

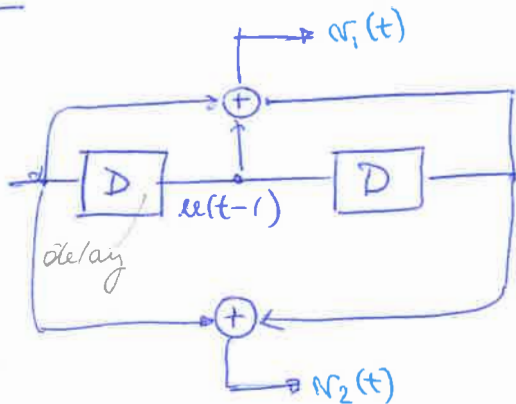
Convolutional Codes

1

Tree codes:

Example 1

input: $u(t)$



$$r_1(t) = u(t) + u(t-1) + u(t-2)$$

$$r_2(t) = u(t) + u(t-2)$$

$$u(t) = (u(t=0) \quad u(1) \quad u(2) \quad \dots)$$

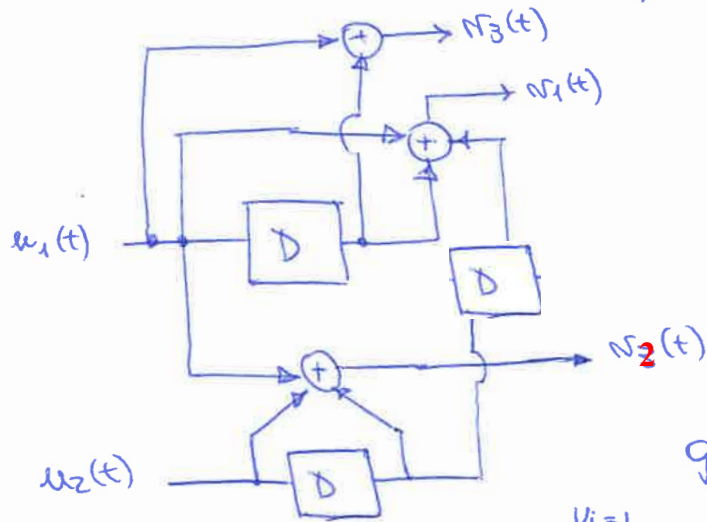
$$r_1(t) = (r_1(t=0) \quad \dots)$$

$$r_2(t) = (r_2(t=0) \quad r_2(t=1) \quad \dots)$$

General $k \times m$: $\frac{k}{m}$ convolutional code (k inputs, m outputs) 2

$$r_j(t) = \sum_{i=1}^K \sum_{m=0}^{V_i} g_{ij}(m) u_i(t-m)$$

Example 2



In the previous example

$$\begin{cases} g_{i=1, j=2}(m=1) = 0 \\ V_i = 2 \end{cases}$$

$$r_1(t) = u_1(t) + u_1(t-1) + u_2(t-2)$$

$$r_2(t) = u_2(t) + u_2(t-1) + u_1(t)$$

$$r_3(t) = u_1(t) + u_1(t-1)$$

General expression :

$$r_j = \sum_{m=0}^{V_1} g_{1j}(m) u_1(t-m) + \sum_{m=0}^{V_2} g_{2j}(m) u_2(t-m)$$

$$g_{ij}(0) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}_{2 \times 3} \quad D^0$$

$$g_{ij}(1) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}_{2 \times 3} \quad D^1$$

$$g_{ij}(2) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}_{2 \times 3} \quad D^2$$

transition to polynomials

Conversion of previous matrices to polynomials:

will see soon \rightarrow

$$\begin{bmatrix} 1+D & 1 & 1+D \\ D^2 & 1+D & 0 \end{bmatrix} \begin{matrix} 3 \\ 3 \end{matrix}$$

(PGM)

Formal Power Series (FPS)

$$r_J(D) \triangleq \sum_{t=0}^{\infty} r_J(t) D^t$$

$$u_i(D) \triangleq \sum_{t=0}^{\infty} u_i(t) D^t$$

$$r_J(D) = \sum_{t=0}^{\infty} \underbrace{\sum_{i=1}^K \sum_{m=0}^{n_i} g_{iJ}(m) \cdot u_i(t-m)}_{r_J(t)} D^t =$$

$$= \sum_{t=0}^{\infty} \sum_{i=1}^K \sum_{m=0}^{n_i} g_{iJ}(m) u_i(t-m) D^m D^{t-m}$$

$$= \sum_{i=1}^K \sum_{m=0}^{n_i} g_{iJ}(m) D^m \sum_{t=0}^{\infty} u_i(t-m) D^{t-m}$$

$$\bullet u_i(t) \quad t < 0 \quad \sum_{i=1}^K \sum_{m=0}^{n_i} g_{iJ}(m) D^m \sum_{t=m}^{\infty} u_i(t-m) D^{t-m}$$

Change vars

$$r_J(D) = \sum_{i=1}^K \underbrace{\sum_{m=0}^{n_i} g_{iJ}(m) D^m}_{g_{iJ}(D)} \sum_{t=0}^{\infty} u_i(t) D^t$$

$$g_{iJ}(D) \triangleq \sum_{m=0}^{n_i} g_{iJ}(m) D^m$$

$$r_J(D) = \sum_{i=1}^K g_{iJ}(D) u_i(D)$$

$$g_{iJ}(D) = g_{iJ}(0) + g_{iJ}(1) \cdot D + g_{iJ}(2) \cdot D^2 + \dots \text{ up to } n_i$$

$$u_i(D) = u_i(0) + u_i(1)D + u_i(2)D^2 + \dots$$

Polynomial generating matrix (PGM)

$$\underbrace{\begin{bmatrix} r_1(D) & r_2(D) & \dots & r_m(D) \end{bmatrix}}_{1 \times m} = \underbrace{\begin{bmatrix} u_1(D) & u_2(D) & \dots & u_k(D) \end{bmatrix}}_{1 \times k}$$

$$\begin{bmatrix} g_{11}(D) & \dots & g_{1m}(D) \\ \vdots & & \vdots \\ g_{k1}(D) & \dots & g_{km}(D) \end{bmatrix}$$

3rd example $\begin{cases} k=1 \\ m=2 \end{cases} \Rightarrow$ means that we have 1 input sequence and 2 output sequences (sequences!! not bits!!)

$$\text{memory} = 2 = V_1 = V$$

$$\begin{aligned} v_1(t) &= u(t) + u(t-1) + u(t-2) \\ v_2(t) &= u(t) + u(t-2) \end{aligned}$$

$$\begin{bmatrix} n_1(D) & n_2(D) \end{bmatrix} = (u(D)) \begin{bmatrix} 1+D+D^2 & 1+D^2 \\ g_{11}(D) & g_{12}(D) \end{bmatrix}$$

Total memory of the encoder is $V \triangleq \sum_{i=1}^K n_i$

$$\text{In example 2: } \left. \begin{aligned} u_1(t-1) &\rightarrow n_1 = 1 \\ u_2(t-2) &\rightarrow n_2 = 2 \end{aligned} \right\} \Rightarrow V = V_1 + V_2 = 3 \quad \checkmark$$

State Diagram

State $u(t)$ $u(t-1)$
 ↓ ↓
 1st state 2nd state

"we are pushing bits at the input"



"suppose I'm in state 0, 0"

↓ means

$$\begin{cases} u(t) = 0 \\ u(t-1) = 0 \end{cases}$$

$$v1(t) = u(t) + u(t-1) + u(t-2)$$

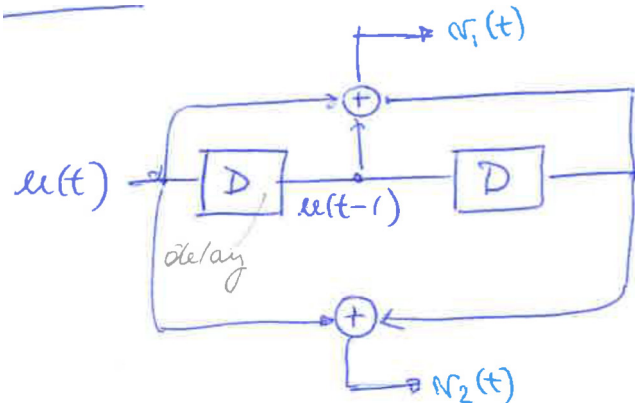
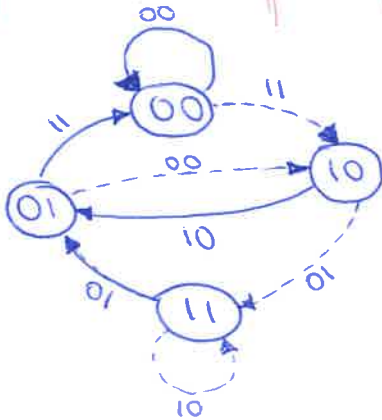
$$v2(t) = u(t) + u(t-2)$$

