Hw 3　　107030 56 - 資訊三 - 孫宏宇

2 nodes set the same countdown value

1. X (∵ ① ~~propagation delay ⇒ different nodes may detect the channel idle at slightly different time ⇒~~ simultaneous transmission ⇒ collision

② The ACK packets themselves may collide)

2. X (WIFI adjusts random backoff range (0, W) based on K (# of send attempts))

3. O (Human hearing range : 20 Hz ~ 20k Hz, & 44100 Hz > 2×20k Hz)

4. X (FM (analog modulation)'s resistance to noise is due to its frequency modulation technique. This has nothing to do with OFDM, which is a digital transmission method that provides robustness through its use of multiple orthogonal sub-carriers.)

3.

	d_1	d_2	d_3	d_4
· dataword :	0	0	0	1

$p1 = d_1 + d_2 + d_4 = 0 + 0 + 1 = 1$

$p2 = d_1 + d_3 + d_4 = 0 + 0 + 1 = 1$

$p3 = d_2 + d_3 + d_4 = 0 + 0 + 1 = 1$

	p_1	p_2	d_1	p_3	d_2	d_3	d_4
· codeword :	1	1	0	1	0	0	1

$((011)_2 = (3)_{10})$ ↓ introduce an 1-bit error

	b1	b2	b3	b4	b5	b6	b7
· received :	1	1	1	1	0	0	1

$c_1 = b_1 + b_3 + b_5 + b_7 = 1 + 1 + 0 + 1 = 1$

$c_2 = b2 + b3 + b6 + b7 = 1 + 1 + 0 + 1 = 1$

$c_3 = b4 + b5 + b6 + b7 = 1 + 0 + 0 + 1 = 0$

Ans: 1 1 1 1 0 0 1

(Starts w/ a valid codeword. Error at bit $(011)_2 = 3$)

(6.)

$$
\begin{array}{rccccccc}
 & 1 & 1 & 1 & & & & \\ \cline{2-8}
1\,0\,0\,0\,1 \;) & 1&1&1&0&1&0&0\\
 & 1&0&0&0&1& & \\ \cline{2-8}
 & &1&1&0&0&0& \\
 & &1&0&0&0&1& \\ \cline{3-8}
 & & &1&0&0&1&0\\
 & & &1&0&0&0&1\\ \cline{4-8}
 & & & &0&0&1&1
\end{array}
$$

✓

codeword $c(x) = d(x)\,x^{5-1} + r(x)$

$$= \underline{\underline{1\,1\,1\,0\,1\,0\,0\;\;0\,0\,1\,1}}$$ #

(7.)

$$
\begin{cases}
C_1 = 0\;0\;0\;0\;0\;0\;0\;0\;0\;0\;0\;0 \\
C_2 = 0\;1\;1\;1\;1\;1\;0\;0\;0\;0\;0\;0 \\
C_3 = 1\;0\;0\;0\;0\;0\;1\;1\;1\;1\;1\;1 \\
C_4 = 1\;1\;1\;1\;1\;1\;1\;1\;1\;1\;1\;1
\end{cases}
$$

