EE 5654 - Digital Communications Spring 2005

Instructor: R. Michael Buehrer

Lecture #20 - Block Codes: Performance and Applications

Symposium Schedule

Time	Group
8:10 – 8:30	**Volos**
8:30 – 8:50	**Phelps**
8:50 – 9:10	**Joshi, Torres**
9:10-9:30	**Phelps**
9:30 – 9:50	**Bouskour**
9:50 – 10:10	**Glien, Lockett, Junankar**
10:10-10:30	**Zhao**
10:30 – 10:50	**Gaeddart, Volos, Hugine, Ganesan**
10:50 – 11:10	**Kim**
11:10-11:30	**Junankar, Kapdi**
11:30 – 1:30	BREAK
1:30 – 1:50	**J.S. Lee**
1:50 – 2:10	**Meng**

Time	Group
2:10-2:30	**Zhou**
2:30 – 2:50	**Haddadin, Bouskour**
2:50 – 3:10	**Gonzalez**
3:10-3:30	**Akbar**
3:30 – 3:50	**B. Le**
3:50 – 4:10	**Moctezuma**
4:10 – 4:30	**Newcomb**
4:30 – 4:50	**Silvers**
4:50 – 5:10	**Waters**
5:10-5:30	**Utgikar**
5:30 – 5:50	**Chen**

Major Classes of Block Codes

- Repetition Codes
- Hamming Codes
- Golay Code
- BCH Codes
- Reed-Solomon Codes
- Walsh Codes
- Others
- BCH and RS codes are the most frequently used.

Classes of Linear Block Codes: (n,1) Repetition Codes

$$r = \frac{1}{n}, \qquad d_{H,\min} = n, \qquad t = \left\lfloor \frac{n-1}{2} \right\rfloor$$

$$0 \Rightarrow 0000000000000$$

$$1 \Rightarrow 1111111111111$$

- These codes are relatively simple, very wasteful of bandwidth, and are not widely used.
- Not particularly useful versus Gaussian noise, but useful (with interleaving) against jamming.
- Spread-Spectrum systems may be viewed as an application of a repetition code.

Classes of Linear Block Codes: Hamming Codes

$$n = 2^j - 1,$$

$$k = 2^j - 1 - j,$$

$$r = \frac{2^j - 1 - j}{2^j - 1},$$

$$d_{H,\min} = 3,$$

$$t = 1$$

$d_{H,min}$ stays the same with *n* but rate increases with *n* thus performance improves with *n*

- Example was presented in previous class.
- Not in widespread practical use.

Plot of BER vs. SNR for several Hamming codes

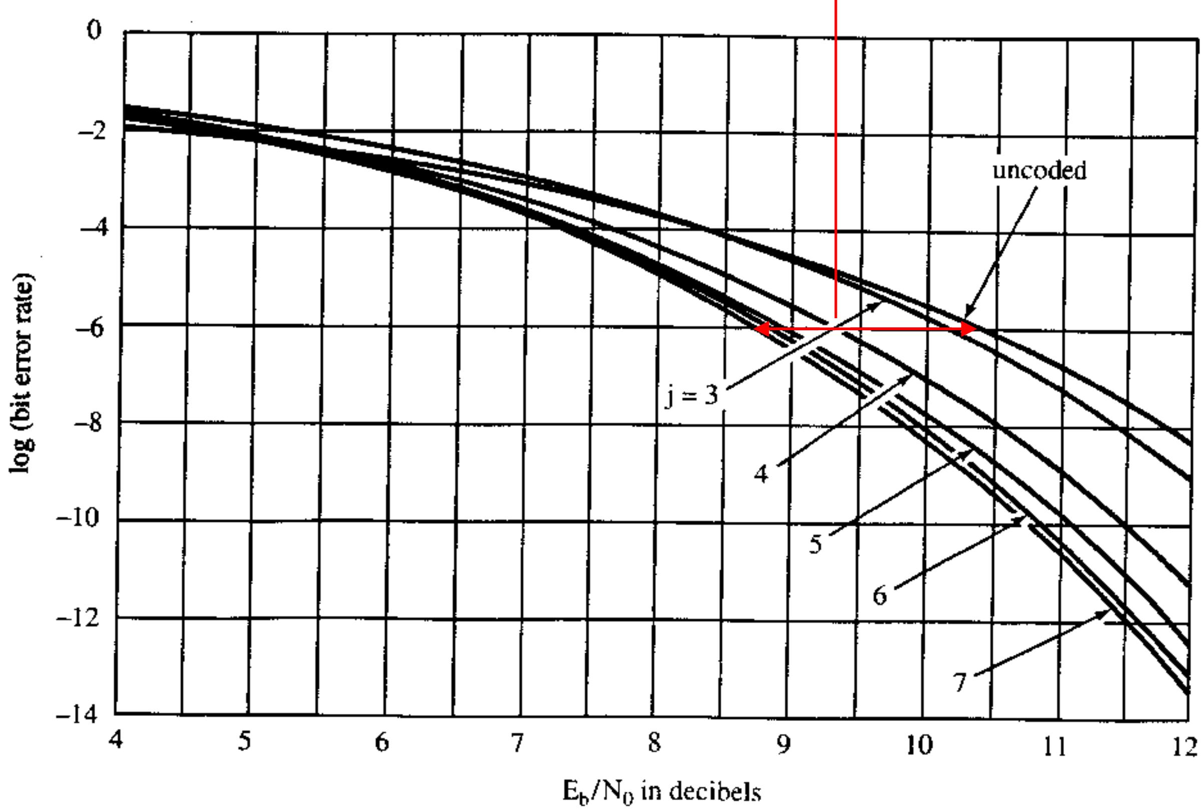


FIGURE 5-23. Bit error rate versus E_b/N_0 for Hamming codes with j = 3 through 7.

j	k	n	r	Gain (dB)
3	4	7	.57	0.2
4	11	15	.73	1.1
5	26	31	.84	1.4
6	57	63	.90	1.5
7	120	127	.94	1.6

***Source: Ziemer and Peters**

Notes on Hamming Code Performance

- Coding gain is achieved at high SNR
- BER is worse than uncoded system for low SNR
- Hamming code is not particularly powerful
  - single error correction only
- Longer Hamming codes provide better performance than short codes because as code length increases the minimum distance remains constant while rate increases.

