

# Error Correction Codes

## Agenda

- Shannon Theory
- History of Error Correction Code
- Linear Block Codes
- Decoding
- Convolution Codes

2012/07/06

Wireless Communication Engineering I

1

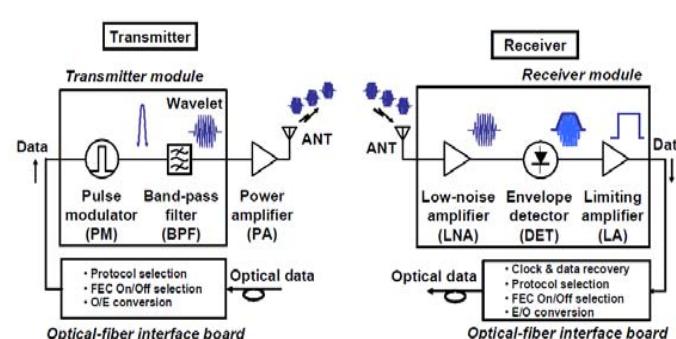
### Shannon Theory:

$R < C \rightarrow$  Reliable communication  
Redundancy (Parity bits)  
in transmitted data stream  
→ error correction capability

2012/07/06

Wireless Communication Engineering I

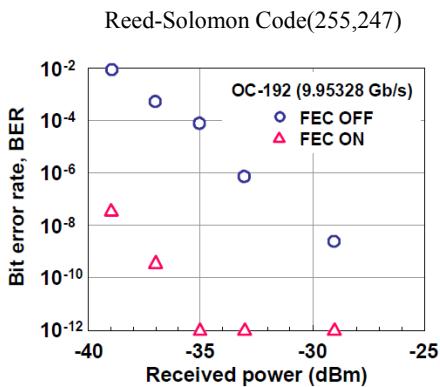
2



2012/07/06

Wireless Communication Engineering I

3



2012/07/06

Wireless Communication Engineering I

4

## Encoding

Block Code

Convolutional Code

Code length is fixed

Coding Rate is fixed

2012/07/06

Wireless Communication Engineering I

5

## Decoding

Hard-Decoding

Soft-Decoding

Digital Information

Analog Information

2012/07/06

Wireless Communication Engineering I

6

## History of Error Correction Code

- Shannon (1948): Random Coding
- Golay (1949): Golay Code(Perfect Code)
- Hamming (1950): Hamming Code  
(Single Error Correction, Double Error Detection)
- Gilbert (1952): Gilbert Bound on Coding Rate

2012/07/06

Wireless Communication Engineering I

7

- Muller (1954): Combinatorial Function & ECC
- Elias (1954): **Convolutional Code**
- Reed ,Solomon (1960): RS Code (**Maximal Separable**)
- Hocquenghem (1959) ,Bose,Chaudhuri (1960): **BCH Code** (Multiple Error Correction)
- Peterson (1960): **Error Location Polynomial**

2012/07/06

Wireless Communication Engineering I

8

- Wozencraft , Reiffen (1961): Sequential decoding
- Gallager (1962) :**LDPC**
- Fano (1963): Fano Decoding Algorithm
- Ziganzirov (1966): Stack Decoding Algorithm
- Forney (1966): Generalized Minimum Distance Decoding (**Error and Erasure Decoding**)
- Viterbi (1967): **Optimal Decoding Algorithm,**  
**Dynamic Programming**

2012/07/06

Wireless Communication Engineering I

9

- Berlekamp (1968): Fast Iterative BCH Decoding
- Forney (1966): **Concatinated Code**
- Goppa (1970): Rational Function Code
- Justeson (1972): Asymptotically Good Code
- Ungerboeck,Csajka (1976): **Trellis Code Modulation,**
- Goppa (1980): **Algebraic-Geometry Code**

2012/07/06

Wireless Communication Engineering I

10

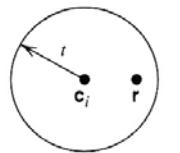
- Welch,Berlekamp (1983): Remainder Decoding Algorithm
- Araki, Sorger and Kotter (1993): Fast GMD Decoding Algorithm
- Berrou (1993): **Turbo Code**(Parallel concatenated convolutional code)

2012/07/06

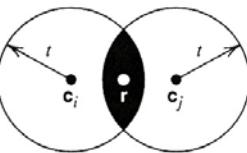
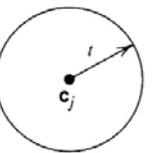
Wireless Communication Engineering I

11

## Basics of Decoding



(a)



(b)

a) Hamming distance  $d(\mathbf{c}_i, \mathbf{c}_j) \geq 2t + 1$

b) Hamming distance  $d(\mathbf{c}_i, \mathbf{c}_j) < 2t$

The received vector is denoted by  $\mathbf{r}$ .

