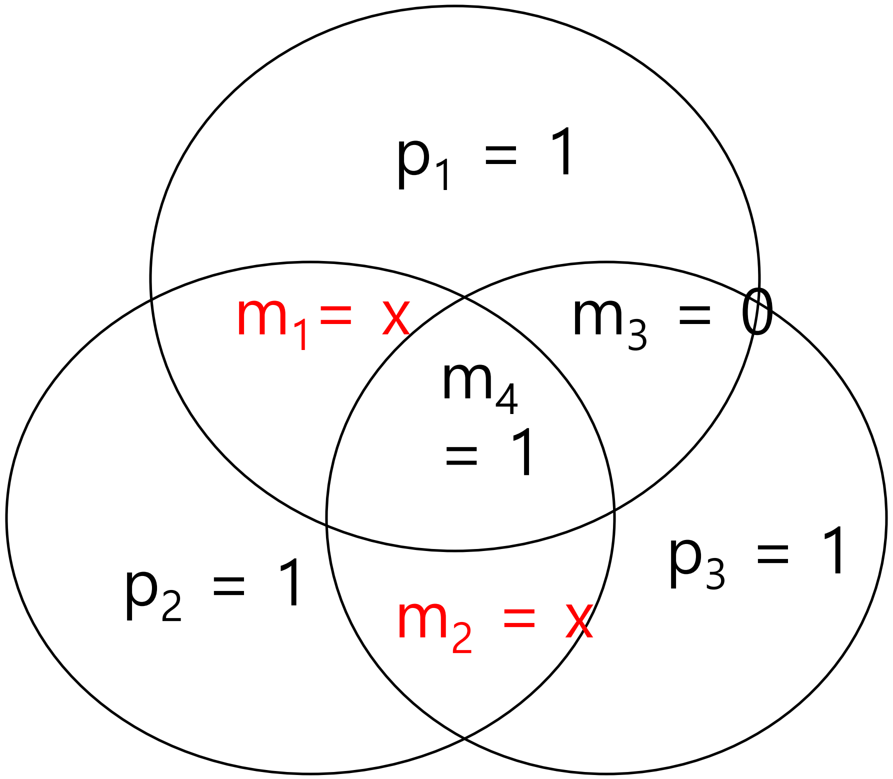
m_1	m_2	m_3	m_4	p_1	p_2	p_3
x	x	0	1	1	1	1

- Rx codeword be (x, x, 0, 1, 1, 1, 1).

- Let us decode it.

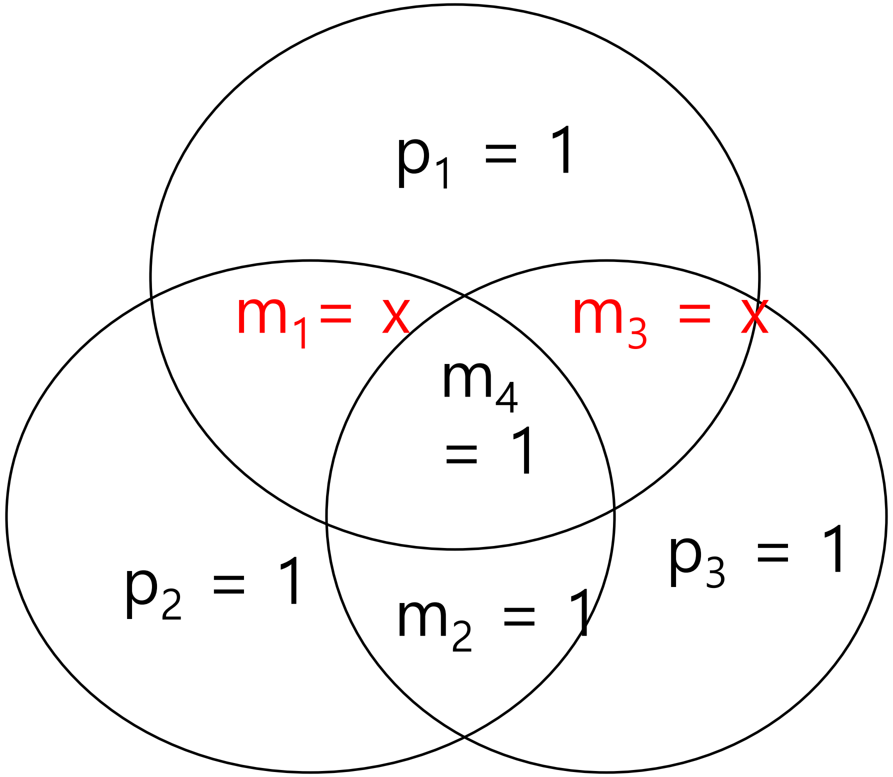
- 2^{nd} circle has two erasures.

