Error Correction Codes

Agenda

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

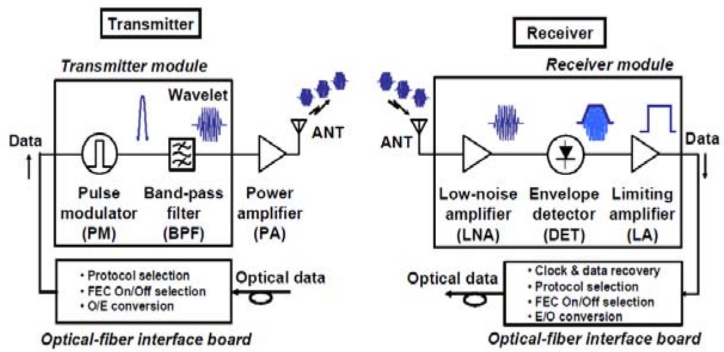
Shannon Theory:

$R < C \rightarrow$ Reliable communication

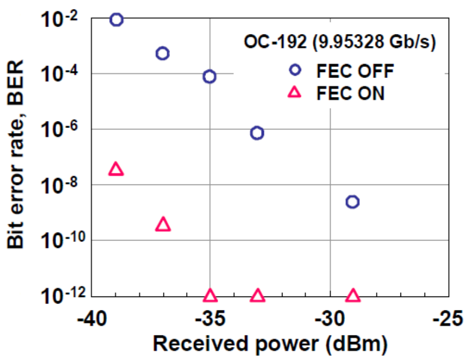
Redundancy (Parity bits)

in transmitted data stream

$\rightarrow$ error correction capability



Reed-Solomon Code(255,247)



Encoding

Block Code	Convolutional Code
Code length is fixed	Coding Rate is fixed

Decoding

Hard-Decoding	Soft-Decoding
Digital Information	Analog Information

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

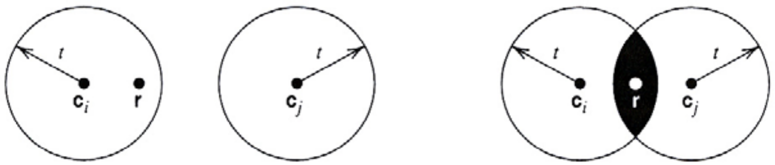
- Muller (1954): Combinatorial Function & ECC
- Elias (1954): Convolutional Code
- Reed ,Solomon (1960): RS Code (Maximal Separable)
- Hocquenghem (1959) ,Bose,Chaudhuri (1960): BCH Code (Multiple Error Correction)
- Peterson (1960): Error Location Polynomial

- 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

- 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

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

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 **r**.

***t* → errors correctable**

Linear Block Codes

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

n : code length

k : number of information bits

$d_{\min}$: minimum distance

k/n : coding rate

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

Trade-off between error correction and coding rate

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

Arithmetic operations $(+, -, \times, /)$ for encoding and decoding over an **finite field** GF(Q)

where $Q = p^r$, p: prime number r: positive integer

Example GF(2):

addition

+	0	1
0	0	1
1	1	0

XOR

multiplication

·	0	1
0	0	0
1	0	1

AND

Analog and Digital Arithmetic Operation

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

[Encoder]

- The Generator Matrix **G** and
  the Parity Check Matrix **H**

k information bits **X** → encoder **G** → n-bits codeword **C**

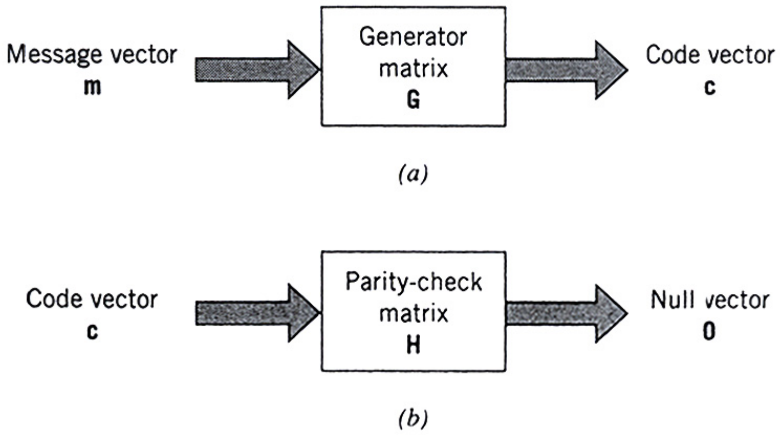
$$\mathbf{C} = \mathbf{X}\mathbf{G}$$

- Dual (n, n - k) code

Complement orthogonal subspace
Parity Check Matrix **H** = Generator Matrix of Dual code

$$\mathbf{C}\mathbf{H}^t = 0$$

$$\mathbf{G}\mathbf{H}^t = 0$$



error vector & syndrome

$\mathbf{c}$: codeword vector

$\mathbf{e}$: error vector

$\mathbf{r}$: received vector (after Hard decision)