**$t \rightarrow$  errors correctable**

2012/07/06

Wireless Communication Engineering I

12

## Linear Block Codes

$(n, k, d_{\min})$  code

$n$  : code length

$k$  : number of information bits

$d_{\min}$  : minimum distance

$k/n$  : coding rate

2012/07/06

Wireless Communication Engineering I

13

For large  $d$ , Good Error correction capability  
 $R=k/n$  (Low coding rate)

*Trade-off between error correction and coding rate*

2012/07/06

Wireless Communication Engineering I

14

$(n, k, d)$  Linear Block Code is  
Linear Subspace with  $k$ -dimension in  $n$ -dimension linear space.

2012/07/06

Wireless Communication Engineering I

15

Arithmetic operations ( $+, -, \times, /$ ) for encoding and decoding over an **finite field**  $\text{GF}(Q)$   
where  $Q = p^r$ ,  $p$ : prime number     $r$ : positive integer

Example GF(2):

	+	0	1
addition	0	0	1
XOR	1	1	0

	.	0	1
multiplication	0	0	0
AND	1	0	1

2012/07/06

Wireless Communication Engineering I

16

## Analog and Digital Arithmetic Operation

- Analog: Real Number Field [R], Complex Number Field [C]
- Digital: Finite Field [GF(Q)]

2012/07/06

Wireless Communication Engineering I

17

## [Encoder]

- The Generator Matrix  $\mathbf{G}$  and the Parity Check Matrix  $\mathbf{H}$

$k$  information bits  $\mathbf{X} \rightarrow$  encoder  $\mathbf{G} \rightarrow n$ -bits codeword  $\mathbf{C}$

$$\mathbf{C} = \mathbf{X}\mathbf{G}$$

2012/07/06

Wireless Communication Engineering I

18

- Dual  $(n, n - k)$  code

Complement orthogonal subspace  
Parity Check Matrix  $\mathbf{H}$  = Generator Matrix of Dual code

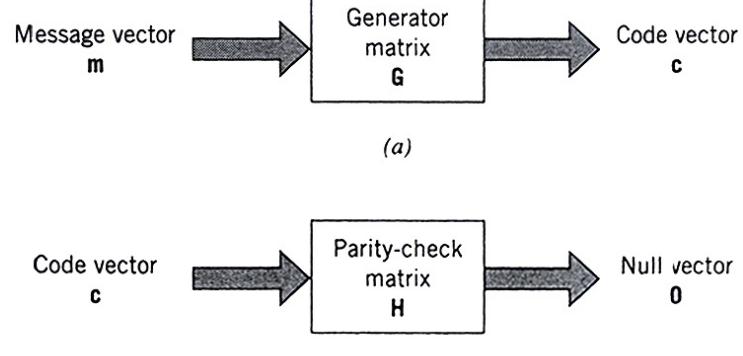
$$\mathbf{CH}^t = 0$$

$$\mathbf{GH}^t = 0$$

2012/07/06

Wireless Communication Engineering I

19



2012/07/06

Wireless Communication Engineering I

20

## error vector & syndrome

**c** : codeword vector

**e** : error vector

**r** : received vector (after Hard decision)

**s** : syndrome

$$\mathbf{s} = \mathbf{r}\mathbf{H}^t = (\mathbf{c} + \mathbf{e})\mathbf{H}^t = \mathbf{e}\mathbf{H}^t$$

**s** → **e** (decoding process)

2012/07/06

Wireless Communication Engineering I

21

## [Minimum Distance]

### Singleton Bound

If no more than  $d_{\min} - 1$  columns of  $\mathbf{H}$  are linearly independent.

$$d_{\min} \leq n - k + 1 \text{ (Singleton Bound)}$$

### Maximal Separable Code:

$d_{\min} = n - k + 1$ , e.g. Reed-Solomon Code

2012/07/06

Wireless Communication Engineering I

22

- Some Specific Linear Block Codes

- Hamming Code  $(n, k, d_{\min}) = (2m - 1, 2m - 1 - m, 3)$
- Hadamard Code  $(n, k, d_{\min}) = (2m, m + 1, 2m - 1)$

2012/07/06

Wireless Communication Engineering I

23

## Easy Encoding

- **Cyclic Codes**

If  $\mathbf{C} = (c_{n-1}, \dots, c_0)$  is a codeword

$\rightarrow (c_{n-2}, \dots, c_0, c_{n-1})$  is also a codeword.