Classes of Linear Block Codes: Golay Code

- This is a special one-of-a-kind code with many interesting properties. The Golay code is one of the few non-trivial "perfect codes": $n = 23, \quad k = 12, \quad r = \frac{12}{23}, \quad d_{H,\min} = 7, \quad t = 3$
  - $2^{12} =$ # of codewords
  - $2^{23} =$ # of possible binary vectors of length 23
  - Every possible received vector lies within distance 3 of exactly one codeword: $2^{12}\left[1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}\right]=2^{23}$
- *n*=23 is fairly short
  - this code is no longer used much in practice. One practical use: in Motorola pager system.

Plot of BER vs. SNR for Golay Code

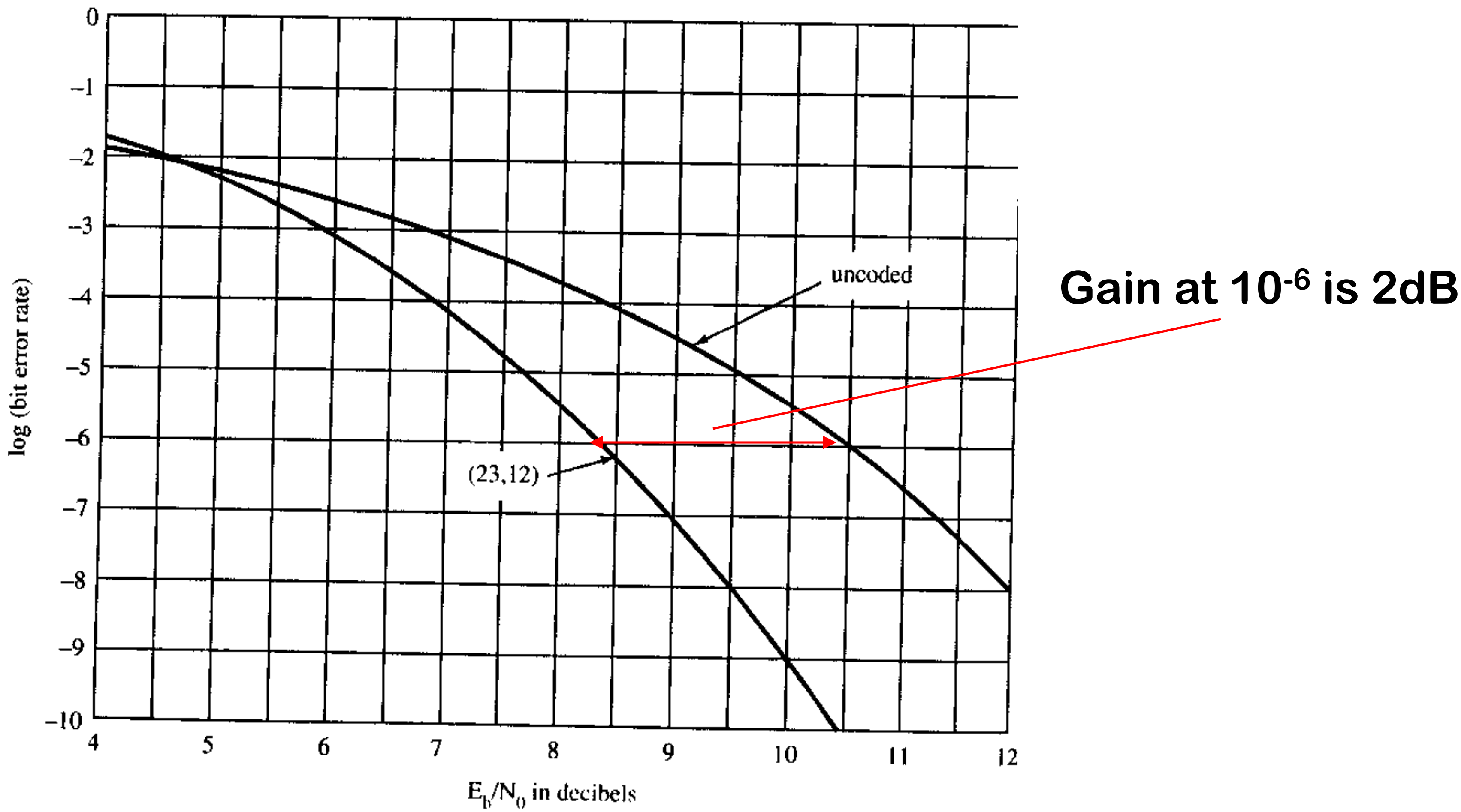


FIGURE 5-30. Bit error probability for Golay (23, 12) code.

*Source: Ziemer and Peters

Classes of Linear Block Codes: BCH Codes

- "Bose-Chaudhuri-Hocquenghem" - 1959
- Very important and useful class of codes.
- $n = 2^j - 1, \quad k = \text{any value}, \quad t \geq \frac{2^j - 1 - k}{j} \text{ (guaranteed)}$
- Widely used in satellite, wireless data links
- Decoded with the Berlekamp-Massey Algorithm
- cyclic codes
- Very useful since they achieve significant coding gain and exist for a wide variety of rates

BER vs. SNR for r=3/4 BCH Codes (BPSK modulation)

