ECE 405/ECE 511
Error Control Coding

Aaron Gulliver

Dept. of Electrical and Computer Engineering

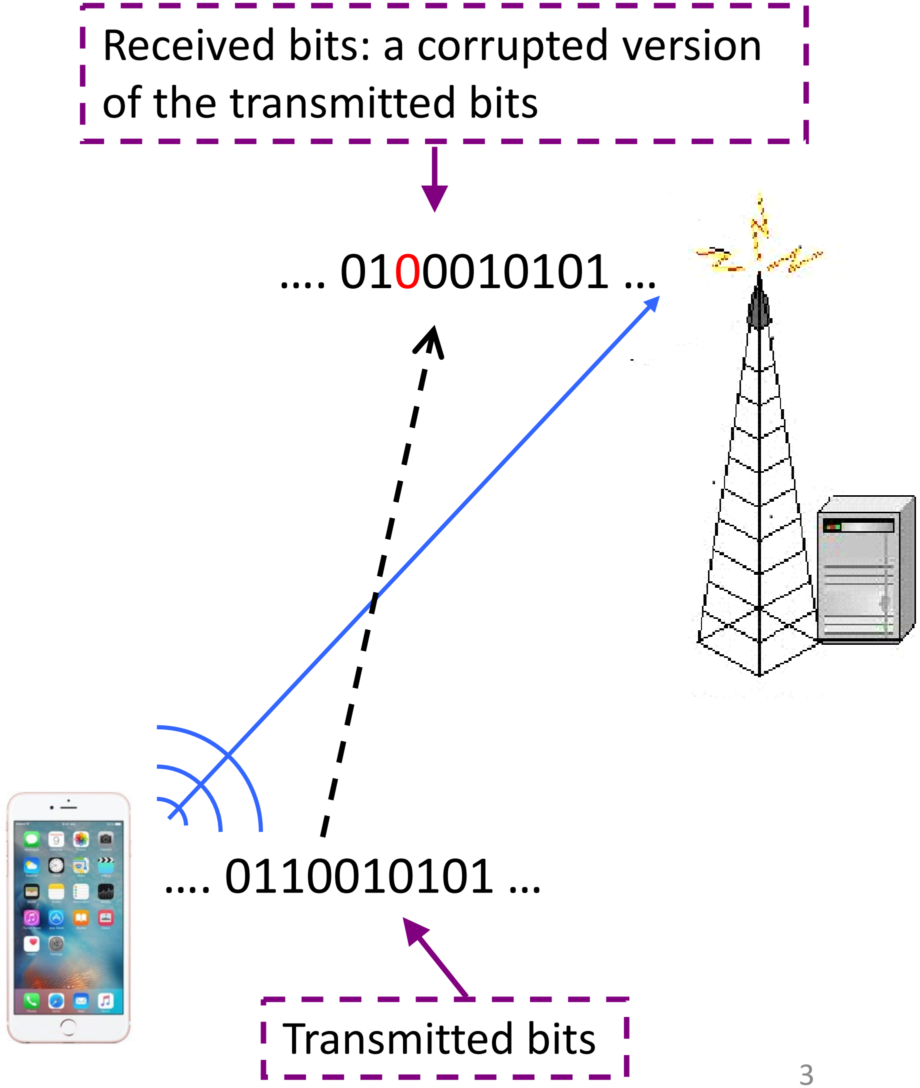
Syllabus

- Introduction; The channel coding problem [Chap. 1]
- Vector spaces; Linear block codes [Chap. 2]
- Groups, rings and fields; Primitive and irreducible polynomials [App. B]
- Polynomial rings and cyclic codes [Chap. 3]
- BCH and Reed-Solomon codes [Chaps. 4-5]
- Convolutional codes and the Viterbi algorithm [Chap. 6]

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.



Received bits: a corrupted version of the transmitted bits

.... 0100010101 ...

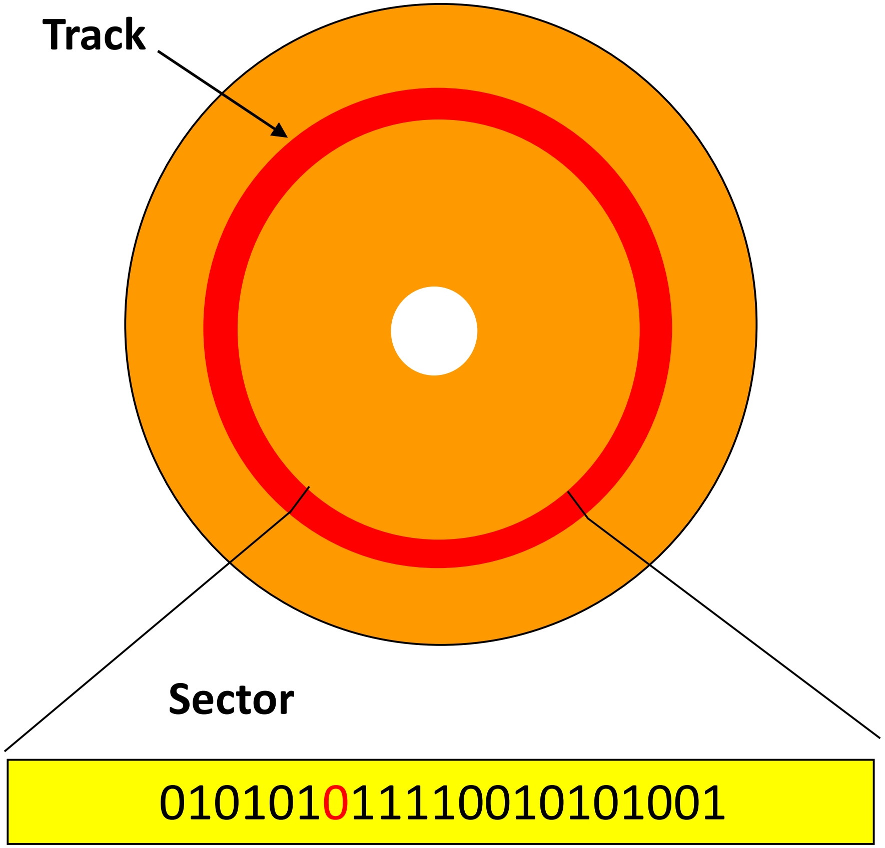
.... 0110010101 ...

Transmitted bits

Errors in Information Storage

Magnetic recording

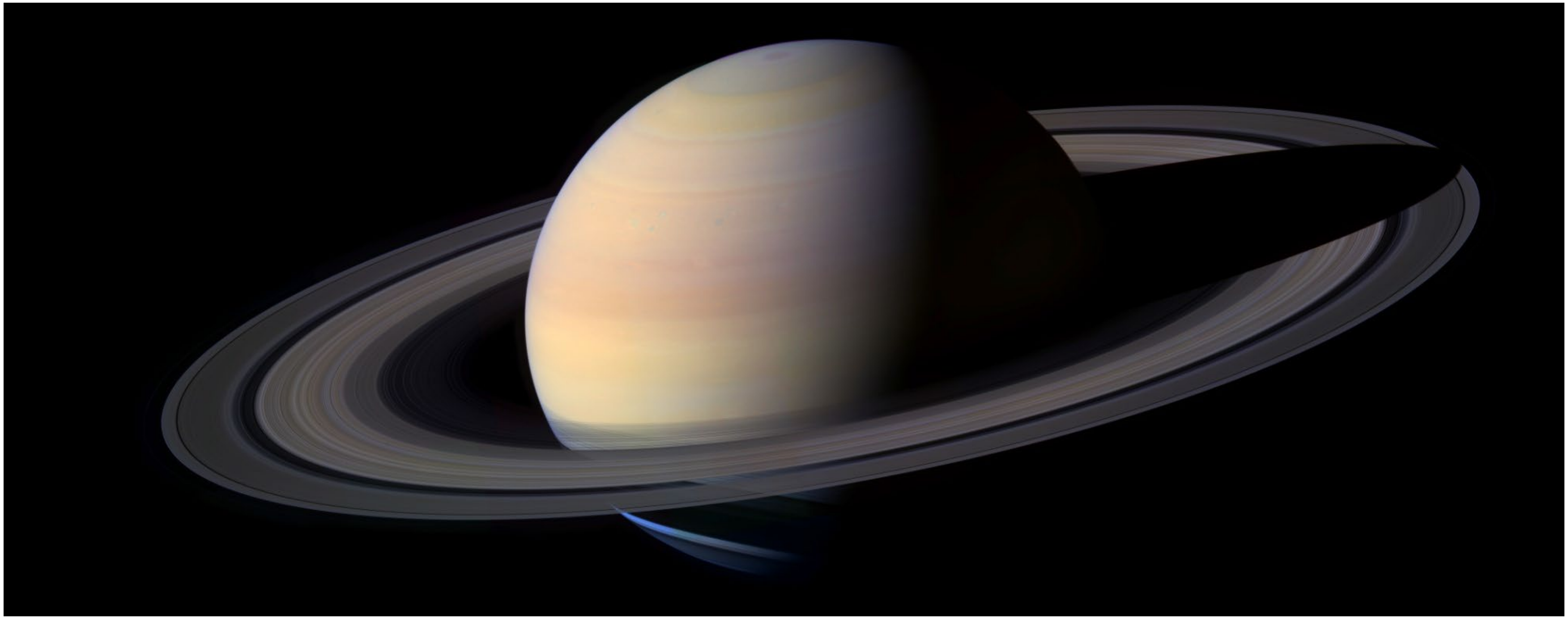
Bits can change during storage or reading from the disk



ECC Memory

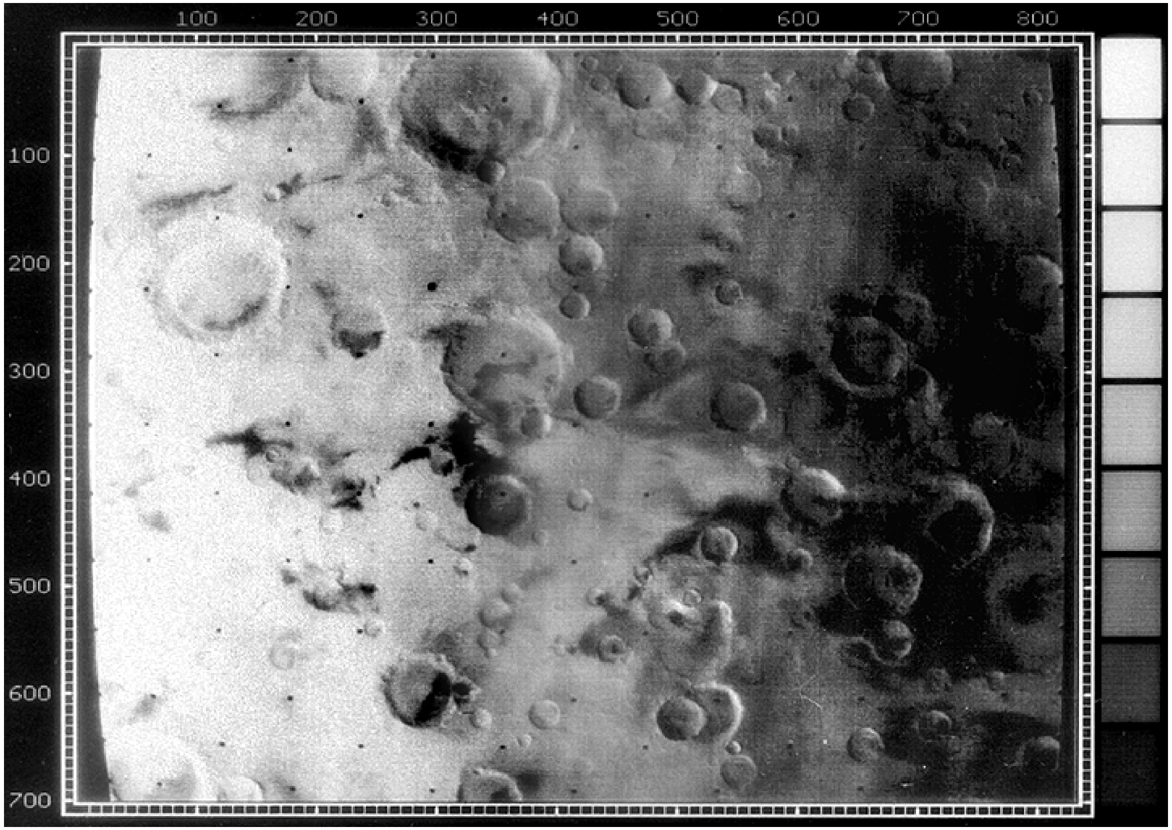
UPGRADE LIKE A PRO
WWW.MEMORYUPGRADE.PRO
PRO
MEMORYUPGRADE
■ 1GB
■ 184-PIN
■ Registered
SPECS
4GB DDR 184-PIN ECC Registered 4x1GB Kit

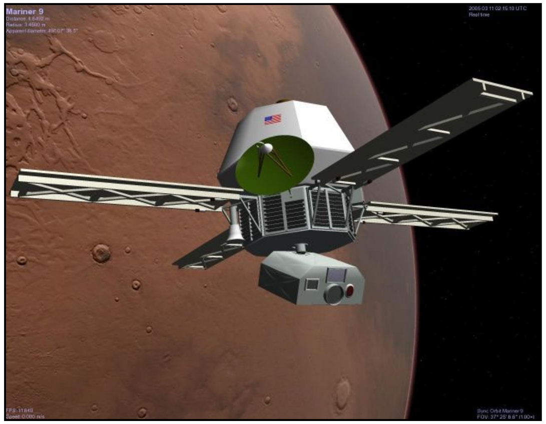
Deep Space Communications



1971: Mariner 9

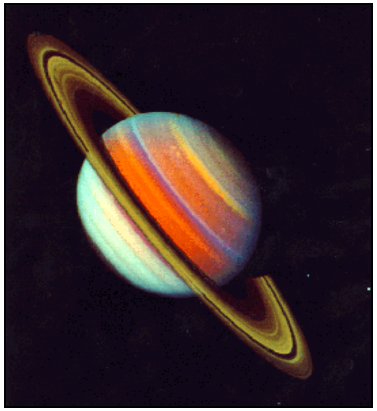
Mariner 9 used a (32,6,16) *Reed-Muller* code to transmit its grey images of Mars.

