ELEC 405
Error Control Coding and Sequences
Introduction

Aaron Gulliver
Dept. of Electrical and Computer Engineering

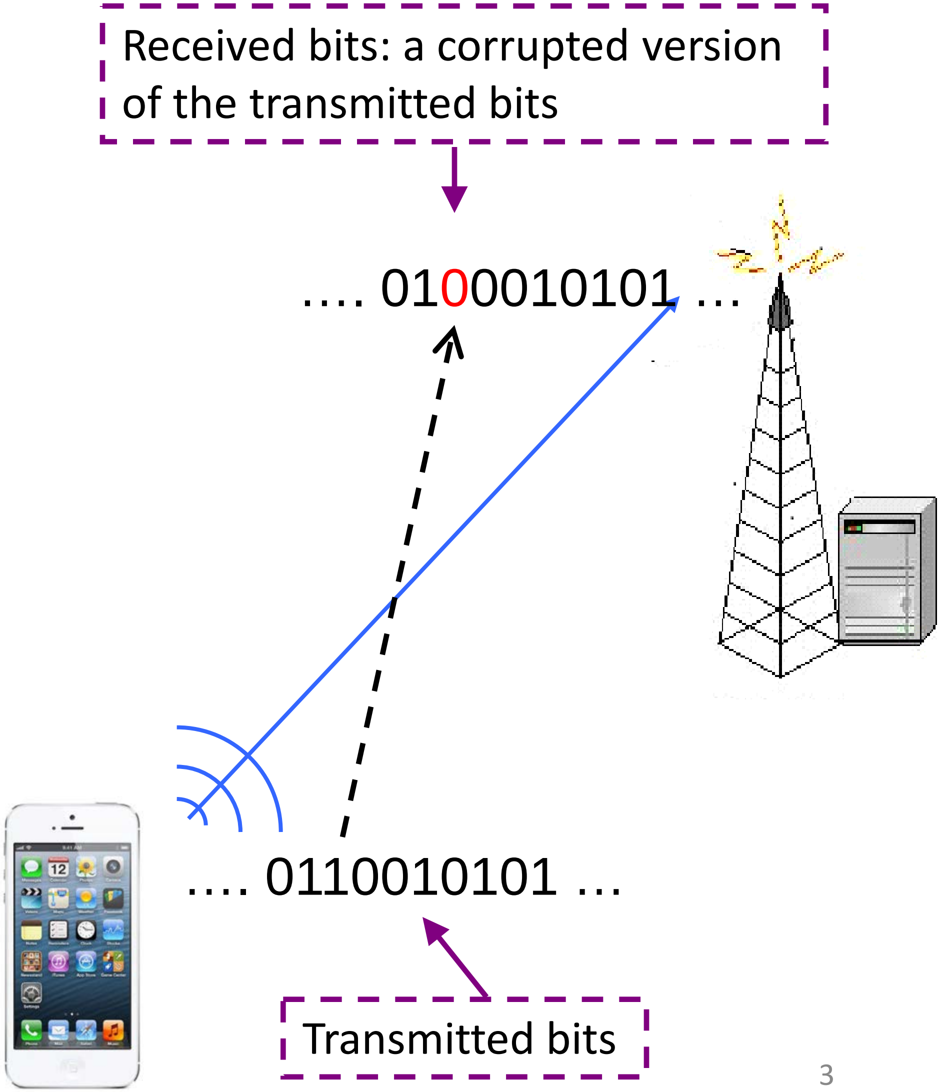
Topics

- Introduction
  - The Channel Coding Problem
- Linear Block Codes
- Cyclic Codes
- BCH and Reed-Solomon Codes
- Convolutional Codes
- Sequence Design

Errors in Information Transmission

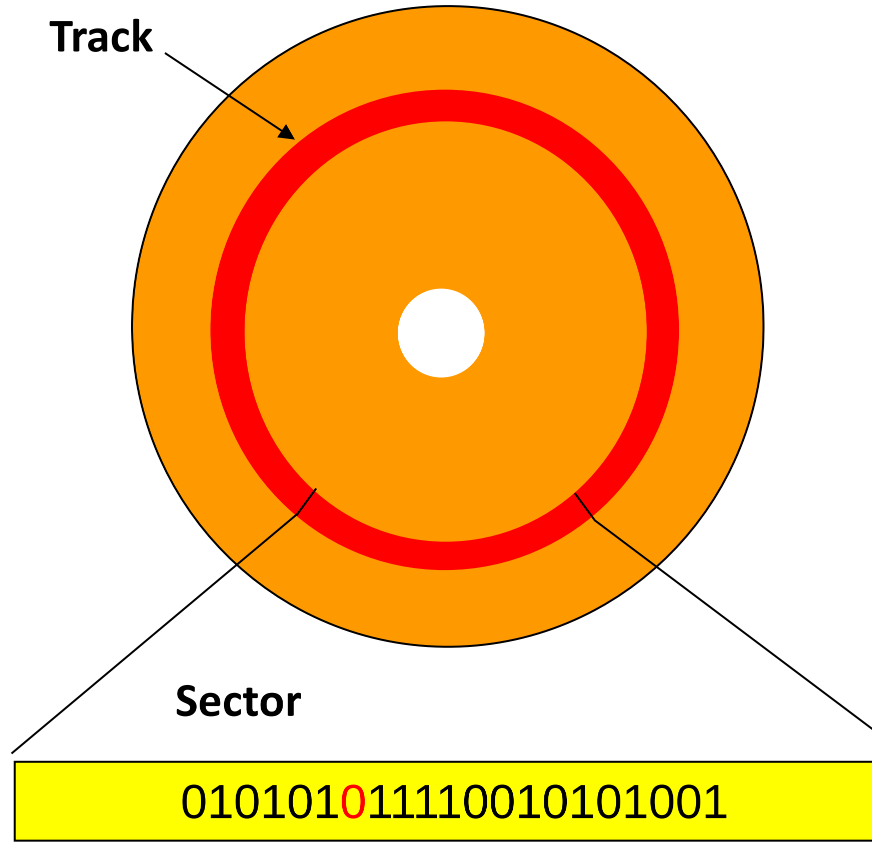
Digital Communications:
Transporting information from one place to another using a sequence of symbols, e.g. bits.

Noise and interference:
The received sequence may differ from the transmitted one.



Errors in Information Storage

Magnetic recording

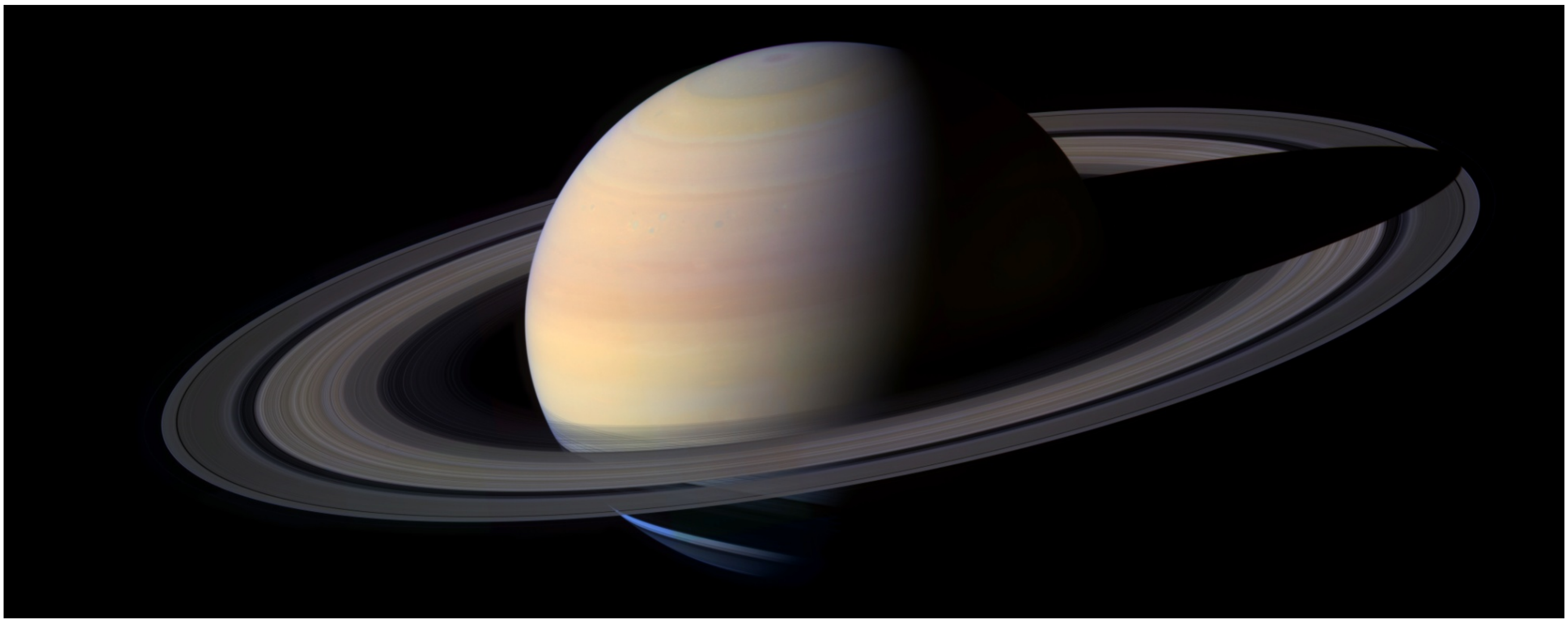


Bits can change during storage or reading from the disk

ECC Memory

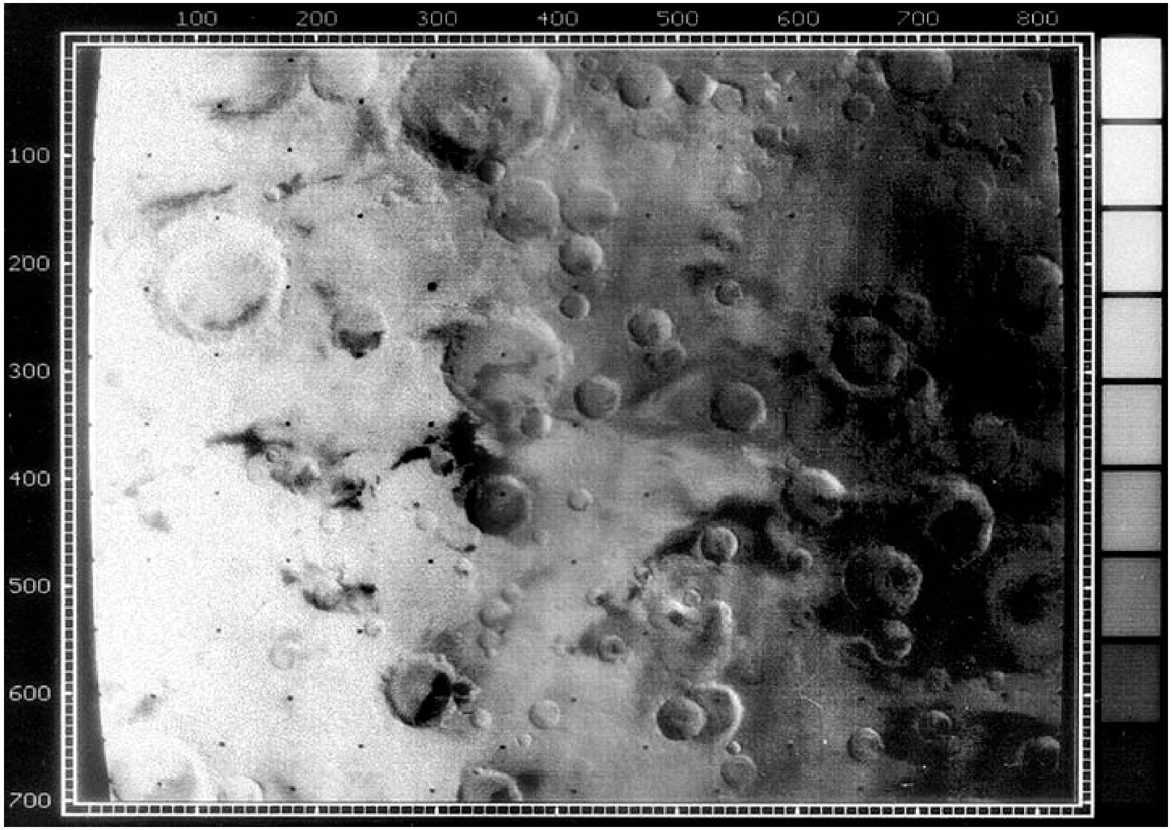
UPGRADE LIKE A PRO
WWW.MEMORYUPGRADE.PRO
PRO
MEMORYUPGRADE
1GB
184-PIN
Registered
4GB DDR 184-PIN ECC Registered 4x1GB Kit

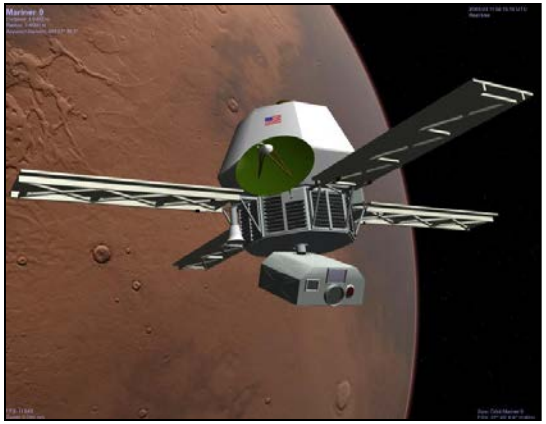
Deep Space Communications



1971: Mariner 9

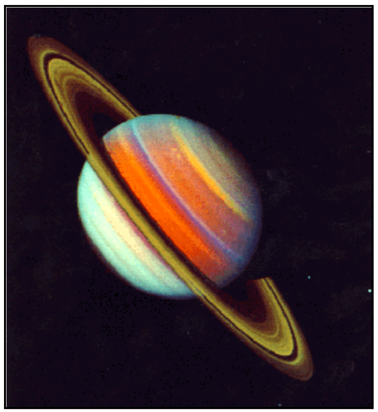
Mariner 9 used a (32,6,16) *Reed-Muller* code to transmit its grey images of Mars.