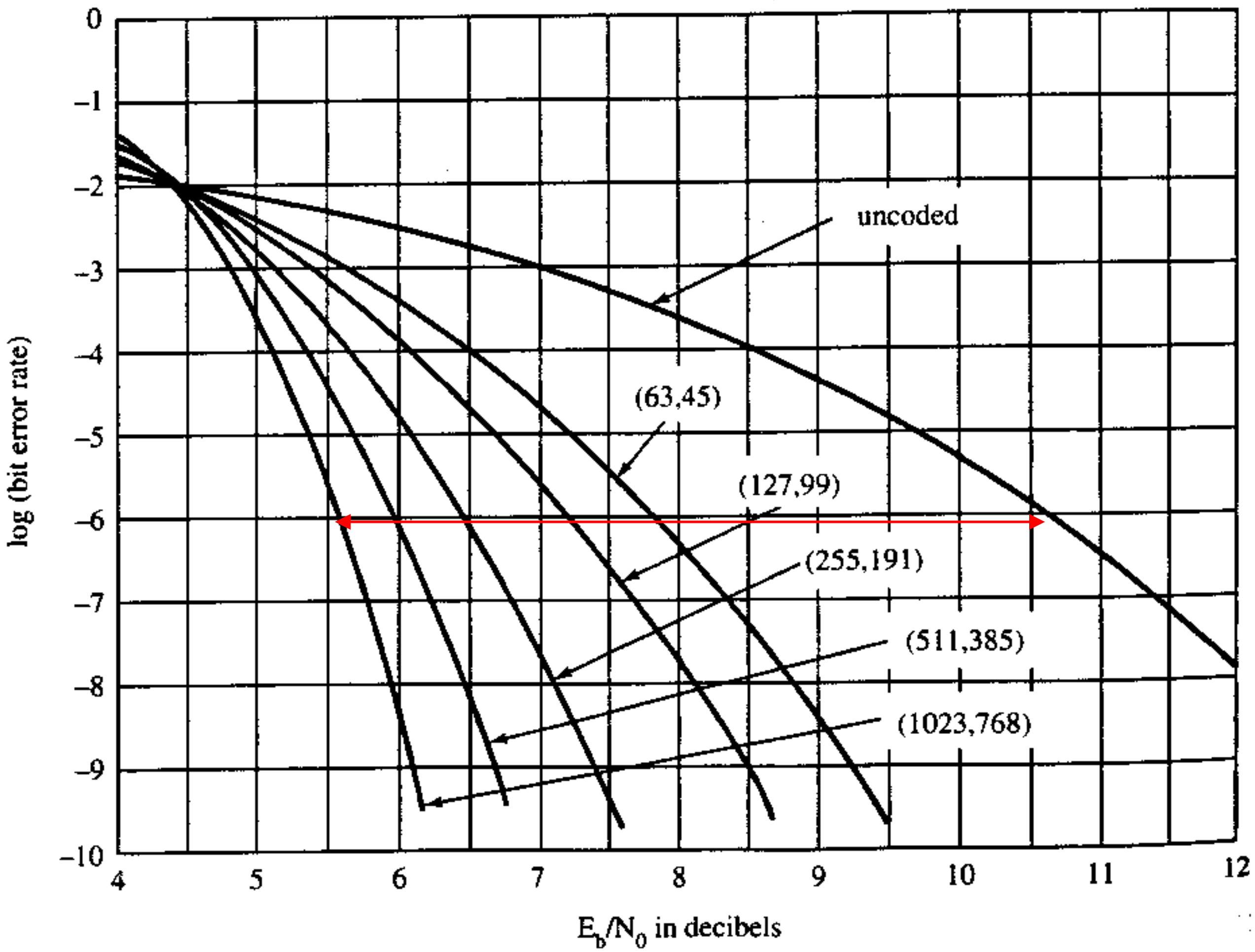


FIGURE 5-28. Bit error probability for BCH codes with $R \cong 3/4$.

k	n	r	Gain (dB)
45	63	.71	2.7
99	127	.78	3.2
191	255	.75	4.0
385	511	.75	4.4
768	1023	.75	4.8

***Source: Ziemer and Peters**

BER vs. SNR for r=1/2 BCH Codes (BPSK modulation)

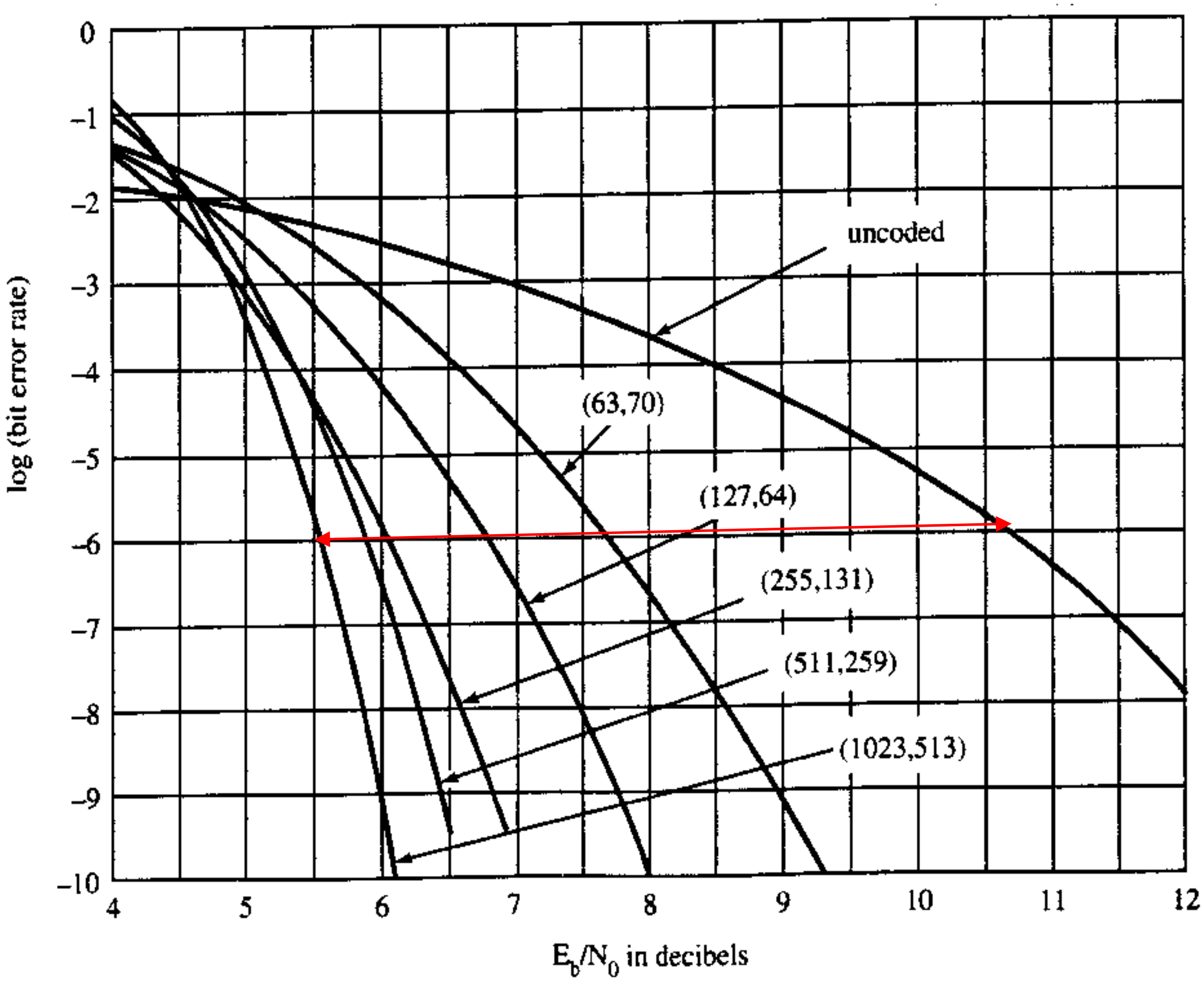


FIGURE 5-27. Bit error probability for BCH codes with $R \cong 1/2$.