$\mathbf{s}$: syndrome

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

$$\mathbf{s} \rightarrow \mathbf{e} \text{ (decoding process)}$$

[Minimum Distance]

Singleton Bound

If no more than d_{min} - 1 columns of **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

- Some Specific Linear Block Codes
  - Hamming Code (n, k, dmin) = (2m - 1, 2m - 1 - m, 3)
  - Hadamard Code (n, k, dmin) = (2m, m + 1, 2m - 1)

Easy Encoding

- Cyclic Codes
  If $\mathbf{C} = (c_{n-1}, \ldots, c_0)$ is a codeword
  $\rightarrow (c_{n-2}, \ldots, c_0, c_{n-1})$ is also a codeword.
- Codeword polynomial: $C(p) = c_{n-1}\, p^{n-1} + \ldots + c_n$

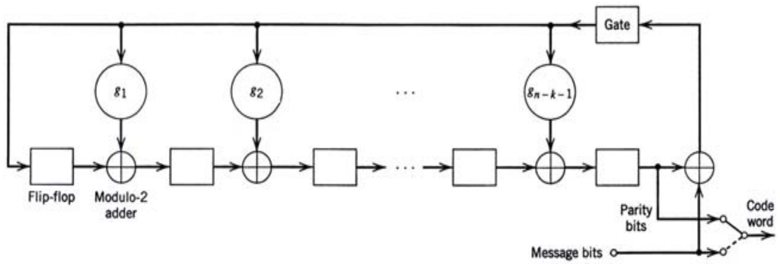
$$pC(p) \bmod p^n - 1 \leftarrow \text{CyclicShift}$$

Encoding: Message polynomial
$X(p) = x_{k-1}\, p^{k-1} + \cdots + x_n \rightarrow$
Codeword polynomial $C(p) = X(p)g(p)$
where $g(p)$: generator polynomial of degree $n-k$

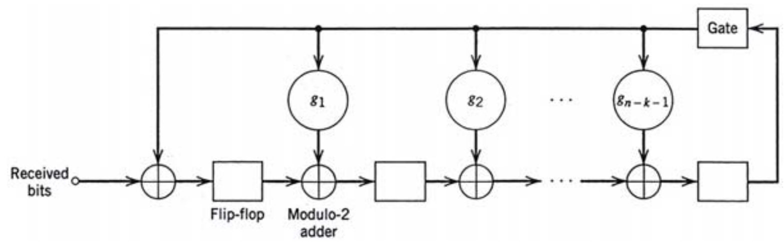
$$p^n + 1 = g(p)h(p)$$

$h(p)$: Parity polynomial

Encoder is implemented by Shift registers.



Encoder for an (n, k) cyclic code.



Syndrome calculator for (n, k) cyclic code.

Digital to Analog (BPSK)

$$c = 1 \quad \rightarrow \quad s = +1$$
$$0 \quad \rightarrow \quad s = -1$$
$$\therefore \quad s = 2c - 1$$

Soft-Decoding & Maximum Likelihood

$$\mathbf{r} = \mathbf{s}^{(k)} + \mathbf{n}$$
$$= (r_1, \cdots, r_n)$$
$$= (s_1, \cdots, s_n) + (n_1, \cdots, n_n)$$

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

$$\underset{k}{\text{Max}}\ \text{Prob}\left[\mathbf{r} \middle| \mathbf{s}^{(k)}\right] \rightarrow \underset{k}{\text{Min}}\left(\mathbf{r} - \mathbf{s}^{(k)}\right)^2$$

$$\rightarrow \underset{k}{\text{Max}} : \text{Correlation}\left[\mathbf{r}, \mathbf{c}^{(k)}\right]$$

- Optimum Soft-Decision Decoding of Linear Block Codes
  Optimum receiver has $M = 2^k$ Matched Filter → 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

→ Largest matched filter output is selected.

