Error Control Block Codes and Convolutional Codes

23 March 2004

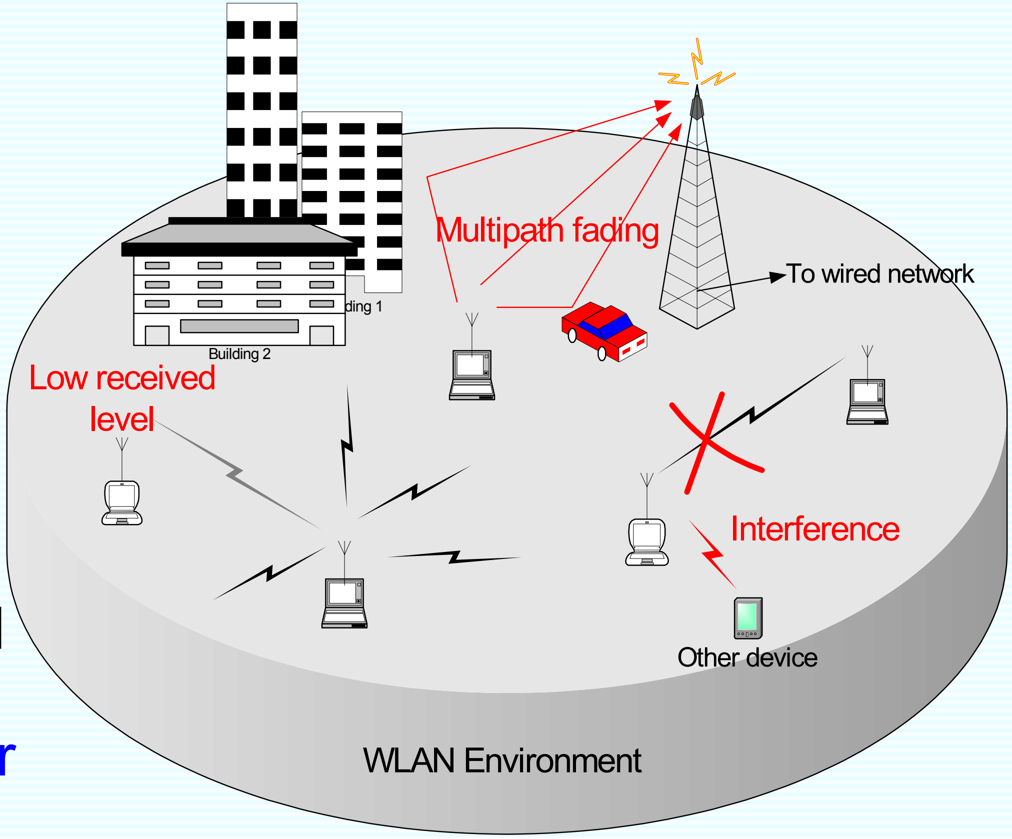
Mei Yen Cheong

mycheong@cc.hut.fi

Content

Introduction (1)

- Why error control?
  - Multipath fading
  - Interference (unlicensed spectrum)
  - Low received signal level (omnidirectional antenna)
- High bit error rate in received data.
  ➡ Error control important for WLAN.



Introduction (2)