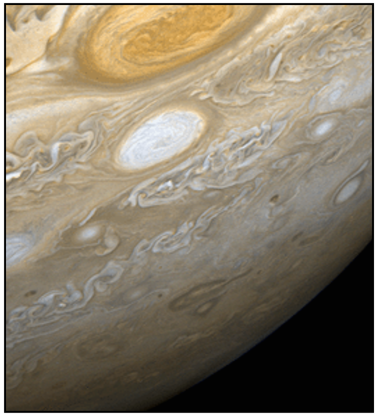




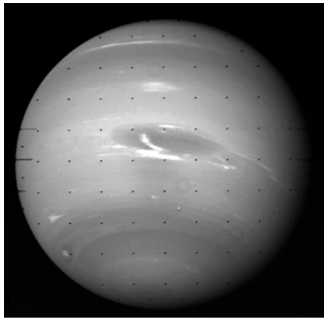
1979+: Voyager I and II

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





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

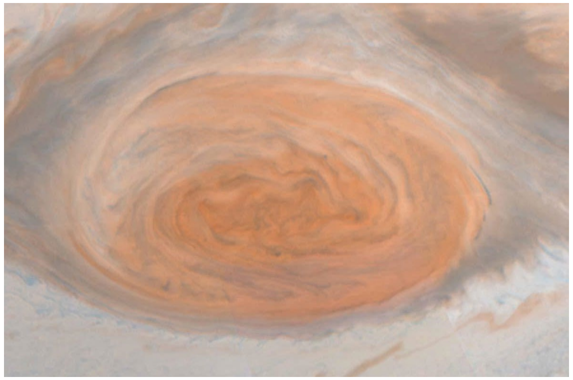


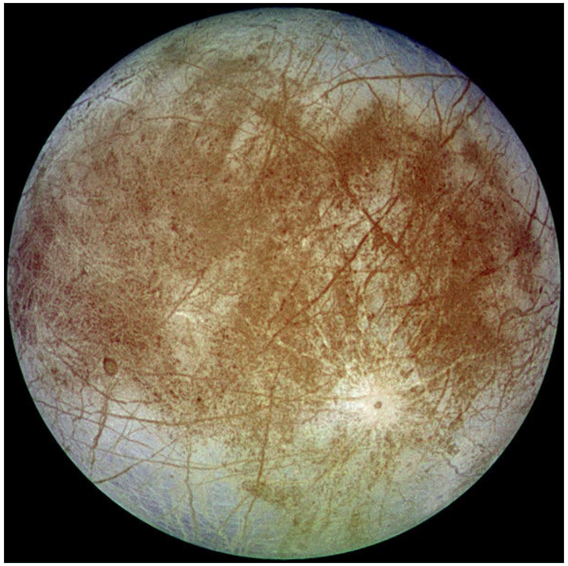
1989: Galileo

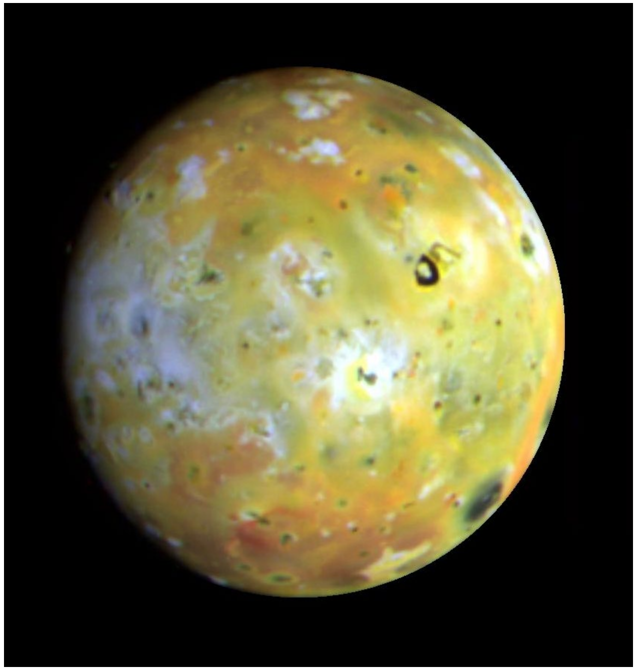
Concatenated *Convolutional* and *Reed-Solomon* codes were used to transmit images of Jupiter and its moons.

Io, Jupiter, Ida

and Europa

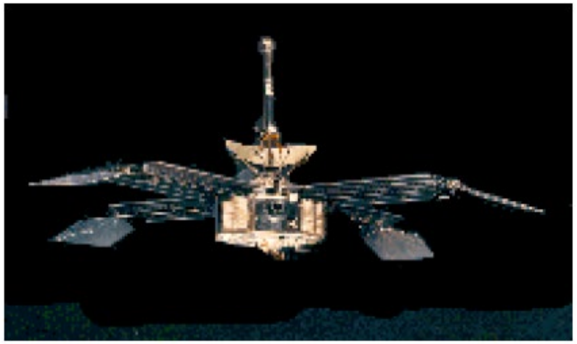






Mars Space Communications

1965 Mariner 4

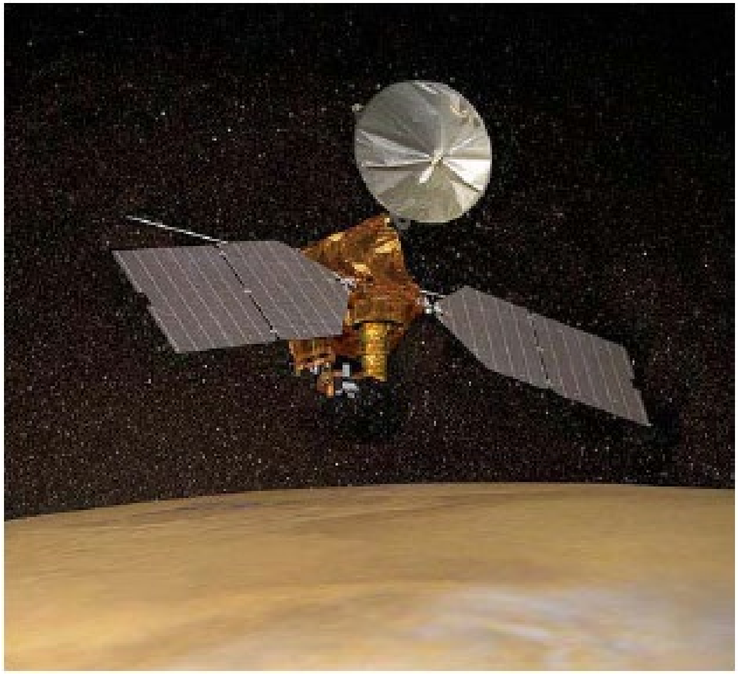


Frequency: 2.3 GHz (S Band)
Data Rate: 8.33 bps
Repetition code (2 x)

2004 Mars Exploration Rover

Frequency: 8.4 GHz (X Band)
Data Rate: 168 kbps
RS/Convolutional Concatenated Code

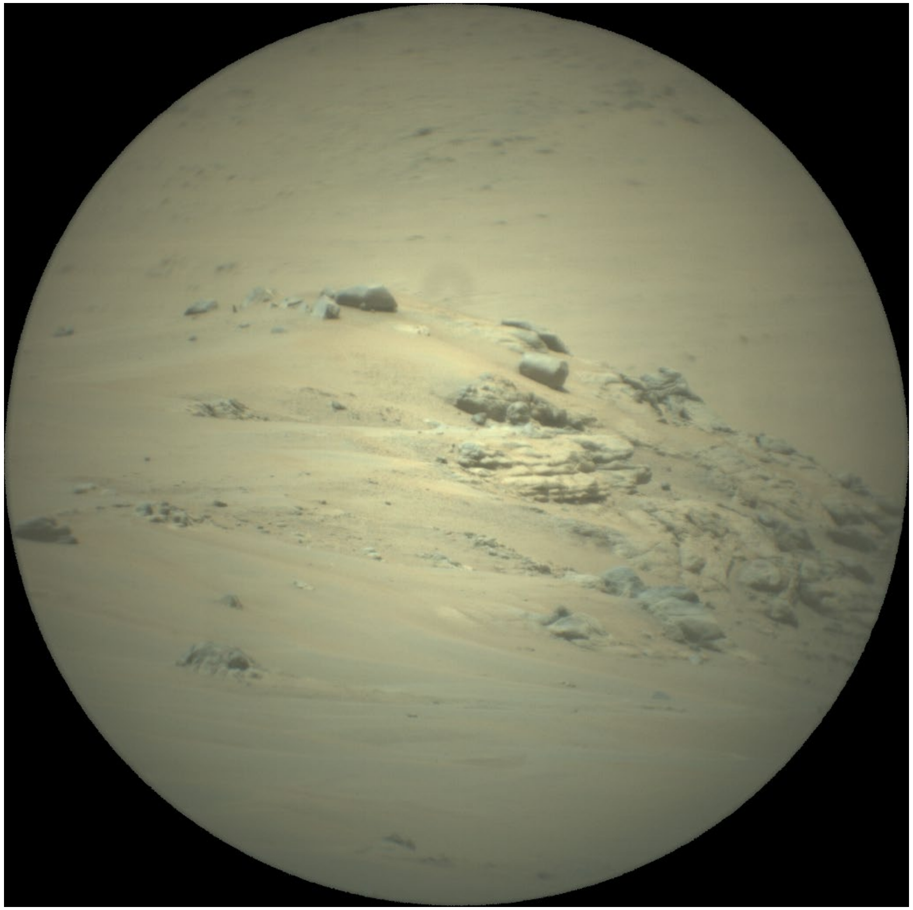
2006 Mars Reconnaissance Orbiter



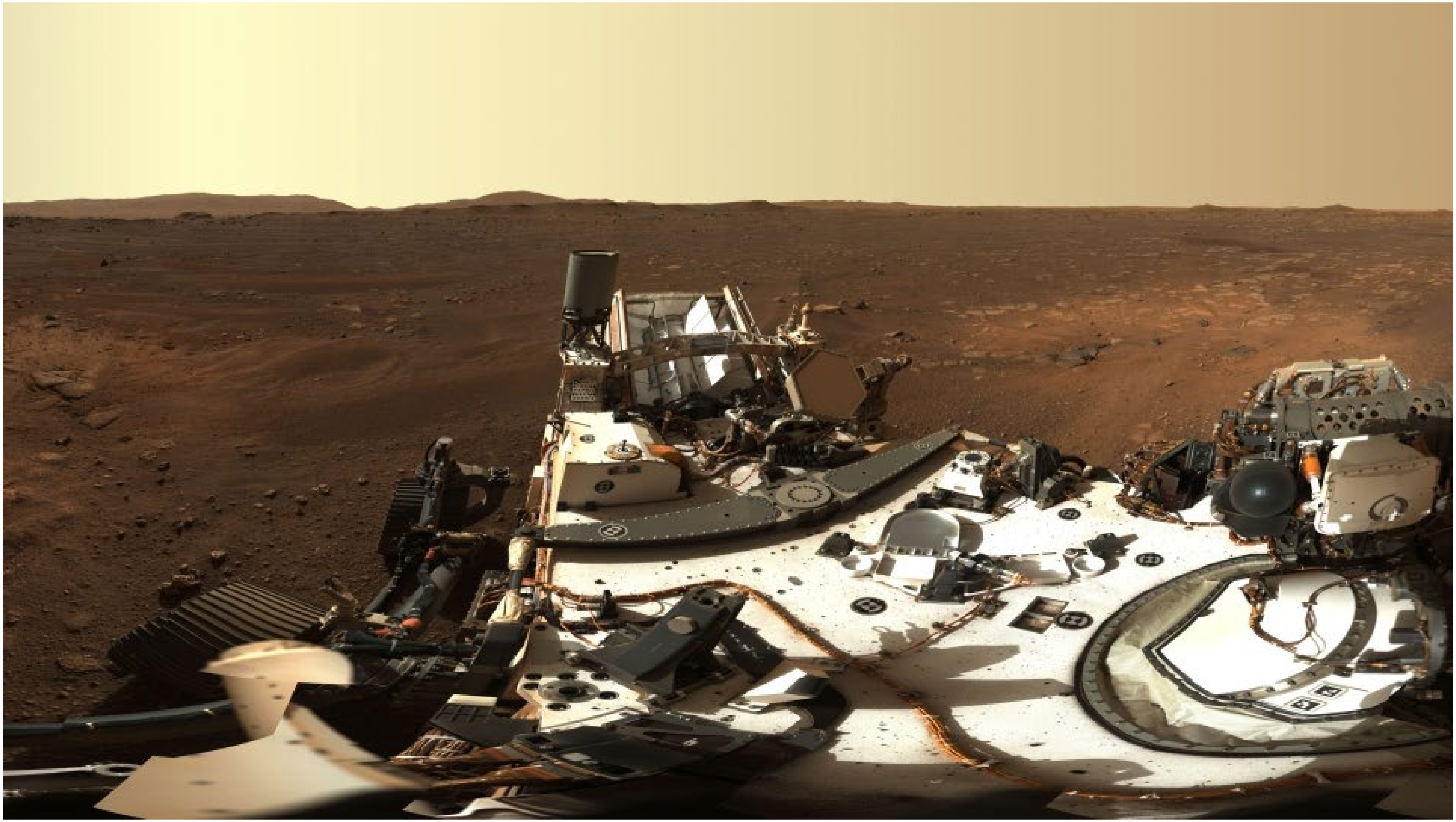
Frequency: 8.4 GHz (X Band)
Data Rate: 12 Mbps
(8920,1/6) Turbo Code
Distance: 2.15 x 10^8 km

2020 Mars Rover

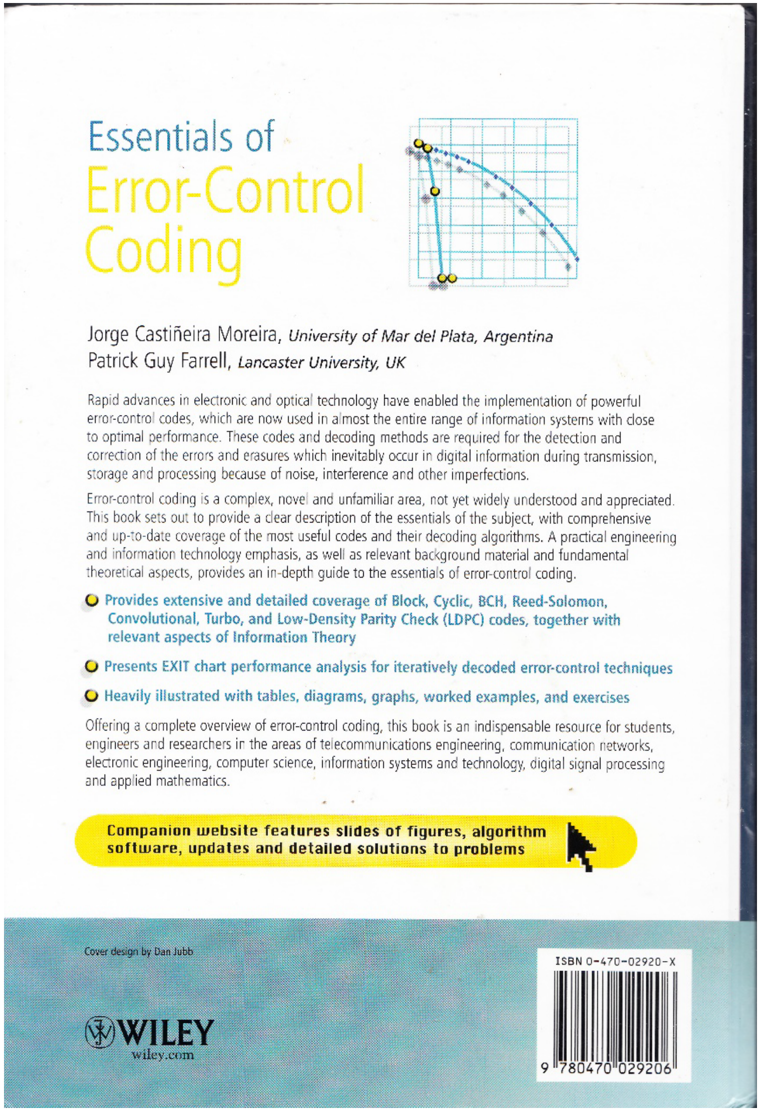
- Frequency: 400 MHz (UHF)
- Data Rate: 2 Mbps
- (1784, 1/2) Turbo Code



Mars Rover 2021



ISBN Codes



Essentials of Error-Control Coding

Jorge Castiñeira Moreira, *University of Mar del Plata, Argentina*
Patrick Guy Farrell, *Lancaster University, UK*

Rapid advances in electronic and optical technology have enabled the implementation of powerful error-control codes, which are now used in almost the entire range of information systems with close to optimal performance. These codes and decoding methods are required for the detection and correction of the errors and erasures which inevitably occur in digital information during transmission, storage and processing because of noise, interference and other imperfections.