- Codeword polynomial:  $C(p) = c_{n-1} p^{n-1} + \dots + c_n$

$$pC(p) \bmod p^n - 1 \leftarrow \text{CyclicShift}$$

2012/07/06

Wireless Communication Engineering I

24

Encoding: Message polynomial

$$X(p) = x_{k-1} p^{k-1} + \dots + x_n \rightarrow$$

Codeword polynomial  $C(p) = X(p)g(p)$

where  $g(p)$ : generator polynomial of degree  $n-k$

$$p^n + 1 = g(p)h(p)$$

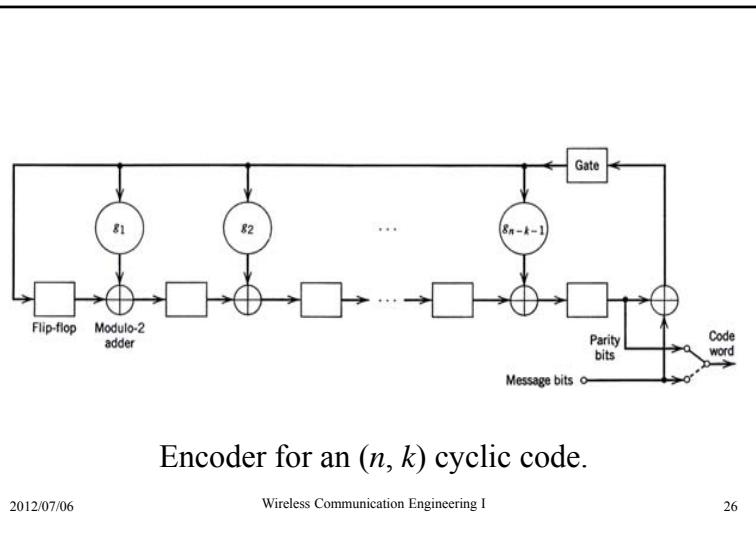
$h(p)$ : Parity polynomial

Encoder is implemented by Shift registers.

2012/07/06

Wireless Communication Engineering I

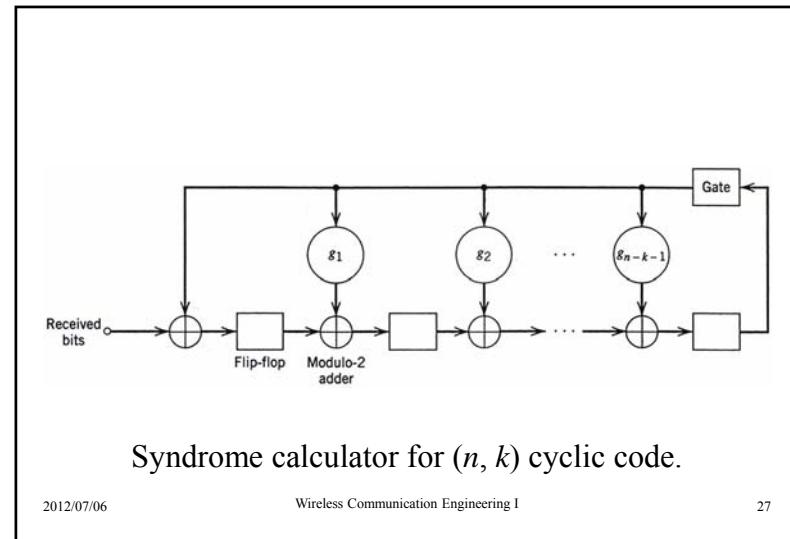
25



2012/07/06

Wireless Communication Engineering I

26



2012/07/06

Wireless Communication Engineering I

27

## Digital to Analog (BPSK)

$$c = 1 \rightarrow s = +1$$

$$0 \rightarrow s = -1$$

$$\therefore s = 2c - 1$$

2012/07/06

Wireless Communication Engineering I

28

## Soft-Decoding & Maximum Likelihood

$$\begin{aligned} \mathbf{r} &= \mathbf{s}^{(k)} + \mathbf{n} \\ &= (r_1, \dots, r_n) \\ &= (s_1, \dots, s_n) + (n_1, \dots, n_n) \end{aligned}$$