- Set m_1 = 0, at 1^{st} circle.
- Set m_2 = 0, at 3^{rd} circle.



Erasure Error Correction Ex 2

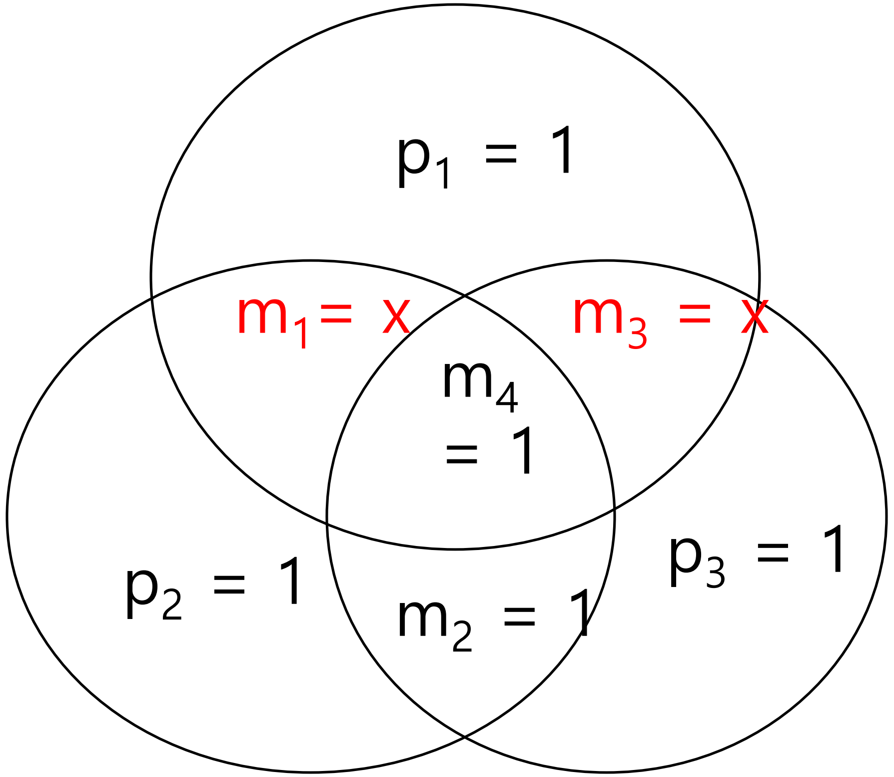
m_1	m_2	m_3	m_4	p_1	p_2	p_3
x	1	x	1	1	1	1