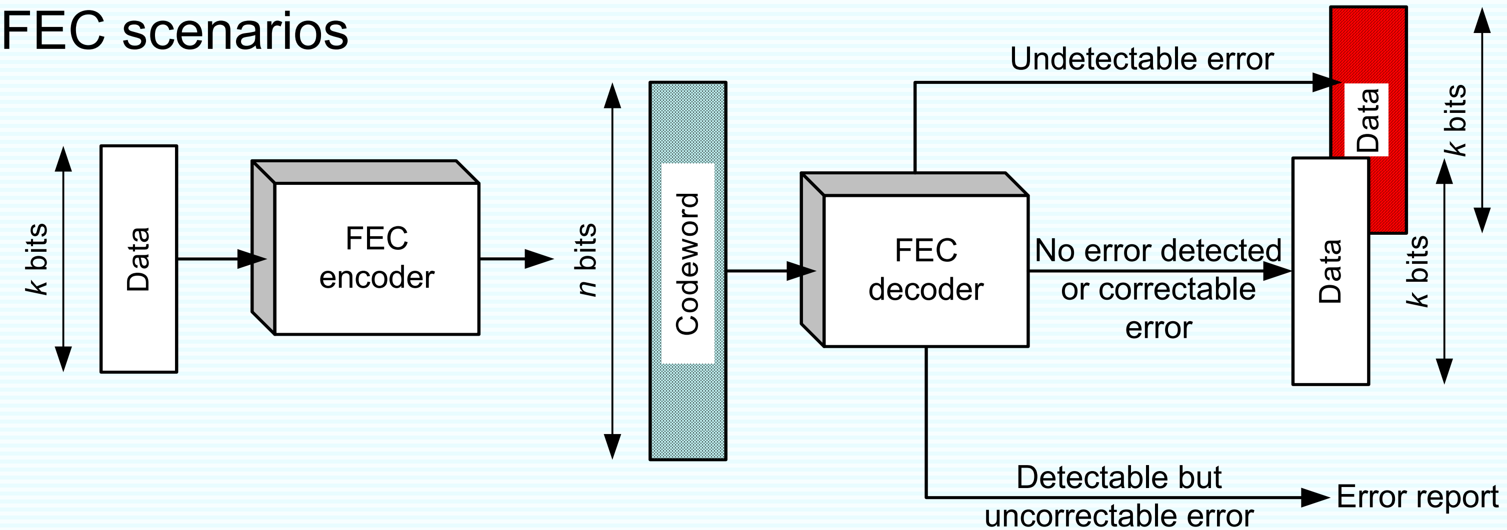
Objective: Error control to compensate transmission impairment in order to increase quality of transmission.

- Datalink layer and transport layer (TCP) protocols

- Approaches for error control
  - Error detection – CRC, parity check
  - Forward error correction (FEC) – channel coding
  - Automatic Repeat Request (ARQ) – Stop-and-wait, Go-back-N, etc..

Forward Error Control

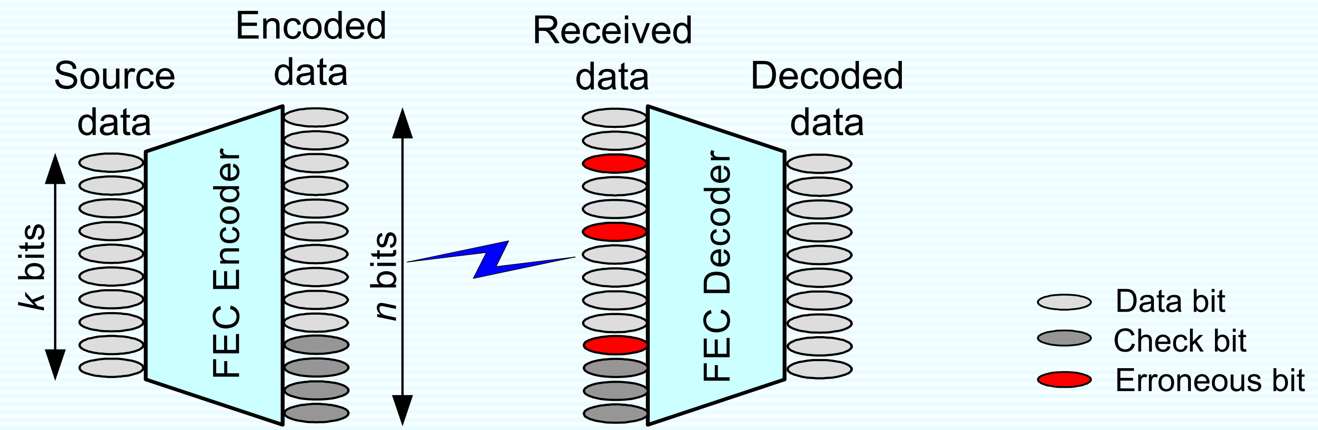
- FEC scheme adds redundant bits to transmitted data to form codeword known as error correcting codes.
- FEC scenarios



- Error correction code can be implemented with block codes or convolutional codes

Block Codes (1)

- Block error coding scheme divides the transmitted bit stream into nonoverlapping blocks of length *k.*
- Each *k*-bit block is map into an *n*-bit block called codeword.