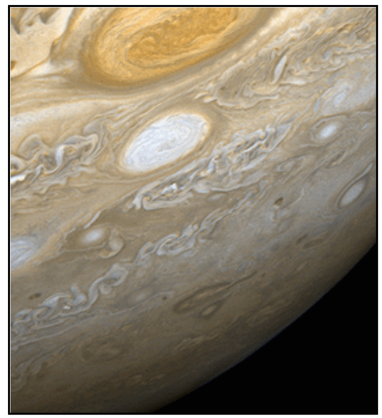




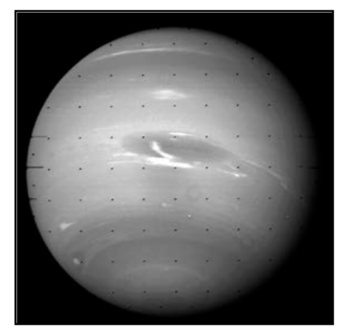
1979+: Voyager I and II

Voyager I and II used a (24,12,8) extended *Golay* code to send its color images of Jupiter and Saturn.





Voyager 2 traveled further to Uranus and Neptune. Because of the higher error rate it switched to a more robust *Reed-Solomon* code.

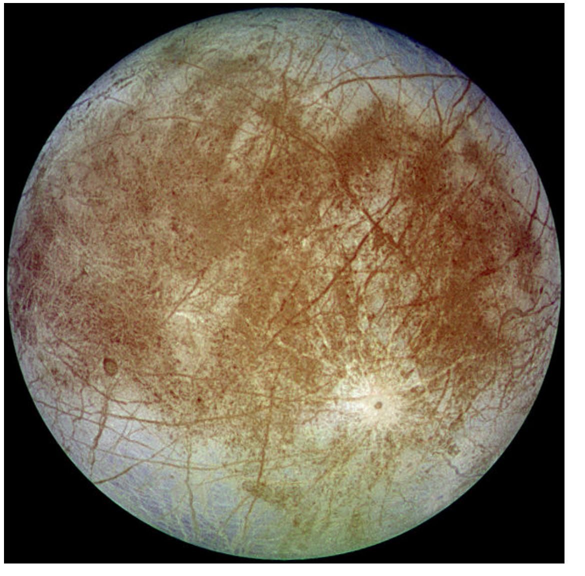


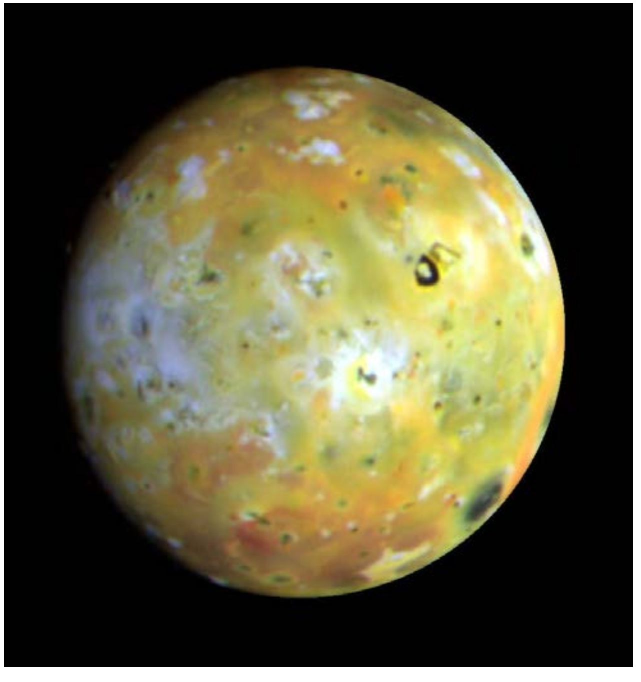
1989: Galileo

Concatenated *Convolutional* and *Reed-Solomon* codes were used to transmit images of Jupiter and its moons.

Io, Jupiter, Ida

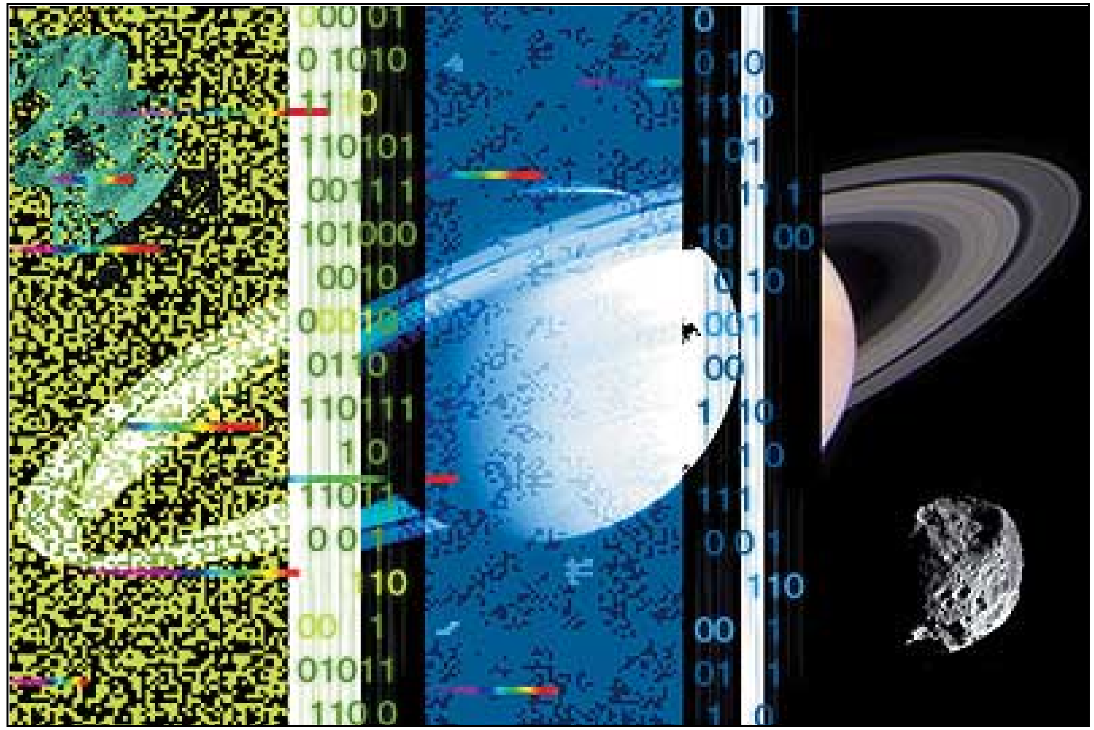
and Europa





Modern Codes

In 1993, *Turbo codes* were discovered. They are used in 3G and later cell phones and in the Cassini-Huygens space probe (1997).

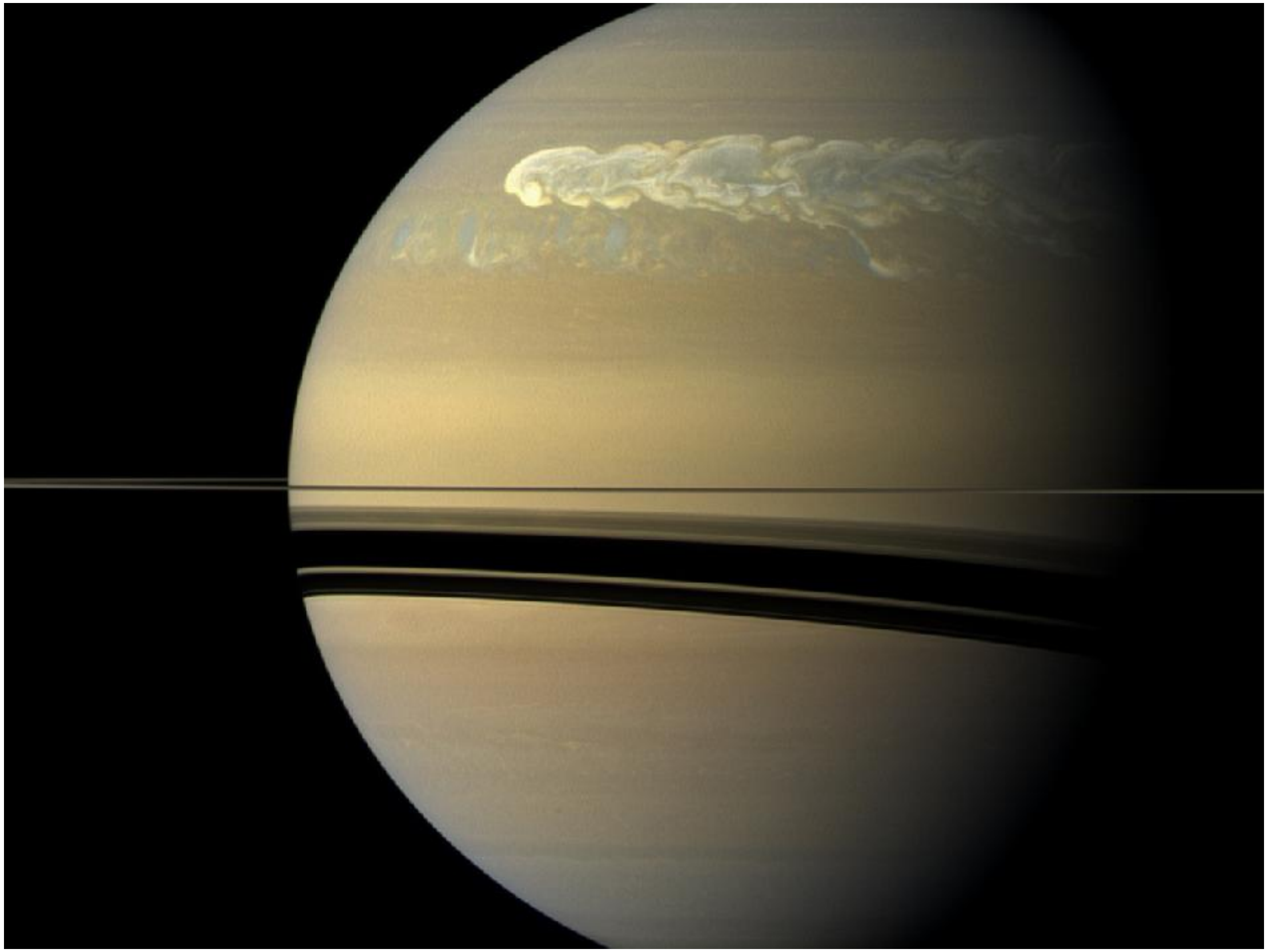


Other modern codes: Expander, Fountain, Raptor, Network

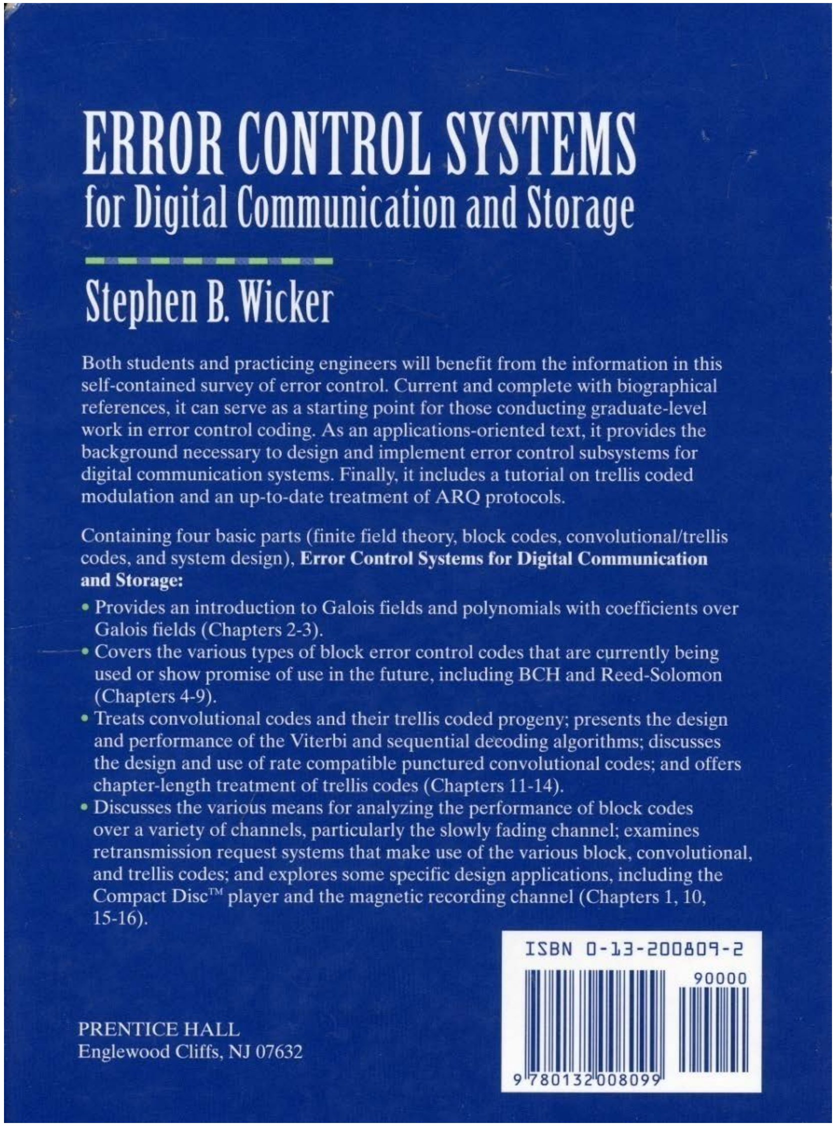
LDPC codes are being proposed for future communications standards.

Cassini-Huygens

Storm on Saturn July 2011



ISBN Codes



ERROR CONTROL SYSTEMS
for Digital Communication and Storage

Stephen B. Wicker

Both students and practicing engineers will benefit from the information in this self-contained survey of error control. Current and complete with biographical references, it can serve as a starting point for those conducting graduate-level work in error control coding. As an applications-oriented text, it provides the background necessary to design and implement error control subsystems for digital communication systems. Finally, it includes a tutorial on trellis coded modulation and an up-to-date treatment of ARQ protocols.