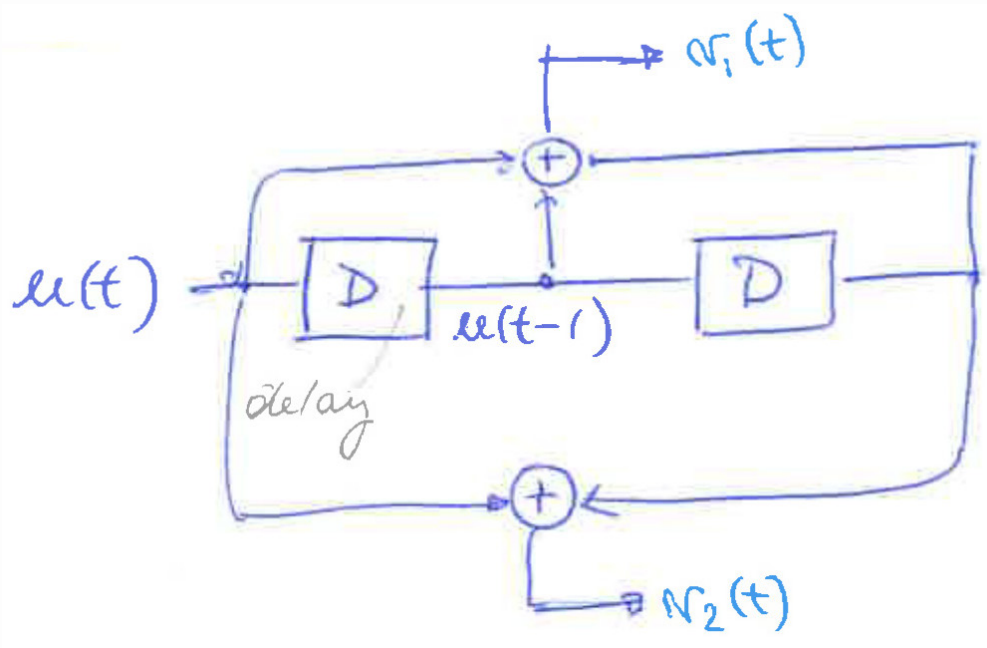
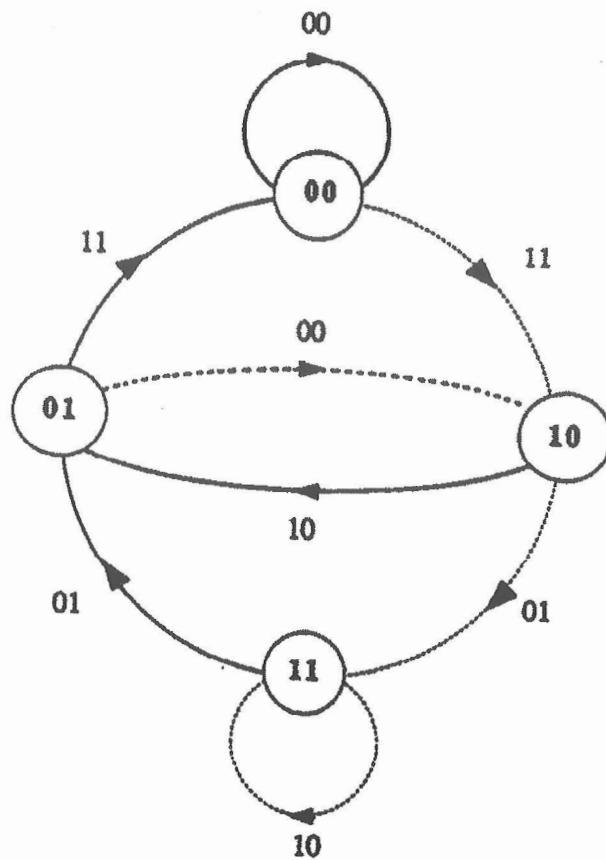
$$\begin{cases} u(t) = 0 \\ u(t-1) = 1 \end{cases}$$

$u(t)$	$u(t-1)$	$u(t-2)$	$v_1(t)$	$v_2(t)$
0	0	0	0	0
0	0	1	1	1
1	0	0	1	1
1	0	1	0	0

- The states represent the memory
 - "what is kept in the register"

Input
(solid line = 0)



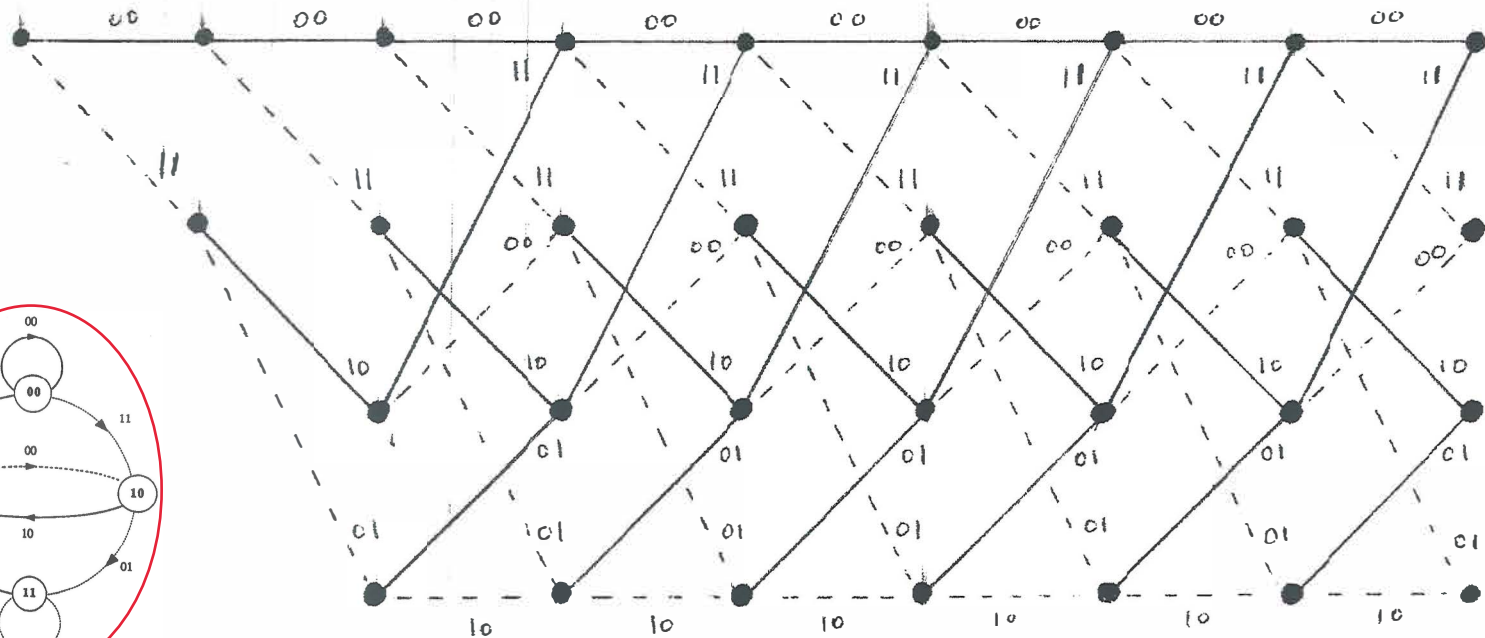
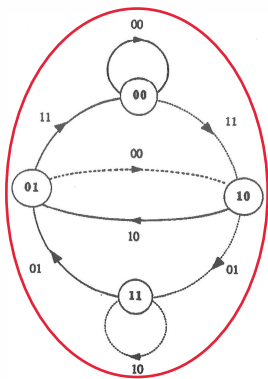