Block Codes (2)

- The ratio *k*/*n* is called the code rate is a measure of how much excess bandwidth is required to transmit the data at the same data rate as without the code.

- The minimum distance $d_{\min}$ of a code is minimum Hamming distance between all vectors the code.

$$d_{\min} = \min_{i \neq j} \left[d\left(c_i, c_j\right) \right]$$

  - Tells the minimum error correcting capability of the code
  - Maximum number of guaranteed correctable errors/code word

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor, \text{ where } \lfloor x \rfloor \text{ is the largest integer } \leq x.$$

Generic Block Codes Encoder (1)

Encoding of an (n,k) block code

- Multiplying data block with the generator matrix $c = mG$.

$$\overbrace{\begin{bmatrix} c_1 & c_2 & \dots & c_n \end{bmatrix}}^{n} = \overbrace{\begin{bmatrix} m_1 & m_2 & \cdots & m_k \end{bmatrix}}^{k} \begin{array}{cc} \text{n columns} & \\ \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix} & \text{k rows} \end{array}$$

(n-k) check bits added

- The rows of **G** contains the basis of the (n,k) code.
- Only 2^k out of the 2^n codes generated are valid codes.

Generic Block Codes Encoder (2)

- Nonsystematic codes
  - *n-k* check bits in random positions

- Systematic codes
  - First k bits contain data
  - Last n-k bits contain the check bits
  - Easier decoding

$$\mathbf{G} = \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1n-k} \\ 0 & 1 & 0 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2n-k} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & p_{kn-k} \end{array}\right]$$

$$= \left[\mathbf{I}_k \,|\, \mathbf{P}\right].$$

Generic Block Codes Decoder (1)

- Decoding involves multiplying the *n*-bit received block with the parity check matrix **H**.
- Let the received block be

$$\mathbf{y} = \mathbf{c} + \mathbf{e}$$
$$= \mathbf{mG} + \mathbf{e}.$$

Then

$$\mathbf{yH}' = (\mathbf{mG} + \mathbf{e})\mathbf{H}'$$
$$= \mathbf{mGH}' + \mathbf{eH}'$$

If = 0,

$$\mathbf{S} = \mathbf{eH}'.$$

Syndrome of the error pattern

H (with dimension n-k) constitute the null space of the code

I.e. $\mathbf{GH}' = \mathbf{0}$.

Generic Block Codes Decoder (2)

- All-zero syndrome vector **S**=**0** indicates no bit error has occured $(\mathbf{e} = \mathbf{0})$.
- Nonzero syndrome vector indicates errors have occured
  - indicate the error positions if the number of errors in the block do not exceed *t*, error correction can be done
- **H** is the generator matrix of the dual code of **G.**
  - For systematic codes, **H** can be deduced from **G** as

$$\mathbf{H} = \left[-\mathbf{P}' \,|\, \mathbf{I}_{n-k} \right].$$

Some well-known block codes

- Hamming codes
- Golay codes
- Hamadard codes
- BCH codes
- Reed Solomon Codes

Cyclic codes

Cyclic codes (1)

- A block code is said to be cyclic if and only if the cyclic shift of a codeword is another codeword.

$$\mathbf{c}_1 = (c_1, c_2, \ldots, c_{n-1}, c_n) \in \mathrm{C}$$

$$\mathbf{c}_2 = (c_n, c_1, \ldots, c_{n-2}, c_{n-1}) \in \mathrm{C}$$

$$\vdots$$

- The cyclical structure of the codes allows us to associate a code with polynomials
  - Can be efficiently implemented using linear shift-register based codecs.

Cyclic Codes (2)

- The generator polynomial g(x) of an (n,k) cyclic codes is a polynomial of degree n-k that divides x^n+1.
- **G** can be obtained by arranging cyclically shifted version of g(x) into an $n \times k$ matrix as follow.

$$\mathbf{G} = \begin{bmatrix} g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots \\ \vdots & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & g_1 & g_2 & \cdots & g_{n-k} \end{bmatrix}$$

⇨ can be reduced by row operation to systematic form

Cyclic Codes (3)

Example 1:

- Find the generator matrix of a (7,4) cyclic code. Encode 1010.
  - Factorization: $x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$
  - g(x) is of degree $n-k=3$, choose $g(x)=\left(x^3+x+1\right)$ ➡ (1011)

$$\mathbf{G}=\begin{bmatrix}1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}\xrightarrow{\text{row operation}}\left[\begin{array}{cccc:ccc}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{array}\right]$$

  - Encode $\mathbf{m}=[1010]$ ➡ $c=\mathbf{mG}$

$c=1010\boxed{011}$ check bits

Cyclic Codes (4)

Example 2

- Find the parity check matrix **H** of the code. Find the syndrome and decode **y**=1011011.
  - **H** can be deduced from **G** $\mathbf{H} = \left[-\mathbf{P}' \,|\, \mathbf{I}_{n-k}\right].$

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \leftarrow \boxed{\begin{array}{l} d_{\min} = 3 \\ \Rightarrow t = 1 \end{array}} \left.\vphantom{\begin{array}{l} d_{\min} = 3 \\ \Rightarrow t = 1 \end{array}}\right\} \text{Number of linearly independent columns}$$

  - Syndrome: $\mathbf{S} = \mathbf{y}\mathbf{H}' = 011$ ⟵ Error pattern, $e = 0001000$
  - Decoded data: $\hat{\mathbf{m}} = y + e$

$$\hat{\mathbf{m}} = 1010011$$

BCH codes (1)

- BCH codes consist of cyclic codes which employ binary and nonbinary alphabets.
- BCH codes are 3-parameter codes expressed as (n,k,t) BCH code.
- For any positive integer $m \geq 3$; $(n \geq 7)$,

Block length:	$n = 2^m - 1$
Check bits:	$n - k \leq mt$
Minimum distance:	$d_{\min} = 2t + 1$

BCH Codes (2)

- The parameter set provide large selection of block lengths, code rates and error correcting capabilities.

- Nonbinary BCH takes *q*-ary symbols where *q* is any power of a prime number *p*; $\Rightarrow q = p^z$.

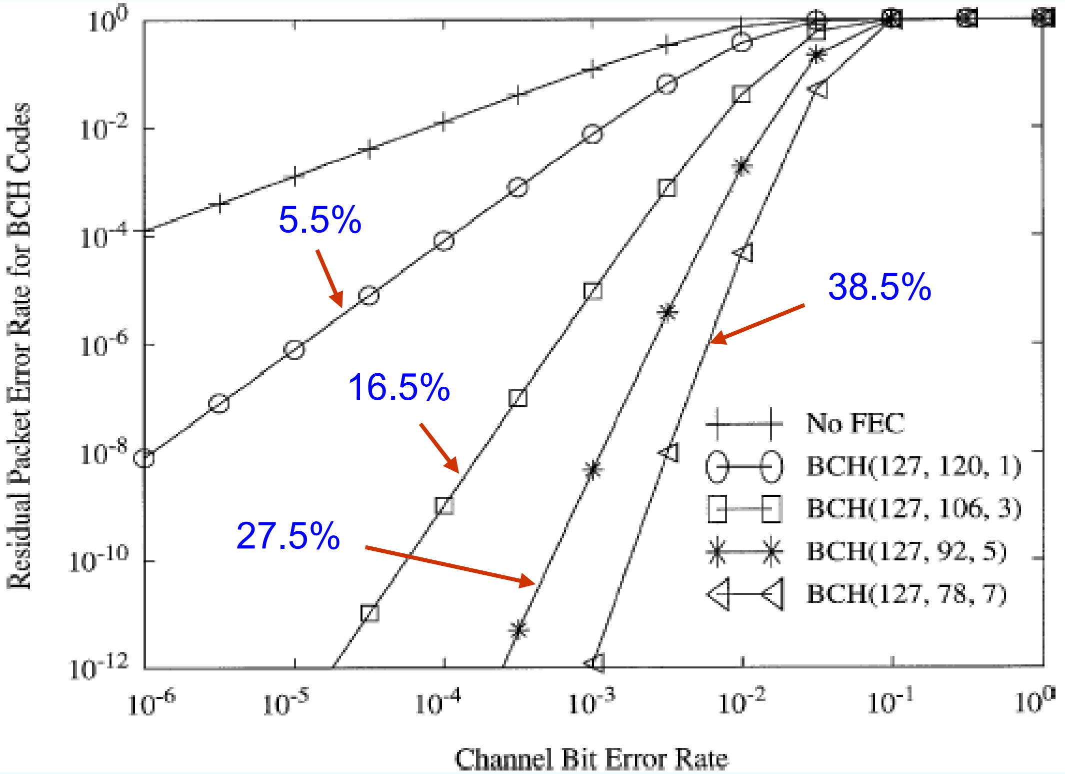
- For any positive integer *s*, *q*-ary BCH code is of length $n = q^s - 1$.