Error probability for soft-decision decoding (Coherent PSK)

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

where γ_b : SNR per bit

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

Uncoded binary PSK

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

Coding gain:

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

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

- Hard-Decision Decoding

  Discrete-time channel =

  modulator + AWGN channel + demodulator

  → BSC with crossover probability (p)

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

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

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

Maximum-Likelihood Decoding →
Minimum Distance Decoding
Syndrome Calculation by Parity check matrix **H**

$$\mathbf{S} = \mathbf{Y}\mathbf{H}^t$$
$$= \left(\mathbf{C}_m + \mathbf{e}\right)\mathbf{H}^t$$
$$= \mathbf{e}\mathbf{H}^t$$

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

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

$\mathbf{e}$: binary error vector

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

→ At most ≈2dB difference

- **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

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

- Elias upper bound

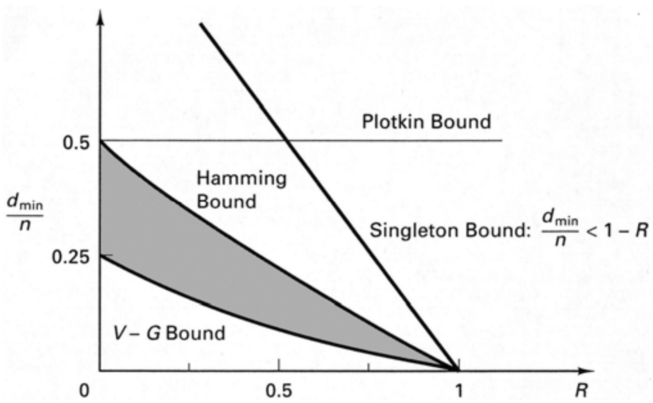
$$\frac{d_{\min}}{n} \leq 2A(1-A)$$

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

- Gilbert-Varsharmov lower bound

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

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



- 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

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

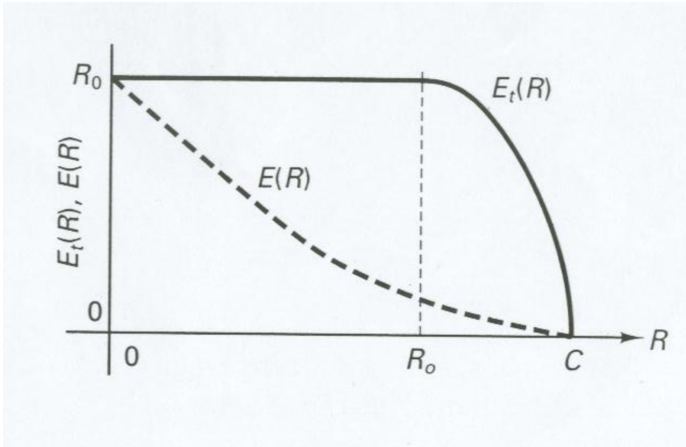
Block and Convolution interleave is effective for burst error.