Containing four basic parts (finite field theory, block codes, convolutional/trellis codes, and system design), **Error Control Systems for Digital Communication and Storage:**

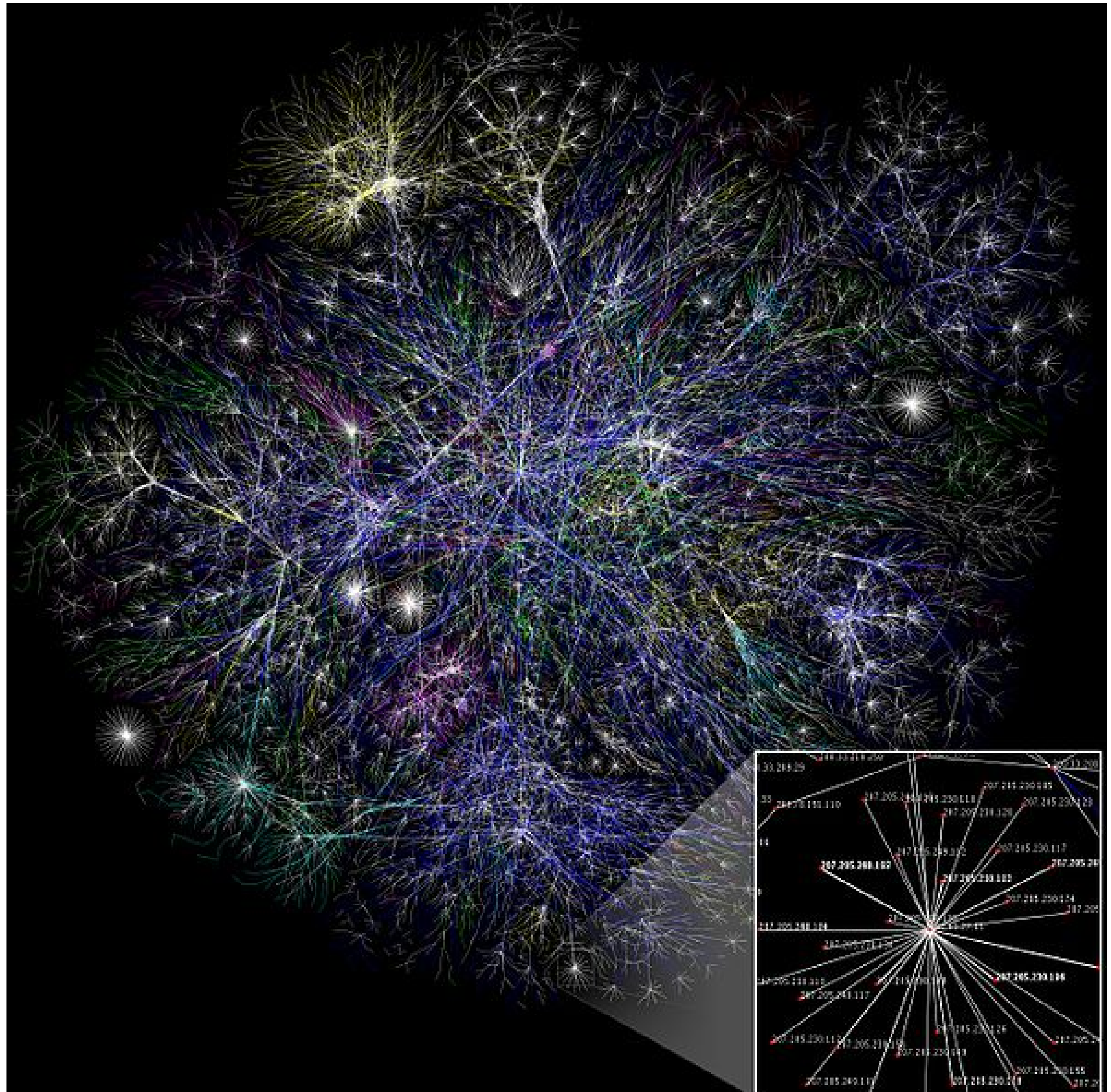
- Provides an introduction to Galois fields and polynomials with coefficients over Galois fields (Chapters 2-3).
- Covers the various types of block error control codes that are currently being used or show promise of use in the future, including BCH and Reed-Solomon (Chapters 4-9).
- Treats convolutional codes and their trellis coded progeny; presents the design and performance of the Viterbi and sequential decoding algorithms; discusses the design and use of rate compatible punctured convolutional codes; and offers chapter-length treatment of trellis codes (Chapters 11-14).
- Discusses the various means for analyzing the performance of block codes over a variety of channels, particularly the slowly fading channel; examines retransmission request systems that make use of the various block, convolutional, and trellis codes; and explores some specific design applications, including the Compact Disc™ player and the magnetic recording channel (Chapters 1, 10, 15-16).

ISBN 0-13-200809-2
90000
9 780132 008099

PRENTICE HALL
Englewood Cliffs, NJ 07632

Internet

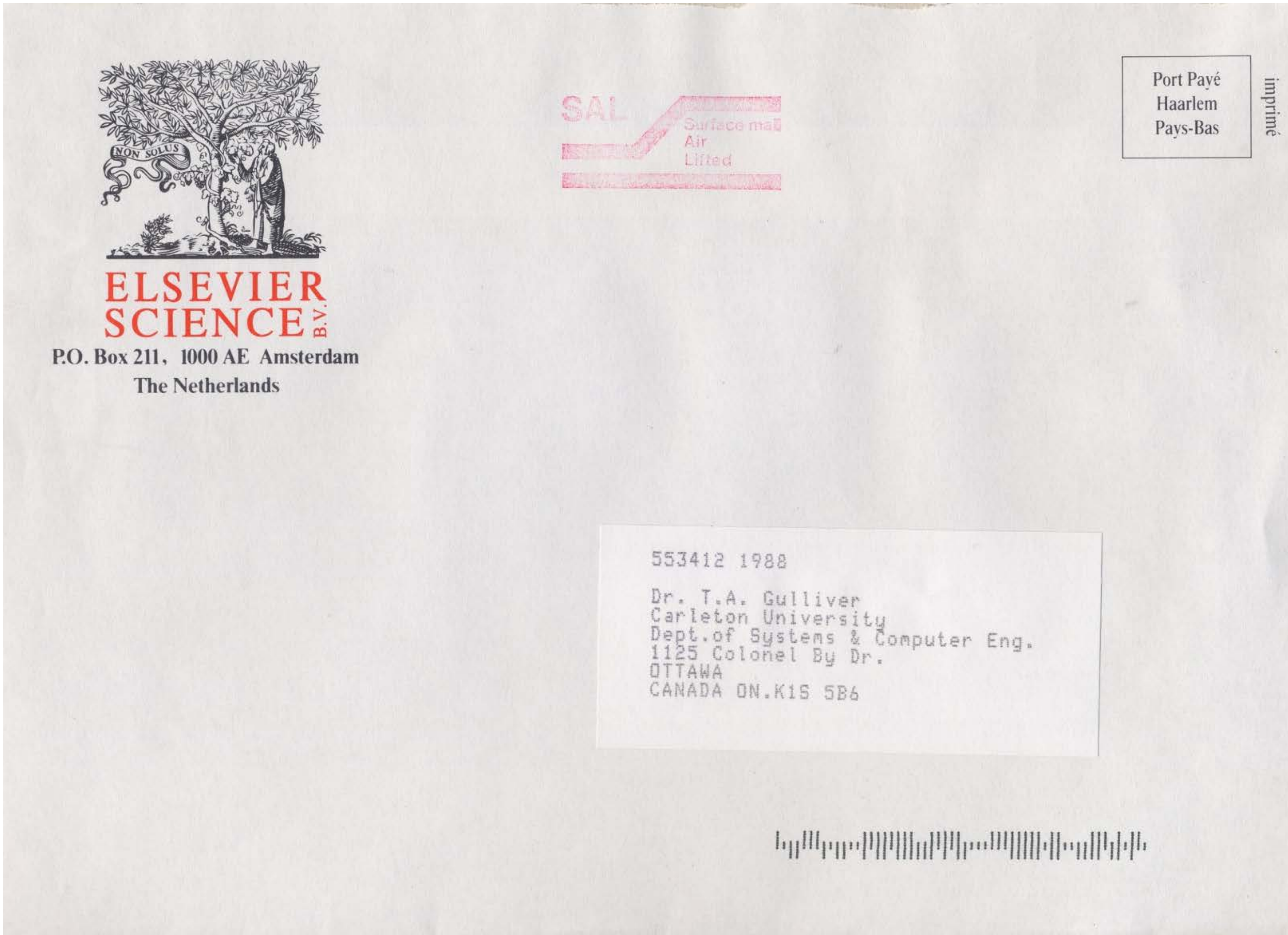
Checksums are used by the standard Internet protocols IP, UDP, and TCP.



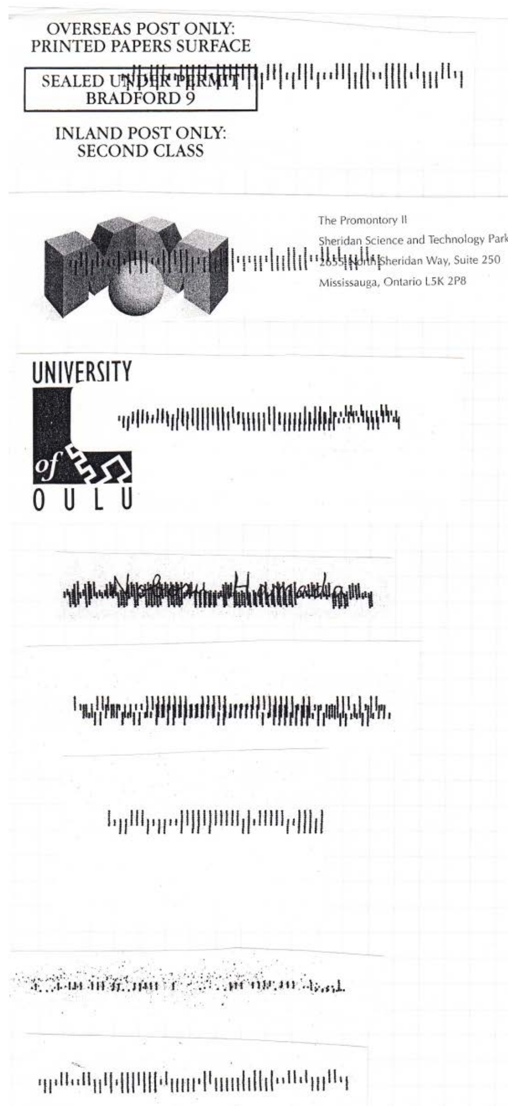
Raid Storage

Mobile Telephone Evolution

Bar Codes


NON SOLUS
ELSEVIER
SCIENCE
B.V.
P.O. Box 211, 1000 AE Amsterdam
The Netherlands
SAL
Surface mail
Air
Lifted
Port Payé
Haarlem
Pays-Bas
imprimé
553412 1988
Dr. T.A. Gulliver
Carleton University
Dept.of Systems & Computer Eng.
1125 Colonel By Dr.
OTTAWA
CANADA ON.K1S 5B6

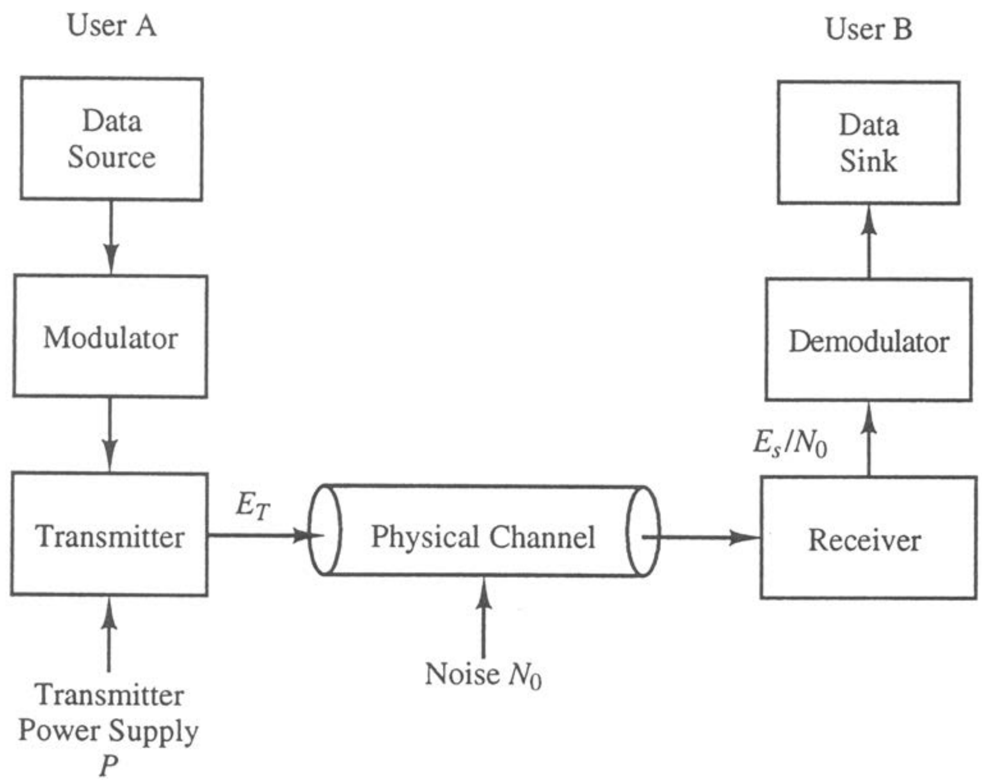
Bar Code Errors



Communication Systems

- Allow the electronic exchange of voice, data, video, music, multimedia data, email, web pages, Twitter, FaceTime, etc.
- Older communication systems include Radio and TV broadcasting, Public Switched Telephone Network (voice, fax, modem)
- Modern communication systems include
  - Cellular telephone systems
  - Computer networks (LANs, WANs, internet)
  - Satellite systems (pagers, voice/data, television)
  - Bluetooth
  - WiFi
  - Ultrawideband
  - …….