- To correct up to *t* errors, the number of parity check bits needed is $n - k \leq 2st$.

Note: Table of binary BCH codes parameters in Appendix

Performance of BCH codes

- BCH codes on channel with random errors [4]



- As expected, as the code overhead increases, the performance improves.

Reed-Solomon Codes (1)

- Reed-Solomon (RS) codes are a special subclass of nonbinary BCH codes with parameter s=1 $\Rightarrow n = q - 1$.

- The parameters of an (n,k,t) RS code are as follows.

Block length:	$n = q - 1$
Check bits:	$n - k \leq 2t$
Minimum distance:	$d_{\text{min}} = 2t + 1$

- RS codes have optimal distance properties
  - the extra reduncdancy provided by nonbinary alphabets.
  - For fixed number of check bits, RS codes provide optimal error correcting capability.

Reed-Solomon Codes (2)

- Practical RS codes take alphabets of $q = 2^m$.
- Special feature: Extended RS code with length n+2
  - 2 information symbols can be added to the length n RS code without reducing the minimum distance.
- Effective in burst-error correction.
- Efficient for channels where the set of input symbols is large.

Convolutional codes

- Convolutional codes are encoded with encoders with memory
  - Encoder outputs at an instant not only on the current inputs but also some past inputs
- An (n,k,m) convolutional code
  - generates n encoded bits for every k data bits
  - m is the memory of the the encoder
- Code rate is the ratio of number input bits to the corresponding number of output bits k / n.

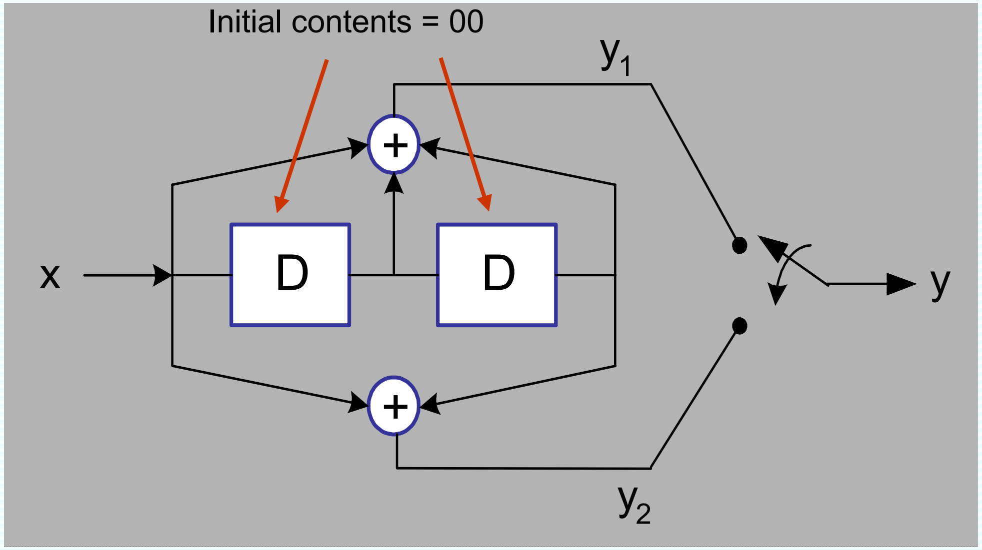
Convolutional Encoding

Example 3:

- A ½-rate (2,1,2) binary convolutional encoder. Encode x=101.
  - $G_1(D) = 1 + D + D^2$

    $G_2(D) = 1 + D^2$

Input	Register contents	y_1 y_2
1	00	11
0	10	10
1	01	00
0	10	10
0	01	11



$y = 11\ 10\ \ 00\ 10\ 11$

Convolutional Decoding (1)

- Convolutional decoding is based on Maximum Likelihood (ML) concept. It's an optimum decoder.