k	n	r	Gain (dB)
36	63	.57	2.9
64	127	.50	3.6
131	255	.51	4.3
259	511	.51	4.6
513	1023	.5	5.0

***Source: Ziemer and Peters**

BER vs. SNR for r=1/4 BCH Codes (BPSK modulation)

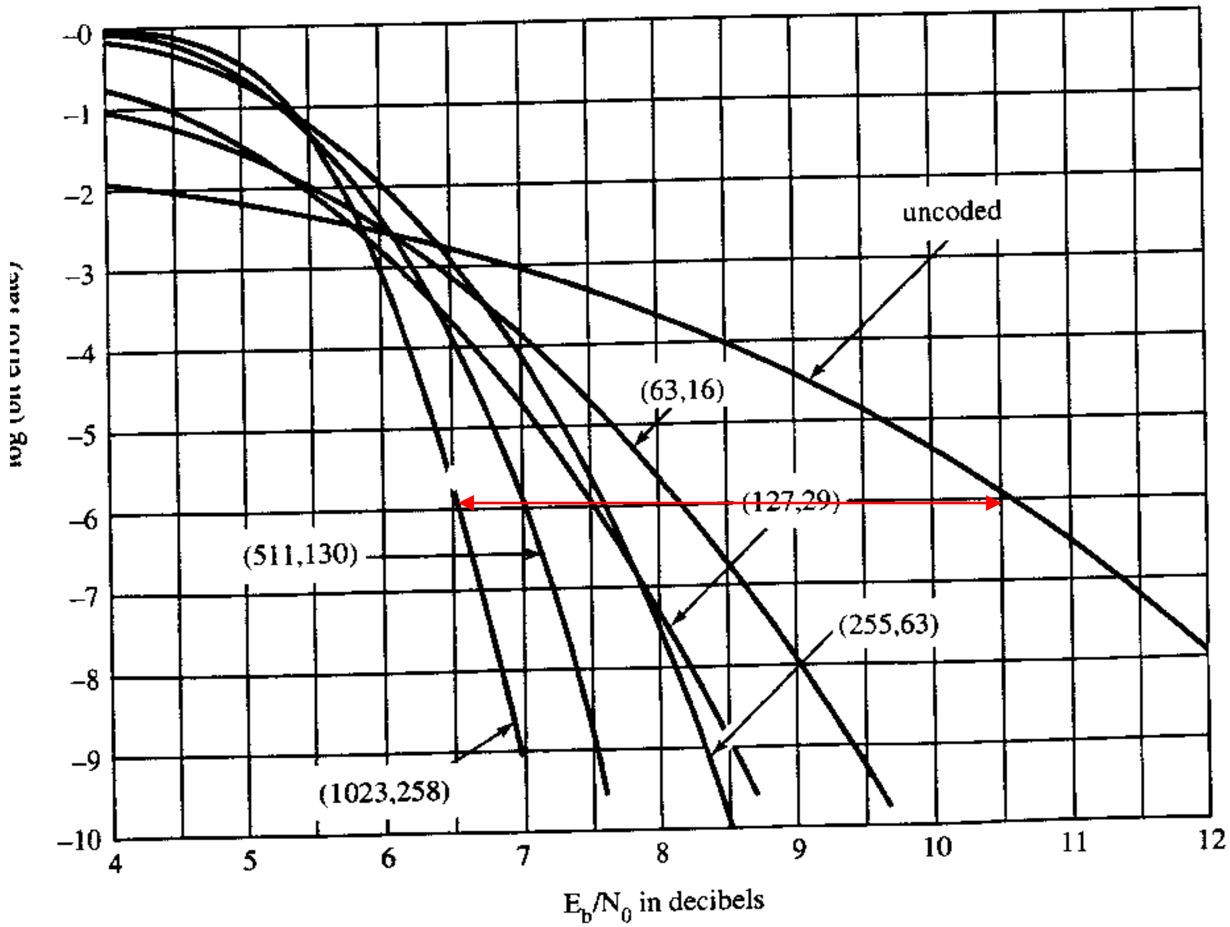


FIGURE 5-26. Bit error probability for BCH codes with $R \cong 1/4$.

k	n	r	Gain (dB)
16	63	.25	2.3
29	127	.23	3.0
63	255	.25	2.9
130	511	.25	3.5
258	1023	.25	4.0

***Source: Ziemer and Peters**

Notes on BCH Code Performance

- BCH Codes Exist for many values of *n,k*
- Large coding gains are possible for high SNR
- Coding gain increases with *n*
  - At low values of E_b/N_o this may not be necessarily true
- Coding gain increases as rate *r* decreases (up to a point)
  - code performance degrades quickly below rate 1/3.
  - At lower rates we must achieve higher values of E_b/N_o to obtain coding gain. However, once we achieve the gain it will likely be larger.

Classes of Linear Block Codes: Reed-Solomon (RS) Code

- 1962 - A generalization of BCH codes
- $n = 2^j - 1, \;\; k = \text{any value}, \;\; d_{H,\min} = n - k + 1, \;\; t = \left\lfloor \frac{n-k}{2} \right\rfloor$
- RS codes are Maximum Distance Separable - have the largest possible distance for any code with the same value of *n* & *k*
- RS codes are constructed for nonbinary (*M*-ary) symbol sets - frequently used with *M*-ary FSK.

Applications of Reed-Solomon Codes

- RS codes are used for data communications in severely power-limited environments:
  - deep-space communications
  - military communications systems in conjunction with spread-spectrum
  - Compact Disks
  - Cellular Digital Packet Data Standard.

