An introduction to Information Theory

Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

July 18, 2016

Lecture #1A: Introduction

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)

Introduction Basic blocks of communication system

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)
- Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2nd Edition, John Wiley & Sons, 2006.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)
- Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2nd Edition, John Wiley & Sons, 2006.

Introduction Basic blocks of communication system

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)
- Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2nd Edition, John Wiley & Sons, 2006.

References:

- Robert G. Gallager, "Information Theory and Reliable Communications", John Wiley & Sons, 1968.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)
- Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2nd Edition, John Wiley & Sons, 2006.

References:

- Robert G. Gallager, "Information Theory and Reliable Communications", John Wiley & Sons, 1968.
- Raymond W. Yeung, "Information Theory and Network Coding", Springer, 2008.

Introduction Basic blocks of communication system

Books

Textbook:

- James L. Massey, Lecture notes on "Applied Digital Information Theory I". (http://www.isiweb.ee.ethz.ch/archive/massey_scr/)
- Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2nd Edition, John Wiley & Sons, 2006.

References:

- Robert G. Gallager, "Information Theory and Reliable Communications", John Wiley & Sons, 1968.
- Raymond W. Yeung, "Information Theory and Network Coding", Springer, 2008.
- David J. C. MacKay, "Information Theory, Inference, and Learning Algorithms", Cambridge University Press.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Books

References:

- Robert Ash, "Information Theory", Dover Publications, 1965.

Introduction Basic blocks of communication system

Books

References:

- Robert Ash, "Information Theory", Dover Publications, 1965.
- Imre Csiszar and Jonos Korner, "Information Theory", Second edition, Cambridge University Press, 2011.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Books

References:

- Robert Ash, "Information Theory", Dover Publications, 1965.
- Imre Csiszar and Jonos Korner, "Information Theory", Second edition, Cambridge University Press, 2011.
- N. J. A. Sloane and Aaron D Wyner, "Claude Elwood Shannon: Collected Papers", IEEE Press 1993.

Introduction Basic blocks of communication system

Books

References:

- Robert Ash, "Information Theory", Dover Publications, 1965.
- Imre Csiszar and Jonos Korner, "Information Theory", Second edition, Cambridge University Press, 2011.
- N. J. A. Sloane and Aaron D Wyner, "Claude Elwood Shannon: Collected Papers", IEEE Press 1993.
- Abbas El Gamal and Yong-Han Kim, "Network Information Theory", 1st Edition, Cambridge University Press, 2011.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Books

References:

- Robert Ash, "Information Theory", Dover Publications, 1965.
- Imre Csiszar and Jonos Korner, "Information Theory", Second edition, Cambridge University Press, 2011.
- N. J. A. Sloane and Aaron D Wyner, "Claude Elwood Shannon: Collected Papers", IEEE Press 1993.
- Abbas El Gamal and Yong-Han Kim, "Network Information Theory", 1st Edition, Cambridge University Press, 2011.
- Emmanuel Desurvire, "Classical and Quantum Information Theory", 1st Edition, Cambridge University Press, 2009.

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities
- Block to variable length coding: Huffman coding

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities
- Block to variable length coding: Huffman coding
- Variable to block length coding: Tunstall coding

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities
- Block to variable length coding: Huffman coding
- Variable to block length coding: Tunstall coding
- Variable to variable length coding: Arithmetic codes, Lempel-Ziv codes

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities
- Block to variable length coding: Huffman coding
- Variable to block length coding: Tunstall coding
- Variable to variable length coding: Arithmetic codes, Lempel-Ziv codes
- Block to block length coding: Typical sequences

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Introduction: Entropy, Relative Entropy, Mutual Information
- Information Inequalities
- Block to variable length coding: Huffman coding
- Variable to block length coding: Tunstall coding
- Variable to variable length coding: Arithmetic codes, Lempel-Ziv codes
- Block to block length coding: Typical sequences
- Asymptotic Equipartition Property

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Topics to be covered

Information Theory:

- Coding for sources with memory

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Coding for sources with memory
- Channel capacity

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Topics to be covered

Information Theory:

- Coding for sources with memory
- Channel capacity
- Differential Entropy

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Coding for sources with memory
- Channel capacity
- Differential Entropy
- Gaussian Channel

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Topics to be covered

Information Theory:

- Coding for sources with memory
- Channel capacity
- Differential Entropy
- Gaussian Channel
- Rate Distortion Theory

Introduction Basic blocks of communication system

Topics to be covered

Information Theory:

- Coding for sources with memory
- Channel capacity
- Differential Entropy
- Gaussian Channel
- Rate Distortion Theory
- Network Information Theory

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

What to expect from the course

- What are the fundamendal limits of communication?