Error-control coding is a complex, novel and unfamiliar area, not yet widely understood and appreciated. This book sets out to provide a clear description of the essentials of the subject, with comprehensive and up-to-date coverage of the most useful codes and their decoding algorithms. A practical engineering and information technology emphasis, as well as relevant background material and fundamental theoretical aspects, provides an in-depth guide to the essentials of error-control coding.

- Provides extensive and detailed coverage of Block, Cyclic, BCH, Reed-Solomon, Convolutional, Turbo, and Low-Density Parity Check (LDPC) codes, together with relevant aspects of Information Theory
- Presents EXIT chart performance analysis for iteratively decoded error-control techniques
- Heavily illustrated with tables, diagrams, graphs, worked examples, and exercises

Offering a complete overview of error-control coding, this book is an indispensable resource for students, engineers and researchers in the areas of telecommunications engineering, communication networks, electronic engineering, computer science, information systems and technology, digital signal processing and applied mathematics.

Companion website features slides of figures, algorithm software, updates and detailed solutions to problems

Cover design by Dan Jubb

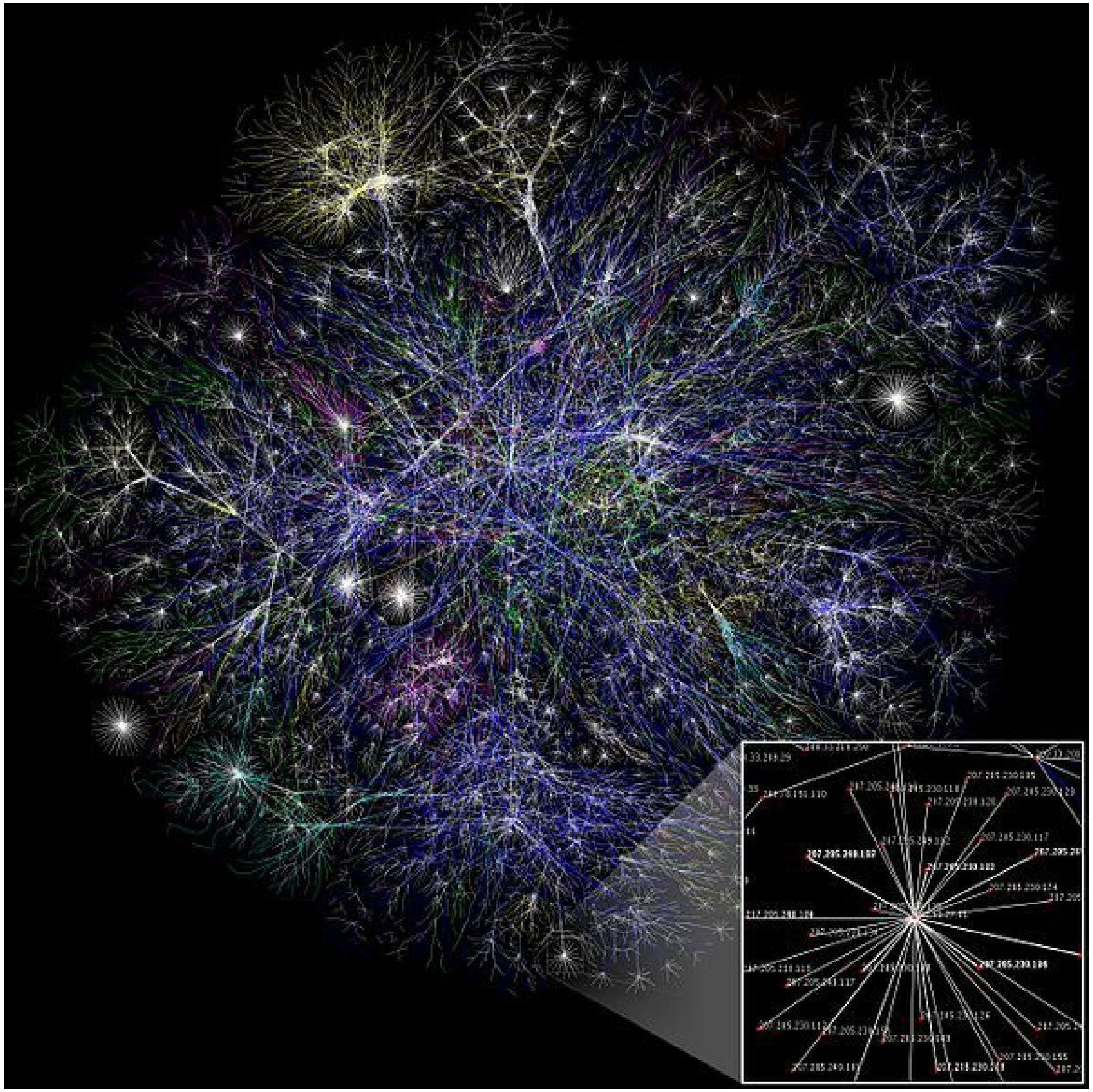
WILEY
wiley.com

ISBN 0-470-02920-X

9 780470 029206

Internet

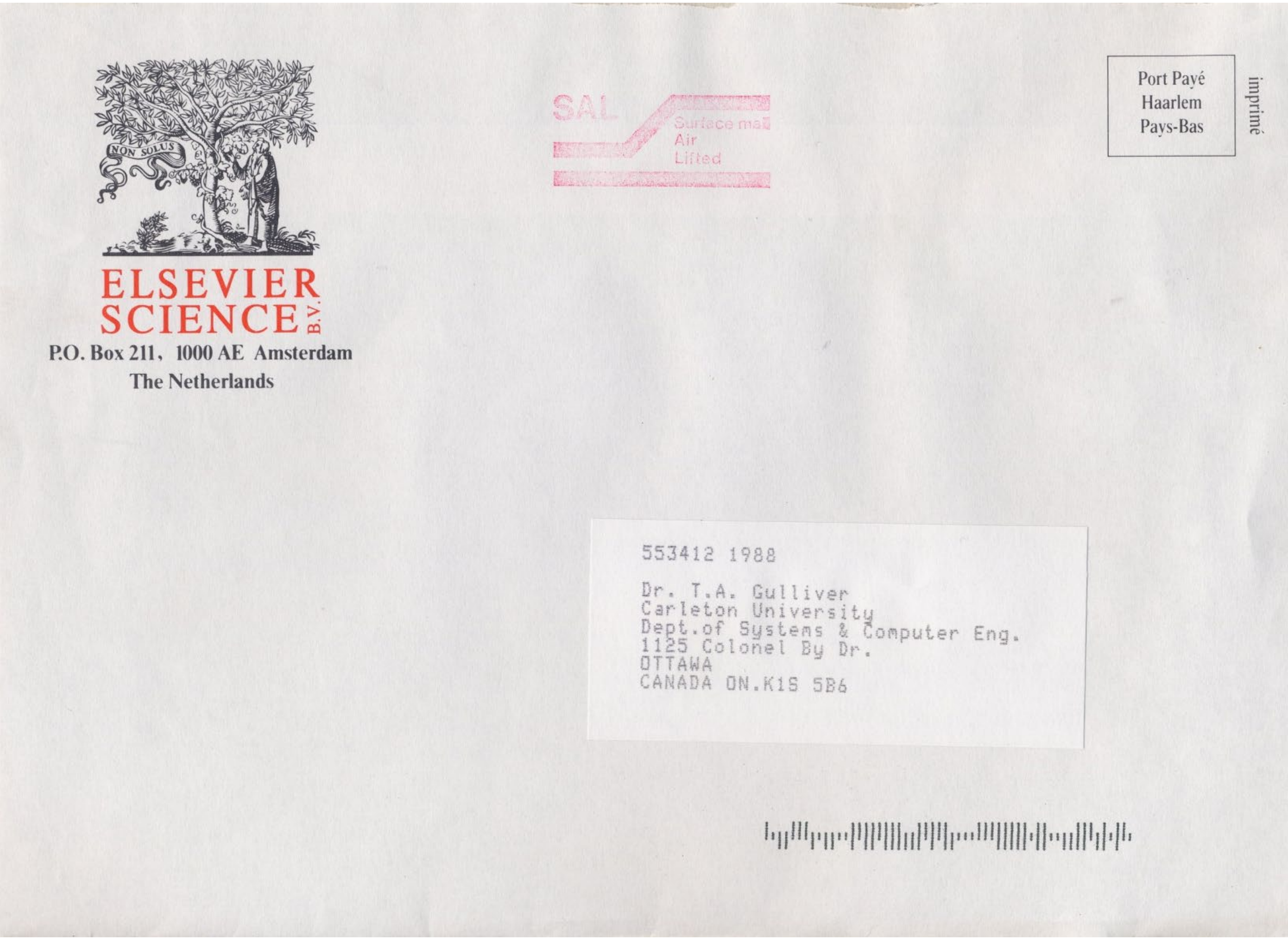
Checksums are used by the standard Internet protocols IP, UDP, and TCP.



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

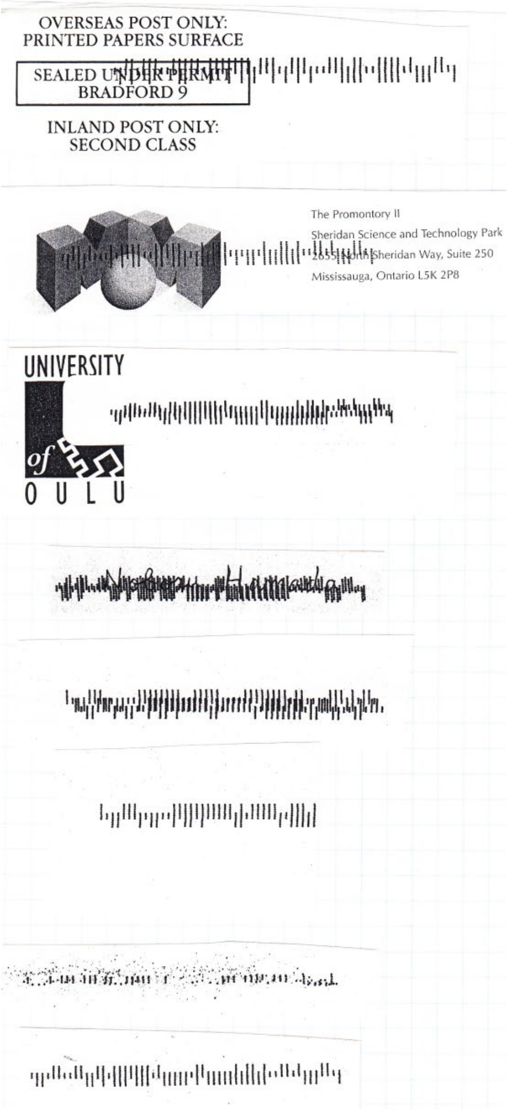
Port Payé
Haarlem
Pays-Bas

imprimé

553412 1988

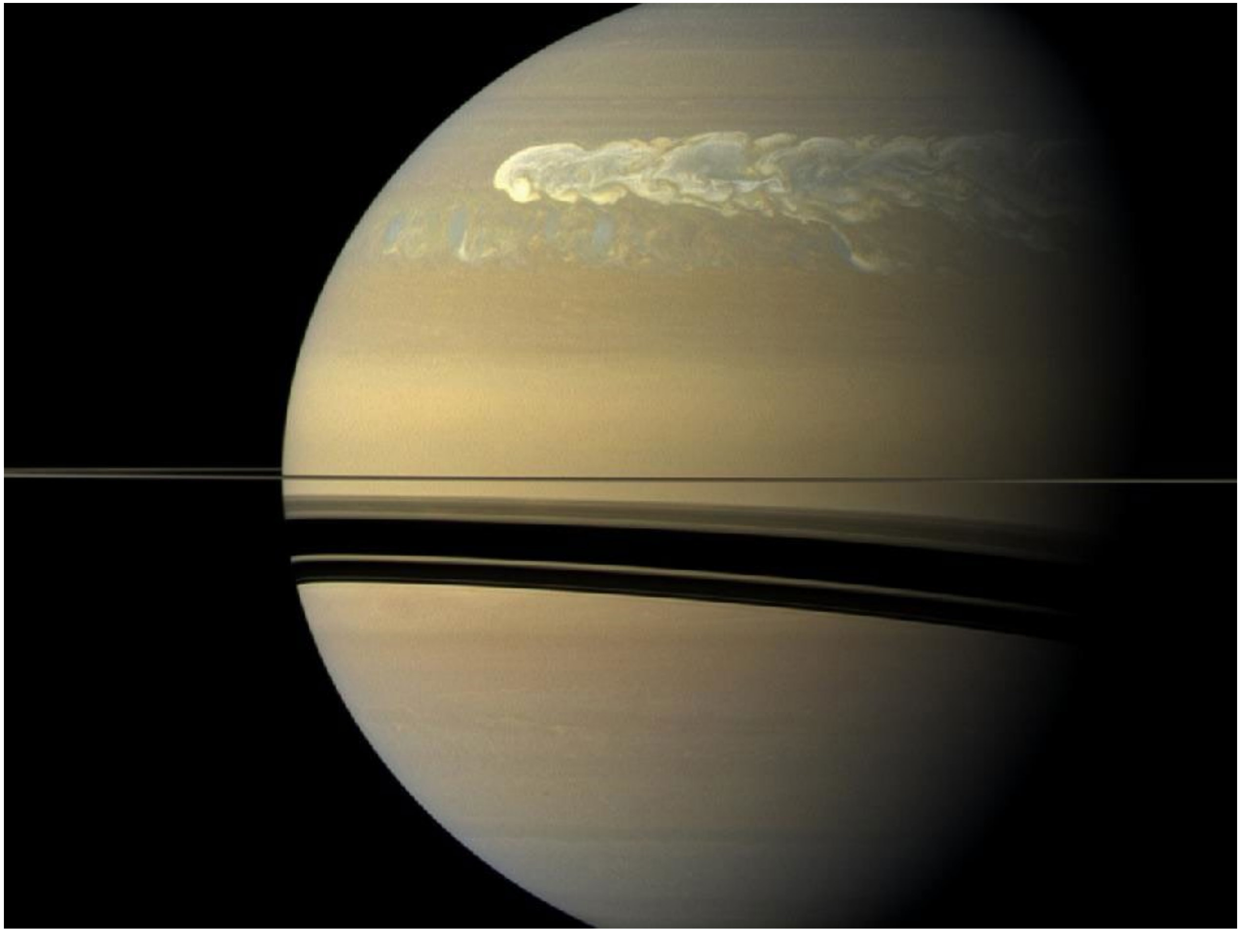
Dr. T.A. Gulliver
Carleton University
Dept.of Systems & Computer Eng.
1125 Colonel By Dr.
OTTAWA
CANADA ON.K1S 5B6