✓

$d(c_1, c_2) = 6$, $d(c_1, c_3) = 6$

$d(c_1, c_4) = 12$, $d(c_2, c_3) = 12$

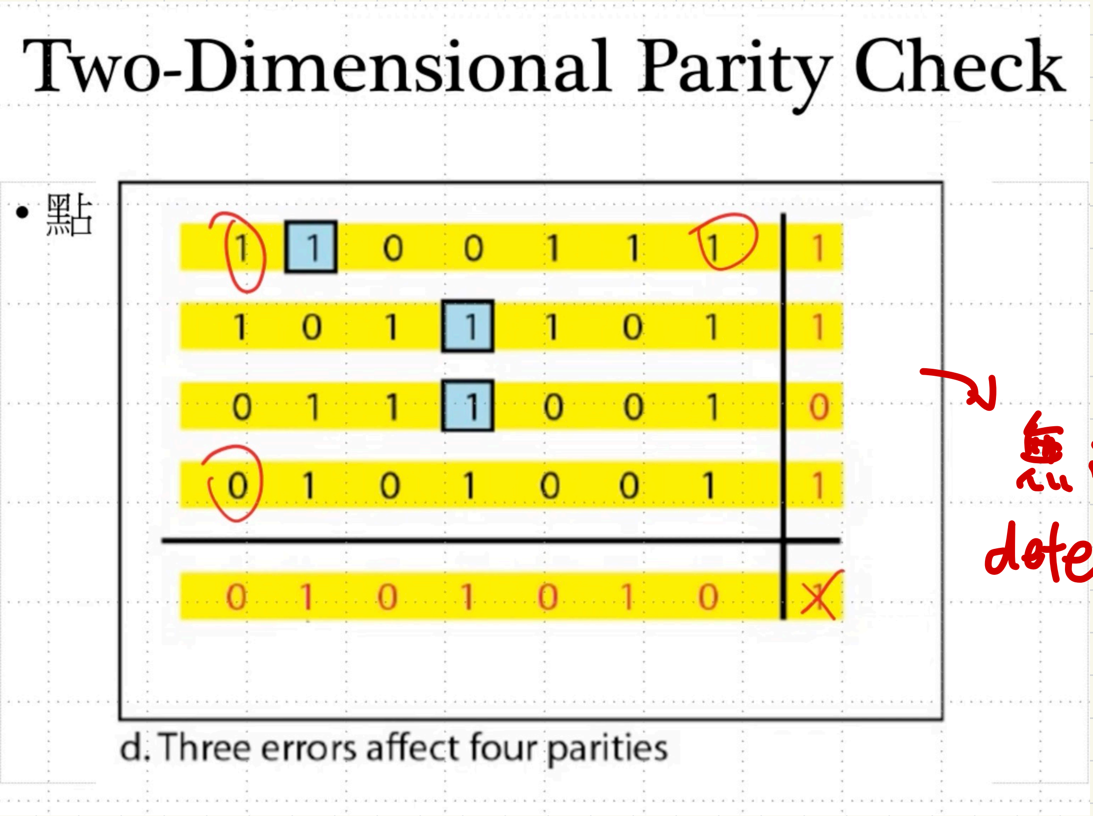
$d(c_2, c_4) = 6$, $d(c_3, c_4) = 6$

⑧ ?

dataword 差 1 bit ⇒ Haming distance = 3

〃 2 〃 ⇒ 〃 = 4

3 ⇒ = 4



Two-Dimensional Parity Check

- 點

1	1	0	0	1	1	1	1
1	0	1	1	1	0	1	1
0	1	1	1	0	0	1	0
0	1	0	1	0	0	1	1
0	1	0	1	0	1	0	✗

d. Three errors affect four parities

→ 無法 detect

⇒ Min. Hamming dist. = 3

9.

- dataword:

	d_1	d_2	d_3	d_4
dataword:	0	0	1	0

$$p1 = d_1 + d_2 + d_4 = 0 + 0 + 0 = 0$$

$$p2 = d_1 + d_3 + d_4 = 0 + 1 + 0 = 1$$

$$p3 = d_2 + d_3 + d_4 = 0 + 1 + 0 = 1$$

	p_1	p_2	d_1	p_3	d_2	d_3	d_4
· codeword:	1	1	0	1	0	1	0
	b_1	b_2	b_3	b_4	b_5	b_6	b_7