Erasure Error Correction Ex 2

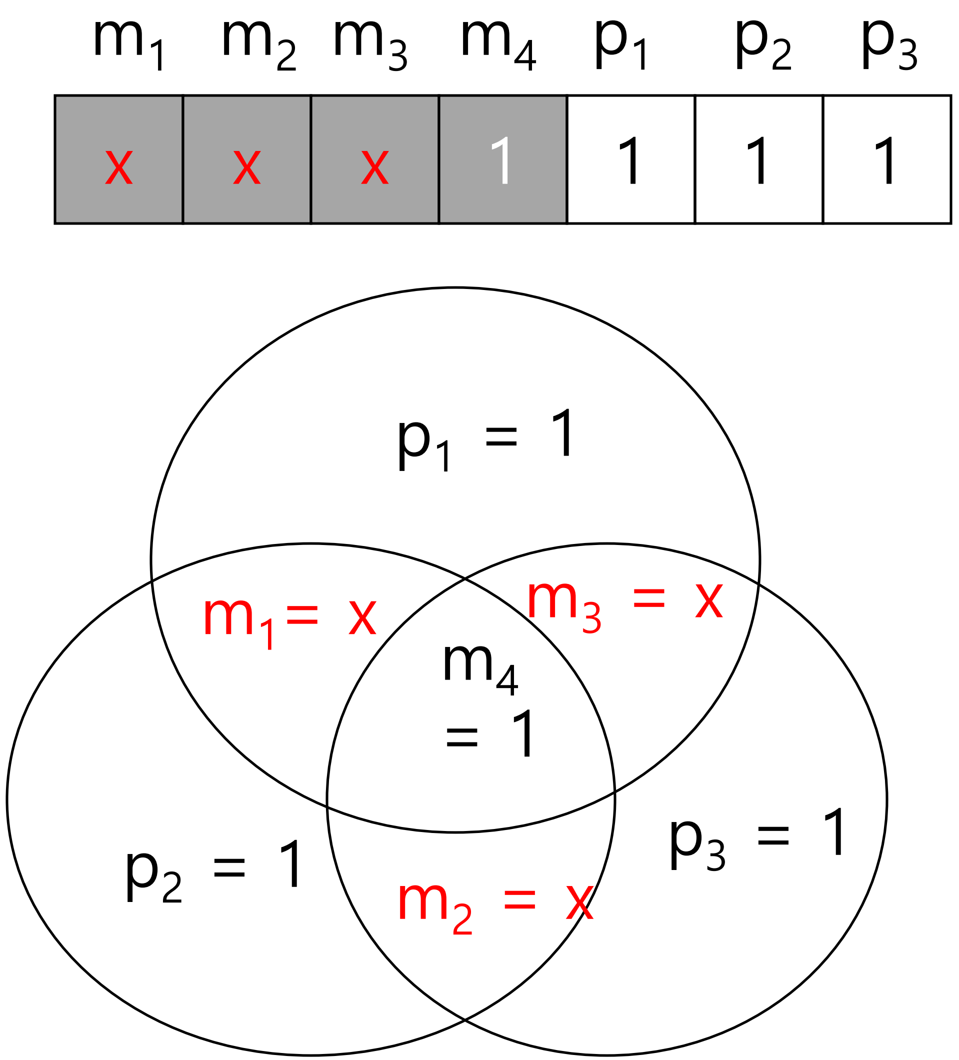
- 받은 비트 패턴이 (x, 1, x, 1, 1, 1, 1).
- 1st circle: 2 erasures → wait
- 2nd circle: $m_1 = 1$.
- 3rd circle: $m_3=1$.