00

10

01

11

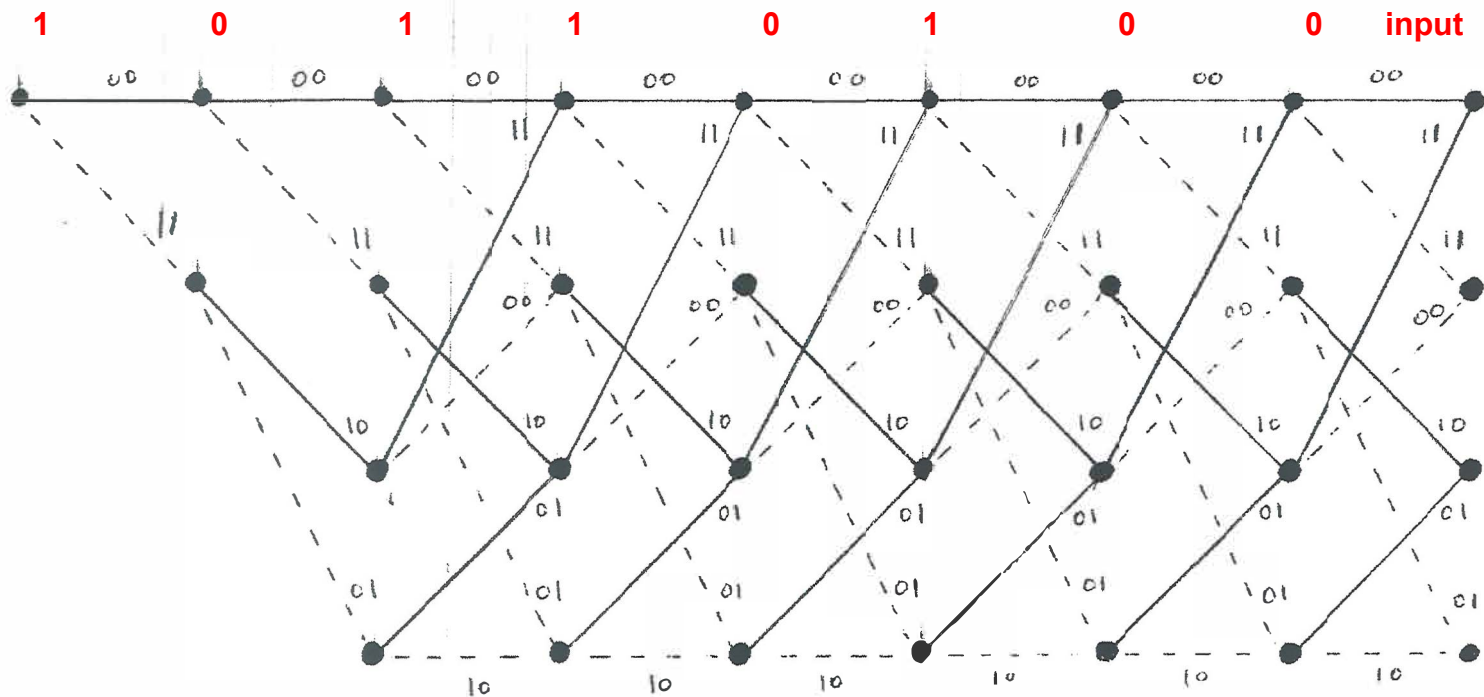


00

10

01

11



11	10	00	01	01	00	10	11	codeword
1	0	1	1	0	1	0	0	input

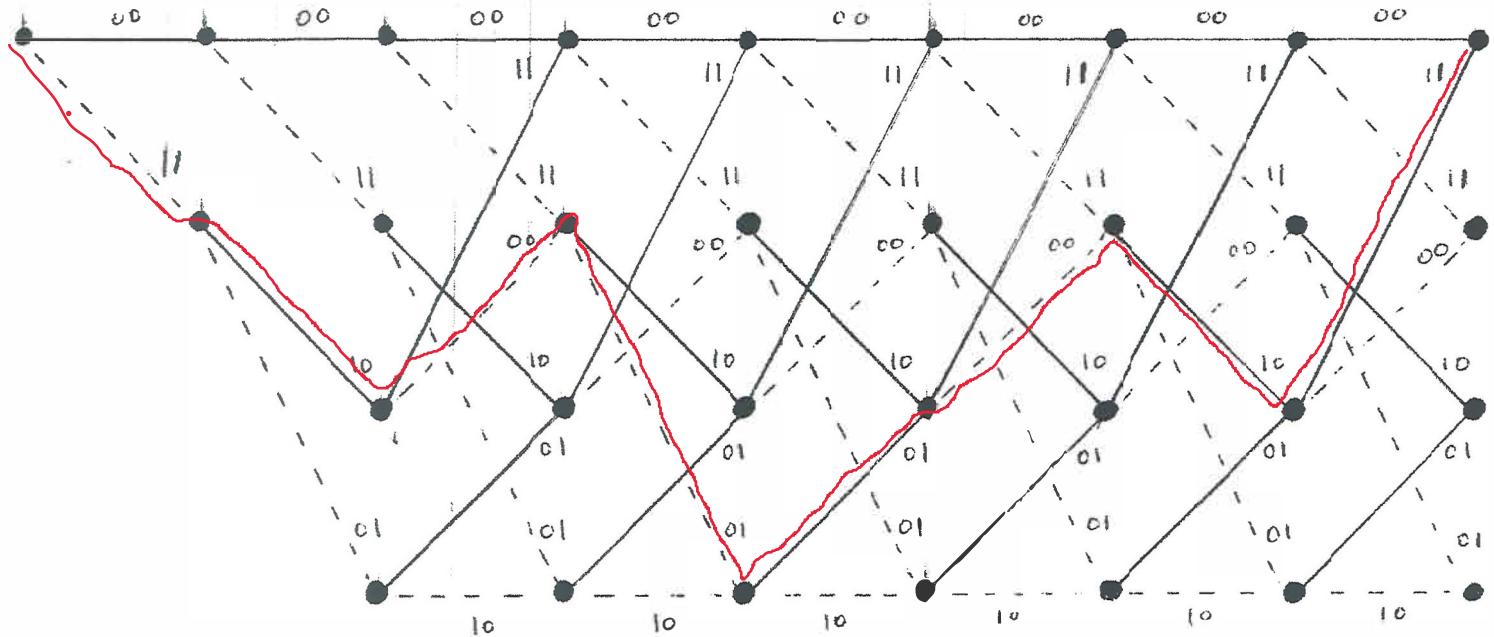


00

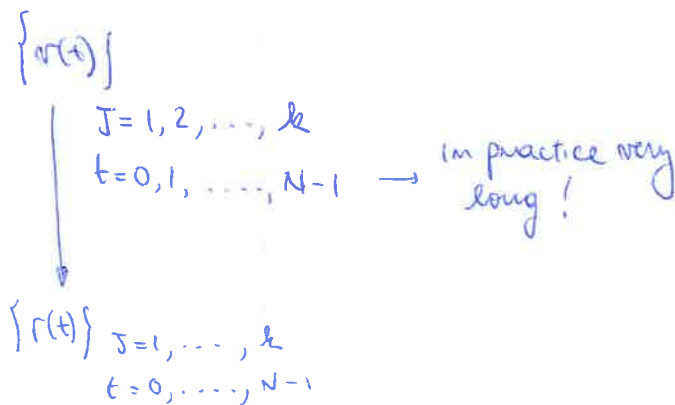
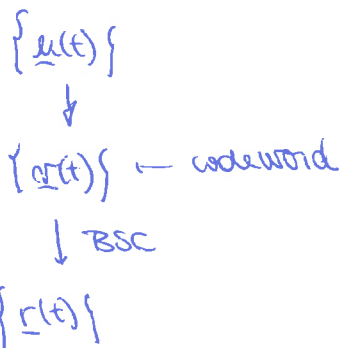
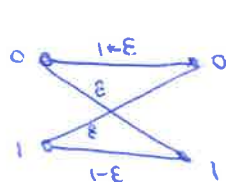
10

01

11



BSC



You want to ~~max~~ ^{find} $\underline{v} \in C$ s.t. maximize $P(\text{detected is correct})$

$$\max_{\underline{v} \in C} P \left[\left\{ r_i(t) \right\}_{\substack{i=1 \rightarrow m \\ t=0 \rightarrow N-1}} \middle| \left\{ v_i(t) \right\}_{\substack{i=1 \rightarrow m \\ t=0 \rightarrow N-1}} \right] \longrightarrow \max \ln P \left[\left\{ r_i(t) \right\} / \left\{ v_i(t) \right\} \right]$$

NOTE: Assume independence in t & i

Linear combination of stat. indep. are still stat. indep!

$$\max \ln \prod_{t=0}^{N-1} \prod_{i=1}^m P(r_i(t) | v_i(t)) =$$

$$= \max \sum_{t=0}^{N-1} \sum_{i=1}^m \ln [P(r_i(t) | v_i(t))]$$

$$P(r_i(t) | v_i(t)) = E^d (1-E)^{m-d}$$

$E < 1$, we are penalizing more large Hamming distances



And then you add along the $t \rightarrow$ and you choose the path of min distance @ each node find path that is smaller. Add node + branch metric.