decode

$$c_1 = b_1 + b_3 + b_5 + b_7 = 1+0+0+0 = 1$$

$$c_2 = b2 + b3 + b6 + b7 = 1+0+1+0 = 0$$

$$c_3 = b4 + b5 + b6 + b7 = 1+0+1+0 = 0$$

$(001)_2 = 1$ ⇒ indicates that there's an error at bit 1

bad conclusion

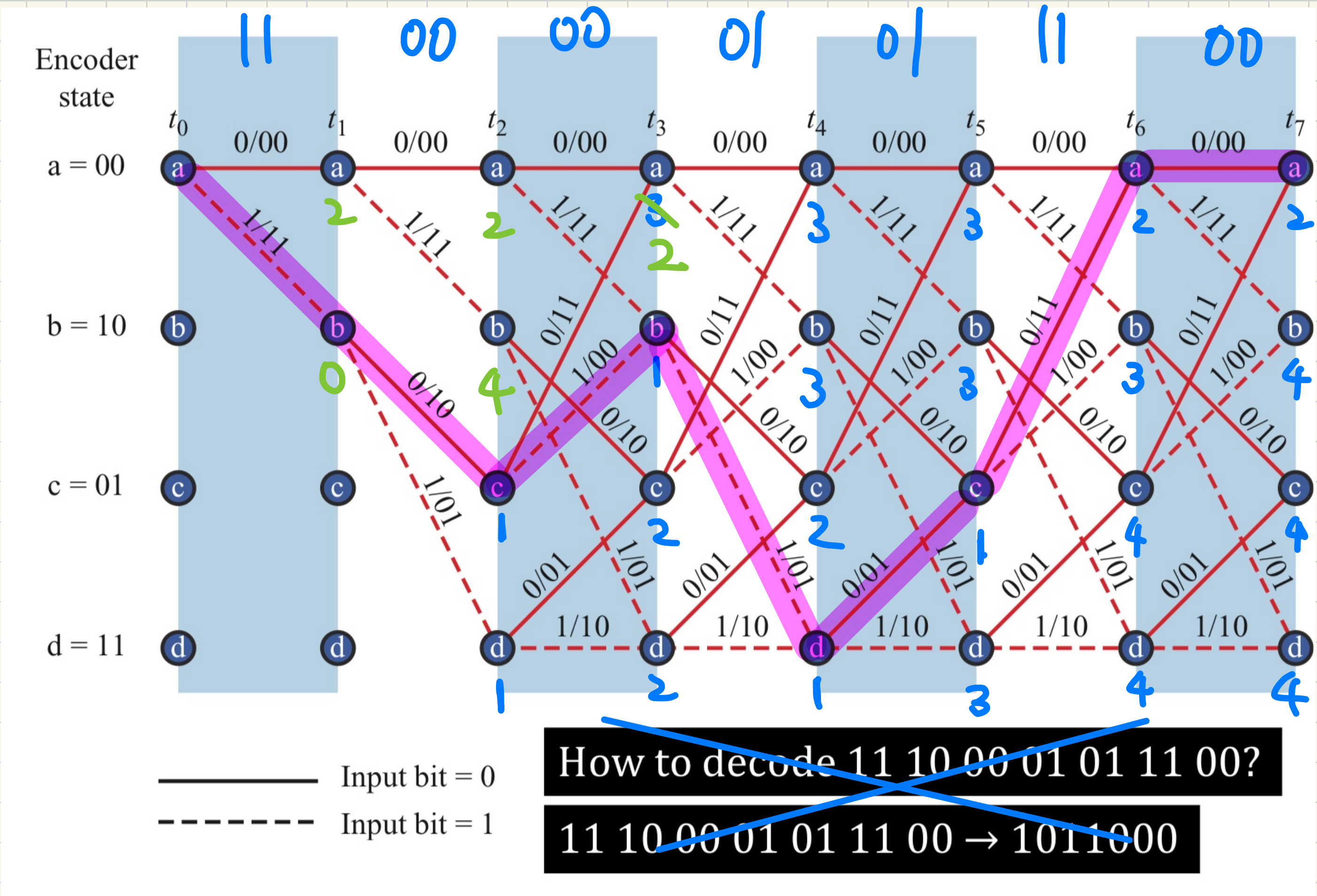
⇒ result = $\underline{\underline{1010}}$ #

10. $x^{10}+1$

① len (generator) = len(burst err.)

② even # of terms ⇒ detects odd # of errors

11.



~~How to decode 11 10 00 01 01 11 00?~~

~~11 10 00 01 01 11 00 → 1011000~~

Ans: 10 11 0 00

12. 3 Parties: A (attacker), B, C

1° A $\xrightarrow{Tx1}$ B, Tx1 is broadcast to the bitcoin network and await confirmation.

2° Before Tx1 is confirmed, A $\xrightarrow{Tx2}$ C (using the same Bitcoins, privately)

3° A starts mining a new block with Tx2 instead of Tx1 (high prob. ∵ A controls the majority of the computational resources) ⇒ making chain longe

4° Broadcast the private chain to the entire Bitcoin network

5° As a result, the block Tx1 is invalidated and dropped from the Bitcoin Network.

(51% Attack)