SC 461 – Coding Theory and Applications

Instructor Manish K Gupta (http://www.mankg.com)
Room 2209 Faculty Block 2 mankg [at] daiict.ac.in
Phone: 91-79-30510549Lab:http://www.guptalab.org

Overview

In last 50 years Information and Communication Technology (ICT) has had a great impact on our society. The most profound and accelerated impact of ICT can be seen in the last decade in the form of cell phones, connected computers and Internet. We even have a virtual currency. ICT is an interdisciplinary discipline combining IT (Information Technology) and CT (Communication Technology). IT has its root in computer science and CT has its root in theory of communication. Both the fields now can be seen as two sides of the same coin. Both deals with information, in IT we store (send information from now to then) and manipulate the information and in CT we send information from here to there (communicate). The mathematical principles of ICT lie in theoretical computer science (Turing machine) and information and coding theory (work of Shannon and Hamming). Realization of ICT is via logic gates and circuits giving birth to the area of Electronics and VLSI.

Coding theory is at the heart of ICT with roots in mathematics, origin in electrical engineering and applications to computer science. Whenever you want to send information from one point to other point (communication) or send information from now to then (storage) you require error-correcting codes. Richard W. Hamming created first error-control codes in 1947 (published in 1949) out of frustration when he was working on Bell Model V computers. Every weekend the machine use to stop because of errors and Hamming said, “Why a computer can not detect and correct the errors itself". This resulted in his invention of Hamming codes that can correct single bit error.

Around the same time in 1948 Shannon published the famous paper on Information theory “A Mathematical Theory of Communication”. Information theory answers two fundamental questions about digital information viz. how much you can compress the digital information? (Answer: The Entropy H) and what is the ultimate transmission rate of digital communication (Answer: The Channel Capacity C). While information theory sets the bounds of data storage, communication etc. Coding theory tells us how to achieve these limits. It is more about algorithm and construction of codes. Thus there are two aspects of coding theory: source coding (for data compression) and channel coding (error correction). We will be focusing more on error correction. Information theory is an interdisciplinary field with connections to Statistical physics (thermodynamics), Computer science (Kolmogorov Complexity: complexity of a string of data is the length of the shortest binary program for computing the string), Communications, Economics, Networks and even to Biology and Chemistry.

Error control coding (ECC) was known before Hamming but very efficient codes were not known and it was after Hamming's discovery it has become a field of research for mathematicians, computer scientist, electrical engineers for about 50 years now. In fact Von Neumann wrote that error control is an integral part of every information processing. So whenever there is information processing, there is error control coding. We can see now its importance in new computing paradigms such as quantum computers, bio-molecular computers. Network coding is another area that is emerging for all kind of networks. Many new applications of coding theory have emerged such as to Cloud computing (Cloud Data Storage and Cloud Security). All ICT applications uses some form of coding from CD/DVD, hard disk data storage, deep space communications, wireless communications, power line communications, cell phones, networks, sensor networks, data compressions, VLSI etc. Applications are endless. Now even people are trying to decipher what kind of error control coding is used in biological information processing? This is the greatest challenge for the ICT in 21st century. We ourselves use a crude form of error control coding in our day-to-day conversation between us (without knowing that it is ECC): Can you guess how? In almost 50 years error control coding has found many deep connections with diverse areas such as the theory of computation, complexity, algorithms, algebra (finite fields and finite rings), linear algebra, cryptography, number theory, algebraic geometry, discrete mathematics and statistical physics. In this course we will study the basics of coding theory with main focus on codes, which are optimal in the sense of Shannon’s results and various bounds.
More in the course…so fasten your seatbelt.

This course is designed for 3rd year BTech and open to MTech students. 4th year BTech can also take this course. This course is useful for any ICT student (both computer science students and communication students) and to anyone who want to learn about ICT.