Viterbi Decoding

9

10

In previous example assume:

Input: 1 0 1 1 0 1 0 0
Output (T_x): 11 10 00 01 01 00 10 11
Received (R_x): 10 00 00 01 01 00 10 11
Decoded: 11 10 00 01 01 00 10 11

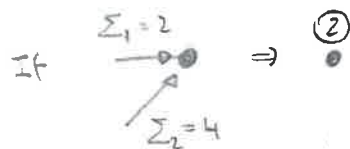
To decode:

- Start by the last node with lowest weight.
- Follow the most probable path, that means following the branches with less weight

The error correcting capabilities of the code depend on its length.

We complete the branches with the distances of the branches to the received vector

⊗ number in each node is the sum through the branches



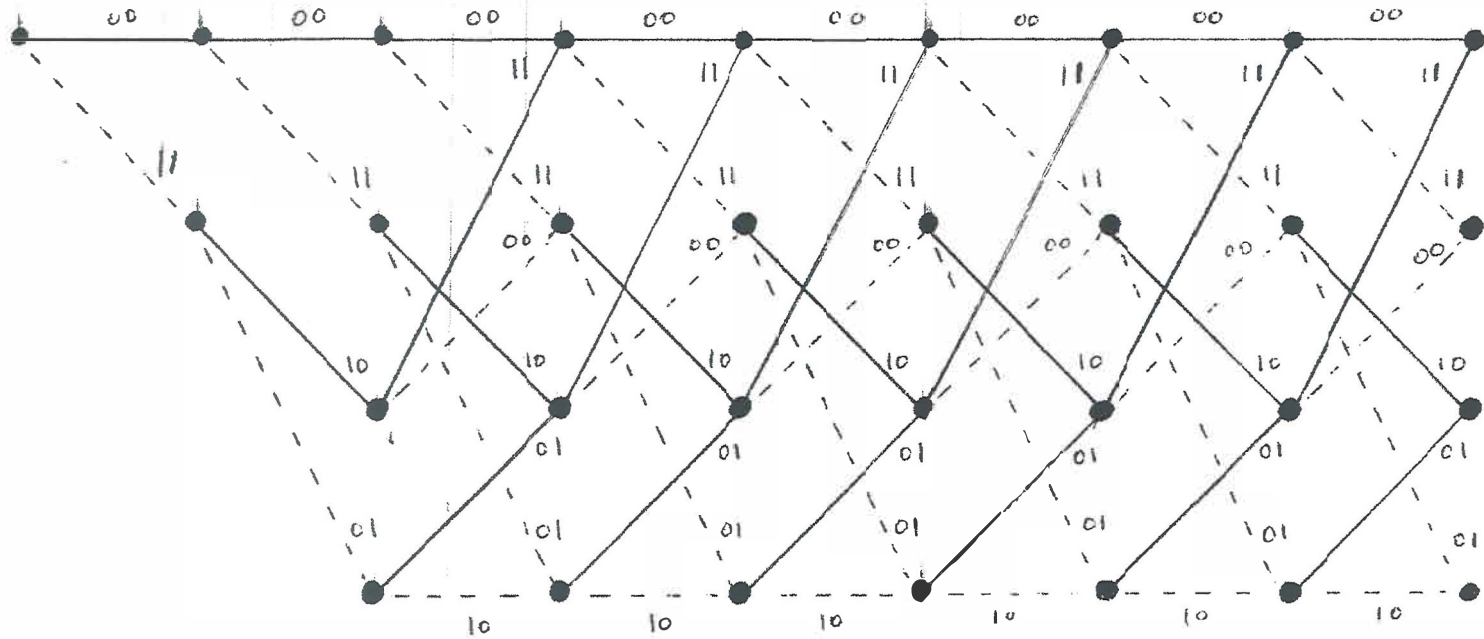
10	00	00	01	01	00	10	11	received
11	10	00	01	01	00	10	11	codeword
1	0	1	1	0	1	0	0	input

00

10

01

11



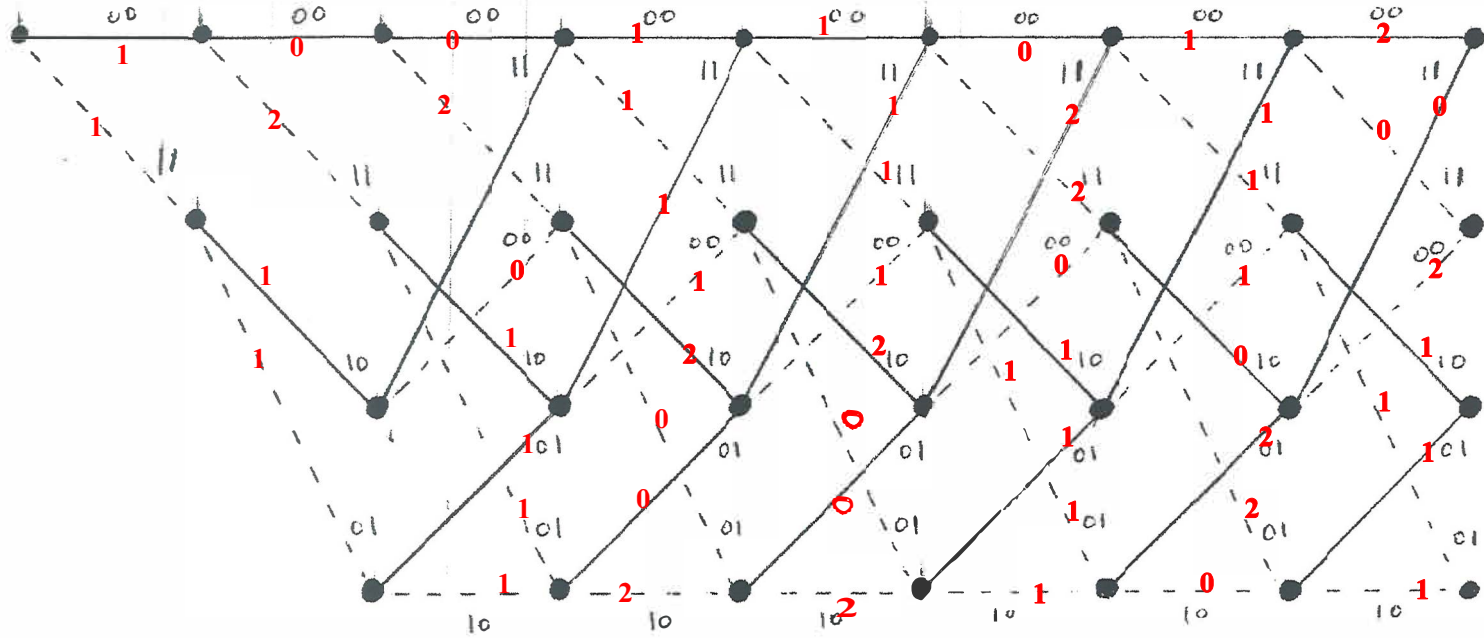
10	00	00	01	01	00	10	11	received
11	10	00	01	01	00	10	11	codeword
1	0	1	1	0	1	0	0	input