BER vs. SNR for RS Codes

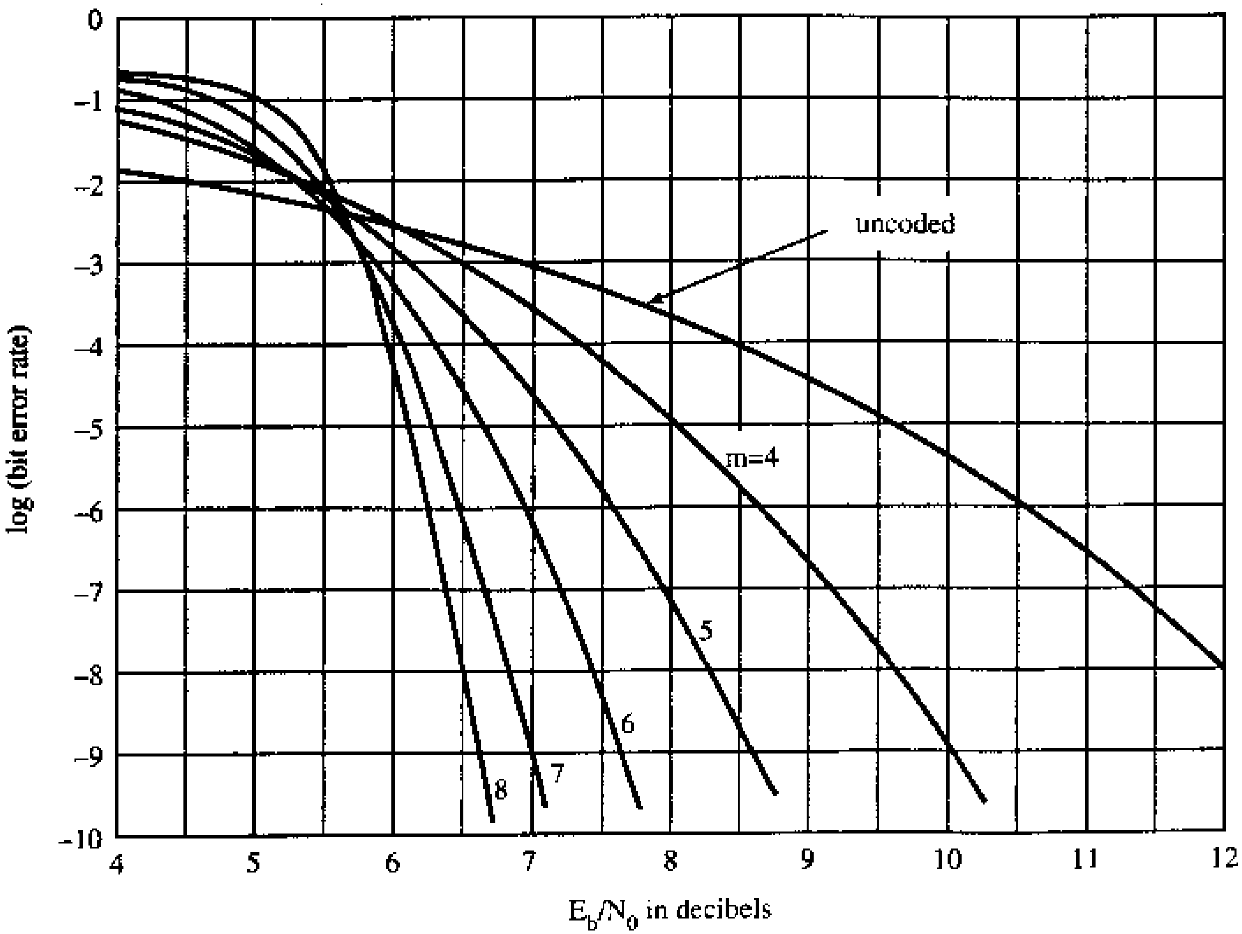


FIGURE 5-29. Bit error probability for Reed–Solomon codes with $R \cong 1/2$.

Symbols are *M-ary where* $M=2^m$

$n=2^m-1$

$k = (2^m-1)/2$

***Source: Ziemer and Peters**

Orthogonal (Walsh) Codes

- Hadamard Matrices: $\mathbf{H}_1 = [1], \mathbf{H}_{2^{i+1}} = \begin{bmatrix} \mathbf{H}_{2^i} & \mathbf{H}_{2^i} \\ \mathbf{H}_{2^i} & \overline{\mathbf{H}}_{2^i} \end{bmatrix}$
- Examples: $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$
- The code parameters in general will be $(k, 2^k)$
- The minimum distance is given by $d_{\min} = n/2 = 2^{k-1}$
- Spectral efficiency becomes very poor but energy efficiency becomes good for large *k*

Other Well-Known Classes of Block Codes

- Reed-Muller Codes
  - discovered in mid-1950s
  - first large class of codes to correct more than a single error
  - used in *Mariner* deep space probes from 1969-1976
  - no longer attractive when compared to BCH and RS codes
- Fire Codes
  - useful in correcting long bursts of errors
  - sometimes used in magnetic data storage systems
  - largely replaced by RS codes in recent applications

Modifications to Known Codes

- Many known codes can be modified by an extra code symbol or deleting a symbol
  - can create codes that approximate almost any desired rate
  - can sometimes create codes with slightly improved performance
- The resulting code can usually be decoded with only slight modification to the decoding algorithm
- Sometimes modification process can be applied multiple times in succession

Modifications to Known Codes

- Puncturing: delete a parity symbol
  - (n,k) code -> (n-1,k) code
  - Code is weakened to some degree
  - Useful for adaptive coding scenarios or anywhere that multiple code rates are needed since it allows for a single encoder/decoder to handle multiple rates
- Shortening: delete a message symbol
  - (n,k) code -> (n-1,k-1) code
- Expurgating: deleting some subset of codewords
  - (n,k) code -> (n,k-1) code