Bar Code Errors



Cassini-Huygens

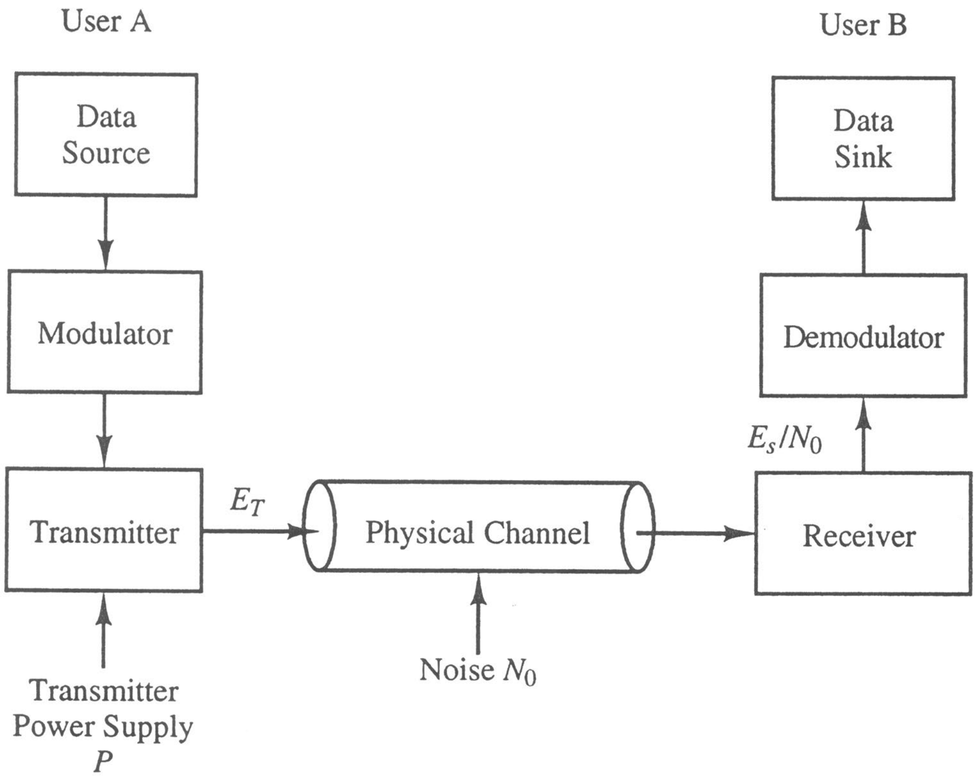
Storm on Saturn July 2011 (Turbo Code)



Communication Systems

- Allow the electronic exchange of voice, data, video, music, multimedia, email, web pages, Twitter, FaceTime, TikTok, ...
- Older communication systems include
  - Radio and TV broadcasting, Public Switched Telephone Network (voice, fax, modem)
- Modern communication systems include
  - Cellular telephone systems (4G, 5G, 6G)
  - Computer networks (LANs, WANs, internet)
  - Satellite systems (phones, voice/data, television)
  - Bluetooth
  - WiFi
  - Sensor and vehicular networks

Digital Communication System



Modulator/Transmitter

- Matches the data to the channel
- Modulation maps the data symbols to the amplitude, phase 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 transmitted signal
- The demodulator extracts the data from the receiver output
    - Converts the receiver output to data symbols (typically bits)

Channel

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

Communications System Design Goals

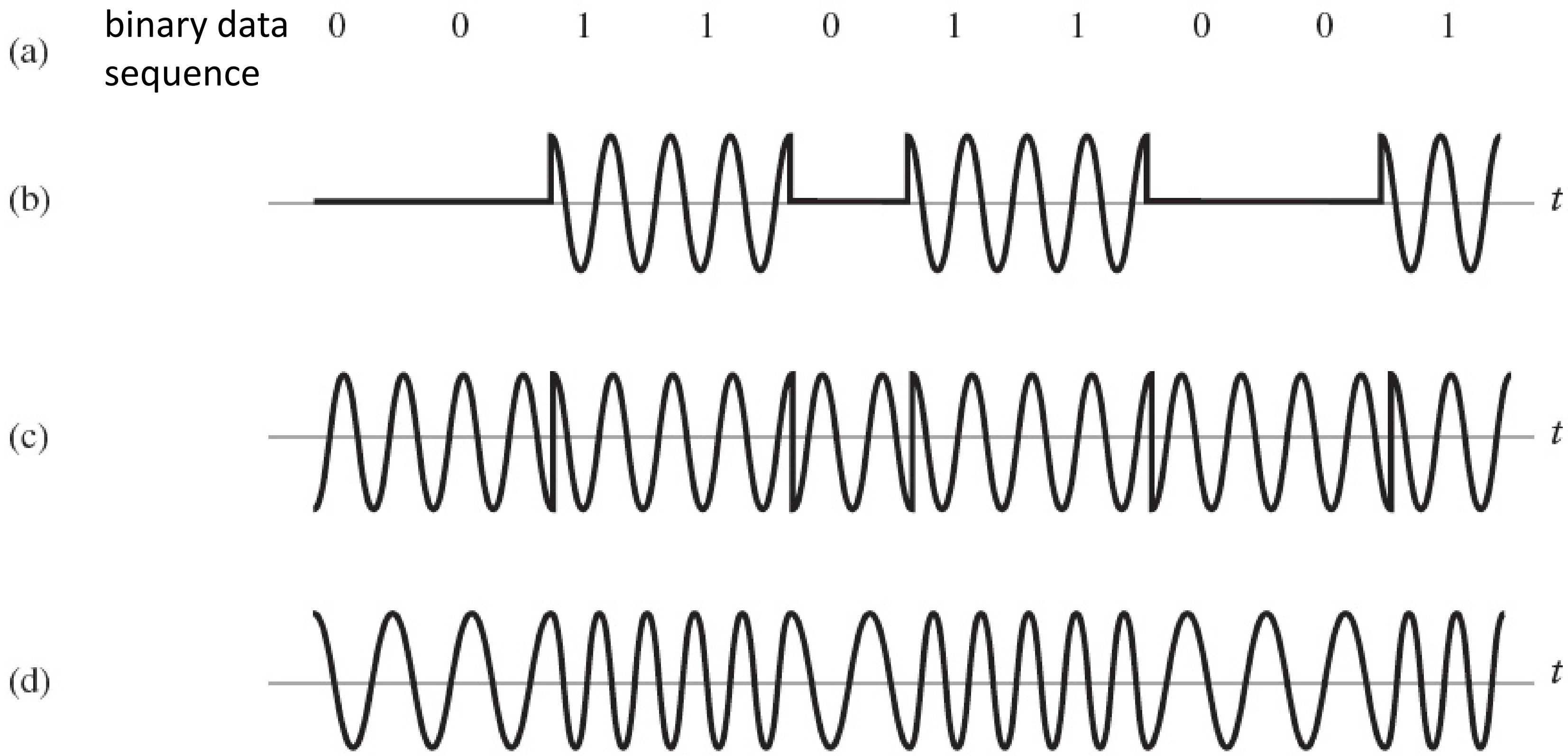
- Maximize the data rate
- Minimize the bit error rate (BER)
- Minimize the required signal-to-noise ratio (SNR)
- Minimize the required bandwidth
- Minimize the system complexity and cost

- These are conflicting goals

System Constraints

- Available bandwidth
- Maximum error rate
- Power limitations
- Government regulations
- Technological limitations

Three Basic Forms of Signalling



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

Binary Modulation

- BPSK

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

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

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

- BFSK

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

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

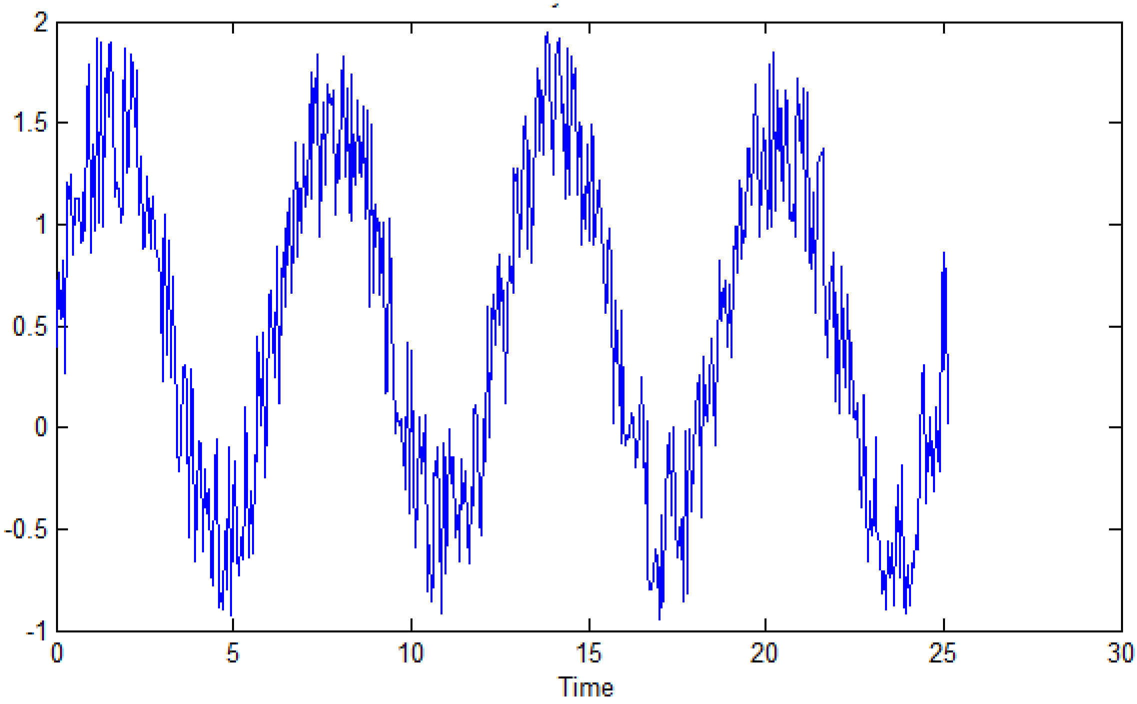
Binary Modulation

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

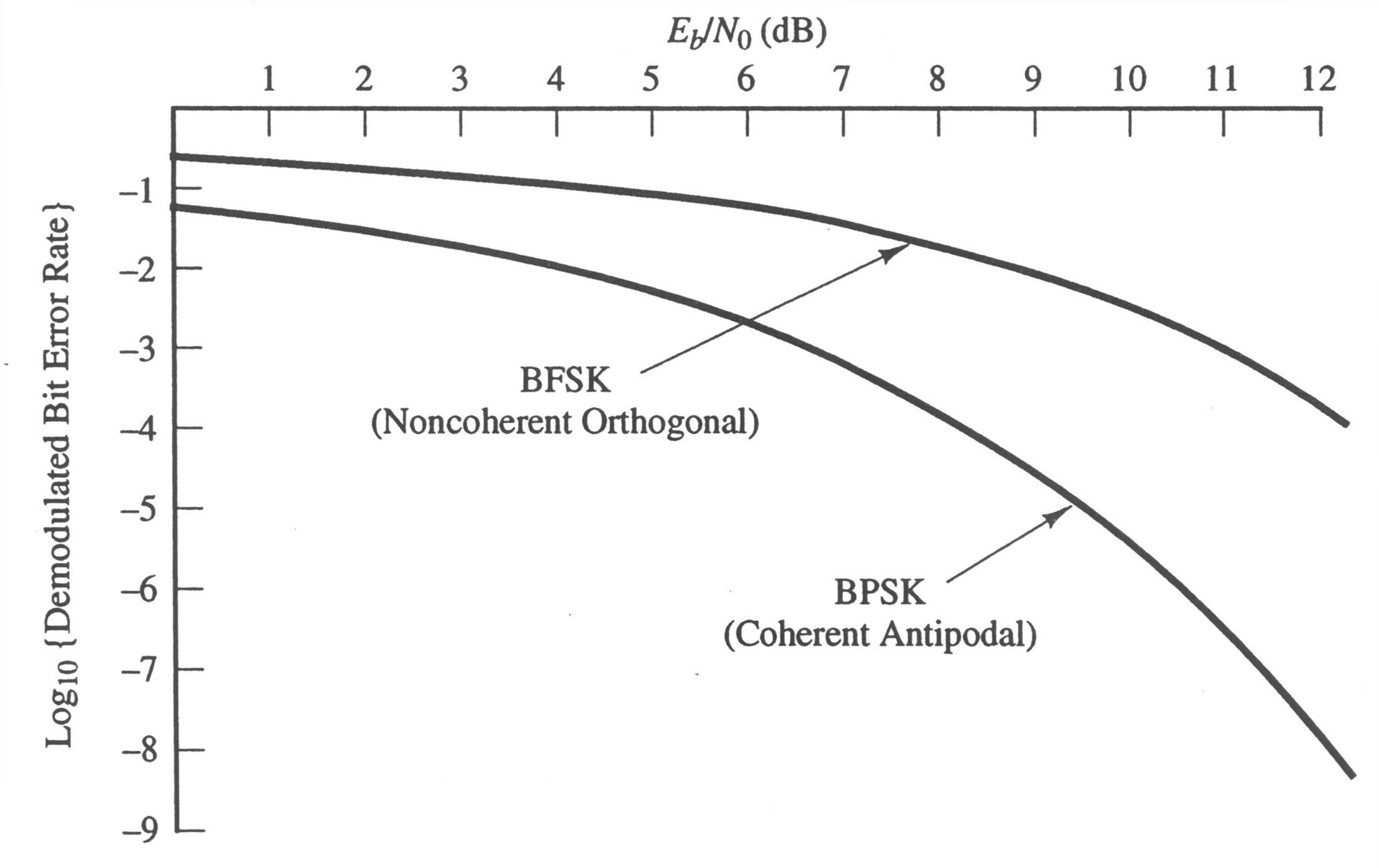
- Power levels are generally expressed in decibels (dB)
  - $P_{\mathrm{dB}} = 10\log_{10} P_{\mathrm{watts}}$