m_1	m_2	m_3	m_4	p_1	p_2	p_3
1	1	1	1	1	1	1

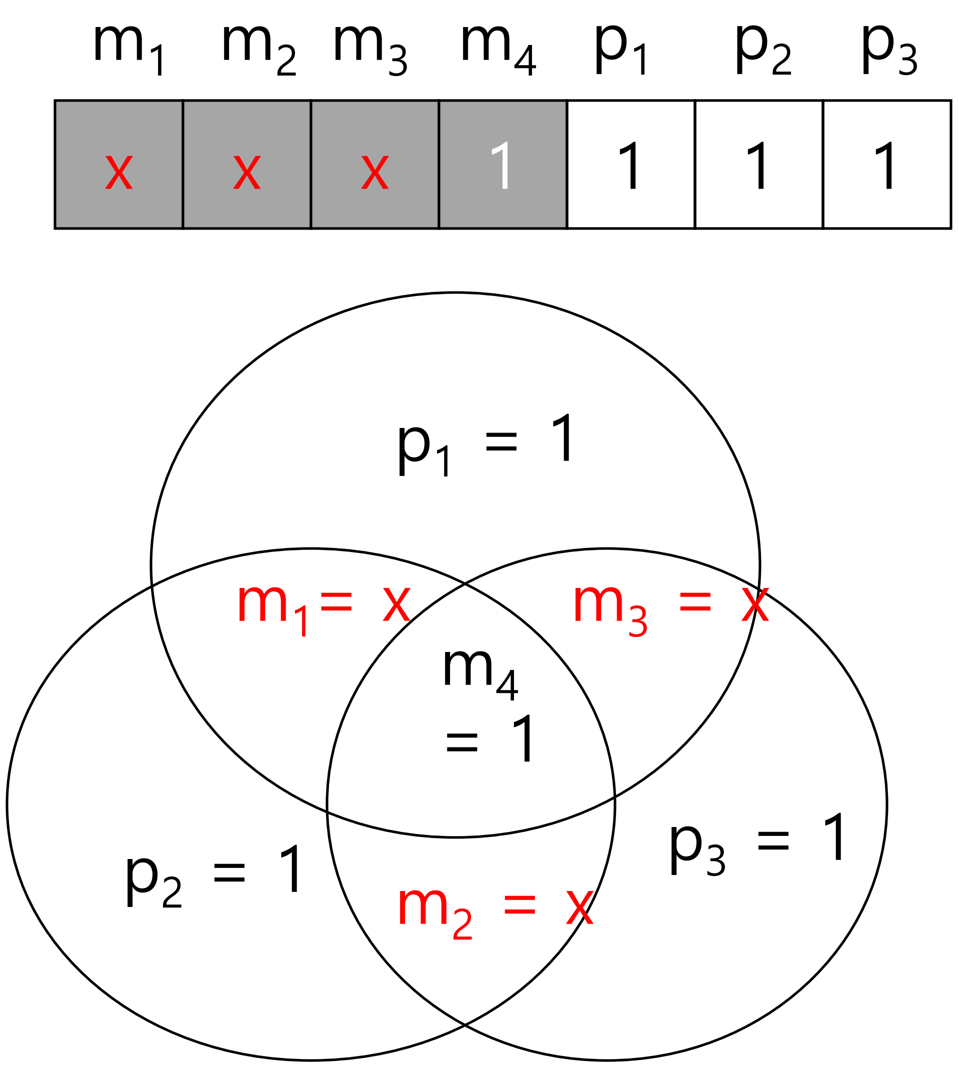


Erasure Error Correction Ex 3

- Three erasures
- **Decoding possible?**



Erasure Error Correction Ex 3

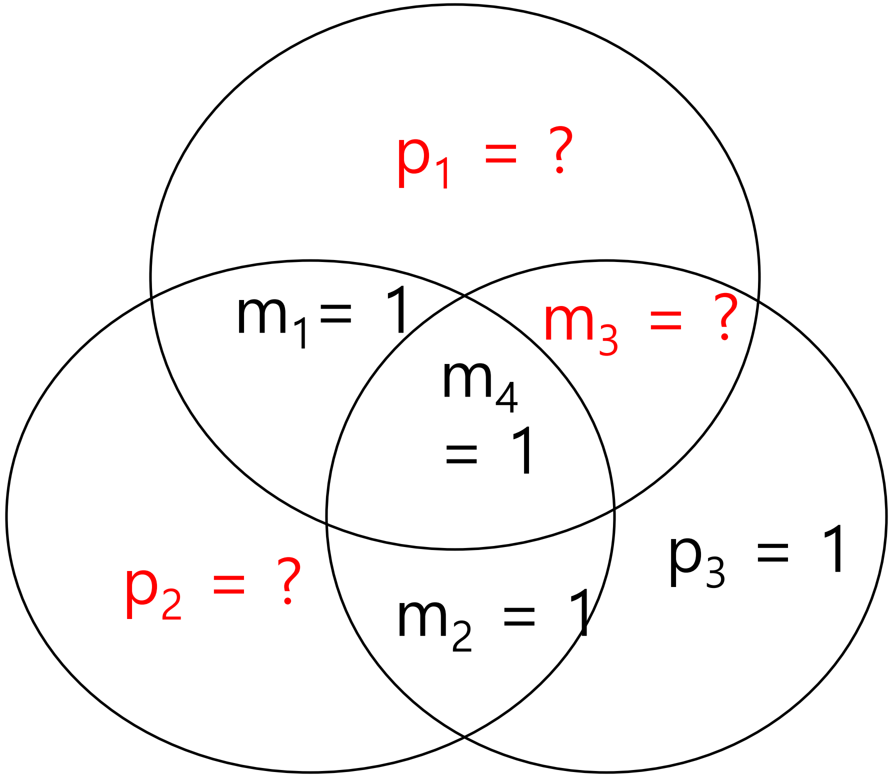


- **Two possible answers are (1, 1, 1) and (0,0,0).**
- **Not uniquely decodable!**