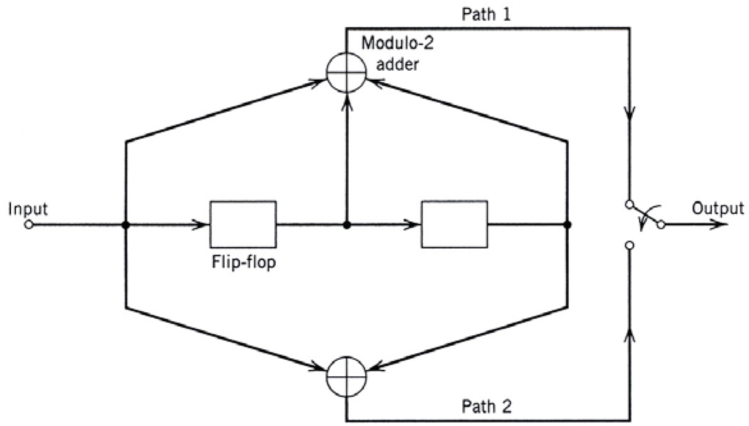
Convolution Codes

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

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

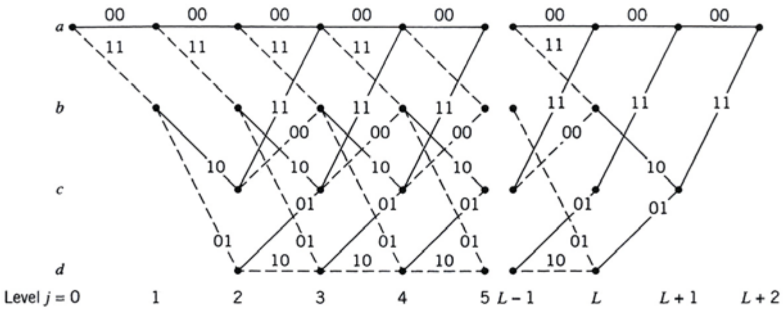
E(R) : Error Exponent





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

- 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



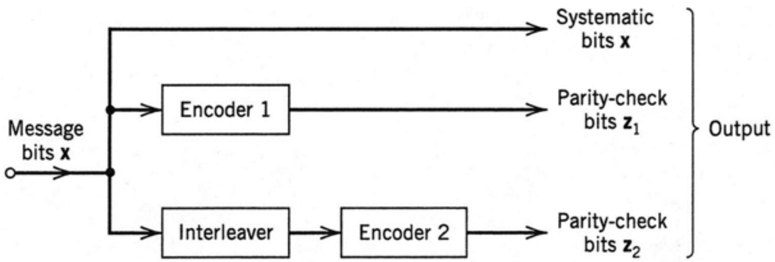
Trellis for the convolutional encoder

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

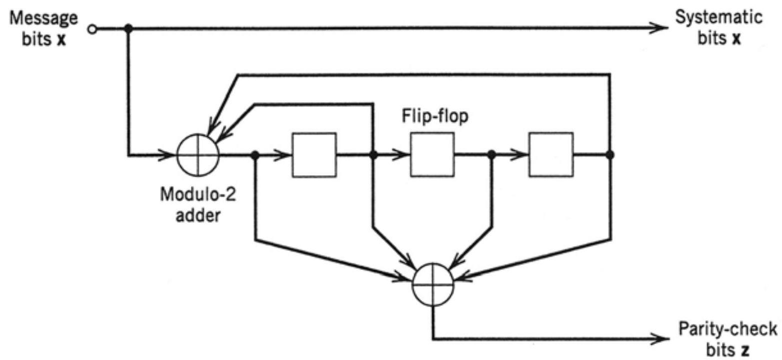
where a_d : the number of paths of distance d

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

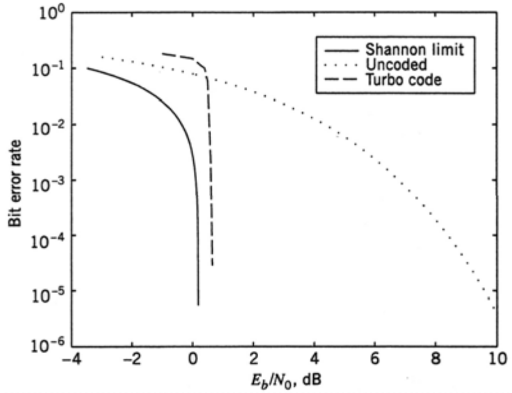
Turbo Coding

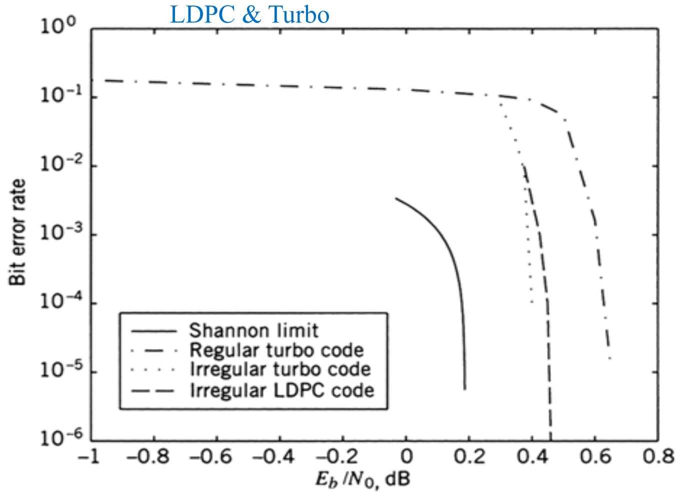


RSC Encoder

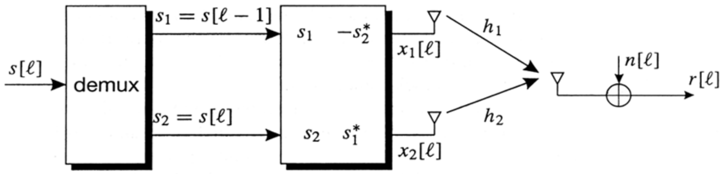


Shannon Limit & Turbo Code





Alamouti's space–time block code



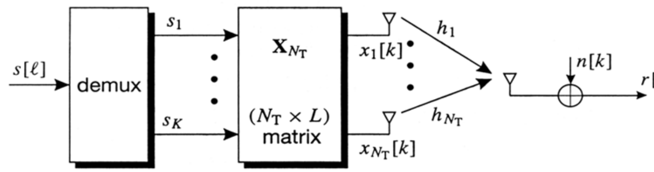
- Received block of two consecutive symbols