- 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



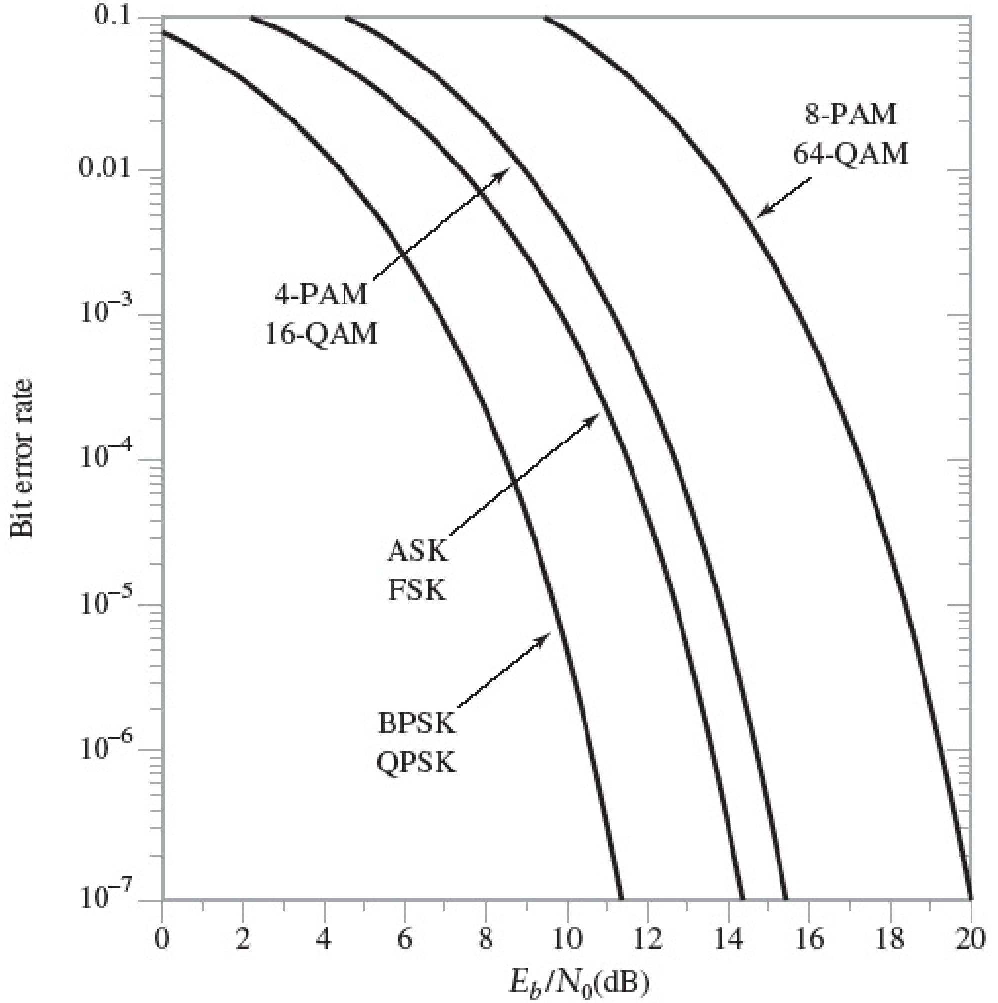
Performance of BPSK and BFSK in AWGN



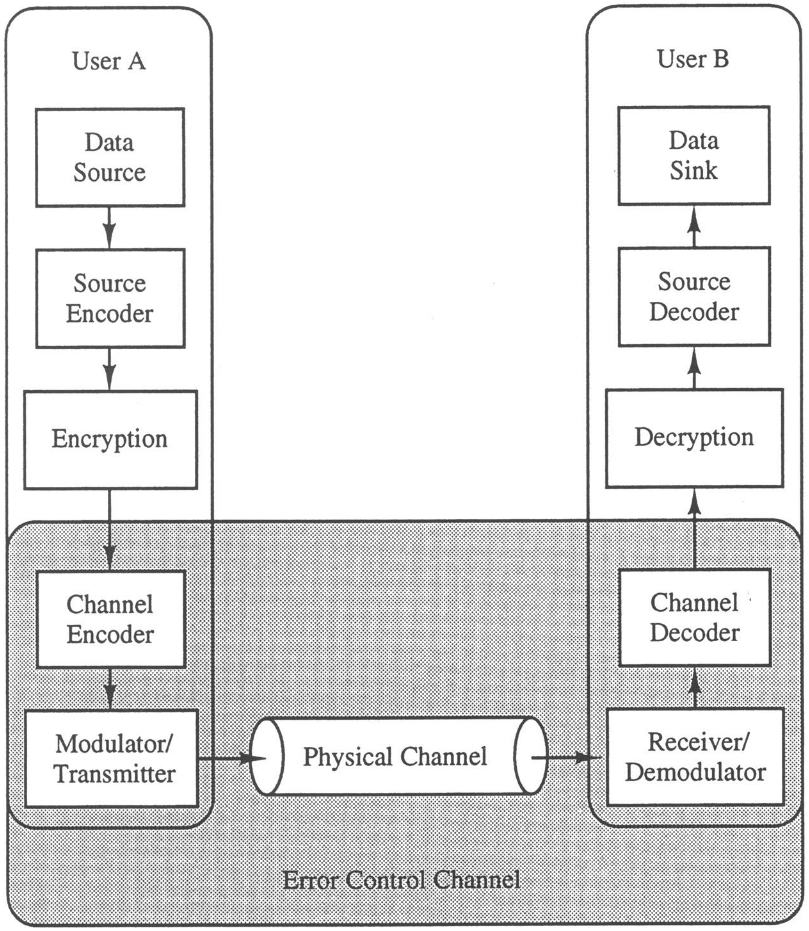
M-ary Modulation

- A group of *n* bits is transmitted in each signaling interval $T=\log_2(M)T_b$
- In MASK a group of *n* bits is transmitted using $M=2^n$ different amplitudes
- In MPSK a group of *n* bits is transmitted using $M=2^n$ different phases
- In MFSK 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



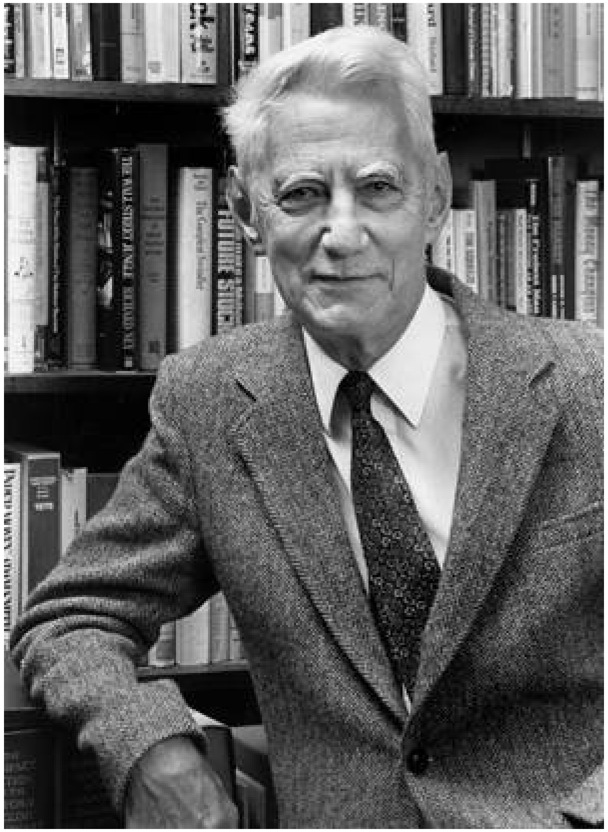
Digital Communication System with Coding



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?
  - There exist **error control codes** such that information can be transmitted through the channel at rates less than *C* with arbitrarily low bit error rate.
- There are only two factors that determine the capacity of a channel
  - – Bandwidth (*W*)
  - – Signal-to-noise ratio (SNR) E_b/N_0

AWGN Channel Capacity

$$C = W\log_2\left(1 + \frac{P}{N_0W}\right)$$

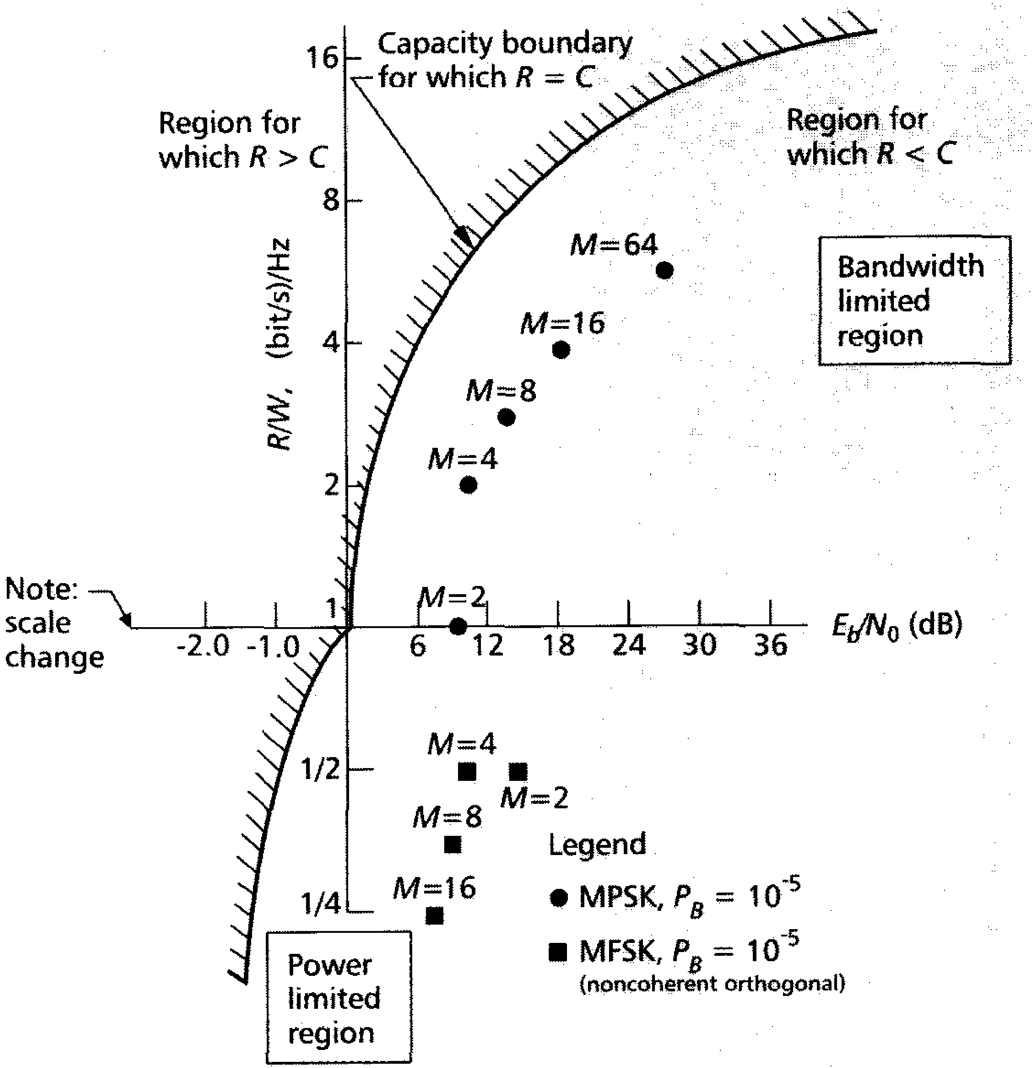
$$E = PT \rightarrow P = E_bR_b$$

$$C = W\log_2\left(1 + \frac{E_bR_b}{N_0W}\right)$$

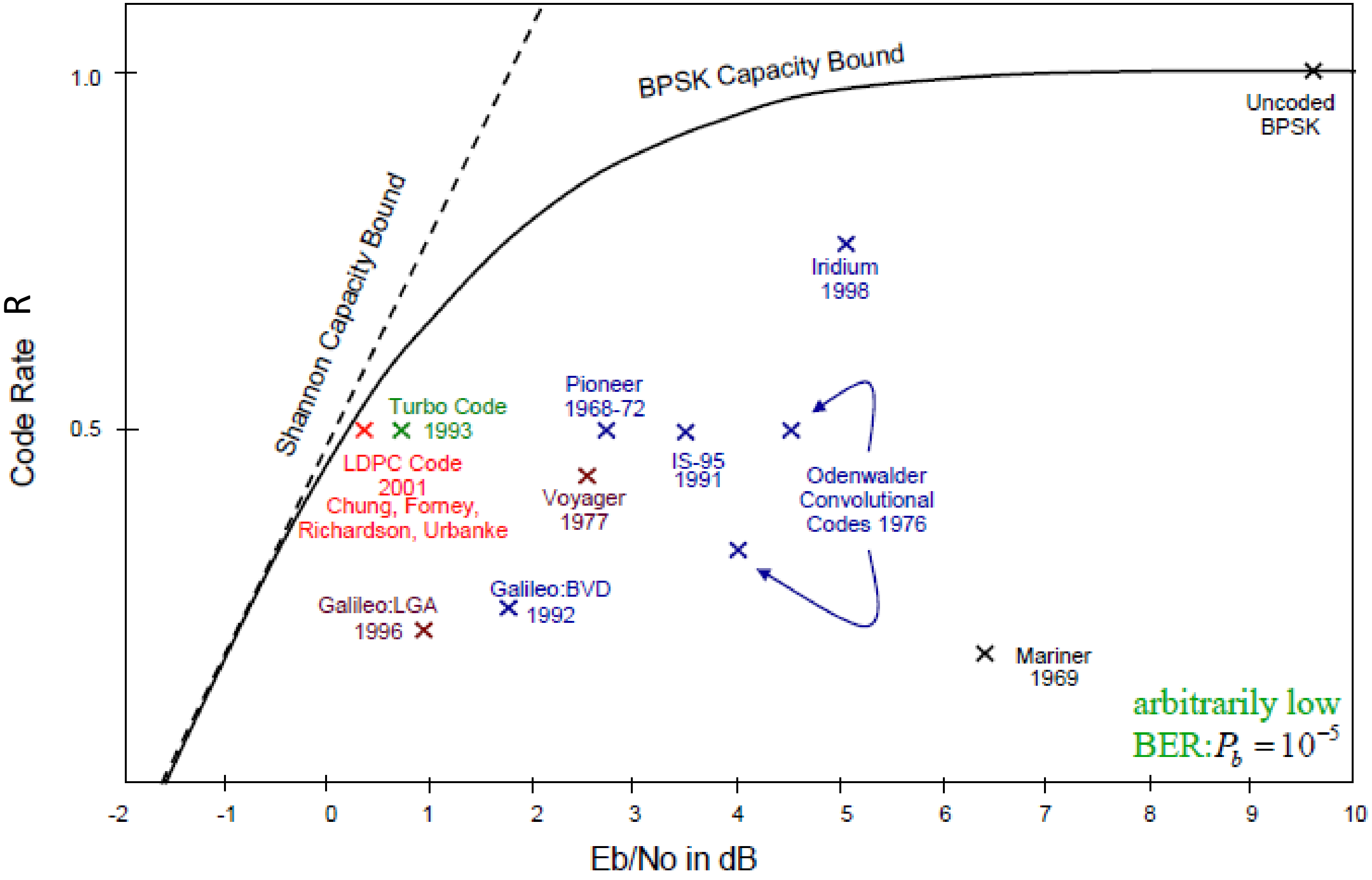
Let $R_b = C$ $$\frac{R_b}{W} = \log_2\left(1 + \frac{E_b}{N_0}\frac{R_b}{W}\right)$$

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

Bandwidth Efficiency (R/W) versus SNR



Efficiency of Binary Codes



State-of-the-Art

- Approaching capacity
  - Long, random-like codes with some structure
  - Practical, near-optimal decoding algorithms with reasonable computational complexity
- 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.