Digital Communication System



Modulator/Transmitter

- Matches the message to the channel
- Modulation encodes the message into the amplitude, phase and/or frequency of the signal
  - PSK, FSK, QAM, OFDM, PAM, PPM, …

Receiver/Demodulator

- The receiver amplifies and filters the signal
- The ideal receiver output is a scaled, delayed version of the message signal
- The demodulator extracts the message from the receiver output
  - Converts the receiver output to bits or symbols

Channel

- Physical medium that the signal is transmitted through or stored on
- Examples: Air, coaxial cables, fiber optic cables, space, CDs, DVDs, flash drives, …
- Every channel introduces some amount of distortion, noise and interference
- The channel affects the
    - Data rate
    - Bit error rate
    - Quality of service

Communications System Design Goals

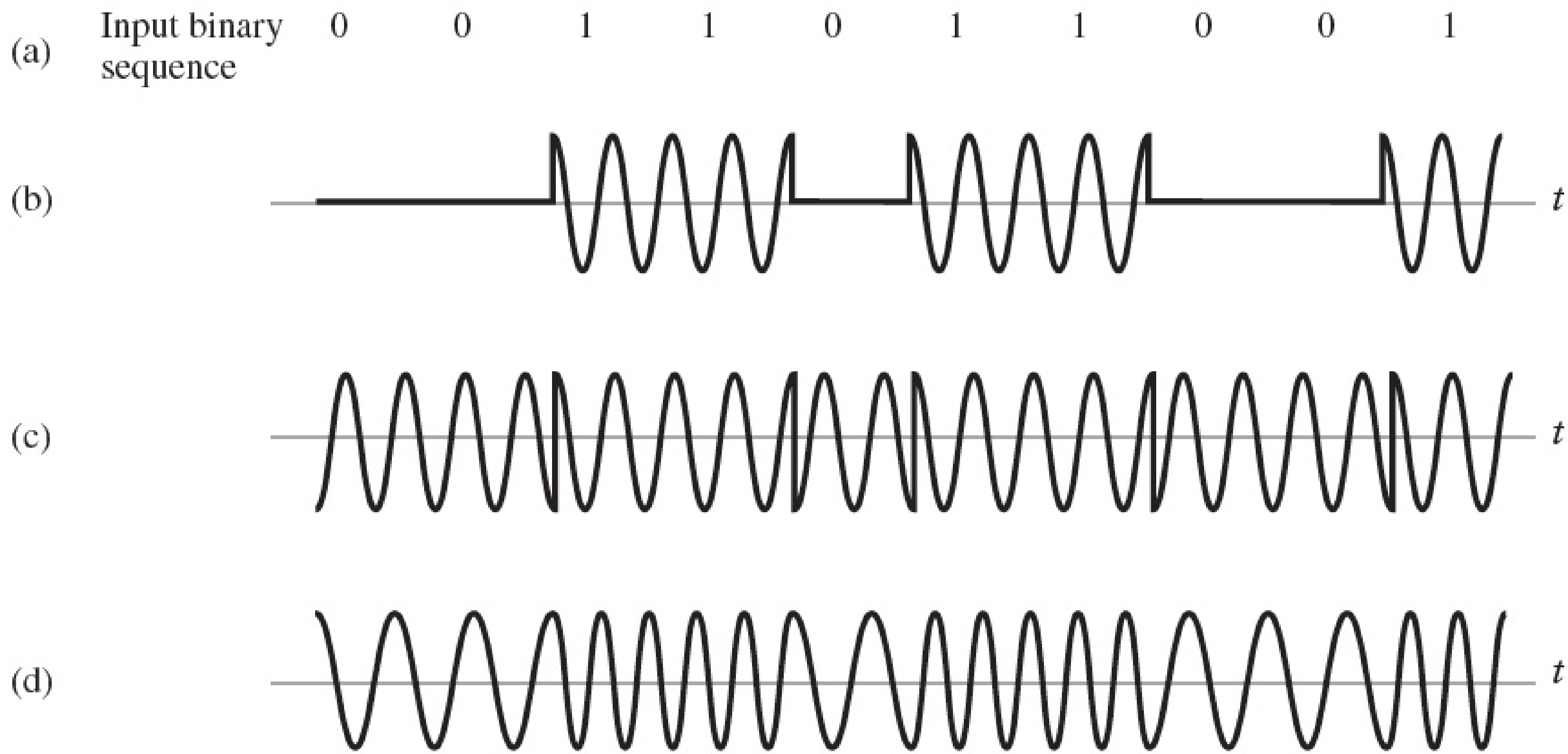
- Maximize the data rate
- Minimize the bit error rate (BER)
- Minimize the required Signal to Noise Ratio (SNR)
- Minimize the required bandwidth
- Minimize the system complexity and cost
- Maximize the throughput

- These are conflicting goals

System Constraints

- Available bandwidth
- Maximum allowable BER
- Power limitations
- Government regulations
- Technological limitations

The Three Basic Forms of Signalling



(a) binary data stream; (b) amplitude shift keying;
(c) phase shift keying; (d) frequency shift keying

Binary Modulation

- BPSK

$$\text{data } 0 \leftrightarrow s_0(t) = \sqrt{2P}\cos(2\pi f_c t) \qquad 0 \le t \le T$$

$$\text{data } 1 \leftrightarrow s_1(t) = -\sqrt{2P}\cos(2\pi f_c t) \qquad 0 \le t \le T$$

$$\text{or} \quad \sqrt{2P}\cos(2\pi f_c t + \pi)$$

- BFSK

$$\text{data } 0 \leftrightarrow s_0(t) = \sqrt{2P}\cos(2\pi f_0 t) \qquad 0 \le t \le T$$

$$\text{data } 1 \leftrightarrow s_1(t) = \sqrt{2P}\cos(2\pi f_1 t) \qquad 0 \le t \le T$$

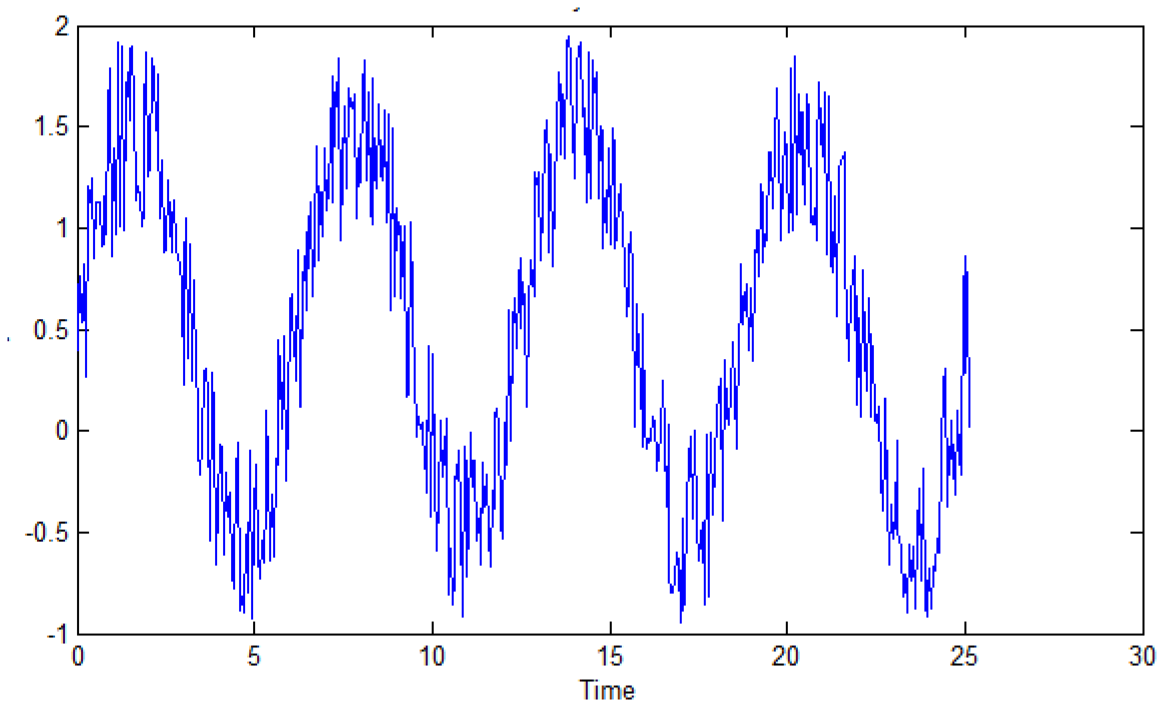
Binary Modulation

- Energy = Power×Time
- $P = E_b/T_b = E_bR_b$
- $R_b = 1/T_b$ bits/s

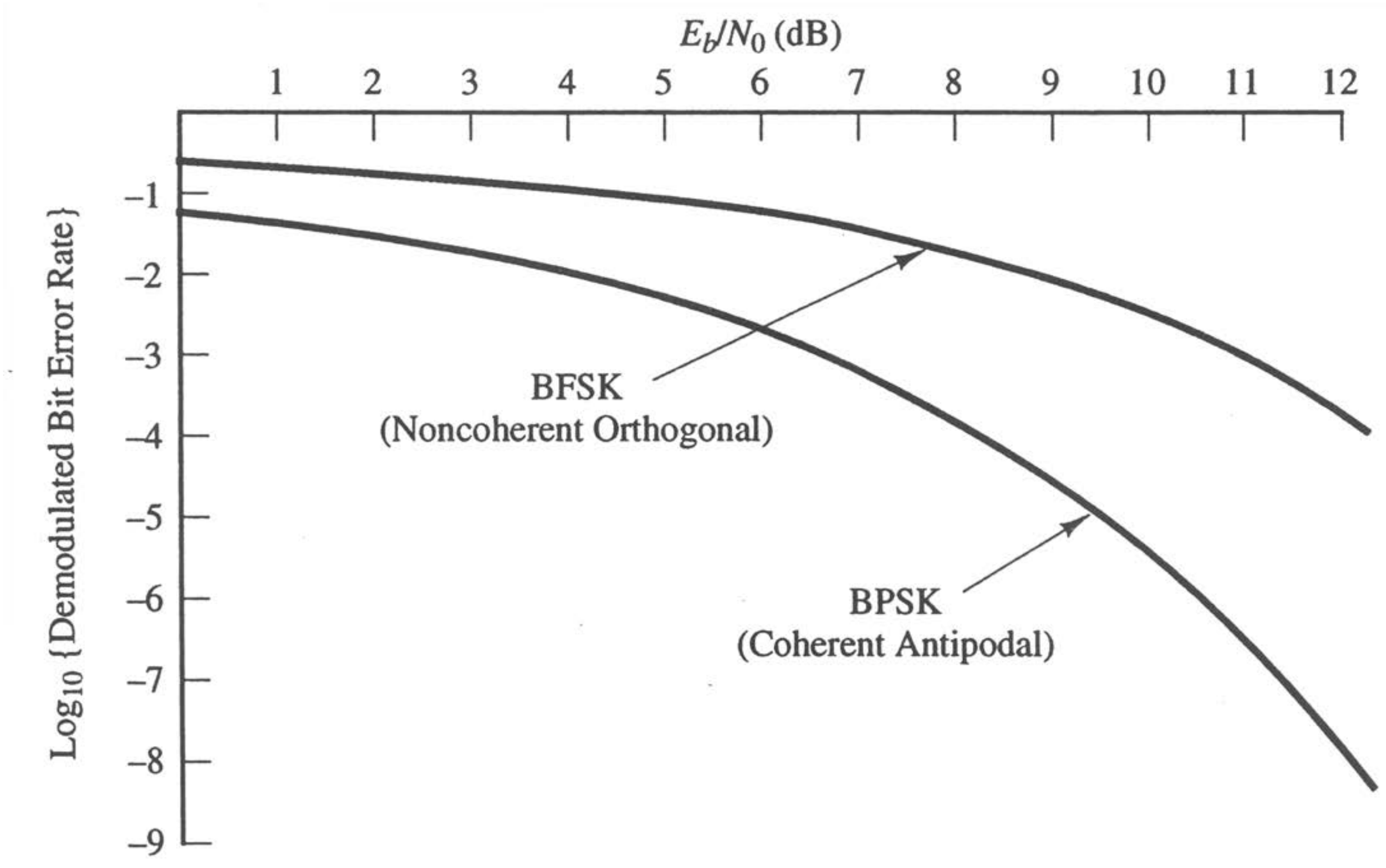
- Power levels are generally expressed in decibels (dB)
  - $P_{dB} = 10\log_{10}P_{watts}$

- The most commonly assumed noise model is Additive White Gaussian Noise (AWGN)
  - Noise power spectral density - N_0
- Signal to noise Ratio (SNR) - E_b/N_0

Effect of Noise on a Signal



Performance of BPSK and BFSK in AWGN

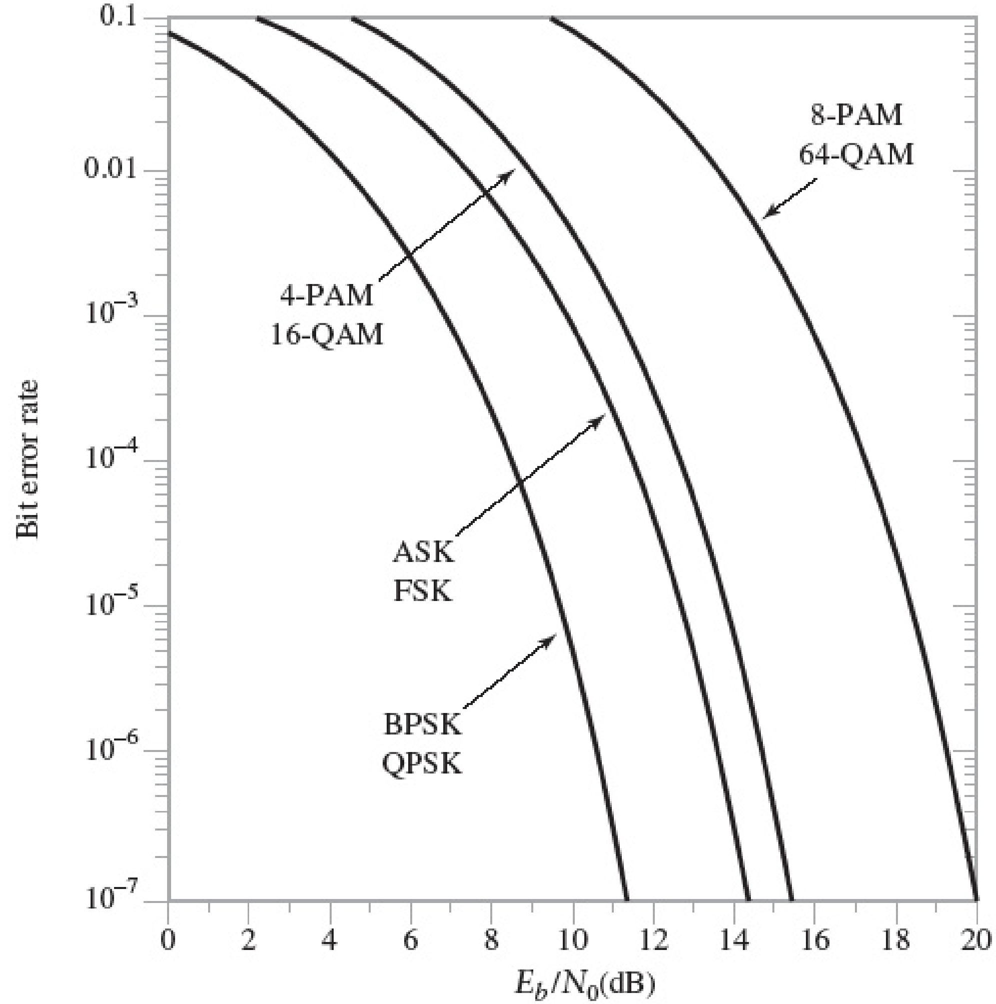


M-ary Modulation

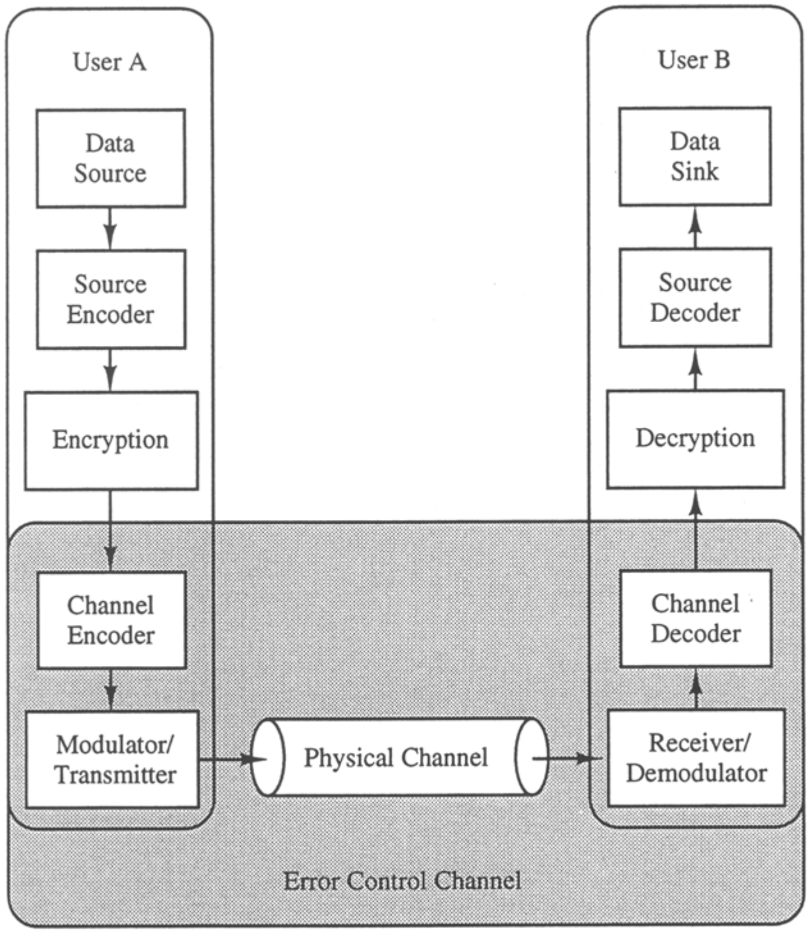
- In M-ASK a group of n bits is transmitted using $M=2^n$ different amplitudes
- In M-PSK a group of n bits is transmitted using $M=2^n$ different phases
- In M-FSK a group of n bits is transmitted using $M=2^n$ different frequencies