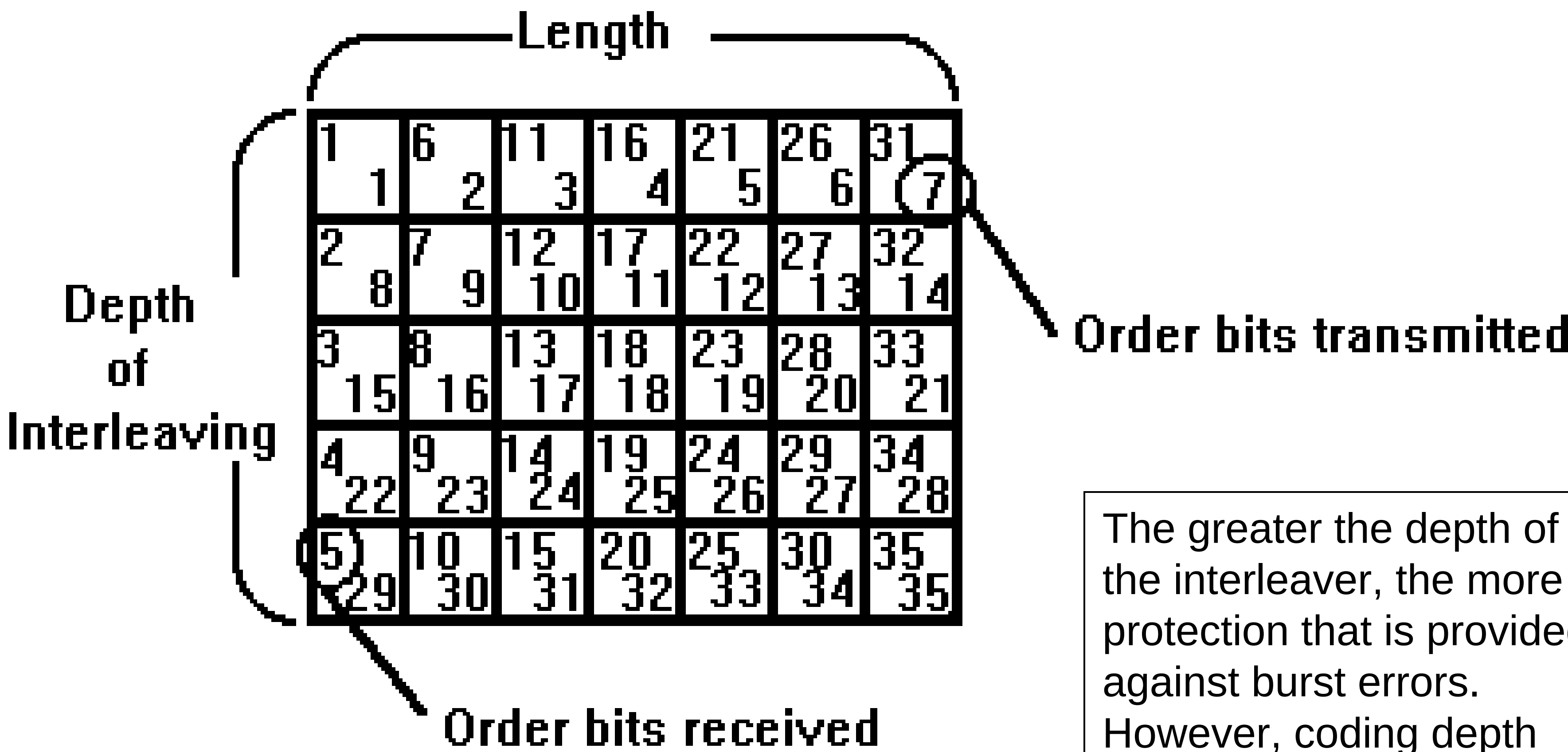
Modifications to Known Codes

- Extending: add an additional parity symbol
  - (n,k) code -> (n+1,k) code
- Lengthening: add an additional message symbol
  - (n,k) code -> (n+1,k+1) code
- Augmenting: add a subset of additional code words
  - (n,k) code -> (n,k+1) code

Interleaving

- The vast majority of Forward Error Correction (FEC) codes are designed for an AWGN channel which exhibits no memory.
- Thus, they do not handle bursts of errors well.
- Burst errors are common in jamming scenarios (esp. pulse jammers) as well as in time-varying (i.e., fading) channels
- Interleavers randomize the order of bits going into the channel. Bursts of errors are then spread out after deinterleaving.
- Ideally, this provides the decoder with random, independent errors.

Block Interleaver



The greater the depth of the interleaver, the more protection that is provided against burst errors. However, coding depth also introduces delay.

Interleaver - Example

- Bits going into the interleaver

b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}

- Coming out of the interleaver

b_1	b_6	b_{11}	b_{16}	b_{21}	b_{31}	b_2	b_7	b_{12}	b_{17}	b_{22}	b_{27}	b_{32}

- After demodulator (errors due to pulse interference)

b_1	b_6	b_{11}	b_{16}	**b_{21}**	**b_{31}**	**b_2**	**b_7**	b_{12}	b_{17}	b_{22}	b_{27}	b_{32}

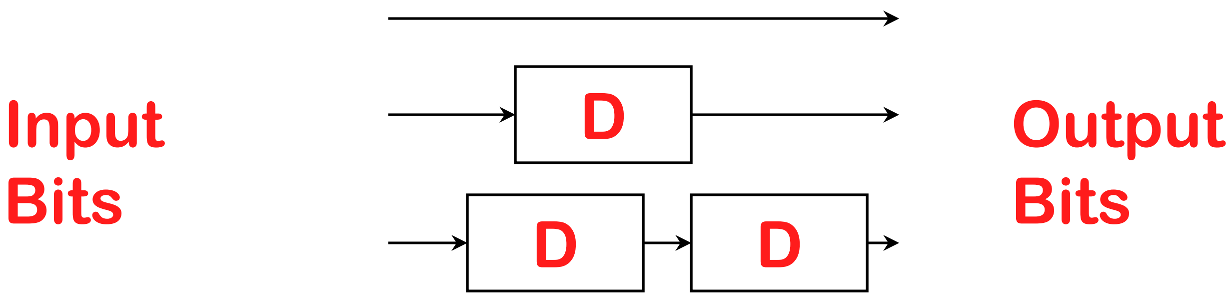
Error Burst

- After de-interleaving – errors dispersed

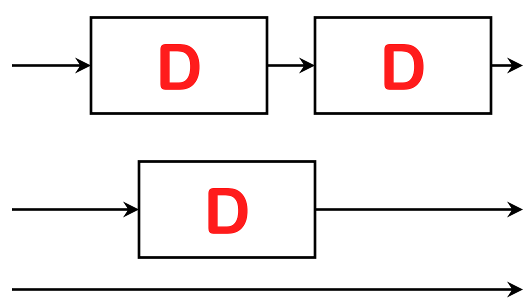
b_1	**b_2**	b_3	b_4	b_5	b_6	**b_7**	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}