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	Codewords
E = 1000101	**c** = 10001011
G = 1000111	**c** = 10001110

- Received word

  r = 10001010

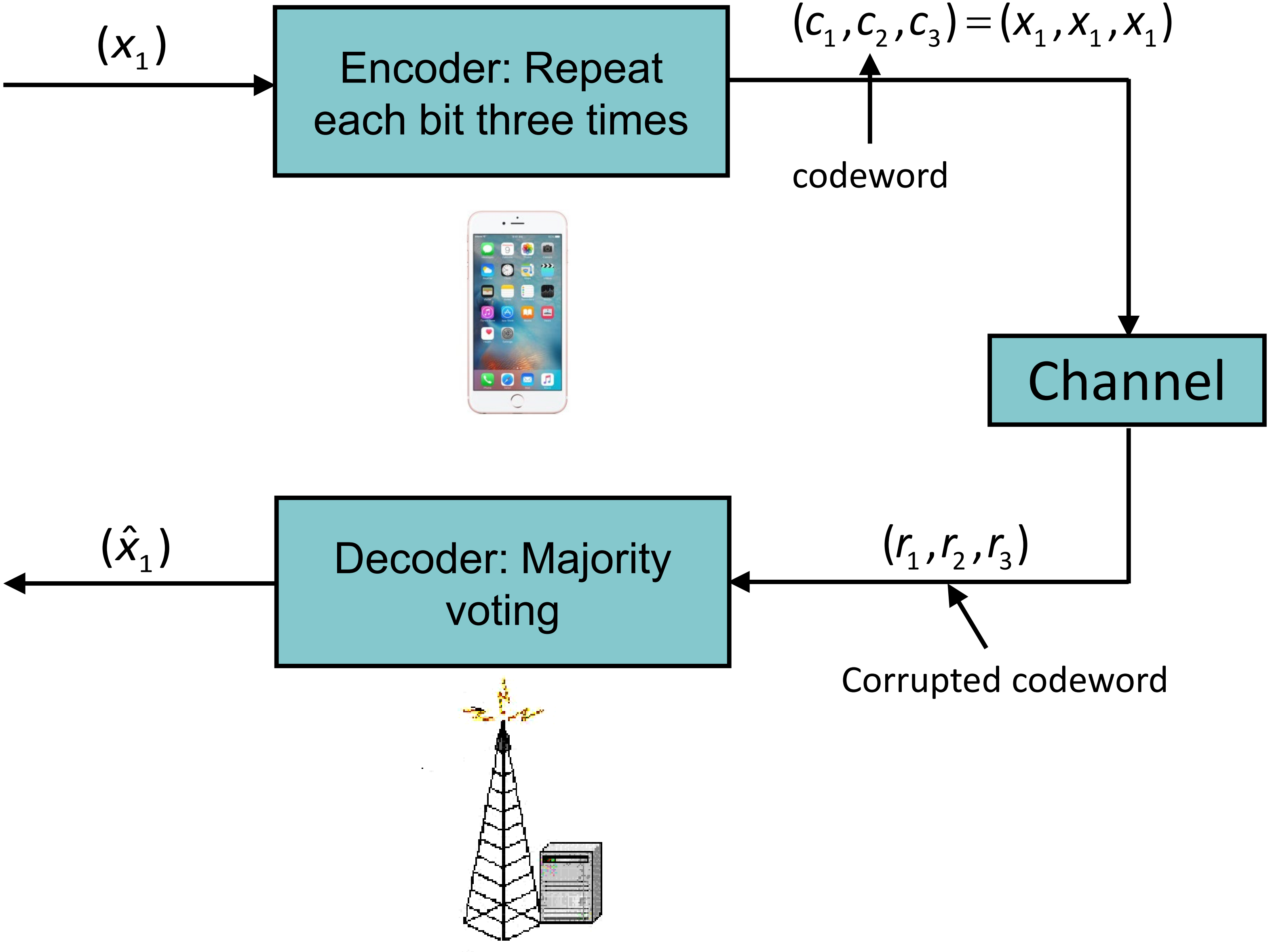
Triple Repetition Code – Example 2

	Codewords
m = 0	**c** = 000
m = 1	**c** = 111

Received word

r = 100

Triple Repetition Code



(x_1)

Encoder: Repeat each bit three times

$(c_1, c_2, c_3) = (x_1, x_1, x_1)$

codeword

Channel

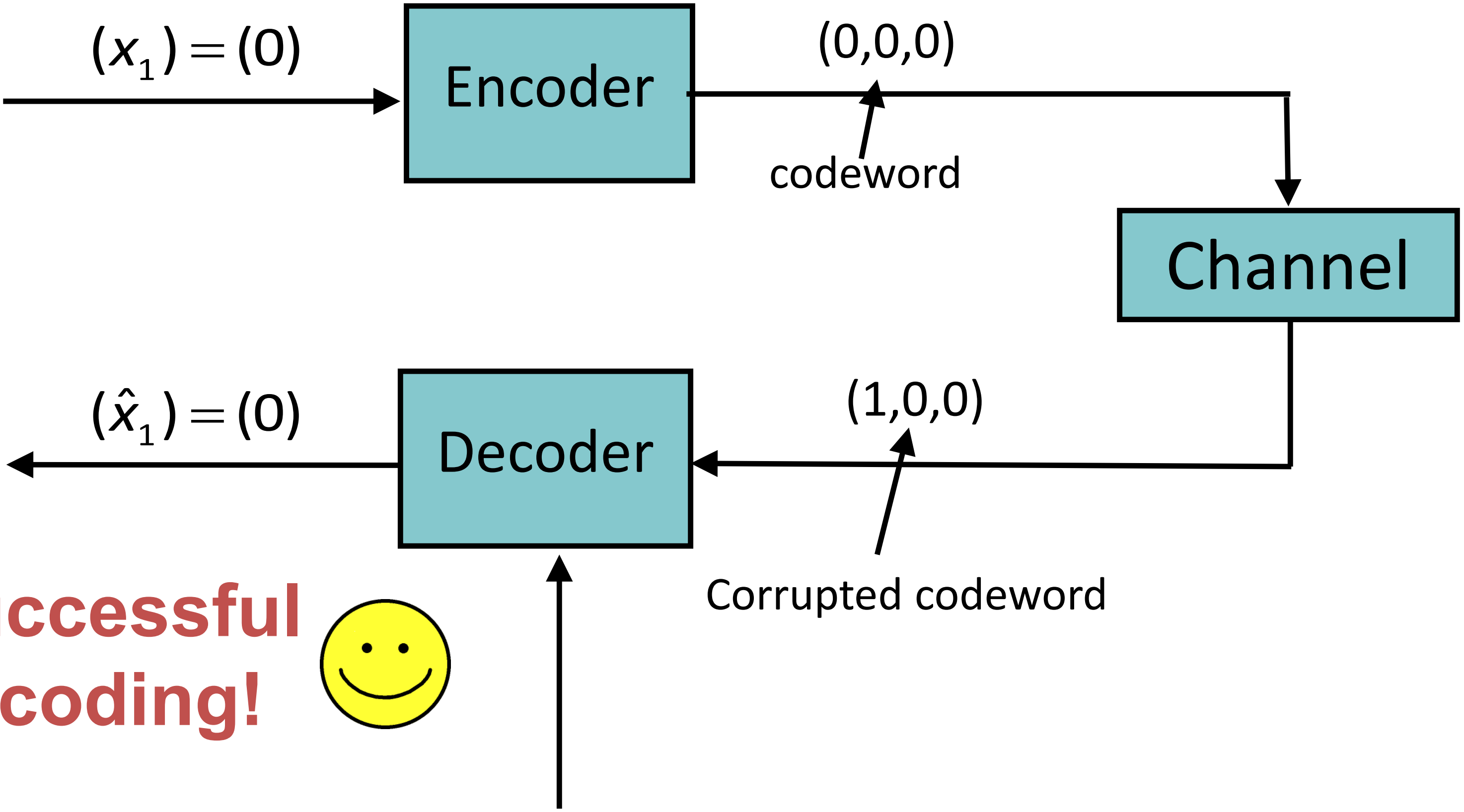
(r_1, r_2, r_3)

Corrupted codeword

Decoder: Majority voting

$(\hat{x}_1)$

Triple Repetition Code (Cont.)



Successful decoding!

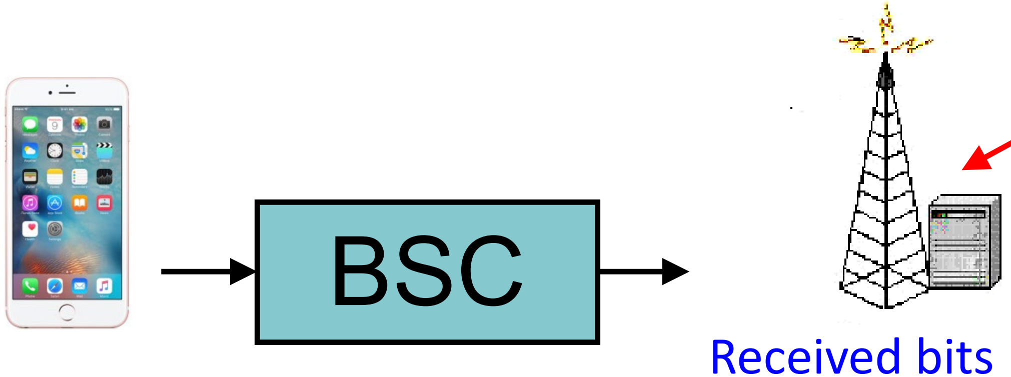
Decoding: Majority voting

Triple Repetition Code – Decoding

Received Word **r**			Codeword **c**			Error Pattern **e**		
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

Transmission Errors

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



Sender

Receiver

BSC

Transmitted bits

10010…10101…

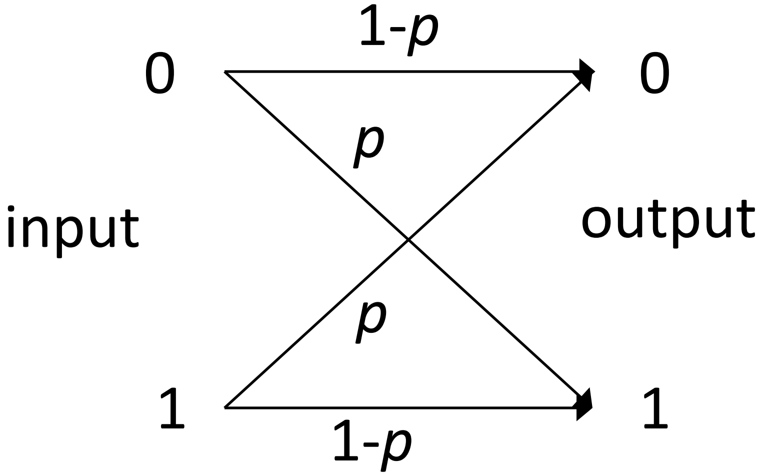
Received bits

10110…00101…

Each bit is flipped (in error) 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

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

- The probability of exactly *m* errors is

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

- The probability of *m* or more errors is

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

Triple Repetition Code 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

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

- If p = 0.01, then $P(E)$ = 0.000298 and only one word in 3356 will be in error after decoding.
- A reduction by a factor of 33.

- For the coded system

$$\hat{T}_b = T_b R$$

$$R = \frac{1}{3}$$ is called the CODE RATE

$$E_b = PT_b$$

$$\hat{E}_b = P\hat{T}_b = PT_b R = E_b R = E_b \frac{1}{3}$$

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.)