Erasure Error Correction Ex 4

- Three erasures occurred!
- Decodable or not?

m_1	m_2	m_3	m_4	p_1	p_2	p_3
1	1	?	1	?	?	1



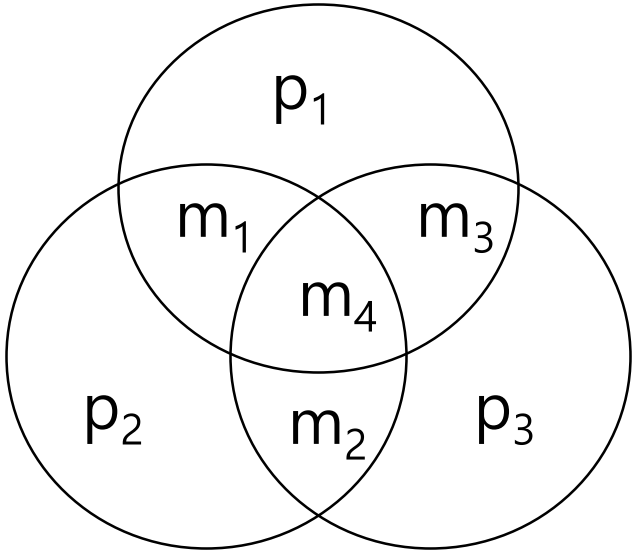
Challenges

- How many bit flip errors can be corrected?

- Up to how many erasures can be corrected?

Check Equations

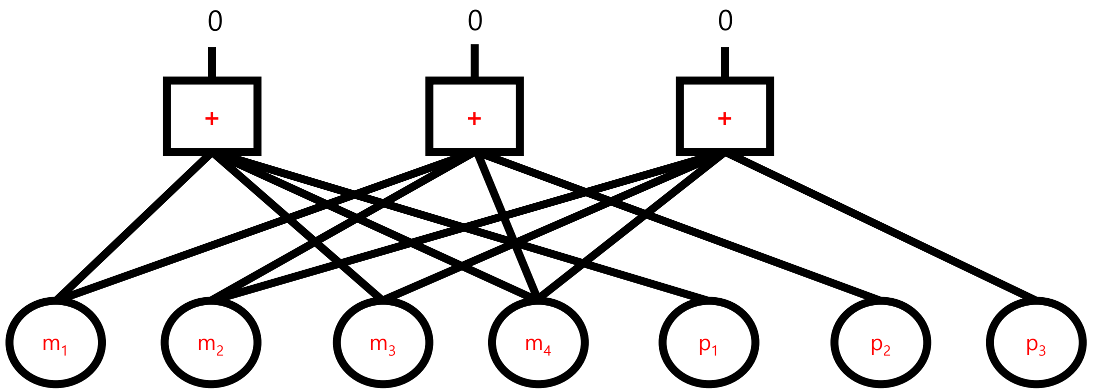
- Three check equations
  - $m_1+m_3+m_4+p_1 = 0$
  - $m_1+m_2+m_4+p_2 = 0$
  - $m_2+m_3+m_4+p_3 = 0$



- Relation among bits
  - Use this relation to encode
  - Use this relation to decode

- With simple simultaneous relations, we have learned that errors across a wireless channel or an Internet channel can be corrected at the receiver.

