SC561 Error Control Codes

Prereq. CAS Ma 193

Introduction to codes detecting and correcting errors in communication channels, computation channels and computer memories, linear algebra over finite fields, perfect and quasi-perfect codes, capacity of a channel, Shannon's Theorem, Hamming, BCH, MDS and Reed-Solomon codes, arithmetical codes, robust codes. Applications in communications, data compression, testing of computer hardware and fault-tolerant computing. Applications in cybersecurity, design of secure hardware resistant to attacks.

SC561 Syllabus
Faculty: Mark Karpovsky
Office: Rm. 331, Pho
Phone: 353-9592
E-mail: markkar@bu.edu

Lecture notes: http://MARK.BU.EDU/SC561/class_notes.htm


HWs: The homework assignments will be distributed in class one week before due dates. Copies of current hws will be also available outside Rm.331, Pho. Graded hws will be returned in class.

Exams: All exams (Midterms and Finals) are closed books - closed notes.

Paper work: Please keep your graded hws and midterms until you get a grade in the course.

SC561 Error control codes. Main Topics.

Statistical Description of communication and computation channels.

Finite fields. Fields of binary and non-binary vectors.
Linear spaces over finite fields.

Conditions for existence of codes, perfect and quasi-perfect codes.

Linear codes. Generating and parity check matrices. Encoding and decoding.

Capacity of a channel. Shannon’s theorem.

Sums and products of codes. Shortening of a code.

Covering radius of a code. Application of codes for data compression.

Binary and non-binary Hamming and extended Hamming codes. Applications for computer memories.

Non-binary codes for Lee metric.

Cyclic codes.

Binary and non-binary BCH codes.

Detection of burst errors. MDS and Reed-Solomon codes.

Detection and correction of unidirectional errors.

Arithmetical codes

Applications of codes for on-line and off-line testing and diagnosis
of computer hardware and in fault-tolerant computing.

Robust codes and their application for design of secure hardware resistant to attacks.