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

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

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

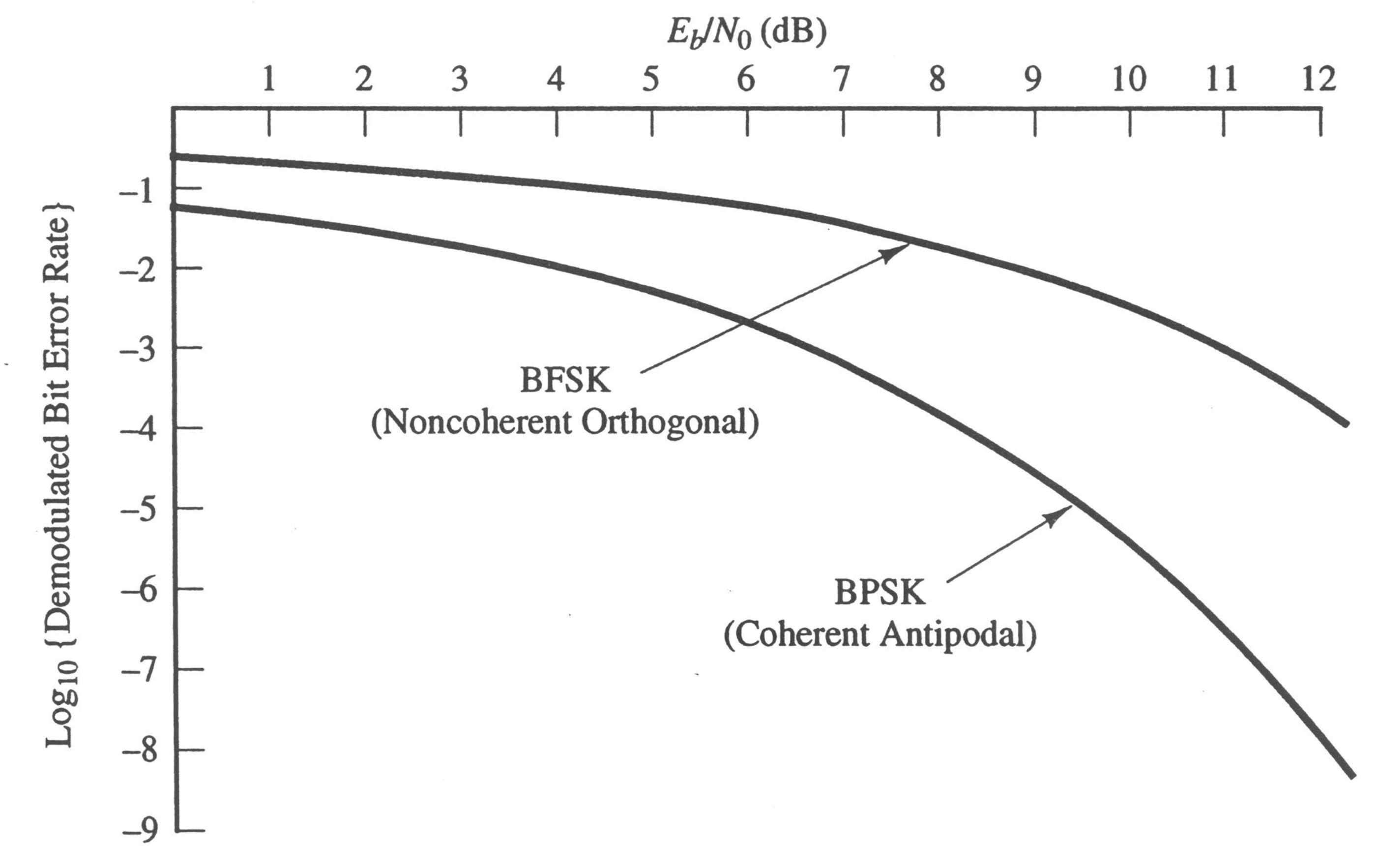
$$P(E) = 5.5 \times 10^{-4}$$

Bit Error Rate Approximation

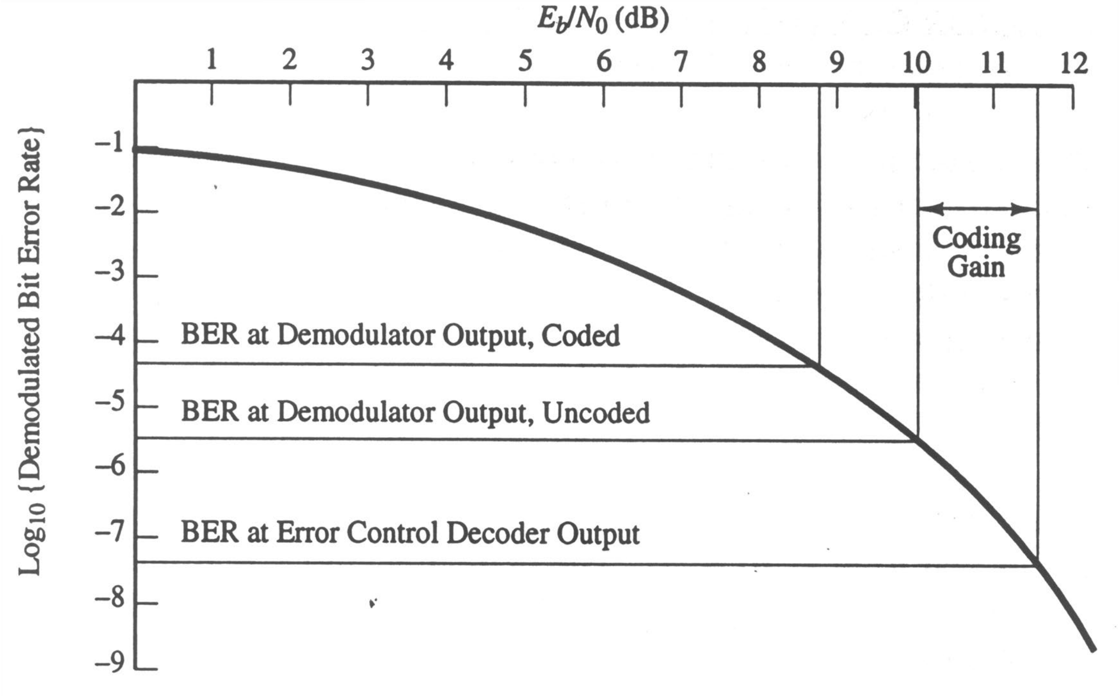
- *P*(*E*) is the probability of a codeword being in error
- For a *t* error correcting code, it can be assumed that *t*+1 errors have occurred
- The worst case is that decoding introduces *t* additional errors
- Thus there are 2*t*+1 errors in the codeword so the Bit Error Rate (BER) can be approximated as

$$\frac{2t+1}{n}P(E)$$

Performance of BPSK and BFSK



Coding Gain with the (15,11) Hamming Code and BPSK



The Fundamental Tradeoff

- Correct as many errors as possible while using as little redundancy as possible
- These are contradictory goals

Constructing Good Codes

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

- Problem:

  randomness + large block length + decoding computations=

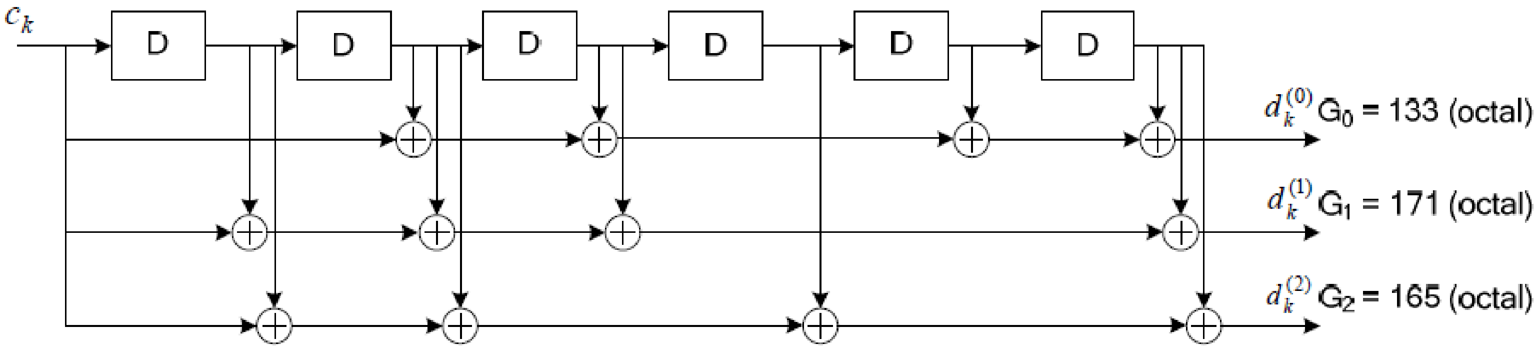
  = COMPLEXITY

- Thus some structure is required

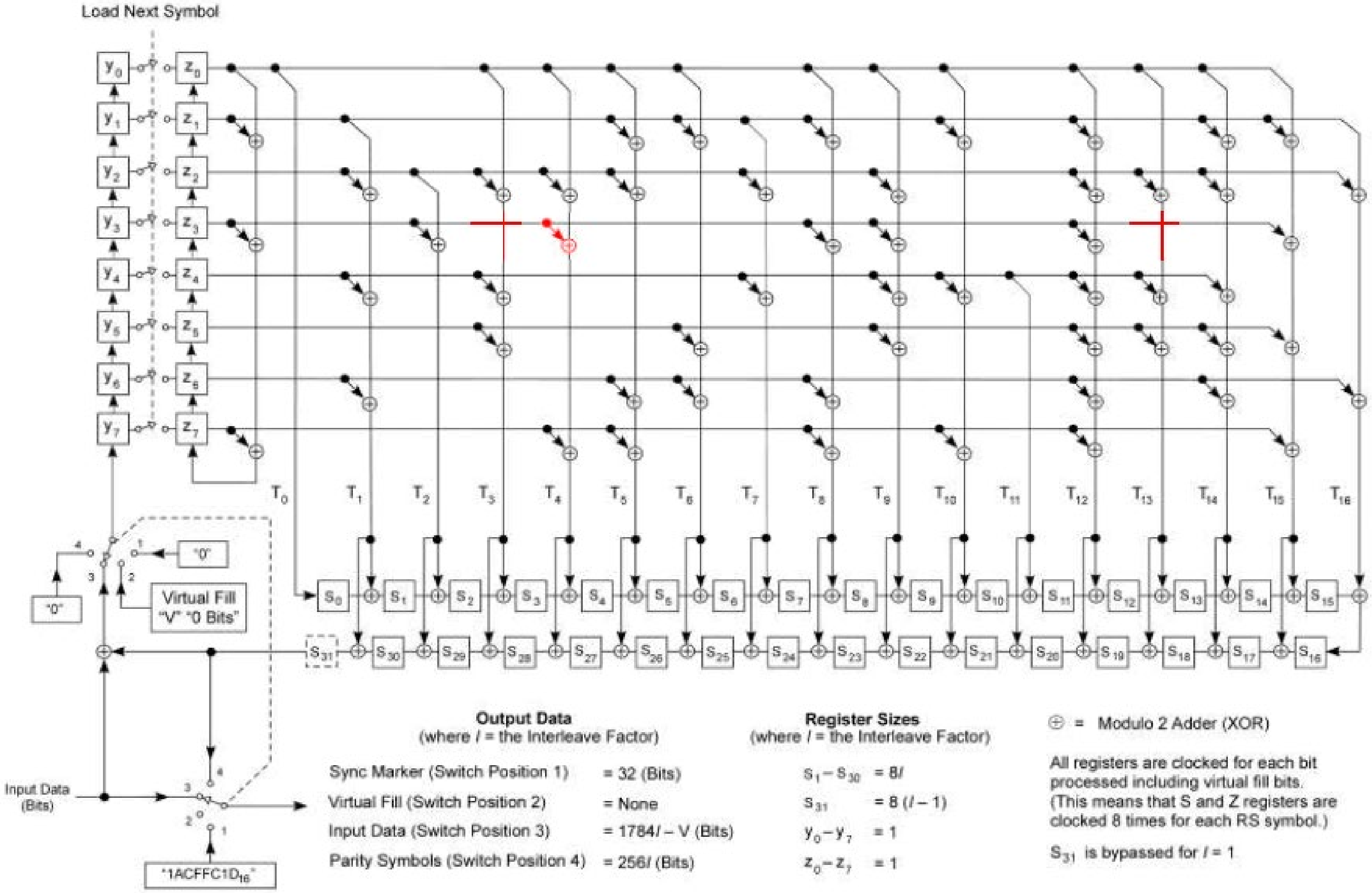
ETSI TS 136 212 V8.4.0 (2008-11) Technical Specification

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

Rate 1/3 Convolutional Encoder


c_k
D
D
D
D
D
D
$d_k^{(0)}$ G_0 = 133 (octal)
$d_k^{(1)}$ G_1 = 171 (octal)
$d_k^{(2)}$ G_2 = 165 (octal)

CCSDS (255,223) Reed–Solomon Encoder



Output Data
(where I = the Interleave Factor)

Sync Marker (Switch Position 1)	= 32 (Bits)
Virtual Fill (Switch Position 2)	= None
Input Data (Switch Position 3)	= 1784I – V (Bits)
Parity Symbols (Switch Position 4)	= 256I (Bits)

Register Sizes
(where I = the Interleave Factor)

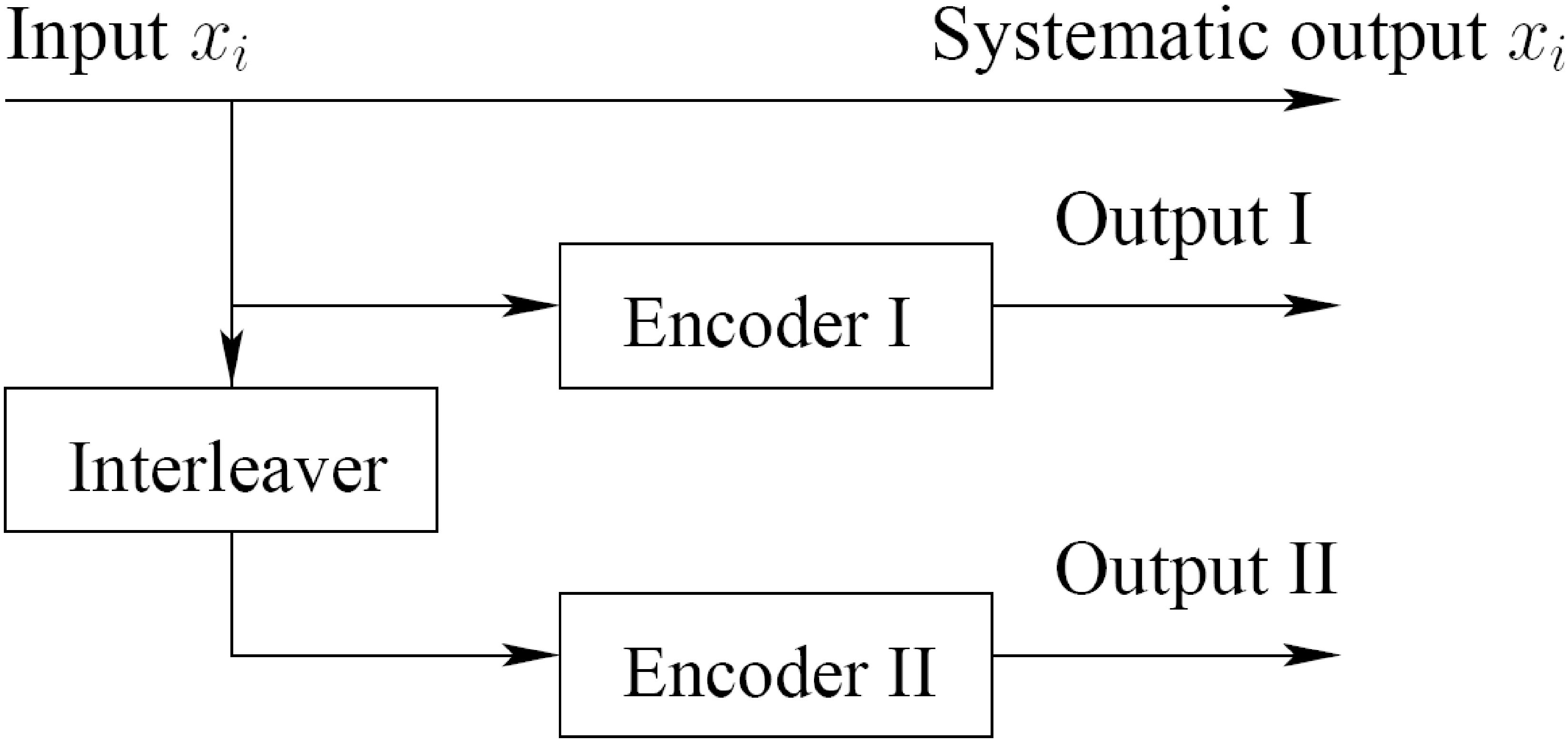
$S_1 - S_{30}$	= 8I
S_{31}	= 8 (I – 1)
$y_0 - y_7$	= 1
$z_0 - z_7$	= 1

⊕ = Modulo 2 Adder (XOR)

All registers are clocked for each bit processed including virtual fill bits. (This means that S and Z registers are clocked 8 times for each RS symbol.)