- Quadrature amplitude modulation (QAM) uses a combination of amplitude and phase modulation to convey information

BER versus E_b/N_0 for Several Digital Modulation Techniques



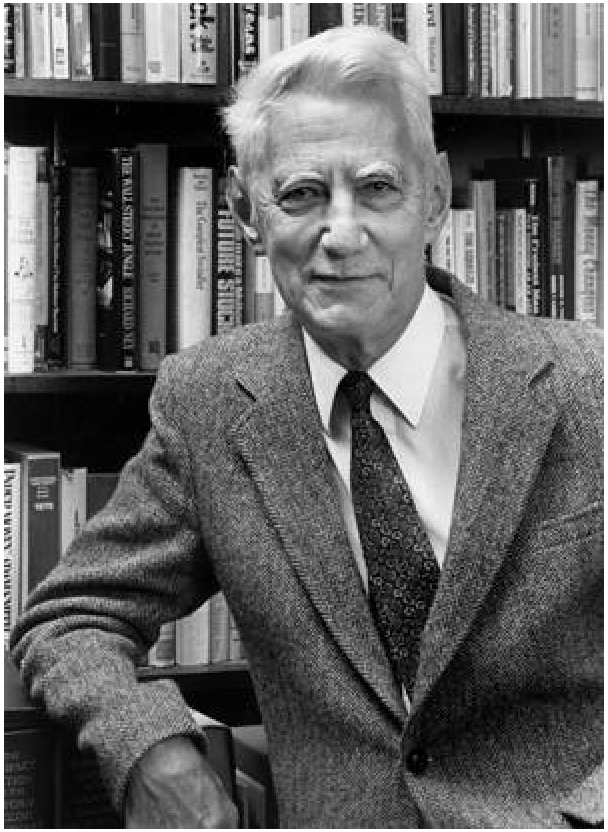
Digital Communication System with Coding



Types of Codes

- **Source codes** are used to remove the redundancy that naturally occurs in information sources.
- **Secrecy codes** are used to encrypt information to protect it from unauthorized use.
- **Error control codes** are used to format the information so as to increase its immunity to channel impairments such as noise.

Claude Shannon (1916-2001)



A Mathematical Theory of Communications, BSTJ, July 1948

``The fundamental problem of communication is that of reproducing at one point exactly or approximately a message selected at another point. …

If the channel is noisy it is not in general possible to reconstruct the original message or the transmitted signal with certainty by any operation on the received signal.''

Channel Capacity

- An important question for a communication channel is the **maximum rate** at which it can transfer information.
- The **channel capacity *C*** is a theoretical maximum rate below which information can be transmitted over the channel with an arbitrarily low probability of error.

Shannon's Noisy Channel Coding Theorem

- How to achieve capacity?
  - With every channel there is an associated channel capacity *C*. There exist **error control codes** such that information can be transmitted across the channel at rates less than *C* with arbitrarily low bit error rate.
- There are only two factors that determine the capacity of an AWGN channel:
  - Bandwidth (*W*)
  - Signal-to-Noise Ratio (SNR) E_b/N_0

AWGN Channel Capacity

$$C = W\log_2\left(1+\frac{P}{N_0 W}\right)$$

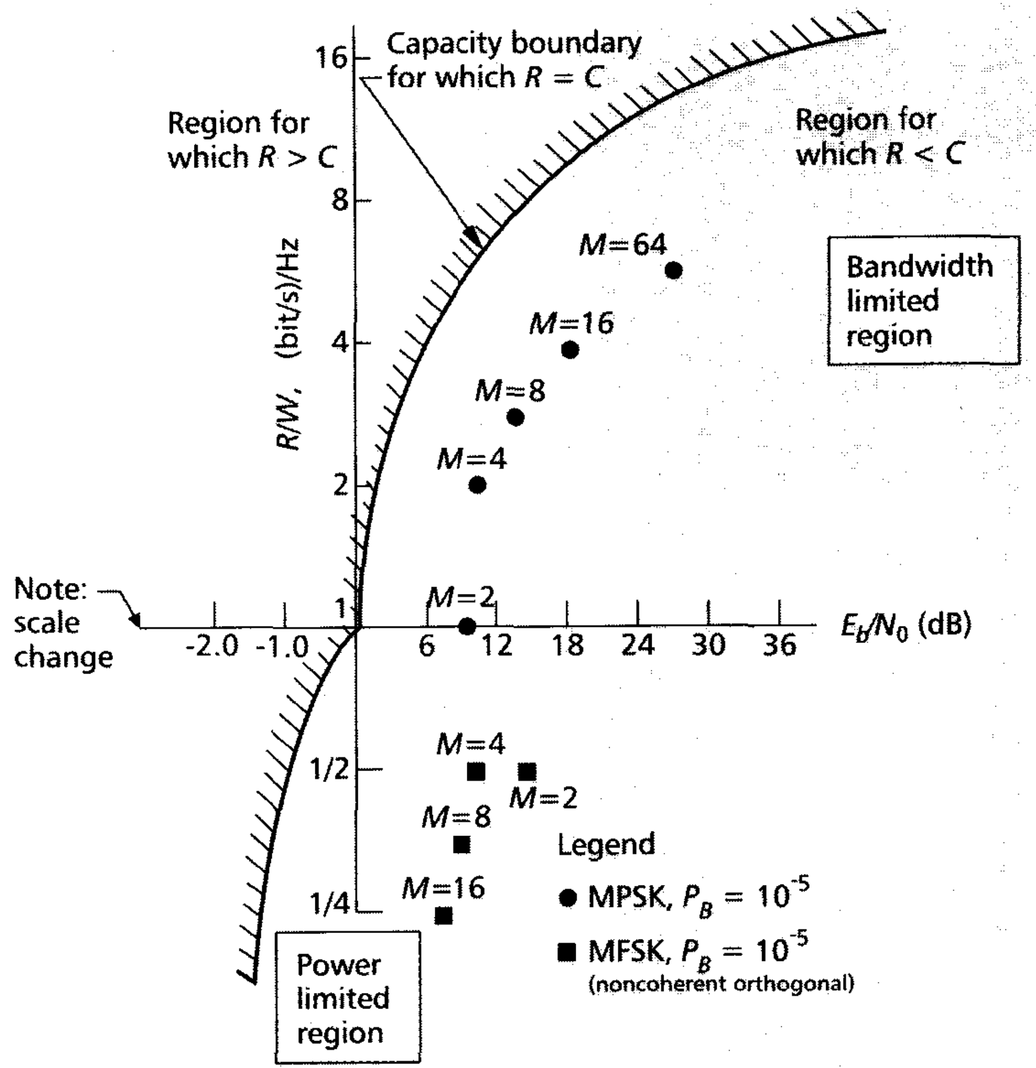
$$E = PT \rightarrow P = E_b R_b$$

$$C = W\log_2\left(1+\frac{E_b R_b}{N_0 W}\right)$$

Let $R_b = C$ $$\frac{C}{W} = \log_2\left(1+\frac{E_b}{N_0}\frac{C}{W}\right)$$

$$\frac{E_b}{N_0} = \frac{2^{C/W}-1}{C/W}$$

Bandwidth Efficiency versus SNR



ASCII Character Set

Least Significant Bits

Most Significant Bits

	0 0000	1 0001	2 0010	3 0011	4 0100	5 0101	6 0110	7 0111	8 1000	9 1001	A 1010	B 1011	C 1100	D 1101	E 1110	F 1111
0 000	**NUL** (0) 00	**SOH** (1) 01	**STX** (2) 02	**ETX** (3) 03	**EOT** (4) 04	**ENQ** (5) 05	**ACK** (6) 06	**BEL** (7) 07	**BS** (8) 08	**HT** (9) 09	**LF** (10) 0A	**VT** (11) 0B	**FF** (12) 0C	**CR** (13) 0D	**SO** (14) 0E	**SI** (15) 0F
1 001	**DLE** (16) 10	**DC1** (17) 11	**DC2** (18) 12	**DC3** (19) 13	**DC4** (20) 14	**NAK** (21) 15	**SYN** (22) 16	**ETB** (23) 17	**CAN** (24) 18	**EM** (25) 19	**SUB** (26) 1A	**ESC** (27) 1B	**FS** (28) 1C	**GS** (29) 1D	**RS** (30) 1E	**US** (31) 1F
2 010	**SP** (32) 20	**!** (33) 21	**"** (34) 22	**#** (35) 23	**$** (36) 24	**%** (37) 25	**&** (38) 26	**'** (39) 27	**(** (40) 28	**)** (41) 29	***** (42) 2A	**+** (43) 2B	**,** (44) 2C	**-** (45) 2D	**.** (46) 2E	**/** (47) 2F
3 011	**0** (48) 30	**1** (49) 31	**2** (50) 32	**3** (51) 33	**4** (52) 34	**5** (53) 35	**6** (54) 36	**7** (55) 37	**8** (56) 38	**9** (57) 39	**:** (58) 3A	**;** (59) 3B	**<** (60) 3C	**=** (61) 3D	**>** (62) 3E	**?** (63) 3F
4 100	**@** (64) 40	**A** (65) 41	**B** (66) 42	**C** (67) 43	**D** (68) 44	**E** (69) 45	**F** (70) 46	**G** (71) 47	**H** (72) 48	**I** (73) 49	**J** (74) 4A	**K** (75) 4B	**L** (76) 4C	**M** (77) 4D	**N** (78) 4E	**O** (79) 4F
5 101	**P** (80) 50	**Q** (81) 51	**R** (82) 52	**S** (83) 53	**T** (84) 54	**U** (85) 55	**V** (86) 56	**W** (87) 57	**X** (88) 58	**Y** (89) 59	**Z** (90) 5A	**[** (91) 5B	**** (92) 5C	**]** (93) 5D	**^** (94) 5E	**_** (95) 5F
6 110	**`** (96) 60	**a** (97) 61	**b** (98) 62	**c** (99) 63	**d** (100) 64	**e** (101) 65	**f** (102) 66	**g** (103) 67	**h** (104) 68	**i** (105) 69	**j** (106) 6A	**k** (107) 6B	**l** (108) 6C	**m** (109) 6D	**n** (110) 6E	**o** (111) 6F
7 111	**p** (112) 70	**q** (113) 71	**r** (114) 72	**s** (115) 73	**t** (116) 74	**u** (117) 75	**v** (118) 76	**w** (119) 77	**x** (120) 78	**y** (121) 79	**z** (122) 7A	**{** (123) 7B	**|** (124) 7C	**}** (125) 7D	**~** (126) 7E	**DEL** (127) 7F