Introduction Basic blocks of communication system

What to expect from the course

- What are the fundamendal limits of communication?
- What are the fundamental limits of data compression?

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

What to expect from the course

- What are the fundamendal limits of communication?
- What are the fundamental limits of data compression?
- Practical source compression algorithm.

Introduction Basic blocks of communication system

What to expect from the course

- What are the fundamendal limits of communication?
- What are the fundamental limits of data compression?
- Practical source compression algorithm.
- Some mathematical techniques.

Outline of the lecture

- Introduction

Introduction Basic blocks of communication system

Outline of the lecture

- Introduction
- Basic blocks of communication system

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Outline

Introduction

All communications involves three basic steps

- Encoding a message at its source.

Introduction

All communications involves three basic steps

- Encoding a message at its source.
- Transmitting that message through a communication medium.

Introduction Basic blocks of communication system

Introduction

All communications involves three basic steps

- Encoding a message at its source.
- Transmitting that message through a communication medium.
- Decoding the message at its destination.

Information Theory

Information Theory answers two fundamental questions in communications

- What is the ultimate data compression?

Introduction Basic blocks of communication system

Information Theory

Information Theory answers two fundamental questions in communications

- What is the ultimate data compression?
- What is the ultimate transmission rate?

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

What is Information?

- A flip of coin with two heads? Does it convey any information?

Introduction Basic blocks of communication system

What is Information?

- A flip of coin with two heads? Does it convey any information?
- A source produces successive bits of $\pi : 3, 1, 4, 1, 5, 9, 2, 6$. Does it convey any information?

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

What is Information?

- A flip of coin with two heads? Does it convey any information?
- A source produces successive bits of $\pi : 3, 1, 4, 1, 5, 9, 2, 6$. Does it convey any information?
- No, no uncertainty in the source.

Introduction Basic blocks of communication system

What is Information?

- A flip of coin with two heads? Does it convey any information?
- A source produces successive bits of $\pi : 3, 1, 4, 1, 5, 9, 2, 6$. Does it convey any information?
- No, no uncertainty in the source.
- Shannon's Information Theory regards only those symbols as information that are not predictable.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.

Introduction Basic blocks of communication system

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.
- Simple encoding (Dumb way!), black=00, red=01, blue=10, green=11. An average of 2.0 bits/color

Introduction Basic blocks of communication system

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.
- Simple encoding (Dumb way!), black=00, red=01, blue=10, green=11. An average of 2.0 bits/color
- Smart way? black=0, red=10, blue=110, green=111. An average of 1.75 bits/color

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.
- Simple encoding (Dumb way!), black=00, red=01, blue=10, green=11. An average of 2.0 bits/color
- Smart way? black=0, red=10, blue=110, green=111. An average of 1.75 bits/color
- Can you figure out the color of the balls from the sequence 0110100111?

Introduction Basic blocks of communication system

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.
- Simple encoding (Dumb way!), black=00, red=01, blue=10, green=11. An average of 2.0 bits/color
- Smart way? black=0, red=10, blue=110, green=111. An average of 1.75 bits/color
- Can you figure out the color of the balls from the sequence 0110100111?
- Black, blue, red, black, green.

Encoding Information

- Use the statistical structure of a source to represent its output efficiently.
- Example: A bag contains 50% black balls, 25% red balls, 12.5% blue balls, 12.5% green balls. You are randoming picking a ball from the bag and want to convey the information about the color of the ball.
- Simple encoding (Dumb way!), black=00, red=01, blue=10, green=11. An average of 2.0 bits/color
- Smart way? black=0, red=10, blue=110, green=111. An average of 1.75 bits/color
- Can you figure out the color of the balls from the sequence 0110100111?
- Black, blue, red, black, green.
- Main principle of data compression: "Only infrmatn esentil to understnd mst b tranmitd."

Information Theory

- The transmission medium in communication is known as channel.

Information Theory

- The transmission medium in communication is known as channel.
- In his landmark paper in 1948, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, Shannon introduced the concept of channel capacity.