Prob  $[\mathbf{r}|\mathbf{s}^{(k)}]$ : Likelihood

$$\begin{aligned} \max_k \text{Prob} [\mathbf{r}|\mathbf{s}^{(k)}] &\rightarrow \min_k (\mathbf{r} - \mathbf{s}^{(k)})^2 \\ &\rightarrow \max_k : \text{Correlation} [\mathbf{r}, \mathbf{c}^{(k)}] \end{aligned}$$

2012/07/06

Wireless Communication Engineering I

29

- Optimum Soft-Decision Decoding of Linear Block Codes

Optimum receiver has  $M = 2^k$  Matched Filter  $\rightarrow M$  correlation metrics

$$C(\mathbf{r}, \mathbf{C}_i) = \sum_{j=1}^n (2c_{ij} - 1)r_j$$

where  $\mathbf{C}_i$  :  $i$ -th codeword

$c_{ij}$  :  $j$ -th position bit of the  $i$ -th codeword

$r_j$  :  $j$ -th received signal

$\rightarrow$  Largest matched filter output is selected.

2012/07/06

Wireless Communication Engineering I

30

Error probability for soft-decision decoding (Coherent PSK)

$$P_M < \exp(-\gamma_b R_c d_{\min} + k \ln 2)$$

where  $\gamma_b$  : SNR per bit

$R_c$  : Coding rate ( $= k/n$ )

Uncoded binary PSK

$$P_e < \frac{1}{2} \exp(-\gamma_b)$$

2012/07/06

Wireless Communication Engineering I

31

Coding gain:

$$Cg = 10 \log(R_c d_{\min} - k \ln 2 / \gamma_b)$$

$$d_{\min} \uparrow \rightarrow Cg \uparrow$$

2012/07/06

Wireless Communication Engineering I

32

- Hard-Decision Decoding

Discrete-time channel =  
modulator + AWGN channel + demodulator  
→ BSC with crossover probability (p)

$$p = Q\left(\sqrt{2\gamma_b R_c}\right); \text{coherent PSK}$$

$$Q\left(\sqrt{\gamma_b R_c}\right); \text{coherent FSK}$$

$$\frac{1}{2} \exp\left(-\frac{1}{2} \gamma_b R_c\right); \text{noncoherent FSK}$$

2012/07/06

Wireless Communication Engineering I

33

Maximum-Likelihood Decoding →  
Minimum Distance Decoding  
Syndrome Calculation by Parity check matrix  $\mathbf{H}$

$$\begin{aligned} \mathbf{S} &= \mathbf{Y}\mathbf{H}^t \\ &= (\mathbf{C}_m + \mathbf{e})\mathbf{H}^t \\ &= \mathbf{e}\mathbf{H}^t \end{aligned}$$

where  $\mathbf{C}_m$  : transmitted codeword

$\mathbf{Y}$  : received codeword at the demodulator

$\mathbf{e}$  : binary error vector

2012/07/06

Wireless Communication Engineering I

34

- Comparison of Performance between **Hard-Decision** and **Soft-Decision** Decoding

→ At most  $\approx 2$ dB difference

2012/07/06

Wireless Communication Engineering I

35

- **Bounds on Minimum Distance of Linear Block Codes ( $R_c$  vs.  $d_{min}$ )**

– Hamming upper bound ( $2t < d_{min}$ )

$$1 - R_c \geq \frac{1}{n} \log_2 \sum_{i=0}^t \binom{n}{i}$$

– Plotkin upper bound

$$\frac{d_{min}}{n} \left( 1 - \frac{1}{2d_{min}} \log_2 d_{min} \right) \leq \frac{1}{2} \left( 1 - R_c + \frac{2}{n} \right)$$