SPC Code – Example 1

- ASCII symbols

  E = 1000101 c = 10001011

  G = 1000111 c = 10001110

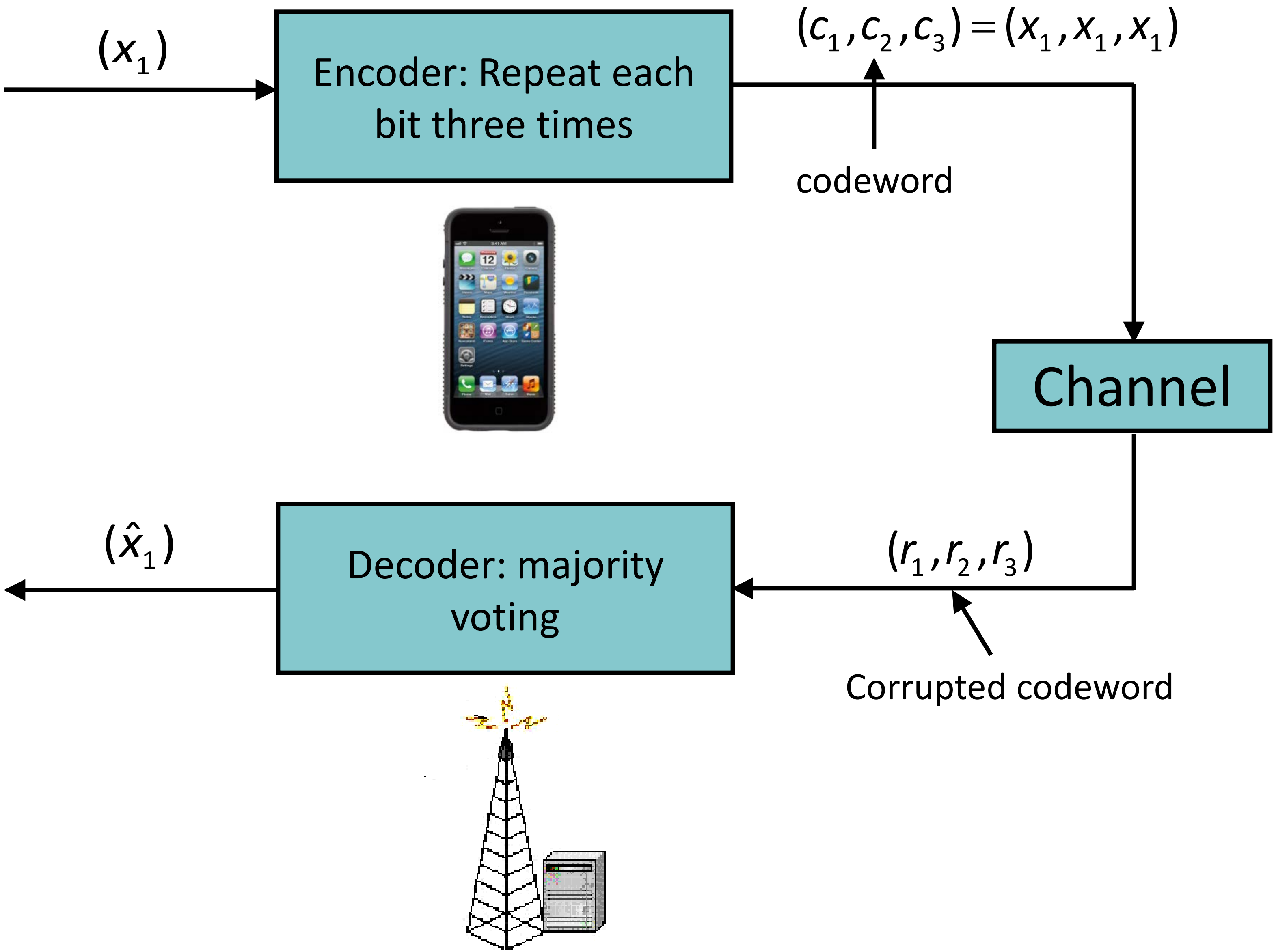
- Received word

  r = 10001010

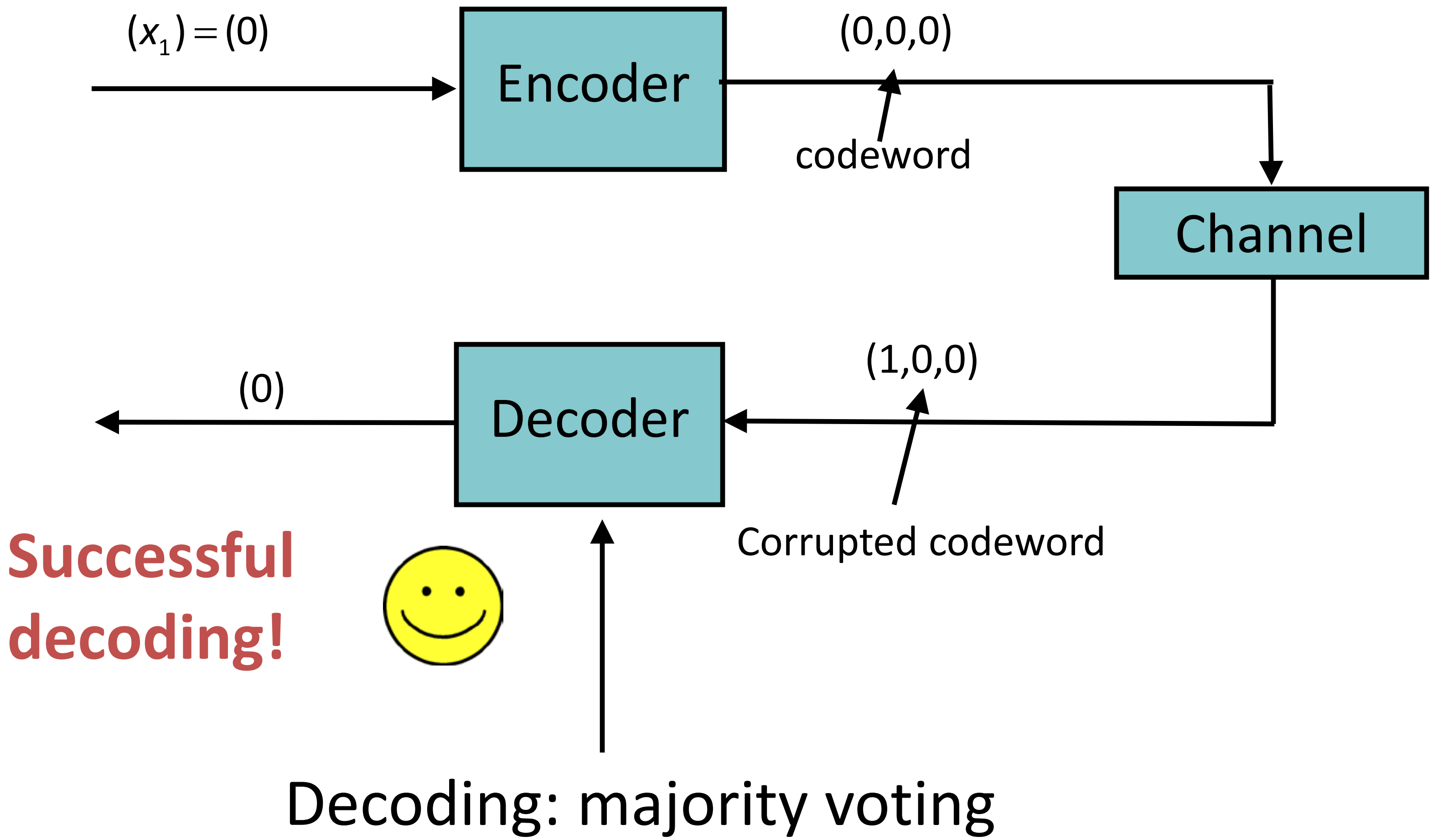
Triple Repetition Code – Decoding

Received Word	Codeword	Error Pattern
0 0 0	0 0 0	0 0 0
0 0 1	0 0 0	0 0 1
0 1 0	0 0 0	0 1 0
1 0 0	0 0 0	1 0 0
1 1 1	1 1 1	0 0 0
1 1 0	1 1 1	0 0 1
1 0 1	1 1 1	0 1 0
0 1 1	1 1 1	1 0 0

Triple Repetition Code



Triple Repetition Code (Cont.)

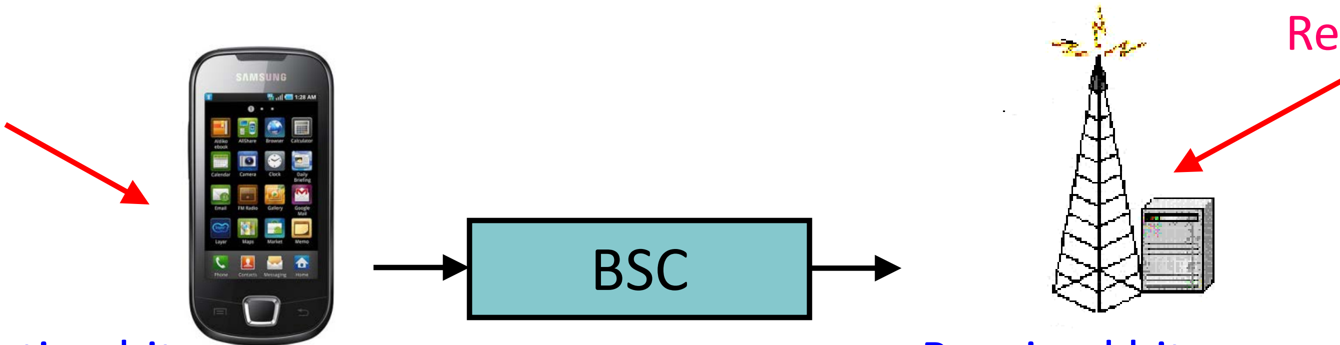


Transmission Errors

A communication channel can be modeled as a
Binary Symmetric Channel (BSC)

Sender

Receiver



Information bits

10010…10101…

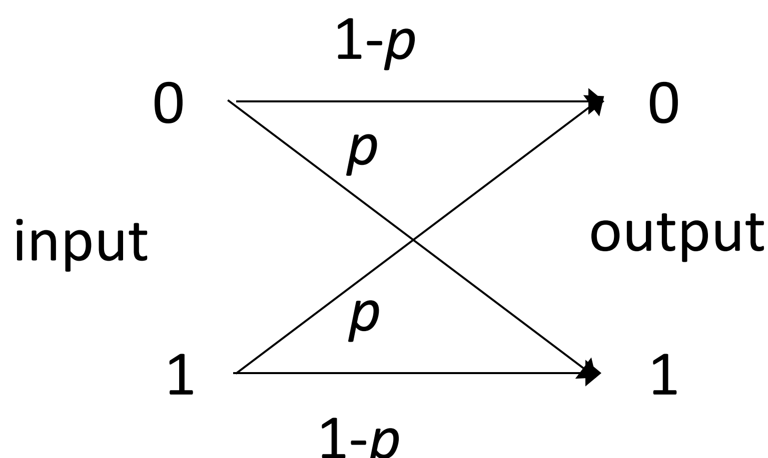
Received bits

10110…00101…

Each bit is flipped with probability *p*

Binary Symmetric Channel

- Transmitted symbols are binary
- Errors affect 0s and 1s with equal probability (symmetric)
- Errors occur randomly and are independent from bit to bit (memoryless)



p is the probability of bit error – the crossover probability

Binary Symmetric Channel

- If n symbols are transmitted, the probability of an m error pattern is

$$p^m(1-p)^{n-m}$$

- The probability of exactly m errors is

$$p^m(1-p)^{n-m}\binom{n}{m}$$

- The probability of m or more errors is

$$\sum_{i=m}^{n} p^i(1-p)^{n-i}\binom{n}{i}$$

Example

- The BSC bit error probability is $p < \frac{1}{2}$
- majority vote or nearest neighbor decoding

$$000, 001, 010, 100 \rightarrow 000$$
$$111, 110, 101, 011 \rightarrow 111$$

- the probability of a decoding error is

$$P(E) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3 < p$$

- **Example:** If $p = 0.01$, then $P(E) = 0.000298$ and only one word in 3555 will be in error after decoding.

Example with BFSK

$$p = \frac{1}{2} e^{-E_b/2N_0}$$

$$\text{SNR} \ = E_b/N_0 = 8.93 \text{ dB} \Rightarrow p = 10^{-2}$$

code rate $R = \frac{1}{3}$

$$\hat{E}_b = E_b R = E_b/3 = 4.16 \text{ dB}$$

$$\hat{p} = .136$$

$$P(E) = 3\hat{p}^2(1 - \hat{p}) + \hat{p}^3 = 0.050$$

Example (cont.)

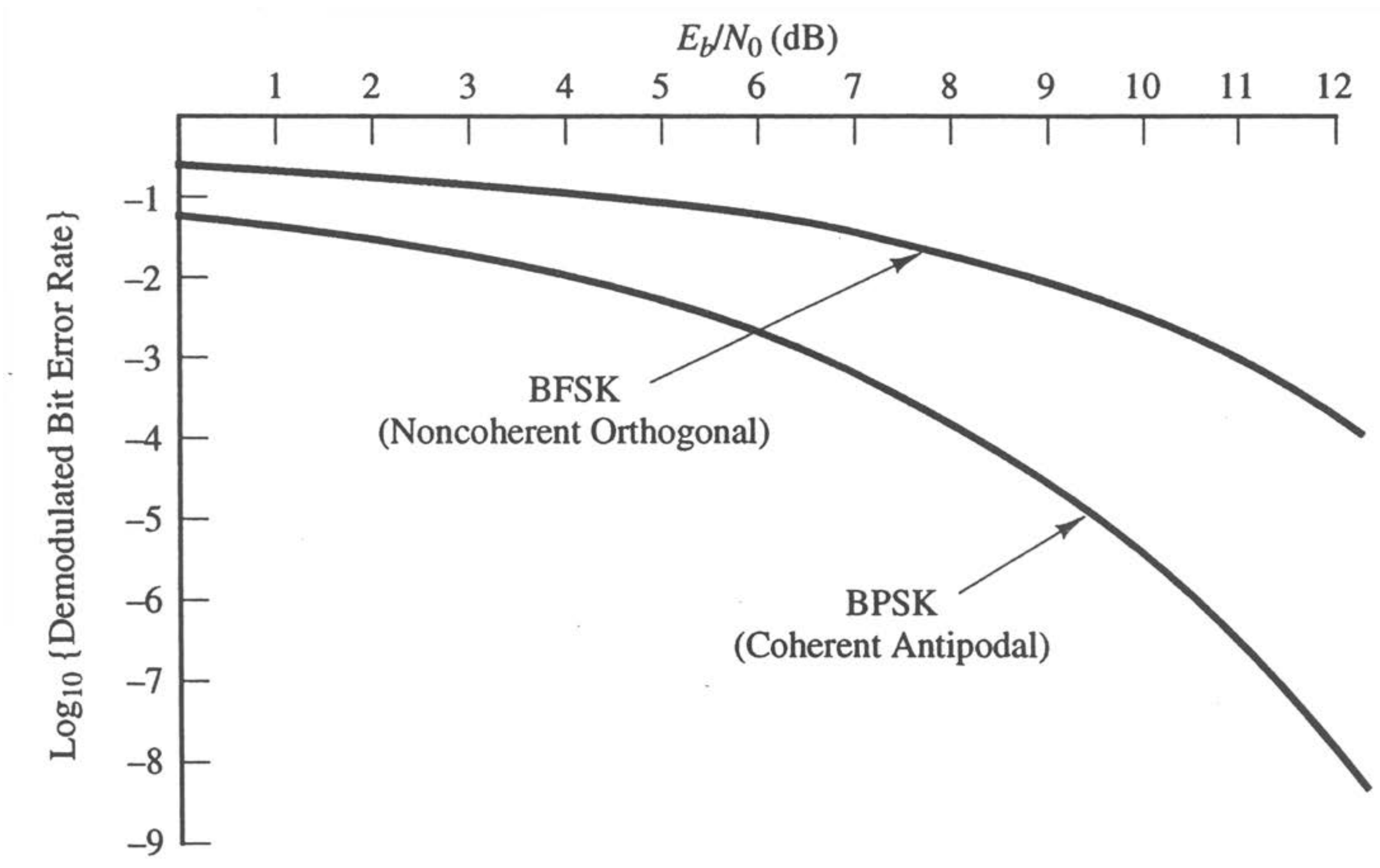
$$p = 10^{-5} \Rightarrow E_b/N_0 = 21.6 \text{ W or } 13.35 \text{ dB}$$