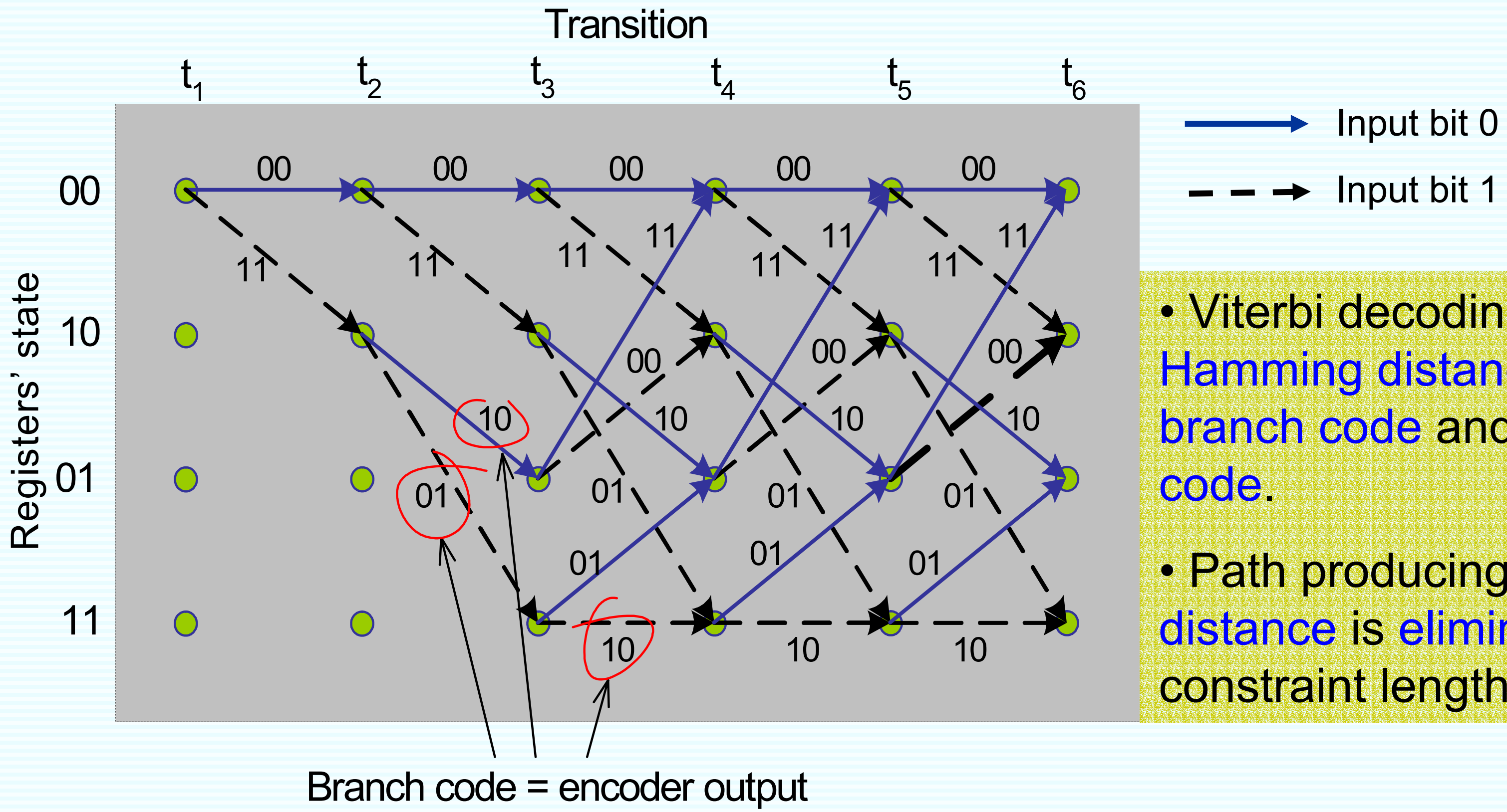
$$P\left(Z \mid X^{(m')}\right) = \max_{\text{all } X^{(m)}} \left\{P\left(Z \mid X^{(m)}\right)\right\}$$

- Viterbi algorithm performs reduced complexity ML decoding
  - Eliminate least likely trellis path at each transition stage
  - Reduced decoding complexity with early rejection if unlikely paths

- Code trellis structure is exploited in viterbi decoding.