2012/07/06

Wireless Communication Engineering I

36

– Elias upper bound

$$\frac{d_{min}}{n} \leq 2A(1-A)$$

$$R_c = 1 + A \log_2 A + (1-A) \log_2 (1-A)$$

– Gilbert-Varshamov lower bound

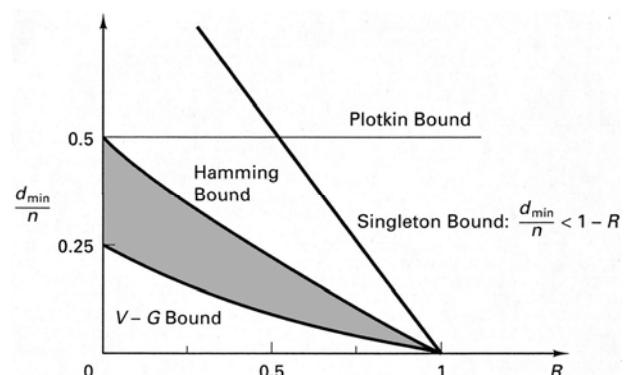
$$\frac{d_{min}}{n} \geq \alpha$$

$$R_c = 1 - H(\alpha)$$

2012/07/06

Wireless Communication Engineering I

37



2012/07/06

Wireless Communication Engineering I

38

- Interleaving of Coded Data for Channels with Burst Errors  
Multipath and fading channel → burst error  
**Burst error correction code: Fire code**  
Correctable burst length  $b$

$$b \leq \left\lfloor \frac{1}{2}(n-k) \right\rfloor$$

Block and Convolution interleave is effective for burst error.

2012/07/06

Wireless Communication Engineering I

39

## Convolution Codes

Performance of **convolution code > block code**  
shown by Viterbi's Algorithm.

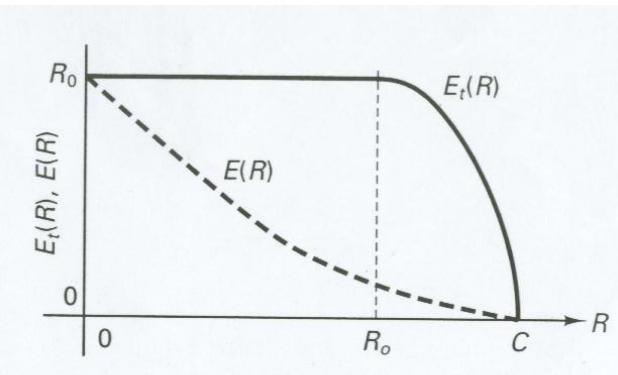
$$\overline{P(e)} \leq e^{-nE(R)}$$

$E(R)$  : Error Exponent

2012/07/06

Wireless Communication Engineering I

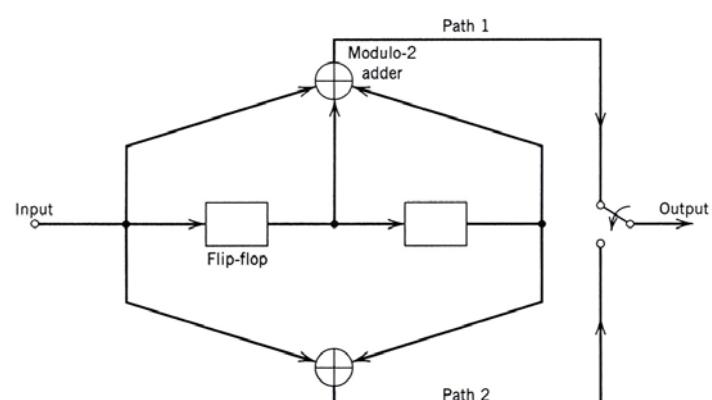
40



2012/07/06

Wireless Communication Engineering I

41



Constraint length-3, rate-1/2 convolutional encoder.

2012/07/06

Wireless Communication Engineering I

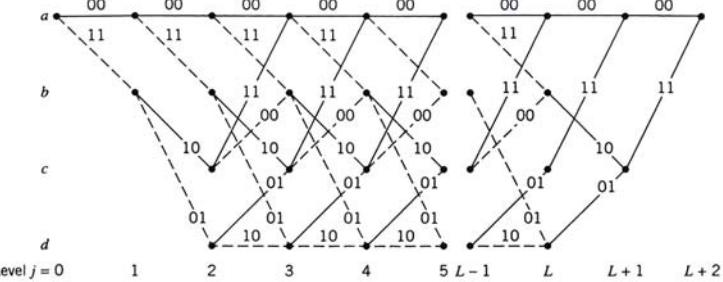
42

- Parameter of convolution code:  
Constraint length,  $K$   
Minimum free distance
- Optimum Decoding of Convolution Codes –  
The Viterbi Algorithm  
For  $K \leq 10$ , this is practical.
- Probability of Error for Soft-Decision Decoding