00

10

01

11



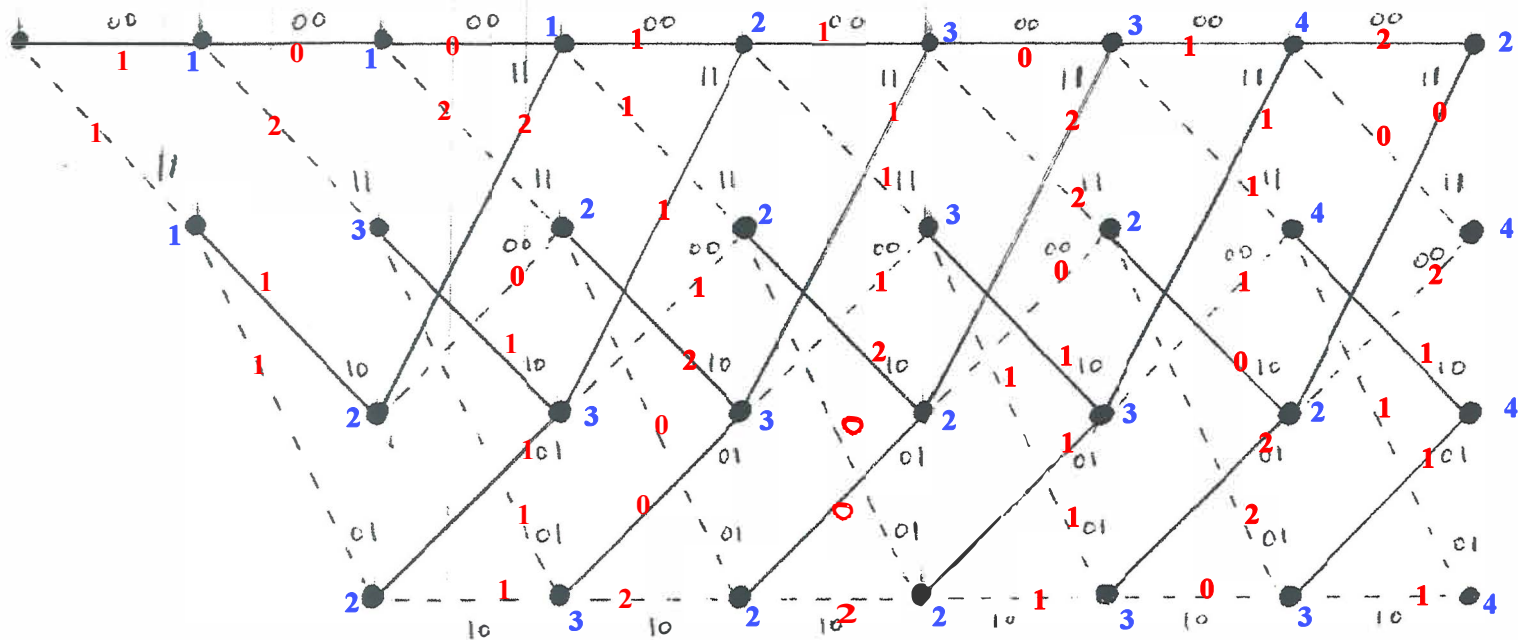
10	00	00	01	01	00	10	11	
11	10	00	01	01	00	10	11	codeword
1	0	1	1	0	1	0	0	input

00

10

01

11



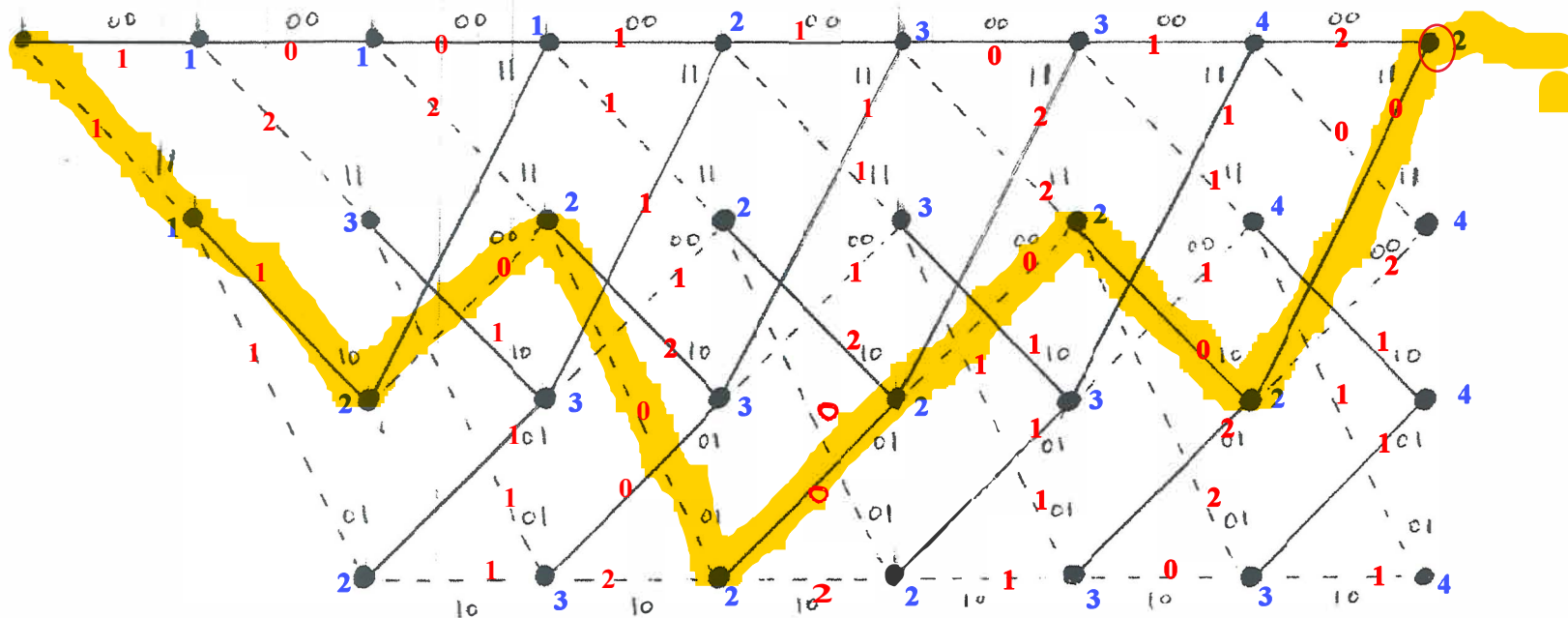
10	00	00	01	01	00	10	11	
11	10	00	01	01	00	10	11	codeword
1	0	1	1	0	1	0	0	input

00

10

01

11



The last 2 zeros are forced to go back to (00) ↗

* What is the true rate of the convolutional code?

- B is the # of (pure) info bits. (In our example, 6, because $B=6, k=1$)

- # of flush input bits is $n_{\max} \cdot k$

- # of flush output bits is $n_{\max} \cdot m$

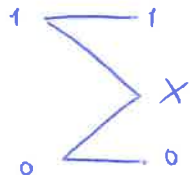
The actual length of the codeword is

$$B \cdot m + n_{\max} \cdot m = m(B + n_{\max})$$

Rate: $\frac{kB}{m(B + n_{\max})} \xrightarrow{B \rightarrow \infty} \frac{k}{m}$

In the example $R = \frac{1 \cdot 6}{2(6+2)} = \frac{3}{8}$

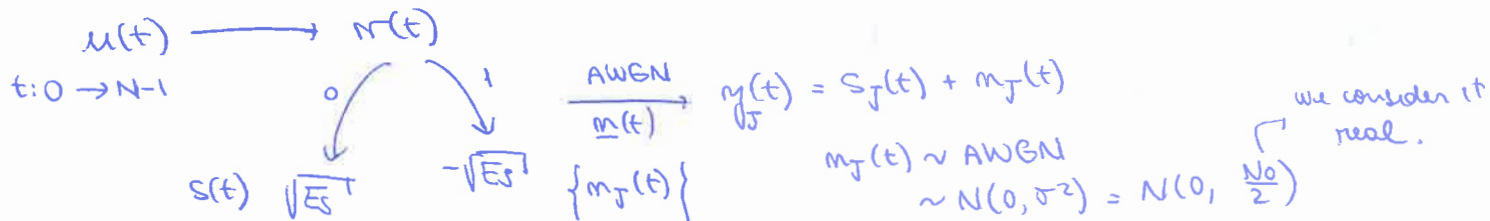
Channel in the Internet: Not flip, but loss model



BSC \rightarrow AWGN

11

AWGN decoding of convolutional codes



$$\max_{\substack{J=1 \rightarrow m \\ t=0 \rightarrow N-1}} \mathcal{P}(\{r_J(t)\} | \{s_J(t)\}_{t,J}) \xrightarrow{\text{independence}} \max_S \sum_{t=0}^{N-1} \sum_{J=1}^m \ln \left[\mathcal{P}(r_i(t) | s_i(t)) \right]$$

$P(r_i(t)|s_i(t)) = P_r(\text{noise } n(t) \text{ is @ a value } r_i(t) - s_i(t) \text{ away from its zero mean})$

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} = \frac{1}{\sqrt{2\pi \frac{N_0}{2}}} e^{-\frac{(r_i(t) - s_i(t))^2}{2 \frac{N_0}{2}}}$$

$$\max \sum_{t=0}^{N-1} \sum_{j=1}^m -(r_i(t) - s_i(t))^2 = \sum_{t=0}^{N-1} \sum_{j=1}^m \underbrace{-r_i^2(t)}_{\text{Constant}} + 2r_i(t)s_i(t) - \underbrace{s_i^2(t)}_{\text{ES}}$$

$$= \max \sum_{t=0}^{N-1} \sum_{j=1}^m r_i(t) s_i(t) = \max \sum_{t=0}^{N-1} \sum_{j=1}^m r_i(t) (-1)^{b_i(t)}$$

we assumed BPSK
at the beginning

Same process as the BSC except now metric is not d_H (Hamming distance) (at each t).