Tentative Course Content

Historical Introduction and Motivation of Coding and Information Theory, Basic Review of Finite Fields and Finite Rings, Introduction to Algebraic Coding Theory, Codes over finite fields and finite rings, Linear and Non-linear Codes, Hamming Codes, Golay Codes, Cyclic, Quasi-cyclic and Quasi Twisted Codes, Quadratic Residue Codes, Reed Muller, Reed Solomon Codes and BCH Codes, Quadratic Residue Codes, Art of Decoding, Convolutional Codes, Turbo Codes and Low density parity check (LDPC) codes, Algebraic Geometry codes - Goppa codes, Applications of Coding Theory to Networks (Cloud Computing: Cloud Data Storage and Cloud Security), Cryptography, Wireless Communications, Quantum Computing, and DNA computing.

Expected Outcome

The students after completing the course will get a basic overview of Coding and Information theory. They will get an insight on how codes are used in various applications (both old and new). It exposes them various construction algorithms for error correcting problems of ICT. Projects in the course provide first hand research opportunities in niche and hot area to the students.

Text Book

The following textbooks will be helpful. We will provide many additional materials such as videos, handouts etc during the course. There is no need to purchase any book.

1. Raymond Hill, A first course in coding theory, Oxford University Press, 1990 (Elementary Text Book for Coding Theory)
2. Norman Abramson, Information theory and Coding, McGraw-Hill, 1993 (Classic Book)
3. Richard W. Hamming, Coding and Information Theory, Prentice Hall, 1986 (Classic Book)
4. Thomas M. Cover and Joy A. Thomas Elements of Information Theory, 2nd Edition, July 2006, 776 pages, Wiley (Standard Text Book for Information Theory)
5. David MacKay, Information Theory, Pattern Recognition and Neural Networks, CUP, 2003, online see http://www.inference.phy.cam.ac.uk/itprnn/book.html (Light Text Book for Information Theory)

Other Books and References (Incomplete List)

1. R.M. Roth, Introduction to Coding Theory, Cambridge University Press, 2006
2. E.R. Berlekamp, Algebraic coding theory, McGraw-Hill, 1968. Revised edition published by Aegean Park Press in 1984.
3. R.E. Blahut, Algebraic Codes for Data Transmission, Cambridge University Press, 2002.
4. W.C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, Cambridge University Press, 2003.
5. S. Lin and D.J. Costello, Error Control Coding (2nd edition), Prentice-Hall, 2004.
6. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier/North-Holland, 1977.
7. R.J. McEliece, Theory of Information and Coding (2nd edition), Cambridge University Press, 2002.
8. Vera Pless, Introduction to the Theory of Error-Correcting Codes (3rd edition), Wiley-Interscience, 1998.
9. J.H. van Lint, Introduction to Coding Theory (3rd edition), Springer-Verlag, 1999.
10. Tilborg, Coding Theory: A First Course
11. W.C. Huffman and V. Pless, Handbook of Coding Theory, vol I & II. 1998
12. San Ling and Chaoping Xing, Coding Theory: A First Course, Cambridge University Press, 2004.

Mark Distribution (Tentative) / Grading Policy
Assignments - 10%
Test 1 -20%
Test 2 -30 %
Final Test 3- 40%
Projects - Bonus

Project Policy (Bonus Project)
Project has to be done in 3 parts.
Part-1 (10%): Submission of 1 page abstract via Moodle consisting of problem formulation and key references. It is due in approximately 4 weeks after the start of the course.
Part-2 (10%): Mid progress report in another 4 weeks after part-1.
Part-3 (20%): Final report and presentation /demo of the s/w towards the 16th week.

Tutorials: None **Lab:** None
Lectures: Monday (11:00 am), Wednesday (8:30 am) and Thursday (11:00 am)
Place: LT-1

For updated information about the course please visit the course webpage at http://www.guptalab.org/mankg/public_html//WWW/courses/ctasp12/index.shtml
For course tweets follow us at http://twitter.com/guptalab For any further information feel free to contact the instructor.