2012/07/06

Wireless Communication Engineering I

43



Trellis for the convolutional encoder

2012/07/06

Wireless Communication Engineering I

44

$$P_e \leq \sum_{d=d_{\text{free}}}^{\infty} a_d Q\left(\sqrt{2\gamma_b R_c d}\right)$$

where  $a_d$ : the number of paths of distance  $d$

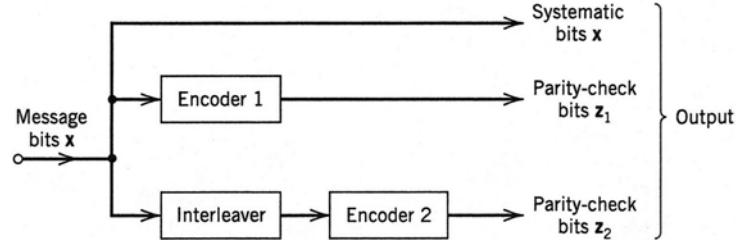
- Probability of Error for Hard-Decision Decoding  
Hamming distance is a metric for hard-decision

2012/07/06

Wireless Communication Engineering I

45

## Turbo Coding

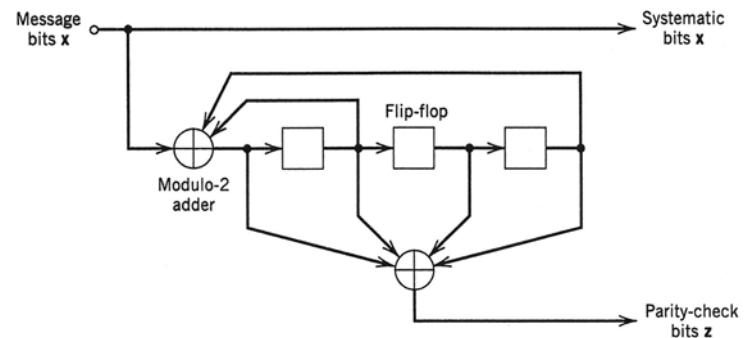


2012/07/06

Wireless Communication Engineering I

46

## RSC Encoder

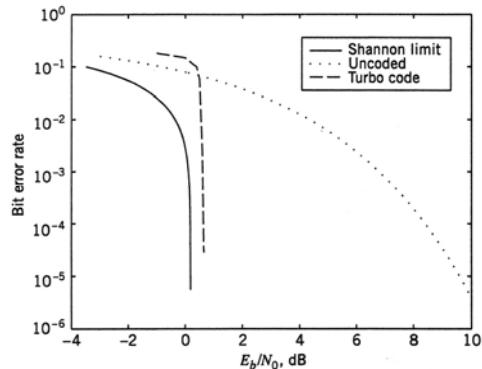


2012/07/06

Wireless Communication Engineering I

47

## Shannon Limit & Turbo Code

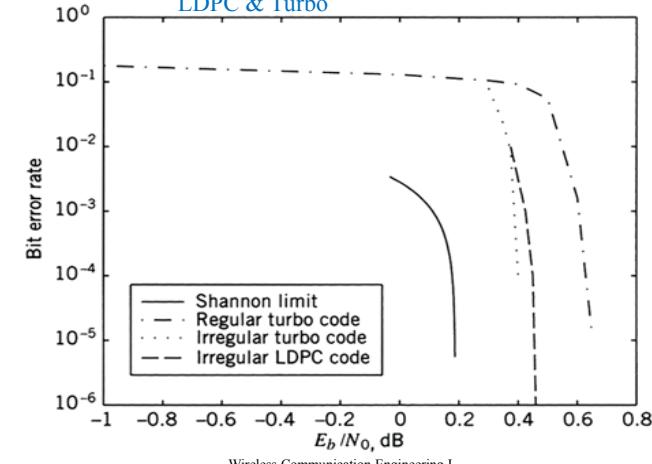


2012/07/06

Wireless Communication Engineering I

48

## LDPC & Turbo

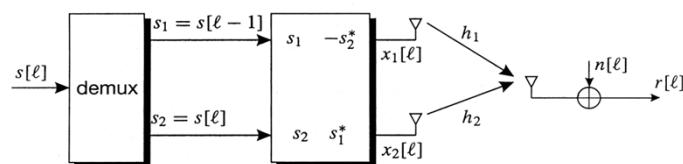


2012/07/06

Wireless Communication Engineering I

49

## Alamouti's space-time block code



- Received block of two consecutive symbols

$$\tilde{\mathbf{r}} = \begin{pmatrix} r[\ell] \\ r[\ell+1]^* \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} n[\ell] \\ n[\ell+1]^* \end{pmatrix} = \tilde{\mathbf{H}} \cdot \mathbf{s} + \tilde{\mathbf{n}}$$