$$\hat{E}_b/N_0 = 13.35 - 4.77 = 8.58 \text{ dB or } 7.21 \text{ W}$$

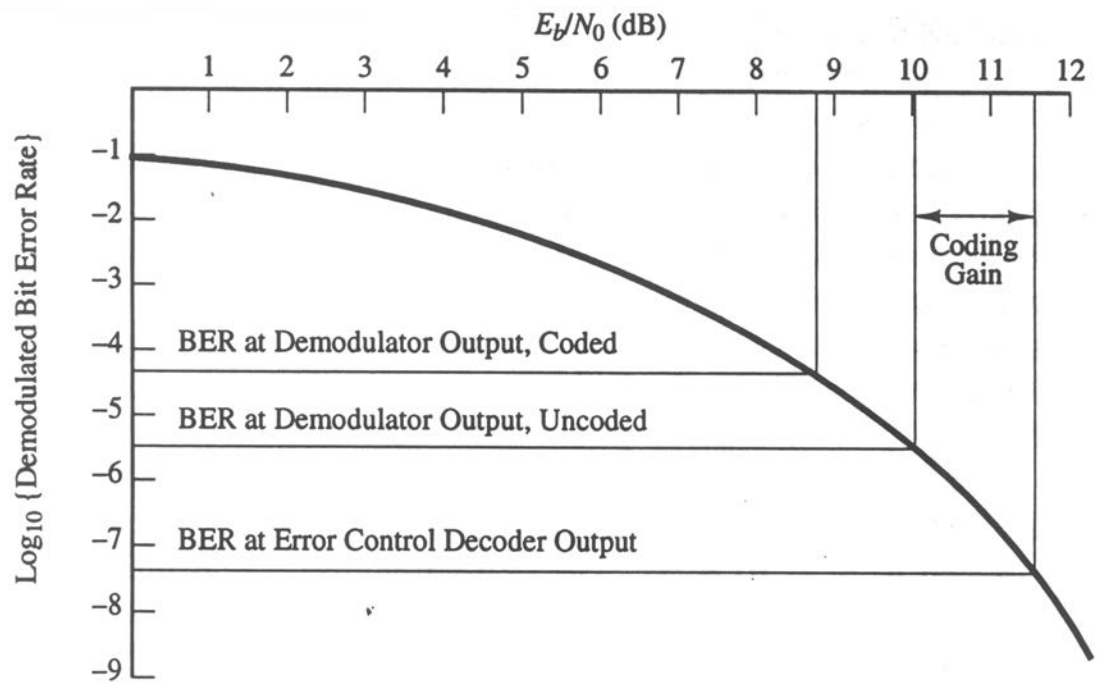
$$\hat{p} = .0136$$

$$P(E) = 5.5 \times 10^{-4}$$

Performance of BPSK and BFSK



Coding Gain with the (15,11) Hamming Code



Constructing Good Codes

- Ingredients of Shannon's proof:
  - Random code construction
  - Large block length

- Problem:

randomness + large block length + decoding =

= COMPLEXITY!

- Thus some structure is required

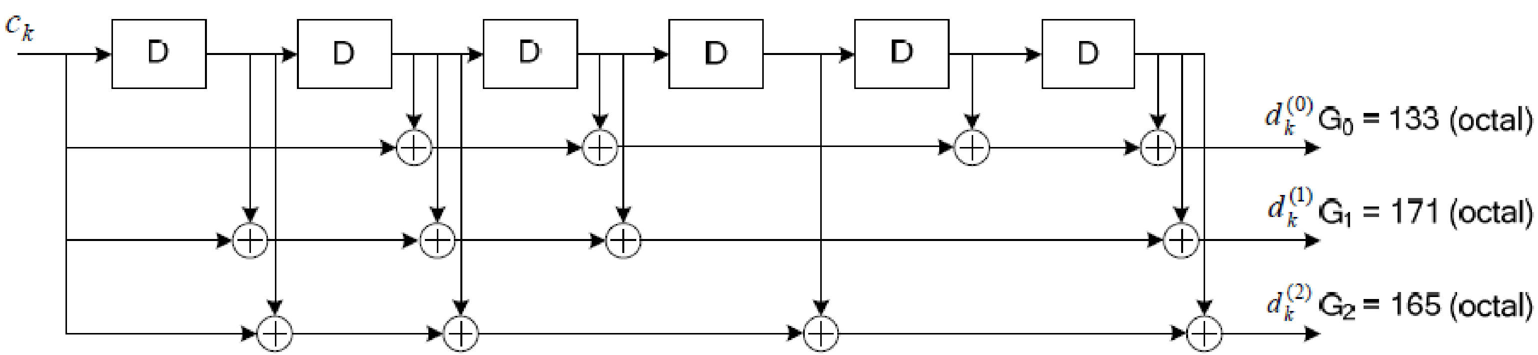
State-of-the-Art

- Solution
  - Long, structured, “pseudorandom” codes
  - Practical, near-optimal decoding algorithms
- Examples
  - Turbo codes (1993)
  - Low-density parity-check (LDPC) codes (1960, 1999)
- Turbo codes and LDPC codes have brought the Shannon limit within reach on a wide range of channels.

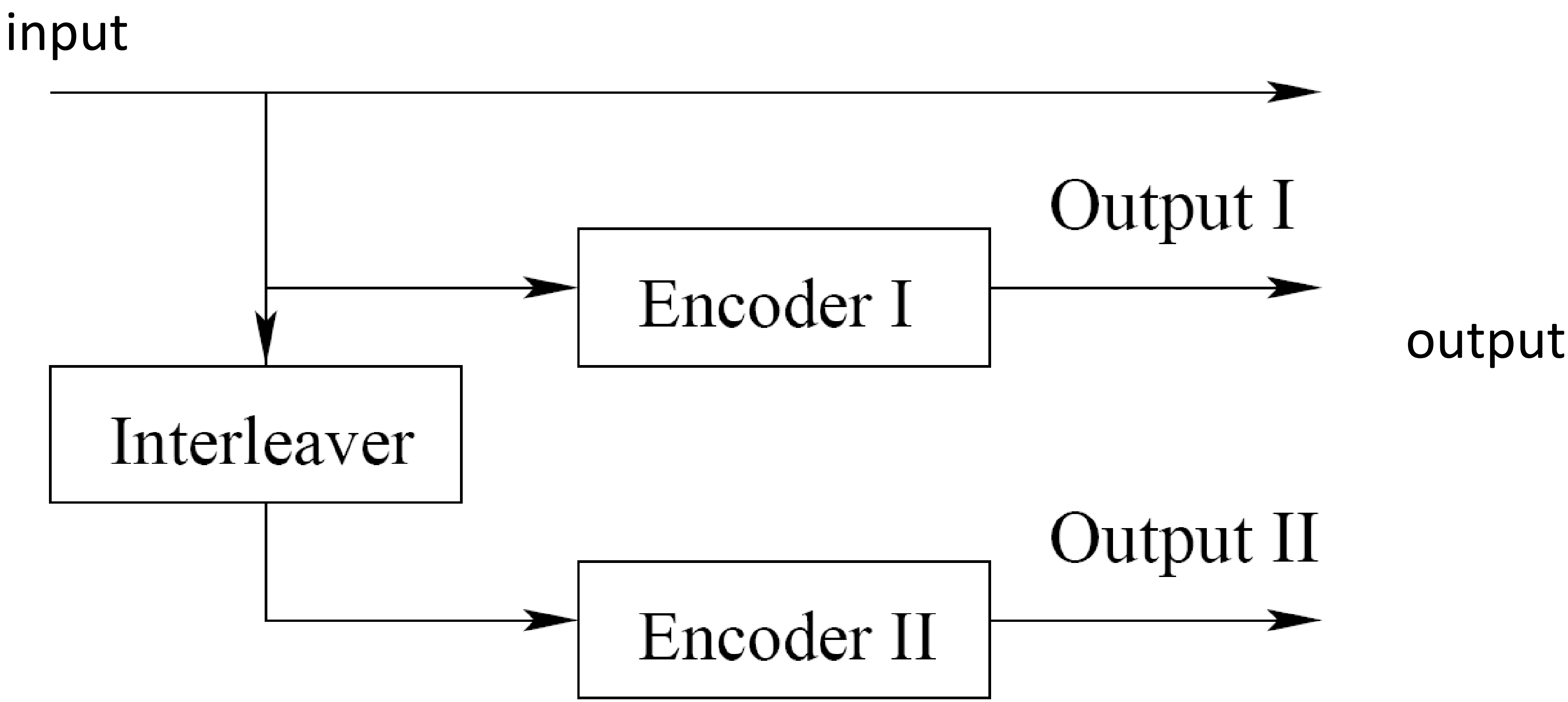
ETSI TS 136 212 V8.4.0 (2008-11) Technical Specification

LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding

Rate 1/3 Convolutional Encoder



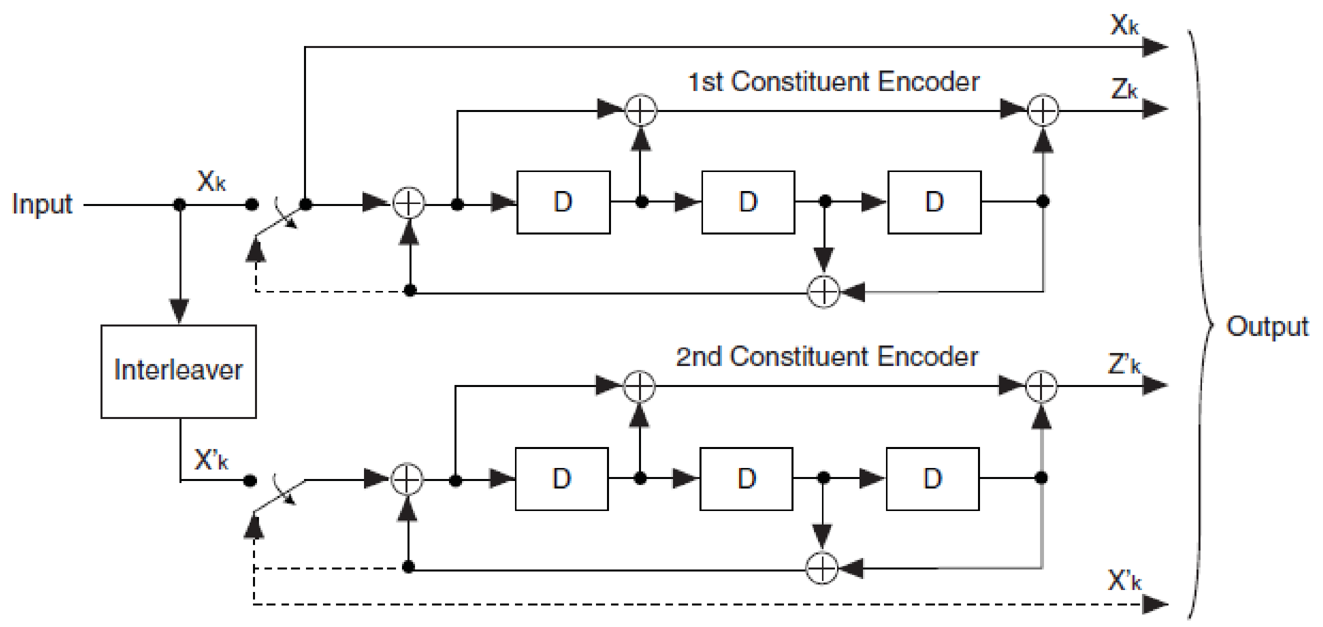
Rate 1/3 Turbo Encoder



3GPP LTE Turbo Reference Design

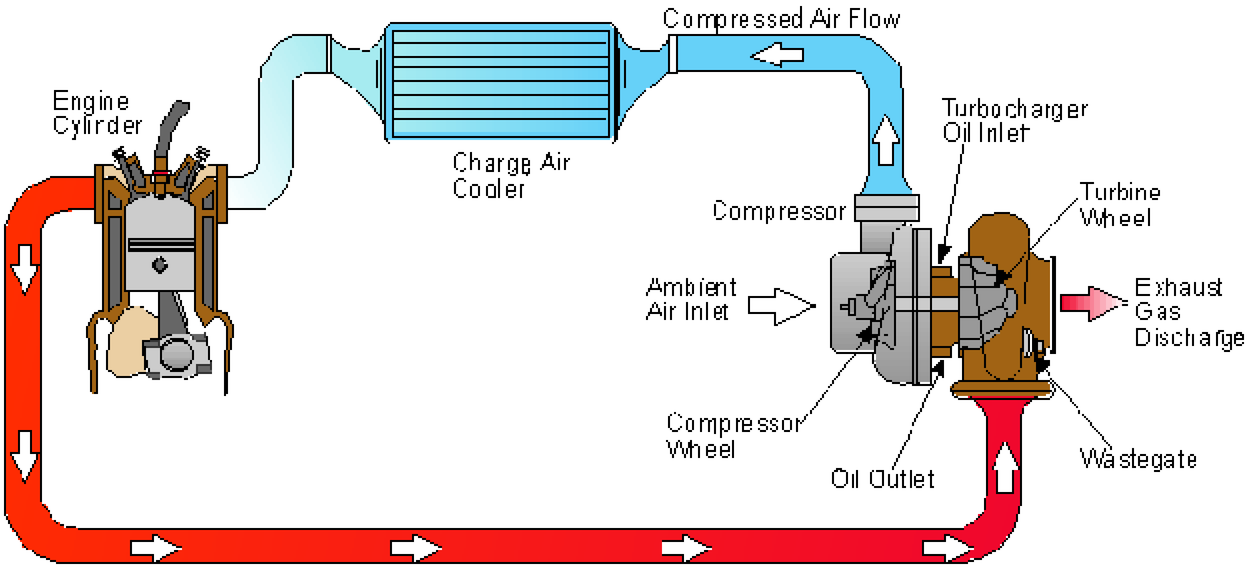
AN-505-2.1 Application Note

Figure 2. Structure of a Rate 1/3 Turbo Encoder

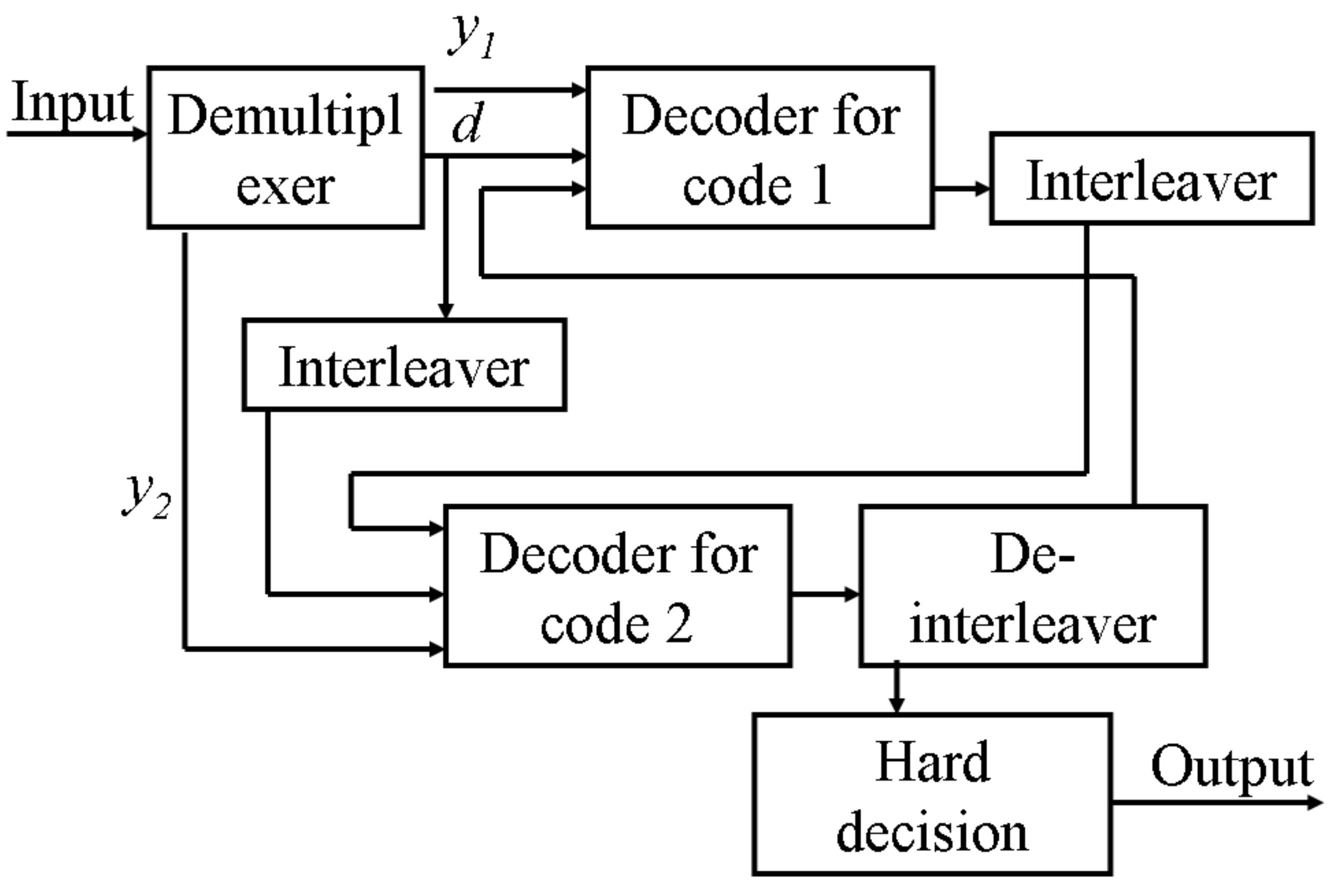


The Turbo Principle

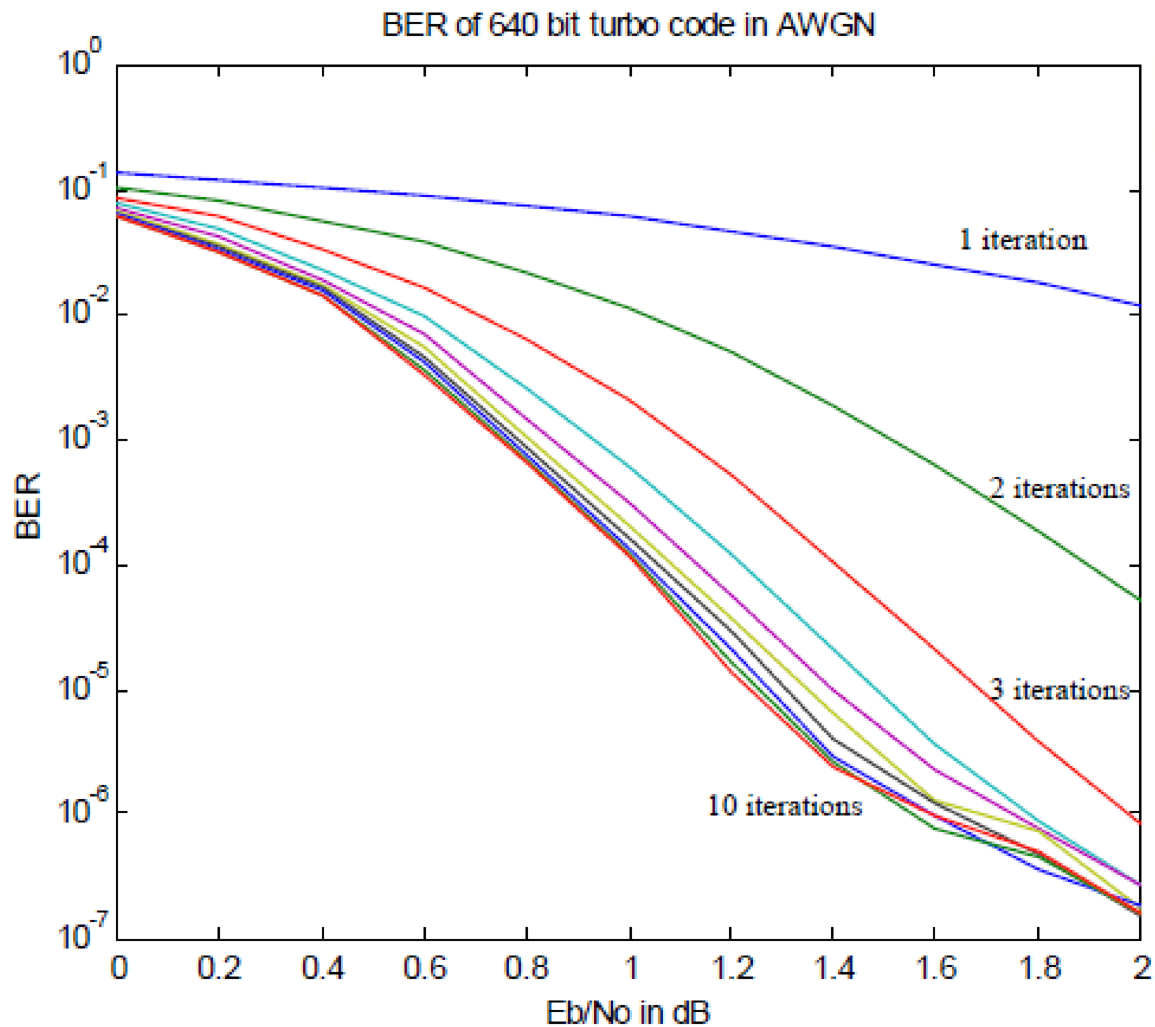
- Turbo codes are so named because the decoder uses feedback, like a turbo-charged engine.



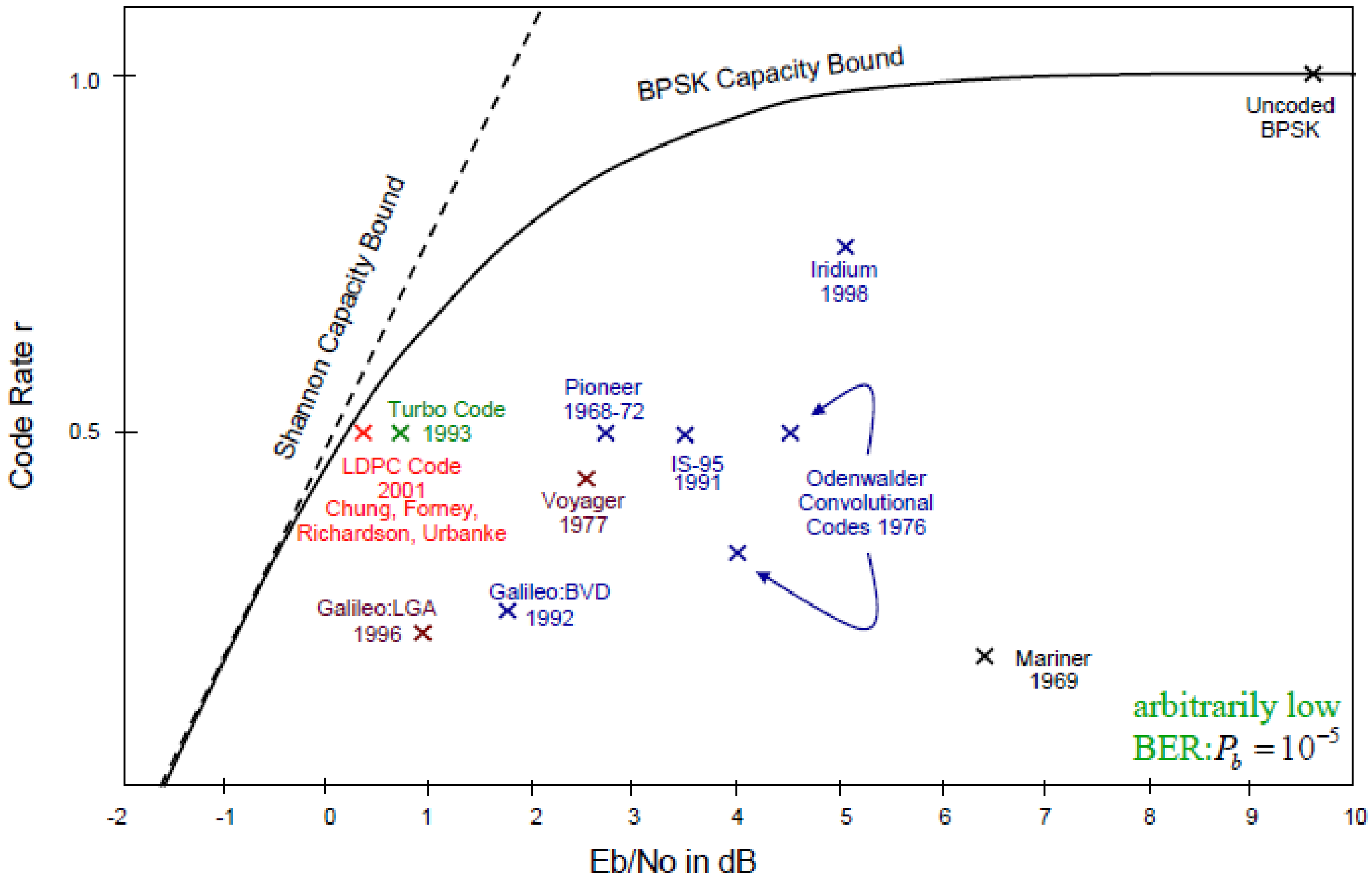
Turbo Code Decoder



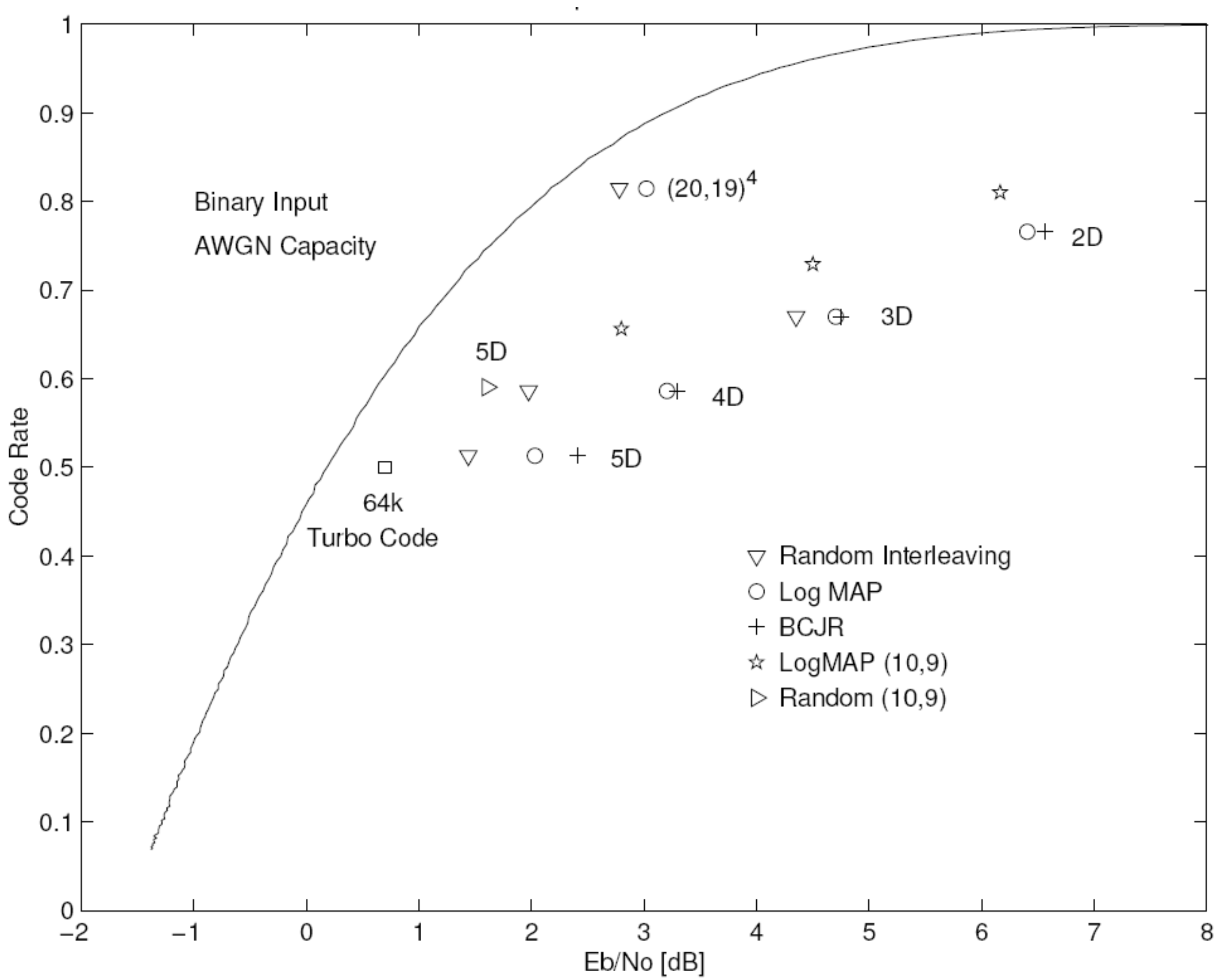
Turbo Code BER in AWGN



Efficiency of Binary Codes



Randomly Interleaved SPC Product Codes with BER=10^{-5}



The Fundamental Tradeoff

- Correct as many errors as possible while using as little redundancy as possible
- Intuitively, these are contradictory goals