(again key to this is independence of noise t, i)

$$\sum_{i=1}^m r_i(t) (-1)^{r_i(t)} \leftarrow \text{our new metric.}$$

Decode with the Viterbi algorithm in the AWGN

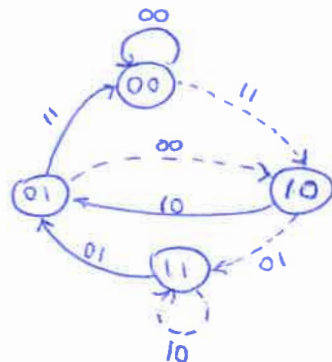
13

$$n_1(t) = u(t) + u(t-1) + u(t-2)$$

$$n_2(t) = u(t) + u(t-2)$$

$$G(D) = [1+D+D^2 \quad 1+D^2]$$

This gave the state diagram



in		<u>triplet</u>	<u>output</u>
0 :	00 → 00	000	00
0 :	10 → 01	010	10
	01 → 00	001	11
	11 → 01	011	01

1	00 → 10	100	11
	10 → 11	110	01
	01 → 10	101	00
	11 → 11	111	10

Branch metric $\sum r_i(t)(-1)^{n_i(t)}$

$$n_i(t) = \begin{cases} 0 \rightarrow \sqrt{E_s} \\ 1 \rightarrow -\sqrt{E_s} \end{cases} = s_i(t)$$

$$r_i(t) = s_i(t) + n_i(t)$$

Example

to go back to 00

u: 0 1 1 0 1 1 0 0
 n_1, n_2 : 00 11 01 01 00 01 01 11

Assume $E_s = 25$

(s, s) (-s, -s) (+s, s) (+s, s) (+s, +s) (+s, -s) (+s, s) (-s, -s)

r: (3, 4) (-2, 0) (4, -2) (4, -3) (3, 4) (3, -5) (6, -4) (-4, -5)

weights on the diagram: dot product

$$\begin{pmatrix} 5 & 5 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} \rightarrow 3(-1)^0 + 4(-1)^0 = 7 \rightarrow 1^{st} \text{ branch}$$