Introduction Basic blocks of communication system

Information Theory

- The transmission medium in communication is known as channel.
- In his landmark paper in 1948, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, Shannon introduced the concept of channel capacity.
- The channel capacity is a measure of the amount of information that can be conveyed between the input X and the output Y of a channel.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Information Theory

- The transmission medium in communication is known as channel.
- In his landmark paper in 1948, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, Shannon introduced the concept of channel capacity.
- The channel capacity is a measure of the amount of information that can be conveyed between the input X and the output Y of a channel.
- Shannon in his celebrated *noisy channel coding theorem* proved the existence of channel coding schemes that can achieve an arbitrarily low error probability as long as the information can be transmitted across the channel at a rate less than the channel capacity, C.

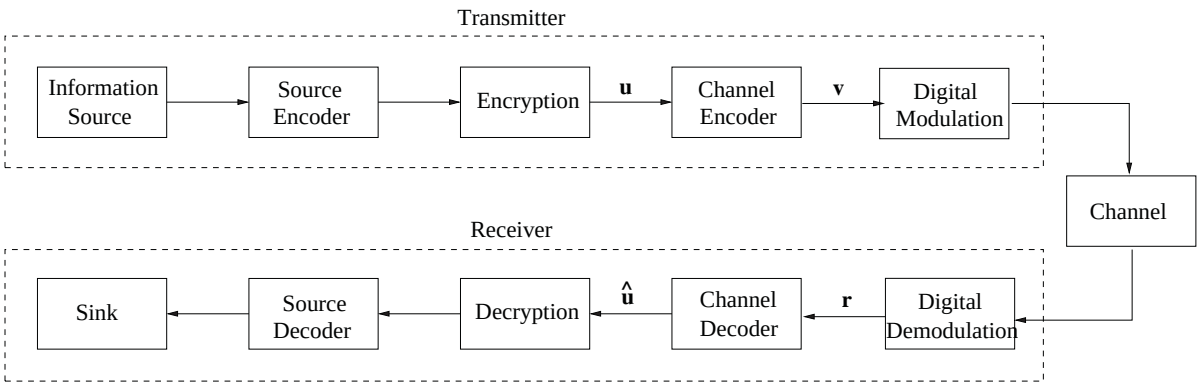
Introduction Basic blocks of communication system

Information Theory

- The transmission medium in communication is known as channel.
- In his landmark paper in 1948, *A Mathematical Theory of Communication*, in *Bell System Technical Journal*, Shannon introduced the concept of channel capacity.
- The channel capacity is a measure of the amount of information that can be conveyed between the input X and the output Y of a channel.
- Shannon in his celebrated *noisy channel coding theorem* proved the existence of channel coding schemes that can achieve an arbitrarily low error probability as long as the information can be transmitted across the channel at a rate less than the channel capacity, C.
- Example: If the channel capacity of a particular communication link is (say) 2 Gbps. We can communicate over this channel at any desired rate less than 2 Gbps, and achieve arbitrary low error rates.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Introduction



Outline

Source Coding

- *Function*: To minimize the number of bits per unit time required to represent the source output.

Introduction Basic blocks of communication system

Source Coding

- *Function*: To minimize the number of bits per unit time required to represent the source output.
- This process is known as *source coding* or *data compression*

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Source Coding

- *Function*: To minimize the number of bits per unit time required to represent the source output.
- This process is known as *source coding* or *data compression*
- *Examples*: Huffman coding, Lempel-Ziv algorithm.

Introduction Basic blocks of communication system

Source Coding

- *Function*: To minimize the number of bits per unit time required to represent the source output.
- This process is known as *source coding* or *data compression*
- *Examples*: Huffman coding, Lempel-Ziv algorithm.
- The output of the source encoder is referred to as the *information sequence*.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Encryption

- *Function*: To make source bits transmission secure.

Introduction Basic blocks of communication system

Encryption

- *Function*: To make source bits transmission secure.
- This process of converting source bits (message text) into a source stream that looks like meaningless random bits of data (cipher text) is known as *encryption*.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Encryption

- *Function*: To make source bits transmission secure.
- This process of converting source bits (message text) into a source stream that looks like meaningless random bits of data (cipher text) is known as *encryption*.
- *Examples*: Data Encryption Standard (DES), RSA system.

Channel Coding

- *Function*: To correct transmission errors introduced by the channel.

Channel Coding

- *Function*: To correct transmission errors introduced by the channel.
- The process of introducing some redundant bits to a sequence of information bits in a controlled manner to correct transmission errors is known as *channel coding* or *error control coding*.