S_{31} is bypassed for I = 1

Rate 1/3 Turbo Encoder

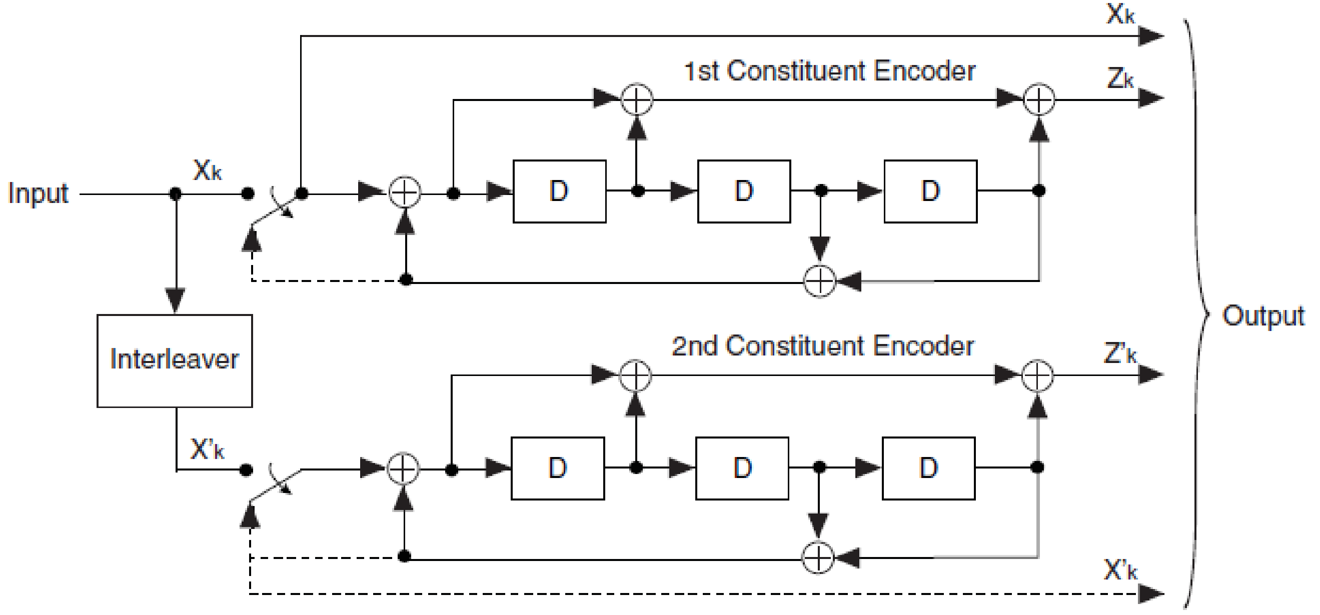


ALTERA®

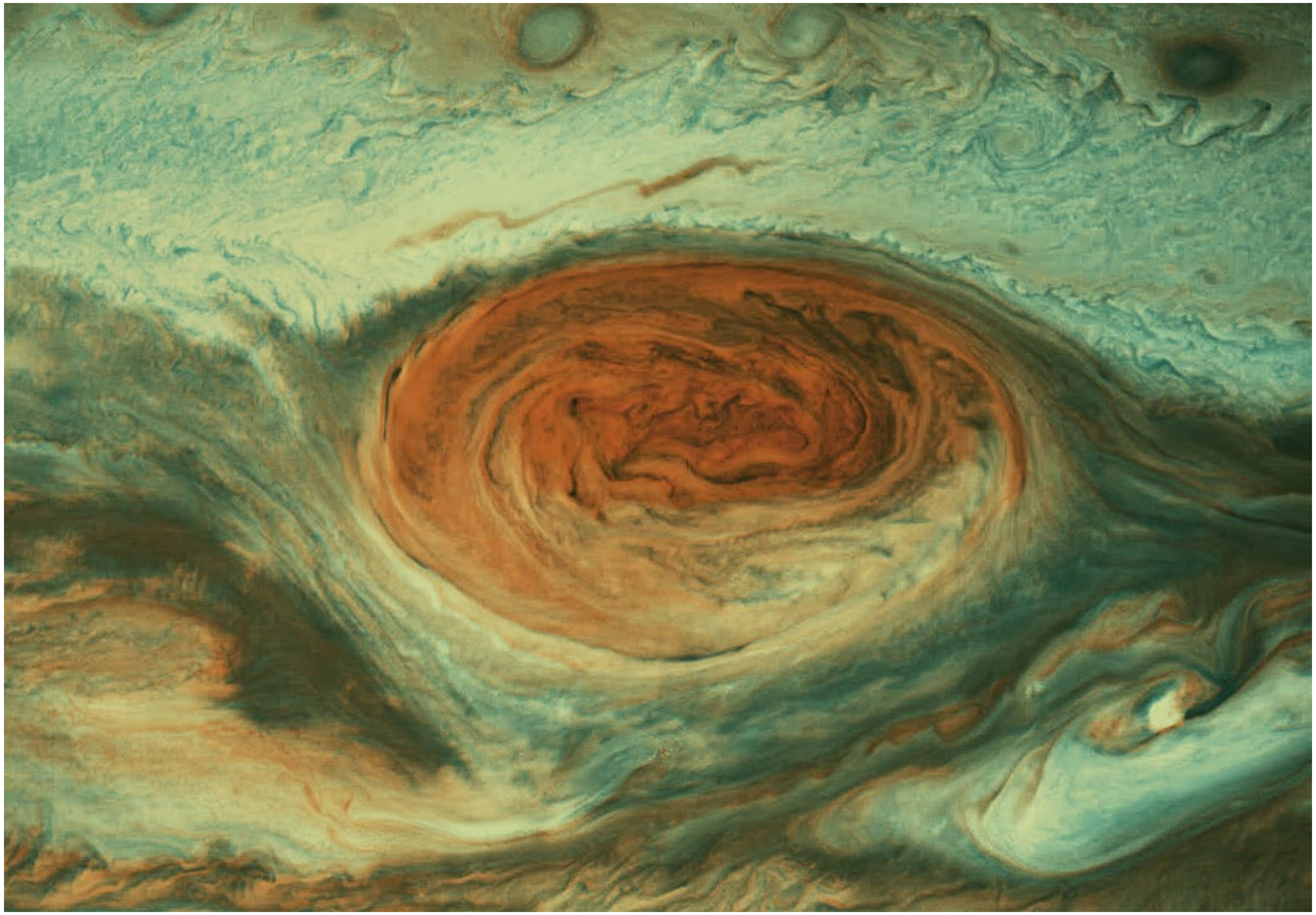
3GPP LTE Turbo Reference Design

AN-505-2.1 Application Note

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

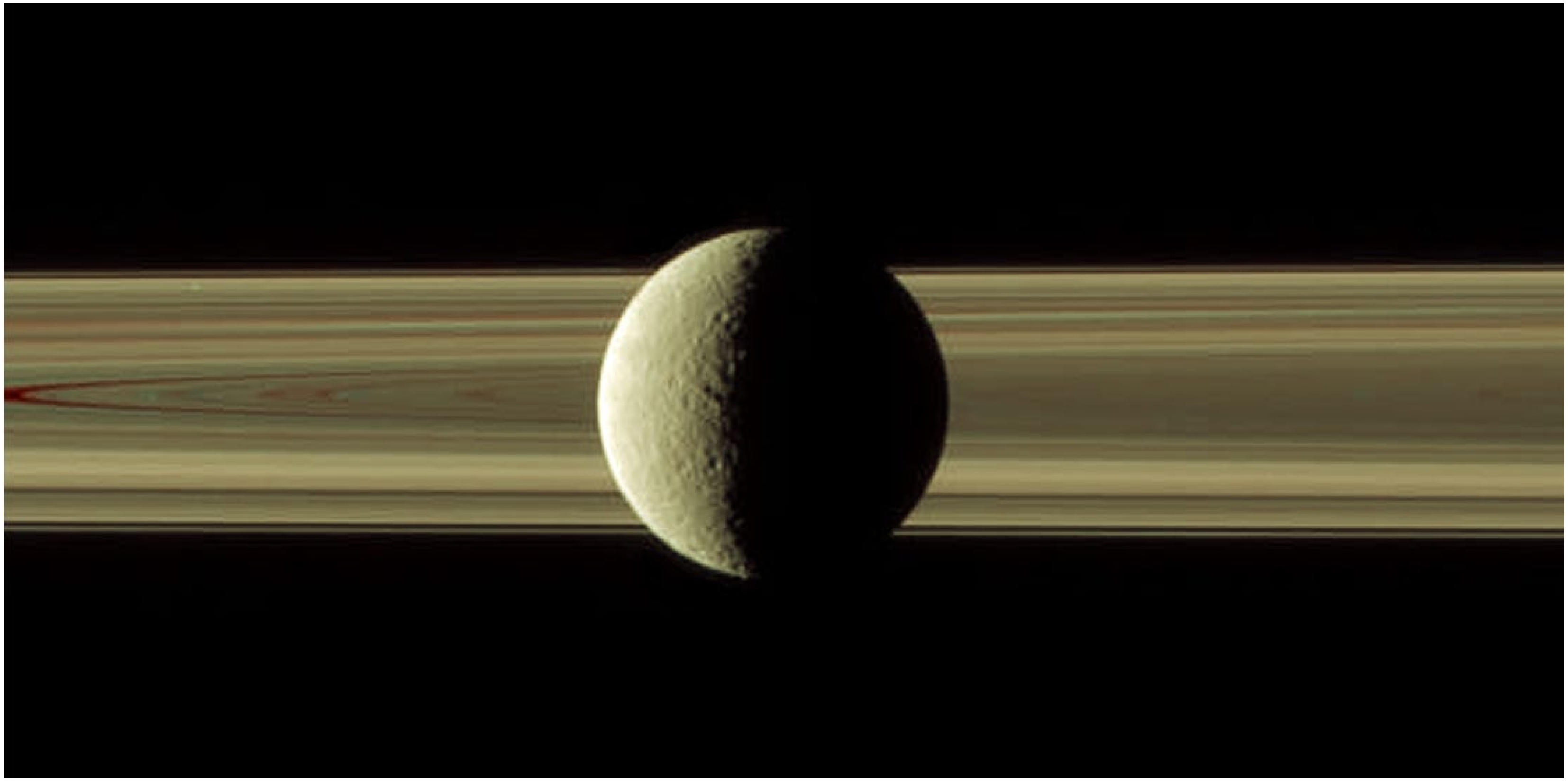


Galileo

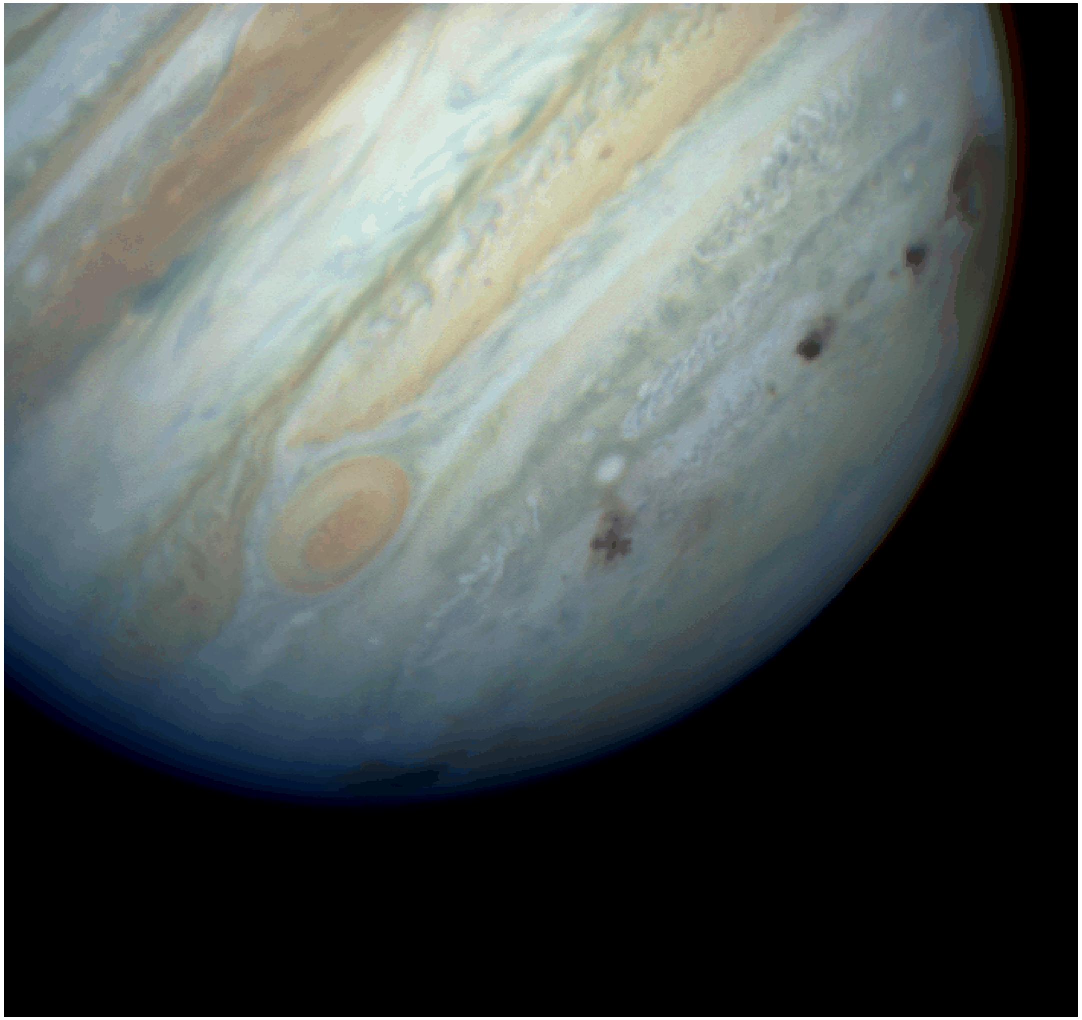


Cassini-Huygens

Rhea against the rings of Saturn March 28, 2010



Hubble Space Telescope



Ganymede from Galileo