MATH 496 SPRING 2016—PROJECT
Due: beginning of class, 9:10am, Friday, 29 April 2016

Your project is to be a paper on a topic appropriate to this course. ***Each student will meet with me*** to discuss a choice of topic and will also meet with me to discuss progress. This project forms our final exam.

The paper should be prepared on a computer. It should be 10 to 15 pages in length (roughly 3500-4000 words). You should submit both hardcopy and softcopy (an MSWord or Latex file).

Each student is to write the paper by his or herself. Material should be collected from several sources (from the library, texts, web), and such material should be properly referenced. Web references alone do not suffice. (There is also the possibility of having original research or computational work form a significant part of your project.)

Make sure you avoid plagiarism (claiming the work or writing of others as your own).

There are many possible topics for your report. If you have an idea what you would like to do, then discuss it with me. But I have provided some possible topics here. (There are many overlaps among these topics, and several topics belong to more than one of the broad areas.)

Some areas to consider:

- Probability:

  Weak and Strong Law of Large Numbers; Central Limit Theorem
  Variance calculations for various random variables
  Information theory and entropy
  Other measures of randomness (Kolmogorov complexity, Chaitin's Ω)
  Stochastic processes

- Correlation properties of sequences:

  Large sets of sequences with good crosscorrelation properties (Gold, Kasami, other sets)

  Sequences with good aperiodic correlation properties (Barker sequences, merit factor)

  Various families of interesting sequences (No sequences, Legendre sequences, Jacobi sequences, Golay complementary sequences)

  Correlation properties of DeBruijn sequences

- Sequence construction and analysis:

  Existence/enumeration of various DeBruijn-like sequences (other alphabets, biased alphabets)

  χ-random sequences and sets for various sets χ of random variables (e.g., various quadratic (SH-random, maximal orthogonal), cubic, quadric, or higher order random)

Algebraic finite shift register generation of sequences. Nonlinear finite state machines.

Complexity of sequences (bent functions, AB functions, APN functions)

Other types of pseudorandom sequences (other alphabets, other random variables, other criteria)

• Combinatorial designs:

Existence and properties of Hadamard matrices and related objects (e.g., conference matrices)

Cyclic Hadamard matrix conjecture

Existence and use of other types of designs (e.g., weighing designs)

Experimental design in statistics

Construction of designs via cyclic difference sets and other number theoretic and algebraic techniques.

Generating/counting Eulerian and Hamiltonian paths in graphs

• Tranform methods:

Walsh transforms (signal processing)

Fourier transform (spectral analysis of sequences)

• Error-correcting codes:

Reed-Muller

Covering codes

2-root codes

Compression algorithms

• Algebra and other math:

Finite fields (trace representation of sequences)

Linear recurrences (continued fractions)

Number theory (normal numbers, balanced ternary representation for weighing)

Hadamard's theorem

• Cryptography:

Use of random sequences in cryptography (linear complexity, Berlekamp-Massey algorithm, nonlinear shift registers)

Quantum cryptography (key exchange protocols, BB84 algorithm, Rabin's "unbreakable" codes)

DES S-boxes (linear and differential cryptanalysis)

OTP simulation

AES—Advanced Encryption Standard

• Various applications:

Spread spectrum uses pseudorandomizing techniques to spread out the frequency spectrum of a signal

CDMA (Code Division Multiple Access): pseudorandom sequences as part of mobile communications (e.g., cell phones)

OFDM (Orthogonal Frequency Division Multiplexing): power control using sequences

GPS (Global Positioning System): sequences for signatures (identification) and synchronization

Wifi etc.

Connections with statistical physics—low energy states. Ising models: spin states modeled by ± 1 arrays with certain correlation properties

Optics—using Hadamard matrices and pseudorandom sequences as optical masks

Bioinformatics—DeBruijn graph-based algorithms

(Pseudorandom) Sequences in the world—biased Euro

Games

- Randomness in algorithms:

  Dithering (m-sequences)

  Random number generators of various types

  Algorithms using randomness (Monte Carlo and Las Vegas algorithms)

  $P = NP$ and the efficacy of probabistic algorithms

- Historical:

  Bernoulli, Euler, DeBruijn, Lamarr, Kolmogorov, Shannon