Introduction Basic blocks of communication system

Channel Coding

- *Function*: To correct transmission errors introduced by the channel.
- The process of introducing some redundant bits to a sequence of information bits in a controlled manner to correct transmission errors is known as *channel coding* or *error control coding*.
- *Example*: Repetition code, Reed-Solomon codes, CRC codes.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Channel Coding

- *Function*: To correct transmission errors introduced by the channel.
- The process of introducing some redundant bits to a sequence of information bits in a controlled manner to correct transmission errors is known as *channel coding* or *error control coding*.
- *Example*: Repetition code, Reed-Solomon codes, CRC codes.
- The encoded sequence that is the output of the channel encoder is referred to as *codeword*.

Modulation

- *Function*: To map the codewords into waveforms which are then transmitted over the physical medium known as the channel.

Modulation

- *Function*: To map the codewords into waveforms which are then transmitted over the physical medium known as the channel.
- *Examples*: Phase shift keying (PSK), quadrature amplitude modulation (QAM).

Channel

- The physical transmission medium; it can be wireless or wireline.

Channel

- The physical transmission medium; it can be wireless or wireline.
- Corrupts transmitted waveforms due to various effects such as noise, interference, fading, and multipath transmission.

Introduction Basic blocks of communication system

Channel

- The physical transmission medium; it can be wireless or wireline.
- Corrupts transmitted waveforms due to various effects such as noise, interference, fading, and multipath transmission.
- *Examples*: Binary erasure channel (BEC), Additive white Gaussian noise (AWGN) channel.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Demodulation

- *Function*: To convert received noisy waveform to a sequence of bits, which is an estimate of the transmitted data bits. This is known as *hard demodulation*.

Introduction Basic blocks of communication system

Demodulation

- *Function*: To convert received noisy waveform to a sequence of bits, which is an estimate of the transmitted data bits. This is known as *hard demodulation*.
- If the demodulator outputs are unquantized (or has more than two quantization levels), this is known as *soft demodulation*.

Demodulation

- *Function*: To convert received noisy waveform to a sequence of bits, which is an estimate of the transmitted data bits. This is known as *hard demodulation*.
- If the demodulator outputs are unquantized (or has more than two quantization levels), this is known as *soft demodulation*.
- Soft demodulation has significant improvement over hard demodulation.

Channel Decoding

- *Function*: To estimate the information bits $\hat{\mathbf{u}}$, and correct the transmission errors.

Channel Decoding

- *Function*: To estimate the information bits $\hat{\mathbf{u}}$, and correct the transmission errors.
- If $\hat{\mathbf{u}} \neq \mathbf{u}$, decoding errors have occurred.

Introduction Basic blocks of communication system

Channel Decoding

- *Function*: To estimate the information bits $\hat{\mathbf{u}}$, and correct the transmission errors.
- If $\hat{\mathbf{u}} \neq \mathbf{u}$, decoding errors have occurred.
- The performance of the channel decoder is usually measured by the *bit error rate* (BER) or the *frame error rate* (FER) of the decoded information sequence.

Channel Decoding

- *Function*: To estimate the information bits $\hat{\mathbf{u}}$, and correct the transmission errors.
- If $\hat{\mathbf{u}} \neq \mathbf{u}$, decoding errors have occurred.
- The performance of the channel decoder is usually measured by the *bit error rate* (BER) or the *frame error rate* (FER) of the decoded information sequence.
- The BER is defined as the expected number of information bit decoding errors per decoded information bit.

Introduction Basic blocks of communication system

Channel Decoding

- *Function*: To estimate the information bits $\hat{\mathbf{u}}$, and correct the transmission errors.
- If $\hat{\mathbf{u}} \neq \mathbf{u}$, decoding errors have occurred.
- The performance of the channel decoder is usually measured by the *bit error rate* (BER) or the *frame error rate* (FER) of the decoded information sequence.
- The BER is defined as the expected number of information bit decoding errors per decoded information bit.
- The coded sequences can be broken up into blocks of data *frames*. A frame error occurs if any information bit in that data frame is in error. The decoded FER is the percentage of frames in error.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Decryption

- *Function*: To recover the plain text from the cipher text with the help of key.

Introduction Basic blocks of communication system

Decryption

- *Function*: To recover the plain text from the cipher text with the help of key.
- It is in the key that the security of a modern cipher lies, not in the details of the cipher.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory

Source Decoding

- *Function*: To reconstruct the original source bits from the decoded information sequence.

Introduction Basic blocks of communication system

Source Decoding

- *Function*: To reconstruct the original source bits from the decoded information sequence.
- Due to channel errors, the final reconstructed signal may be distorted.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to Information Theory