Convolutional Decoding (2)

Trellis diagram of encoder in Example 3

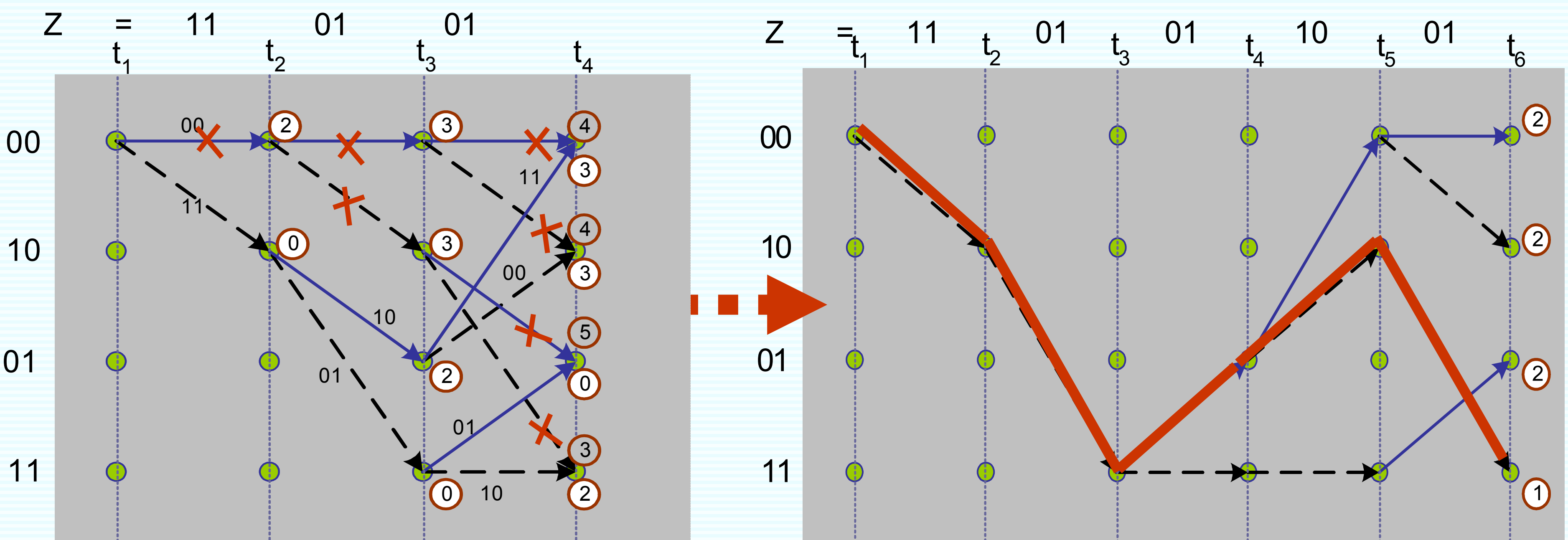


- Viterbi decoding compares the Hamming distance between the branch code and the received code.
- Path producing larger Hamming distance is eliminated (after constraint length).

Convolutional Decoding (3)

Example 4:

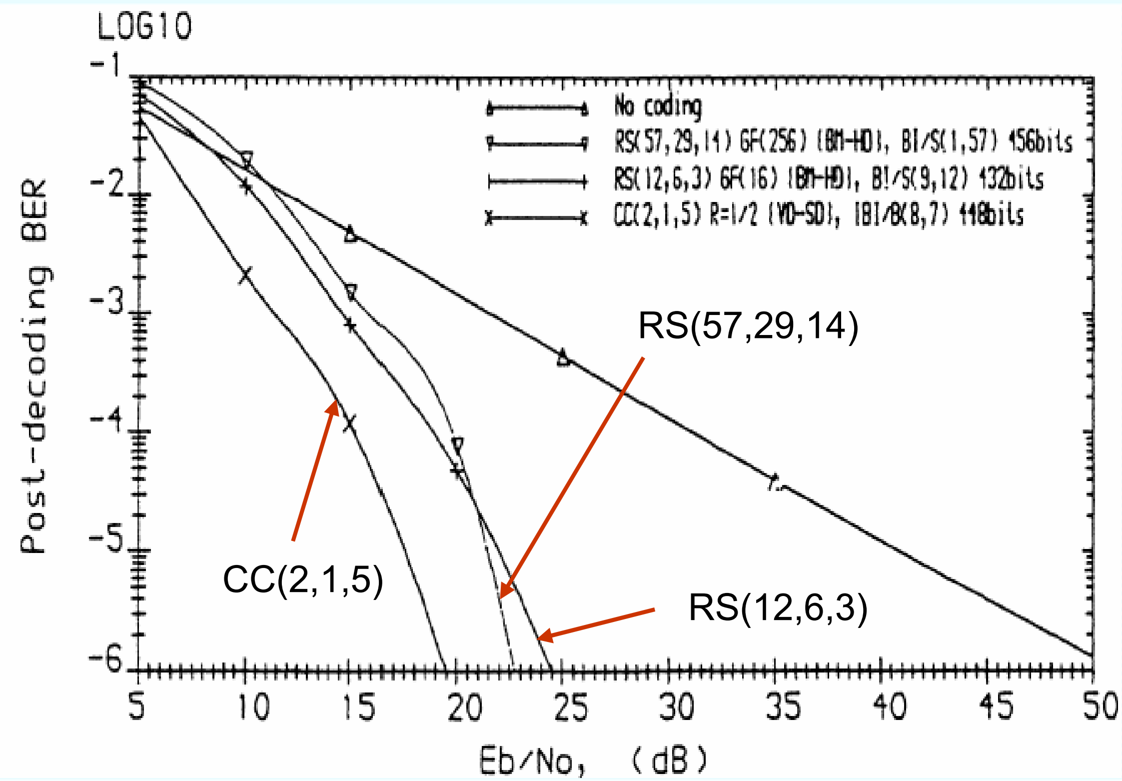
- Input data m = 1 1 0 1 1 and Tx codeword X = 11 01 01 00 01
- Received code Z = 11 01 01 10 01



Decoded bits: 1 1 ....

Performance comparison

- Comparison of diffrent coding schemes over Rayleigh fading channel with MSK modulation [4]



- All the codes have code rate ≈ ½.
- Convolutional code outperforms the RS codes due to soft-decision Viterbi decoding.

Discussion

- Selecting coding scheme for an application, tradeoffs on the following have to be considered
  - Performance – Probability of uncorrected errors, Coding gain
  - Overhead – Throughput, Code rate
  - Complexity – Processing delay, Computational power

- To overcome individual drawbacks of coding schemes the following can be considered
  - Concatenated codes – reduced length, high performance
  - Hybrid ARQ – Improve throughput
  - Interleaving – Alternative to long codes for burst errors
  - Adaptive coding scheme – maximize code rate in varying channel [5]

References

[1] Bernard Sklar, “Digital Communications, Fundamentals and Application,” Int’l ed., Prentice-Hall, 1998.

[2] J. G. Proakis, “Digital Communications,” 4th ed., McGraw-Hill, 2001.

[3] William Stallings, “Wireless Communications and Networks,” Upper Saddle River, New Jersey, Prentice-Hall, 2002.

[4] H. Liu et. al., “Error Control Schemes for Networks: An Overview,” Baltzer Science Publishers BV, 1997.

[5] Pjilip K. McKinley, “A Study of Adaptive Forward Error Correction for Wireless Collaborative Computing,” IEEE Trans. on Parallel & Distributed Systems, vol. 13 no. 9, Sept. 2002.

Homework

1. Block code
   - Given the generator polynomial of a (7,4) cyclic code $g(x) = x^3 + x^2 + 1$.
     - Find the parity check matrix
     - How many errors can this code detect and correct? How do you tell?
     - Decode **y**=1011011 (as in Example 2)

2. Convolutional code
   - What is the principle of convolutional decoding?
   - Based on the encoder in Example 3, decode the received sequence $Z = 11\ 10\ \ 10\ 10\ 01$ using Viterbi algorithm.