$$3(-1)^1 + 4(-1)^1 = -7 \rightarrow 2^{nd} \text{ "}$$

$$3(-1)^0 + 4(-1)^1 = -1$$

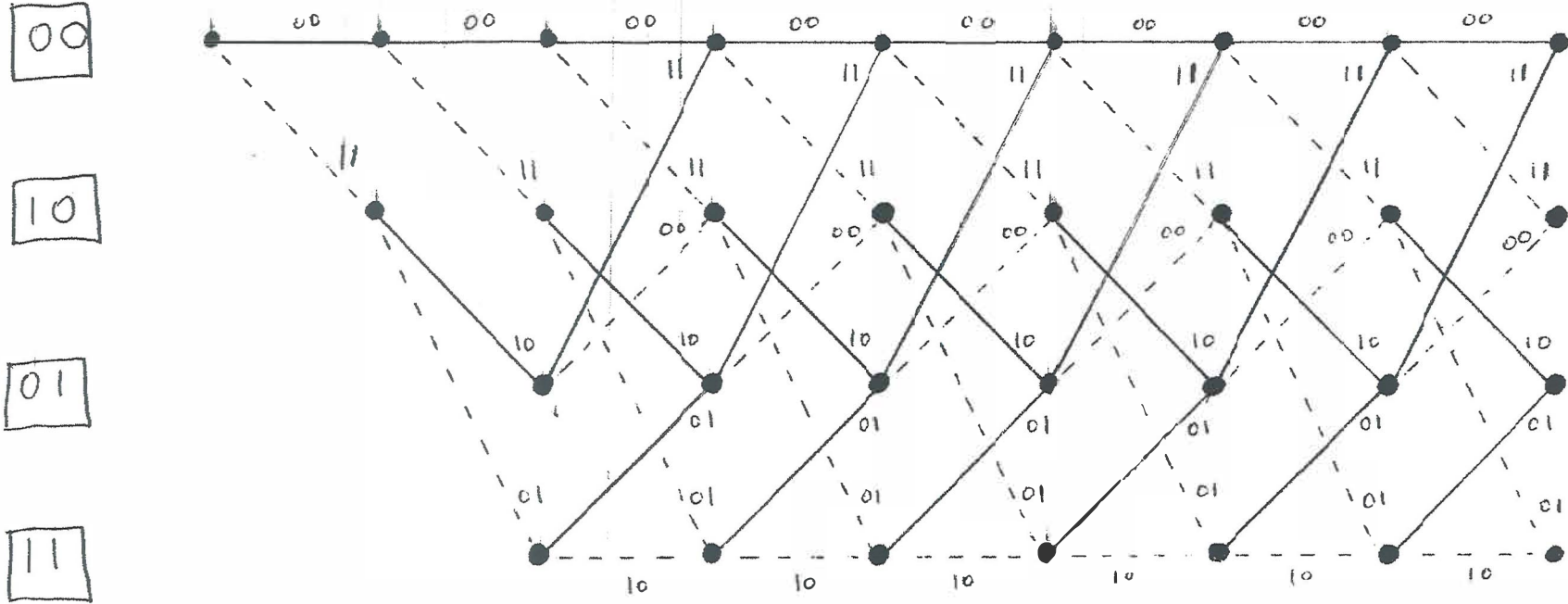
SUM

FLIP & SUM

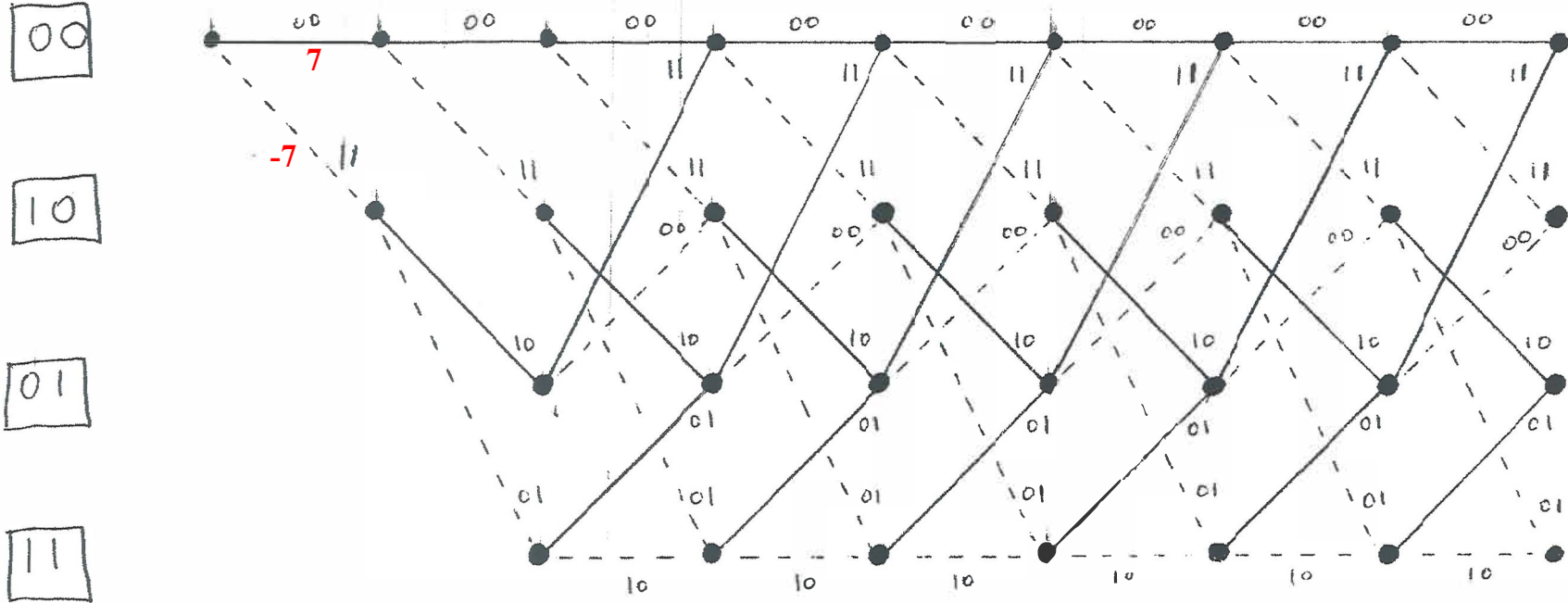
1st - 2nd

Decoded: 00 11 01 01 00 01 01 11

3 4	-2 0	4 -2	4 -3	3 4	3 -5	6 -4	-4 -5 received
5 5	-5 -5	5 -5	5 -5	5 5	5 -5	5 -5	-5 -5 sent
0	1	1	0	1	1	0	0 input



3 4	-2 0	4 -2	4 -3	3 4	3 -5	6 -4	-4 -5 received
5 5	-5 -5	5 -5	5 -5	5 5	5 -5	5 -5	-5 -5 sent
0	1	1	0	1	1	0	0 input



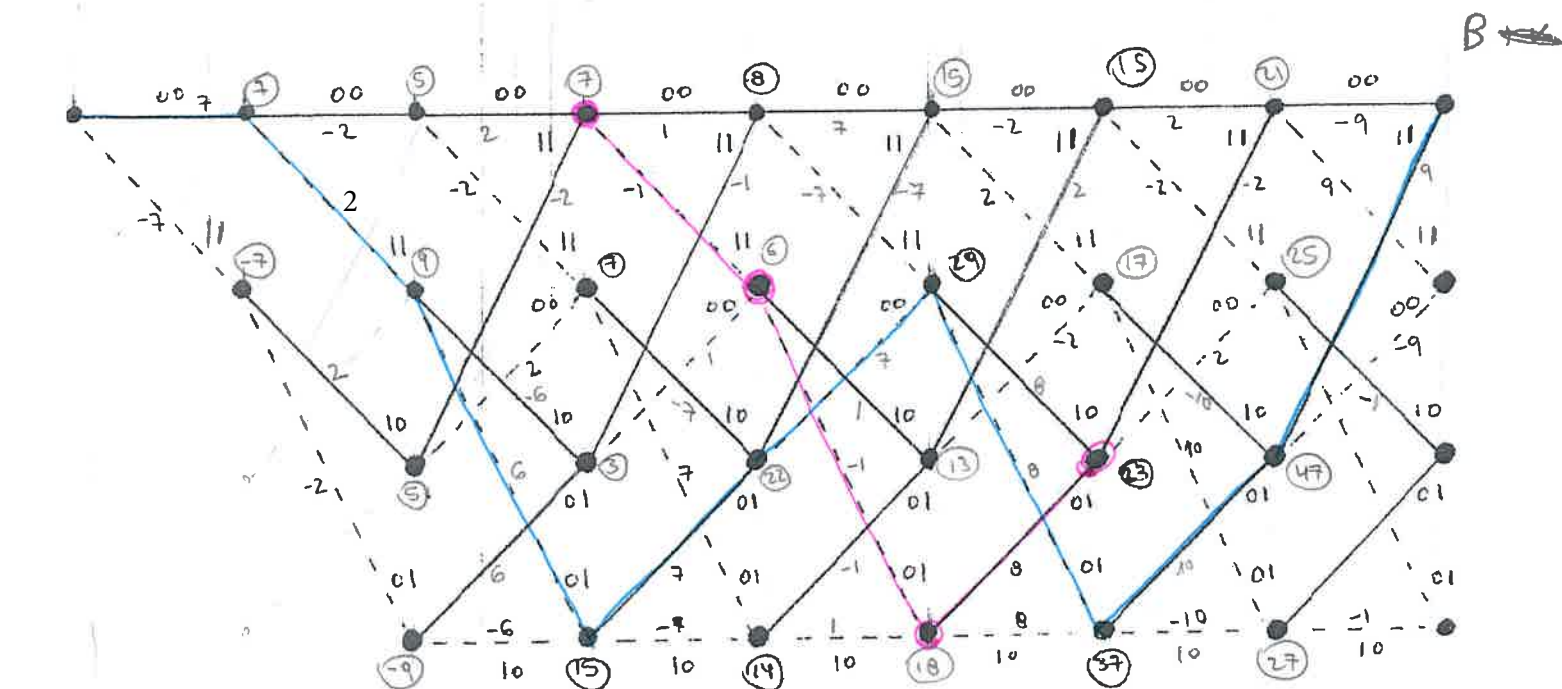
NOW AT NODE PICK MAXIMUM

00

10

01

11



μ	00	01	10	11
r	00	01	10	11
T_x	(5, 5)	(-5, -5)	(5, -5)	(-5, 5)
r	(3, 4)	(-2, 0)	(4, -2)	(-4, 3)

Nice thing about these codes: The structure. We are going to study this a bit more now. 15

Weight distribution of convolutional code

$\{A_d\}_{d=0}^m$: A_d is # of codewords with Hamming weight d

Can say more: Now we care about the paths:

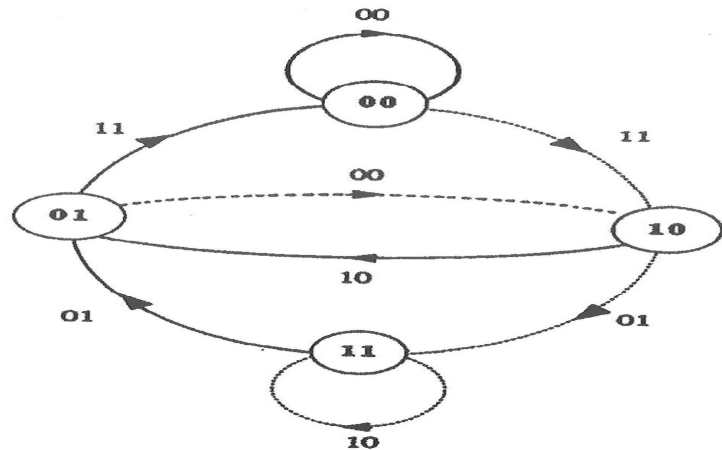
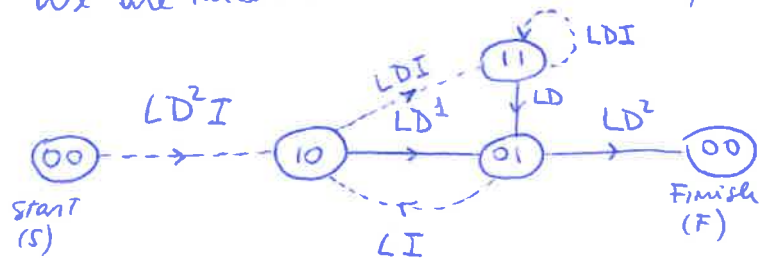
$L^3 D^5 I^1$ \leftarrow Path $\left\{ \begin{array}{l} \text{Length } 3 \text{ \# branches} \\ \text{Input: } 1 \text{ \# --- lines} \\ \text{Output of weight } 5 \text{ \# } 1 \text{ in the output} \end{array} \right.$

$\sum_{i,j,k} a_{i,j,k} L^i D^j I^k \rightarrow \# \text{ of paths}$

We will be looking to understand the # of paths that deviate from the \forall -zero state w/o visiting the \forall zeros state in between.

HERE'S WHERE THE STRUCTURE OF THE CODE COMES INTO.