- Estimated symbol vector after matched filtering

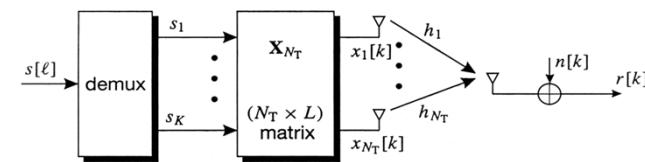
$$\mathbf{y} = \tilde{\mathbf{H}}^H \cdot \tilde{\mathbf{r}} = \frac{1}{2} \cdot \begin{pmatrix} |h_1|^2 + |h_2|^2 & 0 \\ 0 & |h_1|^2 + |h_2|^2 \end{pmatrix} \cdot \mathbf{s} + \tilde{\mathbf{H}}^H \cdot \tilde{\mathbf{n}}$$

2012/07/06

Wireless Communication Engineering I

50

## Orthogonal space-time block codes



- Code rate

$$R = \frac{K}{L}$$

- Spectral efficiency

$$\eta = m \cdot R = m \cdot \frac{K}{L}$$

- Orthogonality constraint

$$\mathbf{X}_{N_T} \mathbf{X}_{N_T}^H = \frac{K}{N_T} \cdot \frac{E_s}{T_s} \cdot \mathbf{I}_{N_T}$$

2012/07/06

Wireless Communication Engineering I

51

### Orthogonal space-time block codes for $R = 1/2$

- $N_T = 3$  transmit antennas ( $L = 8, K = 4$ )

$$\mathbf{X}_3 = \frac{1}{\sqrt{6}} \cdot \begin{pmatrix} s_1 & -s_2 & -s_3 & -s_4 & s_1^* & -s_2^* & -s_3^* & -s_4^* \\ s_2 & s_1 & s_4 & -s_3 & s_2^* & s_1^* & s_4^* & -s_3^* \\ s_3 & -s_4 & s_1 & s_2 & s_3^* & -s_4^* & s_1^* & s_2^* \end{pmatrix}$$

- $N_T = 4$  transmit antennas ( $L = 8, K = 4$ )

$$\mathbf{X}_4 = \frac{1}{\sqrt{8}} \cdot \begin{pmatrix} s_1 & -s_2 & -s_3 & -s_4 & s_1^* & -s_2^* & -s_3^* & -s_4^* \\ s_2 & s_1 & s_4 & -s_3 & s_2^* & s_1^* & s_4^* & -s_3^* \\ s_3 & -s_4 & s_1 & s_2 & s_3^* & -s_4^* & s_1^* & s_2^* \\ s_4 & s_3 & -s_2 & s_1 & s_4^* & s_3^* & -s_2^* & s_1^* \end{pmatrix}$$

2012/07/06

Wireless Communication Engineering I

52

### Orthogonal space-time block codes for $R = 3/4$

- $N_T = 3$  transmit antennas ( $L = 4, K = 3$ )

$$\mathbf{T}_3 = \frac{1}{\sqrt{12}} \cdot \begin{pmatrix} 2s_1 & -2s_2^* & \sqrt{2}s_3^* & \sqrt{2}s_3^* \\ 2s_2 & 2s_1^* & \sqrt{2}s_3^* & -\sqrt{2}s_3^* \\ \sqrt{2}s_3 & \sqrt{2}s_3 & -s_1 - s_1^* + s_2 - s_2^* & s_1 - s_1^* + s_2 + s_2^* \end{pmatrix}$$

- $N_T = 4$  transmit antennas ( $L = 4, K = 3$ )

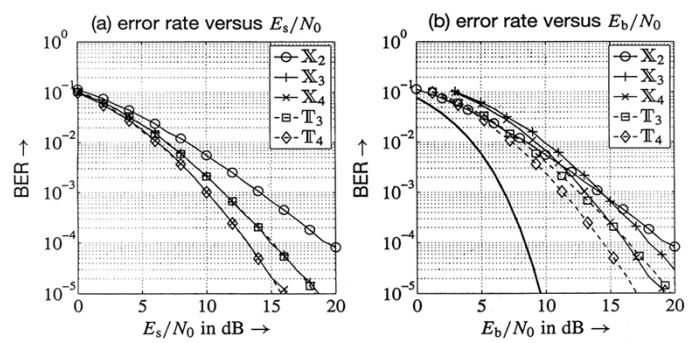
$$\mathbf{T}_4 = \frac{1}{4} \begin{pmatrix} 2s_1 & -2s_2^* & \sqrt{2}s_3^* & \sqrt{2}s_3^* \\ 2s_2 & 2s_1^* & \sqrt{2}s_3^* & -\sqrt{2}s_3^* \\ \sqrt{2}s_3 & \sqrt{2}s_3 & -s_1 - s_1^* + s_2 - s_2^* & s_1 - s_1^* + s_2 + s_2^* \\ \sqrt{2}s_3 & -\sqrt{2}s_3 & -s_1 - s_1^* - s_2 - s_2^* & -(s_1 + s_1^* + s_2 + s_2^*) \end{pmatrix}$$