Convolutional Interleavers

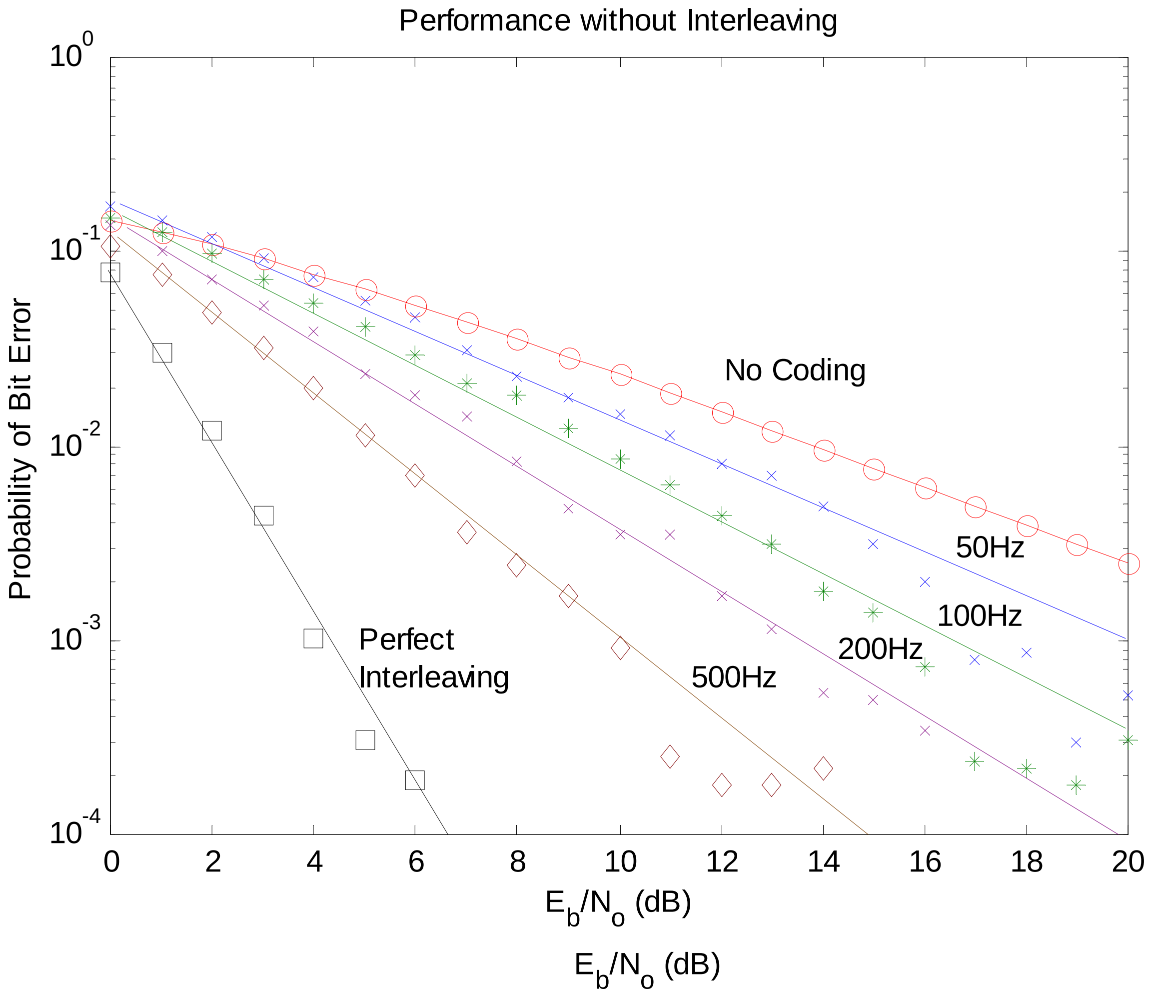
- Also called Cross-Interleaver



- Corresponding Deinterleaver

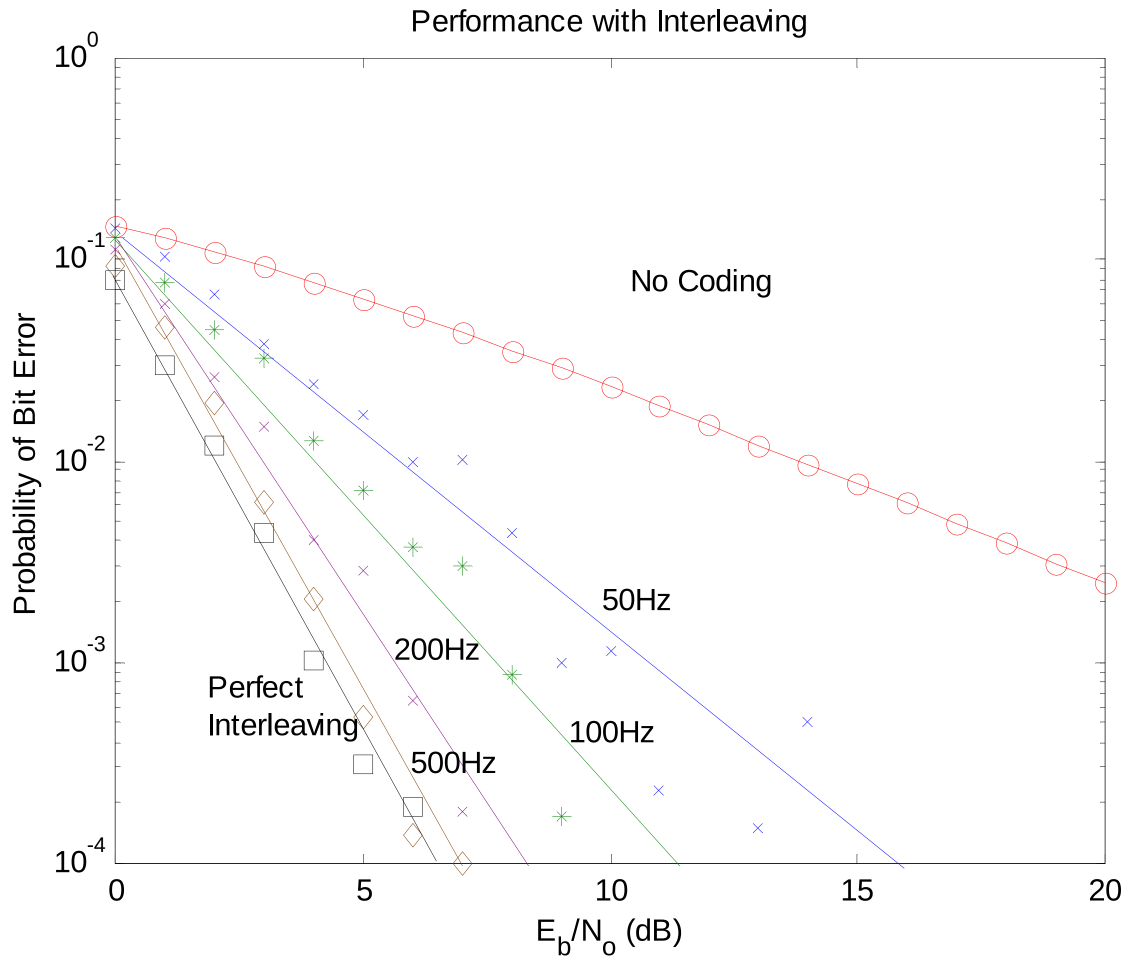


Performance with Interleaving



- Simulated Performance
- Rayleigh Fading
- R = ½ constraint length 7 convolutional code
- 20ms frames
- No interleaving
- 50Hz, 100Hz, 200Hz, 500Hz Maximum Doppler Spreads