We are interested in derivations from \emptyset to path only



$$A_{00} = A_s LD^2I + A_{01} LI$$

$$A_{11} = A_{10} LDI + A_{11} LDI$$

$$A_{01} = A_{11} LD + A_{10} LD$$

$$A_s = 1$$

$$A_F = A_{01} LD^2$$

Once

system of 3 eqs and 3 unknowns
Solve for A_{01} and replace in

$$\begin{pmatrix} A_{00} \\ A_{01} \\ A_{11} \end{pmatrix} = \begin{bmatrix} 0 & LI & 0 \\ LD & 0 & LD \\ LDI & 0 & LDI \end{bmatrix} \begin{pmatrix} A_{10} \\ A_{01} \\ A_{11} \end{pmatrix} + \begin{bmatrix} LD^2I \\ 0 \\ 0 \end{bmatrix}$$

$$(I - M)A = B$$

$$\begin{bmatrix} 1 & -LI & 0 \\ -LD & 1 & -LD \\ -LDI & 0 & 1-LDI \end{bmatrix} \begin{bmatrix} A_{10} \\ A_{01} \\ A_{11} \end{bmatrix} = \begin{bmatrix} LD^2 I \\ 0 \\ 0 \end{bmatrix}$$

Cramer's Rule

$$A_{01} = \frac{\begin{vmatrix} 1 & LD^2 I & 0 \\ -LD & 0 & -LD \\ -LDI & 0 & 1-LDI \end{vmatrix}}{\begin{vmatrix} 1 & -LI & 0 \\ -LD & 1 & -LD \\ -LDI & 0 & 1-LDI \end{vmatrix}}$$

$$A_{01} = \frac{1 \cdot 0 - LD^2 I (-LD(1-LDI) - LD(LDI))}{LI((-LD)(1-LDI) - LD(LDI)) + 1(LDI)}$$

$$A_{01} = \frac{L^2 D^3 I}{-L^2 DI - LDI + 1} \Rightarrow A_{01} = \frac{L^2 D^3 I}{1 - LDI(1+L)}$$

$$\Rightarrow A_F = LD^2 A_{01} = \frac{L^3 D^5 I}{1 - LDI(1+L)}$$

$$\frac{1}{1-f(t)} = 1 + f(t) + f^2(t) + \dots$$

$$A_F = L^3 D^5 I \left[1 + L D I (1+L) + L^2 D^2 I^2 (1+L^2) + \dots \right] = L^3 D^5 I + L^4 D^6 I^2 + L^5 D^7 I^3 + \dots$$

Setting $L=1$, $I=1$; You are getting information about the # of paths of given output weight (without regard to input weight and/or length)

Example: $4 \cancel{L^3} I^1 D^5 + 3 \cancel{L^6} I^3 D^5 = 7 D^5$

$$A_F(L, D, I) \bigg|_{L=I=1} = \frac{L^3 D^5 I}{1 - L D I (1+L)} \bigg|_{L=I=1} = \frac{D^5}{1-2D}$$

$$= D^5 (1 + 2D + 4D^2 + 8D^3 + 16D^4 + \dots)$$

$$= D^5 + 2D^6 + 4D^7 + 8D^8 + 16D^9 + \dots$$

this gives the output weights of paths which go from the ψ -zero state w/o visiting the ψ -zero state in between.

$$P_{be} = \frac{1}{k} \sum_{i=1}^k P_{be,i} = \frac{\text{Expected \# of erroneous messages}}{k}$$

\hookrightarrow probability of bit error
 Assume standard $\frac{k}{n}$ rate code) \hookrightarrow Prob that the i^{th} message bit is in error

$$P_{cwe} \leq \sum_{d=1}^n A_d (PEP)_d \quad (\text{union bound})$$

↑
probability of codeword error.

upper bound because the regions are not disjoint → counting areas + than once

PEP_d is pairwise error probability that a potential codeword \subseteq of Hamming weight d is decoded given that $\underline{0}$ was sent

$$(PEP)_d \leq \sum_{e=1}^d \binom{d}{e} \underbrace{\epsilon^e (1-\epsilon)^{d-e}}_{\text{prob. of a specific pattern of } e \text{ flipped bits}}$$

$e = \lceil \frac{d}{2} \rceil$ bits
for this type of error to happen, at least $\frac{d}{2}$ must flip.

$$P_{be} \leq \sum_{d=0}^n \underbrace{\sum_{w=0}^k [A_{w,d}] I^w D^d}_{\text{how many errors make for each codeword error.}}$$

$\{A_{w,d}\}^k$
codewords of weight d with input w

$A_{w,d} I^w D^d$

is the # of codewords in the code corresponding to input weight w and output weight d

Going from codeword error prob to bit error prob.

input weight = the weight of the message vector underlying the codeword.

$$A_F(L, D, I) \Big|_{L=1} = \sum_{d,w} A_{w,d} I^w D^d$$

$$P_{be} \leq \frac{1}{k} \frac{\partial}{\partial I} (A_F(L=1, D, I))$$

↑
roughly speaking optimization.

$$D = 2 \sqrt{E(L-1)}^T$$

$$I = 1$$

$$Iw$$

→ comes from error analysis in AWGN

Now for AWGN (we skip proof)

sending $\pm \sqrt{E_s}$

$$P_{be} \leq \left(\frac{1}{k} \frac{\partial}{\partial I} A_F(L=1, D, I) \right) \bigg|_{\substack{I=1 \\ D=e^{-E_s/N_0}}} \cdot Q\left(\sqrt{2 \frac{d_{free} E_s}{N_0}}\right) \cdot e^{\frac{E_s d_{free}}{N_0}}$$

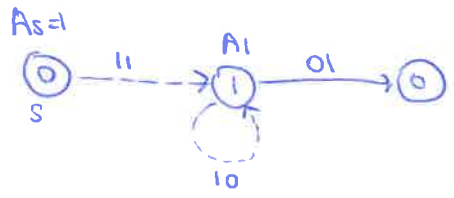
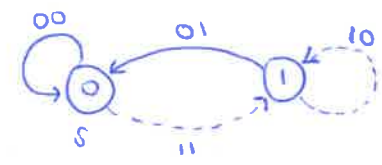
d_{free} is the minimum free distance of convolutional code of ∞ length
the # of smallest weight codewords.

Example

$$G(D) = [1, 1+D]$$

$$v_1(t) = u(t)$$

$$v_2(t) = u(t) + u(t-1)$$



$$A_S = 1$$

$$A_1 = A_S LID^2 + A_1 LID$$

$$= LID^2 + A_1 LID \Rightarrow$$

We don't want a polynomial
that is a ratio
We cannot interpret it

$$\Rightarrow A_1 = \frac{LID^2}{1-LID}$$

$$A_F = A_1 \cdot L \cdot D = \frac{L^2 I D^3}{1-LID}$$

$$A_F = L^2 I D^3 (1 + LID + L^2 I^2 D^2 + \dots)$$

I want to calculate the free distance \triangleq min weight of the codeword when you have ∞ longer paths.

- I don't care about length $\rightarrow L=1$
- " " " " input $\rightarrow I=1$

$$A_F \Big|_{\substack{L=1 \\ I=1}} = \frac{D^3}{1-D} = D^3 (1 + D + D^2 + D^3 + \dots)$$

$$\therefore \boxed{d_{free} = 3}$$

Example

$$E = \frac{1}{2} \quad k=1 \quad m=2$$

$$A_F(I, L, D) = L^4 I^2 D^5 + 2 L^6 I^4 D^7 + \dots$$

Find upper bound on P_{be} in BSC when $E \ll 1$

$$P_{be} \leq \frac{1}{k} \frac{\partial}{\partial I} A_F(L=1, D, I) \Big|_{D=2\sqrt{E(1-E)}, I=1}$$

we do care about the input weights but $I=1$ is the result of the optimization problem.

$$A_F \Big|_{L=1} = I^2 D^5 + 2 I^4 D^7 \quad \cdot \quad \frac{\partial}{\partial I} (A_F \Big|_{I=1}) = 2 I D^5 + 8 I^3 D^7 \Big|_{I=1}$$

$$\Rightarrow P_{be} \leq 2 D^5 + 8 D^7 \Big|_{D=2\sqrt{E(1-E)}} = 2 D^5 (1 + 4 D^2) = 2 \cdot 32 E^2 (1-E)^2 \sqrt{E(1-E)} (1 + 16 E(1-E))$$

$$= 64 E^2 (1-E)^2 \sqrt{E(1-E)} (1 + 16 E(1-E)) \underset{\substack{\uparrow \\ E \ll 1}}{\approx} 64 E^2 \sqrt{E} = 64 E^{5/2}$$