2012/07/06

Wireless Communication Engineering I

53

### Performance of orthogonal space-time block codes for BPSK



2012/07/06

Wireless Communication Engineering I

54

### Network Coding

- $A \rightarrow [X] \rightarrow B$
- $B \rightarrow [X] \rightarrow C$
- $B \leftarrow [Y] \leftarrow C$
- $A \leftarrow [Y] \leftarrow B$   
---- 4 steps ----
- $A \rightarrow [X] \rightarrow B$
- $B \leftarrow [Y] \leftarrow C$
- $A \leftarrow [X+Y] \leftarrow B \rightarrow [X+Y] \rightarrow C$   
---- 3 steps ----

2012/07/06

Wireless Communication Engineering I

55

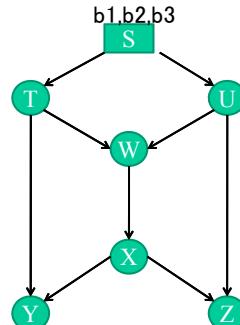
## A famous example – butterfly network

- S: source node
- T, U, W, X: relay nodes
- Y, Z: destination
- S needs to send 3 bits b1, b2, b3 to both Y and Z (multicast)
- Link capacity is 1

2012/07/06

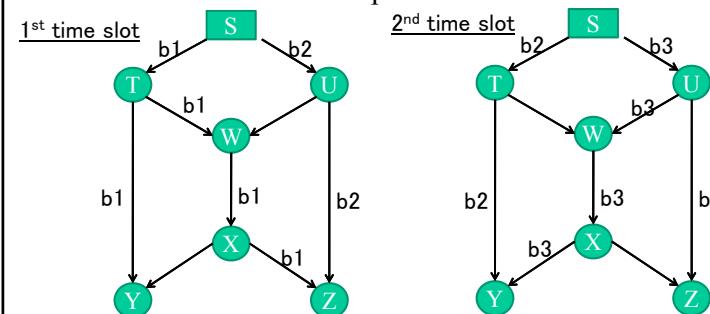
Wireless Communication Engineering I

56



## A famous example – butterfly network without network coding

- Simple store and forward
- Multicast rate of 1.5 bits per time unit



2012/07/06

Wireless Communication Engineering I

57

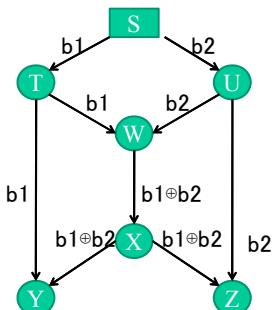
## A famous example – butterfly network with network coding

- W receives b1 and b2, then performs exclusive OR (XOR) on received bits and forward to X
- Y receives b1 and  $b1 \oplus b2$ , then extracts b2 as  $b2 = b1 \oplus (b1 \oplus b2)$
- Z receives b2 and  $b1 \oplus b2$  then extracts b1 as  $b1 = b2 \oplus (b1 \oplus b2)$
- Achieve multicast rate of 2 bits per time unit

2012/07/06

Wireless Communication Engineering I

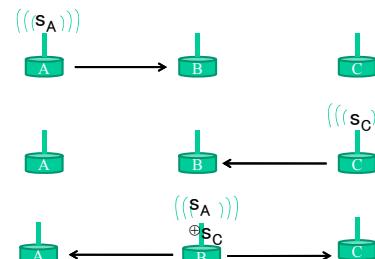
58



## Network coding in wireless environment

- It is easy to apply network coding in wireless environment owing to the broadcast characteristics

- An example shows data from A to C and from C to A can be relayed through B efficiently using network coding



2012/07/06

Wireless Communication Engineering I

59

## Network coding header

- In network coding, since information is processed inside the network, network coding header is required for network decoding at the destination
- Network coding header describes how a packet is processed
- The right figure shows network coding header of the butterfly network example
- If packet length is long enough, we can neglect the inefficiency of header