Performance with Interleaving

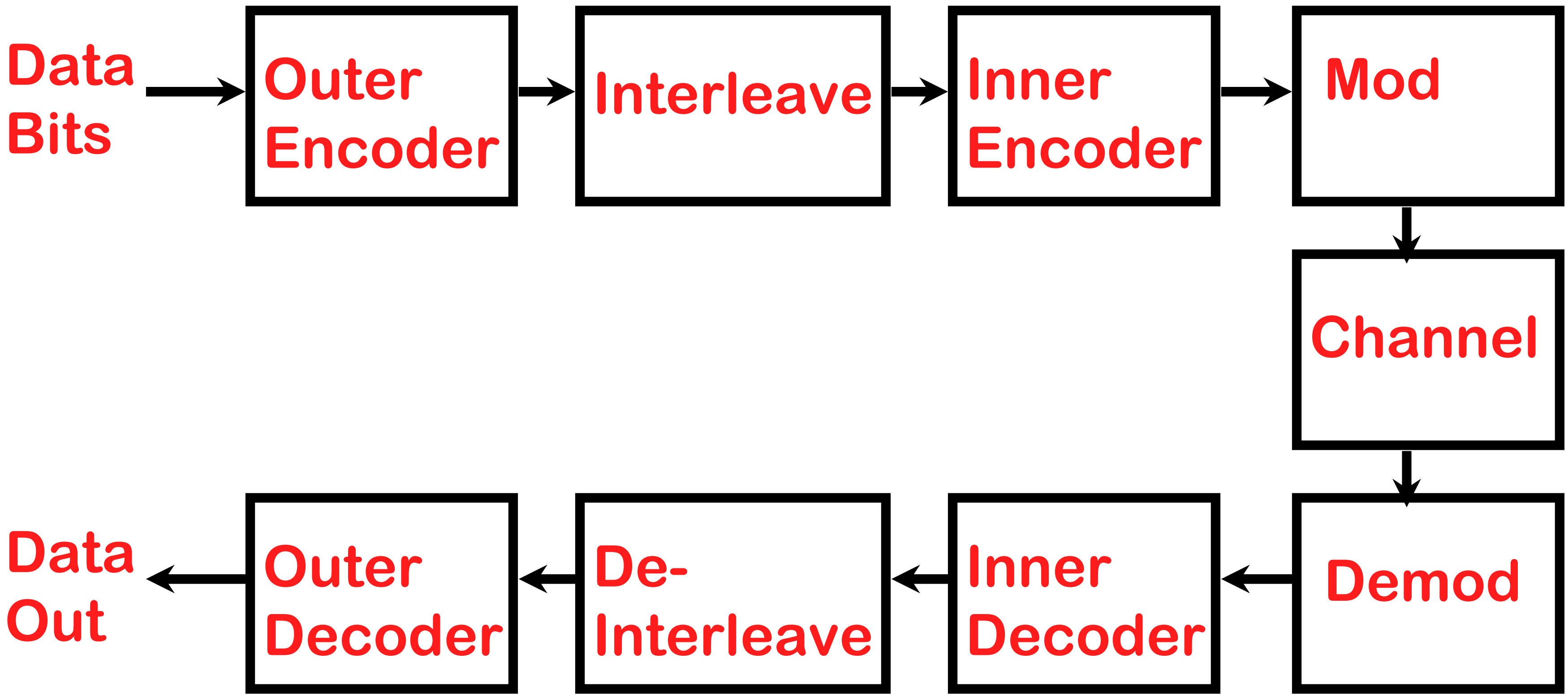


- Simulated Performance
- 1 Path
- R = ½ constraint length 7 convolutional code
- 20ms frames
- Block interleaving
- 50Hz, 100Hz, 200Hz, 500Hz Maximum Doppler Spreads

Concatenated Codes

- Two levels of coding. Achieves performance of very long codes while maintaining shorter decoding complexity.
- Overall rate is product of individual code rates
- Codeword error occurs only if both codes fail.
- Error Probability is found by first evaluating the error probability of "inner" decoder, then evaluating the error probability of "outer" decoder.
- Interleaving is always used with concatenated coding.

Block Diagram of Concatenated Coding System



Practical Application: Coding for CD

- Each channel is sampled at 44,000 samples/second
- Each sample is quantized with 16 bits
- Uses a concatenated RS code
  - Both codes constructed over GF(256) (8 bits/symbol)
  - Outer code is a (28,24) shortened RS code
  - Inner code is a (32,28) extended RS code
  - In between coders is a (28,4) cross-interleaver
  - Overall code rate is $r = 0.75$
- Most commercial CD players don't exploit full power of the error correction coder

Practical Application: Galileo Deep Space Probe

- Used concatenated coding
  - Inner Code was rate 1/2, constraint length 7 convolutional encoder - good for making soft decisions on channel
  - Outer Code was (255,223) RS Code over GF(256) - corrects any bursty errors from convolutional code
  - Overall code rate was r=0.437
  - A block interleaver held 2 RS Code words
  - Deep space channel is severely energy limited but not bandwidth limited

Practical Application: IS-95 CDMA

- The IS-95 standard employs a rate (64,6) orthogonal (Walsh) code on the reverse link
- The inner Walsh Code is concatenated with a rate 1/3, constraint length 9 convolutional code
  - The standard terms this code as ‘orthogonal modulation’, but it is really an error correction code (note the similarity between modulation and error correction)
  - The Walsh Codes on the forward link are used for channelization, not error correction

Practical Application: Data Transmission in 3rd Generation PCS

- Proposed ETSI standard employs RS Codes concatenated with convolutional codes for data communications
- Requirements
  - BER on the order of 10^{-6}
  - Moderate Latency is acceptable
- *cdma2000* uses turbo codes for data transmission
  - ETSI has optional provisions for Turbo Coding

Data Transmission in 3rd Generation PCS Systems (continued)

- RS-coding is of approximate rate 4/5 on GF(256).
- Different rate for different services:
  - 180/225 for 144 and 512 kbps data service.
  - 200/245 for 384 kbps data service.
  - 200/210 for 2048 kbps data service.
- Two levels of Interleaving
  - Outer interleaving is symbol-based block interleaver with interleaver width equal to the block length of the RS code.
  - Inner (channel) interleaver breaks the error bursts due to fading before Viterbi decoder