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

- Estimated symbol vector after matched filtering

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

Orthogonal space–time block codes



- Code rate

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

- Spectral efficiency

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

- Orthogonality constraint

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

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

- $N_\mathrm{T} = 3$ transmit antennas ($L = 8,\ K = 4$)

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

- $N_\mathrm{T} = 4$ transmit antennas ($L = 8,\ K = 4$)

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

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

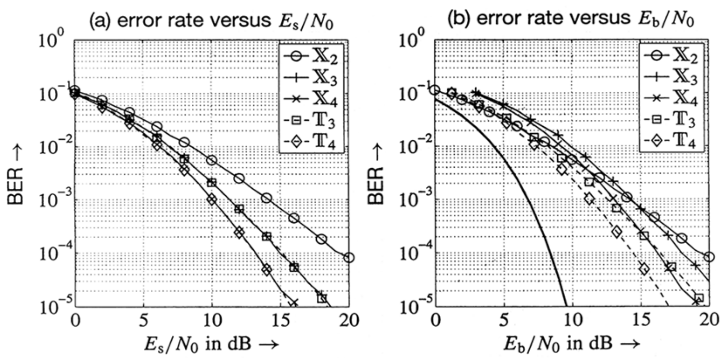
- $N_\mathrm{T} = 3$ transmit antennas ($L = 4,\ K = 3$)

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

- $N_\mathrm{T} = 4$ transmit antennas ($L = 4,\ K = 3$)

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

Performance of orthogonal space–time block codes for BPSK



Network Coding

- A →[X]→ B
- B →[X]→ C
- B ←[Y]← C
- A ←[Y]← B

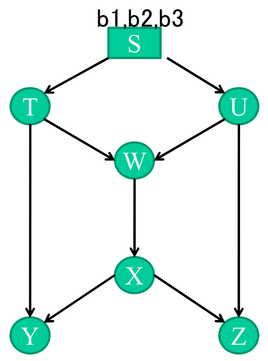
---- 4 steps ----

- A →[X]→ B
- B ←[Y]← C
- A←[X＋Y]←B→[X＋Y]→C

---- 3 steps ----

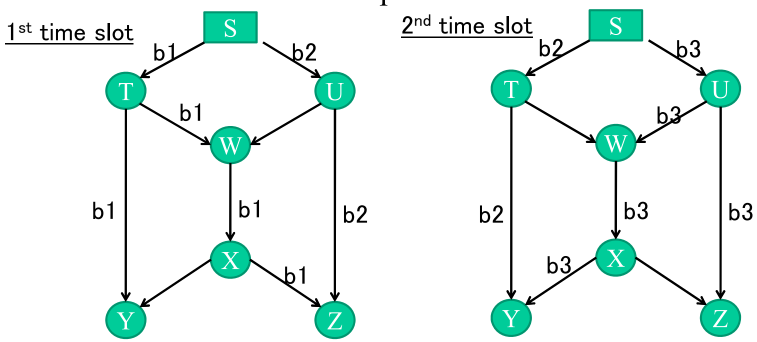
A famous example – butterfly network

- 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



A famous example – butterfly network without network coding

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

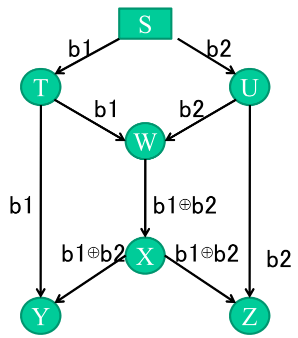


A famous example – butterfly network with network coding

- W receives b1 and b2, then performs exclusive OR (XOR) on received bits and forward to X
- Y receives b1 and b1⊕b2, then extracts b2 as

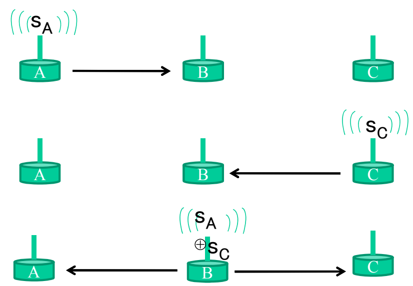
  $b2 = b1 \oplus (b1 \oplus b2)$
- Z receives b2 and b1⊕b2 then extracts b1 as

  $b1 = b2 \oplus (b1 \oplus b2)$
- Achieve multicast rate of 2 bits per time unit



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



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