Parity Check Matrix

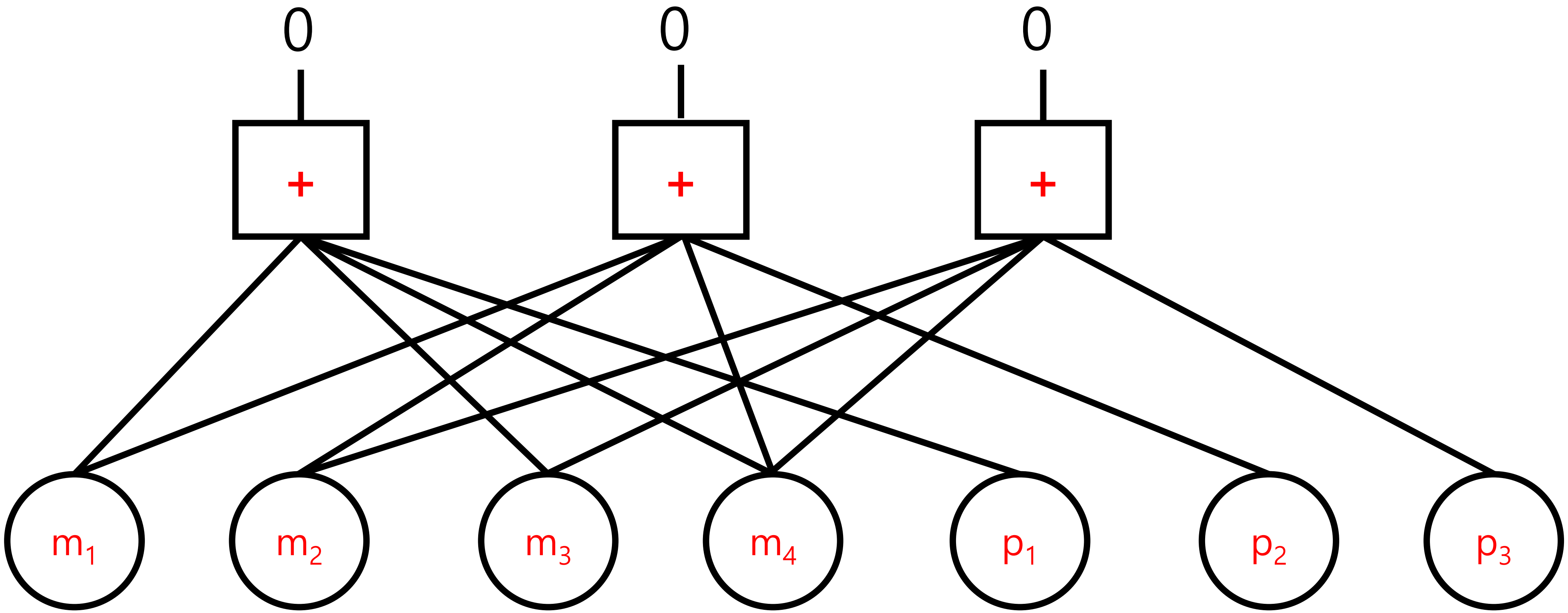


$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

$$0 = Hc$$

1. Parity check matrix H
2. Hc = 0
3. Hr = H(c + e)
   = He
   =: s
4. s is called syndrome.
5. For a single error pattern, syndrome is unique.

Graph Representation vs. Matrix Equation



Standard Array

No error + 7 single error patterns
All 2^3 patterns

All 2^4 codewords

r = c + e

All 2^7 rec. words

Each received word appears once and only once.

Figure out the error pattern

m	p	0000000	0000001	0000010	0000100	0001000	0010000	0100000	1000000
0000	000	0000000	0000001	0000010	0000100	0001000	0010000	0100000	1000000
0001	111	0001111	0001110	0001101	0001011	0000111	0011111	0101111	1001111
0010	101	0010101	0010100	0010111	0010001	0011101	0000101	0110101	1010101
0011									
0100									
0101									
0110									
0111									
1000									
1001									
10									
1111	111								

Hamming Code HW Problems

1. Find all single error patterns of (7, 4) Hamming codes. Show each error pattern is correctable.
2. Find all double error patterns of (7, 4) Hamming codes. Prove/disprove. Some double error patterns are correctable.
3. Find all single and double erasure patterns of (7, 4) Hamming codes. Prove/disprove. All up to double erasures can be corrected.
4. Prove/disprove. There are some triple erasures that can be corrected.

Hamming Code HW Problems

- (Bit flip channel) Consider a binary symmetric channel. Input set is {0, 1} and output set is {0, 1}. The conditional probability p(y|x) is given by

P(y|x)	y=0	y=1
x=0	1 – p	p
x=1	p	1 – p

- The channel introduces bit error probability of $p = 0.1$.
- Suppose using the (7, 4) Hamming code over the channel.
- Find the probability of *information* bit error using (7, 4) Hamming code. Assume the message bits are equi-probable.