Math 512 Syllabus
Spring 2015, LIU Post

Week	Class Date	Material
1	1/26 - Snow Day	ISBN, error-detecting codes Read 1.1, 1.2 HW: Problems 1.1 - 1.6
2	2/2 - Snow Day	
3	2/9	Data rates, Modular arithmetic, probability of errors, repetition codes 1.3, 1.4
4	Tues 2/17	Hamming's square codes, Hamming's $[7, 4]$-code Linear algebra over fields, linear codes, Generating matrix, parity matrix 1.5, 1.6, 1.7, 2.1, 2.6, A.1-3
5	2/23	Linear maps and matrices Generating and parity matrix
6	3/2	Hamming distance Weight enumerator polynomial Equivalent codes 2.2, 2.6
	Spring Break	
7	3/16	Undetected error probability MacWilliams Identity
8	3/23	**Test 1** (weeks 1-6) Error correction Standard array, syndrome decoding
9	3/30	New codes from old
10	4/6	Hamming codes Perfect codes Hat puzzle
11	4/13	Hat puzzle
12	4/20	**Test 2** (weeks 7-11)
13	4/27	Latin squares q-ary codes
	5/4	**Final Exam**

Math 512 - Homework 2
Due February 17, 2015

1. Suppose a binary symmetric channel has symbol error p and transmits words of length n symbols. Calculate the probability of there being more than 1 error in a word. (*Note: You can do this by first calculating the probability of 0 errors or 1 error, or you can calculate the probability of 2 errors, 3 errors, etc. They will give the same answer.*)

2. Find the multiplicative inverse for all non-zero elements of $\mathbb{F}_{11}$.

3. Show that the UPC check digit will not necessarily detect swapping two adjacent digits.

4. This problem concerns the binary repetition code of length 3.
   (a) Encode the message 101.
   (b) Correct and decode the received message 000110111101.

5. This problem concerns the binary repetition code of length 5.
   (a) Encode the message 101.
   (b) Correct and decode the message 010011111100001.
   (c) Calculate the information rate of this code.
   (d) How many errors can be successfully corrected in a given codeword?
   (e) Calculate the word error probability. Evaluate explicitly for a few sample values of p.

Math 512 - Homework 3
Due February 23, 2015

Problems 5cd and 7 postponed.

1. This problem concerns Hamming's 2×2 square code.
   (a) Encode the messages 0000, 0110, 1111.
   (b) Correct and decode the messages $111110011, 011111110, 100110011$.
   (c) Suppose you receive the message 010010000. What are your options?
   (d) Give an explicit example where a message is sent, 3 errors are introduced, and the decoded codeword is incorrect.
   (e) What is the information rate of Hamming's 2×2 square code?
   (f) Compare this square code with the $[12, 4]$-repetition code (given by repeating symbols 3 times). Which code is "better?" Support your argument using mathematical properties of the codes.

2. (a) Replace the 2×2 matrices of Hamming's square code with $n \times n$ matrices and develop an analogous error-correcting code.
   (b) What is the information rate?
   (c) Can you still correct single errors?
   (d) Is this code linear?

3. Let
$$C = \left\{ (x_1, \ldots, x_{10}) \in \mathbb{F}_{11}^{10} \;\middle|\; \sum_{i=1}^{10} i x_i = 0 \right\} \subset \mathbb{F}_{11}^{10},$$
   and let $ISBN \subset \mathbb{F}_{11}^{10}$ be the subset of numbers which are ISBN numbers for some published book.
   (a) What is the relationship between C and $ISBN$?
   (b) Determine whether C and/or $ISBN$ are linear codes.

4. (a) Create your own example of a linear code. Explain/show why it is linear.
   (b) Create your own example of a non-linear code. Explain/show why it is non-linear.

5. Consider the $[6, 3]$ linear code given on p. 12 of "Error-correcting codes" and discussed in class.
   (a) Write the generator matrix G for this encoding.
   (b) Use the generator matrix to send the message 101.
   (c) You receive the message 011010. Correct this if necessary/possible.
   (d) Can you construct the parity matrix H? Try to do this by writing the equations that any valid codeword must satisfy.

6. This problem concerns Hamming's $[7, 4]$-code.
   (a) Write the parity matrix H, and use this to write the generator matrix G.
   (b) Write the digits of 3.14 as 4-bit binary numbers, and encode each of them.
   (c) You receive the following message: $1001011, 0101111, 1101001, 1110010$. Correct and decode the message.

7. Let H be matrix with entries in $\mathbb{F}_q$. Show that the set of vectors y satisfying $yH^T = 0$ determines a linear code. In order for this to make sense, what is the relationship between the length of y and the dimensions of H?

Linear algebra info - MTH 512

In a linear algebra course, one is primarily concerned with linear maps between vector spaces. A map is linear if it is compatible with both vector addition and scalar multiplication.

Definition 0.1. A vector space over a field $\mathbb{F}$ is a set V equipped with binary operations $+$ (vector addition) and $\cdot$ (scalar multiplication)

$$V \times V \xrightarrow{+} V, \qquad \mathbb{F} \times V \xrightarrow{\cdot} V$$

satisfying the following axioms (for all $\mathbf{v}, \mathbf{w}, \mathbf{x} \in V$ and $r, s \in \mathbb{F}$):

1. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ (addition commutative)
2. $(\mathbf{v} + \mathbf{w}) + \mathbf{x} = \mathbf{v} + (\mathbf{w} + \mathbf{x})$ (addition associative)
3. $\exists\, \mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$ (additive identity)
4. $\forall\, \mathbf{v} \in V$, $\exists\, (-\mathbf{v}) \in V$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$ (additive inverse)
5. $r(\mathbf{v} + \mathbf{w}) = r\mathbf{v} + r\mathbf{w}$ (distributive)
6. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$ (distributive)
7. $r(s\mathbf{v}) = (rs)\mathbf{v}$ (scalar associative)
8. $1\mathbf{v} = \mathbf{v}$ (scalar identity)

Definition 0.2. Let V be a vector space and $W \subset V$ a subset. Then V is a *subspace* (or vector subspace or linear subspace) if

$$\mathbf{u}, \mathbf{v} \in W \quad \Rightarrow \quad r\mathbf{u} + s\mathbf{v} \in W.$$

Definition 0.3. Let V, W be vector spaces. A map $T : V \to W$ is *linear* if

$$T(r\mathbf{v} + s\mathbf{w}) = rT(\mathbf{v}) + sT(\mathbf{w})$$

for all $\mathbf{v}, \mathbf{w} \in V$ and $r, s \in \mathbb{F}$. A linear map T is *injective* if it is one-to-one, *surjective* if it is onto, and an *isomorphism* if it is a bijection.

Example 0.4. $\mathbb{F}_p^n = \{(x_1, \ldots, x_n) \;\big|\; x_i \in \mathbb{F}_p\}$.

More specifically, consdier the vectors $(0, 1, 2, 0), (1, 0, 2, 1) \in \mathbb{F}_3^4$. Then

$$(0, 1, 2, 0) + (1, 0, 2, 1) = (1, 0, 1, 1), \quad 2(0, 1, 2, 0) = (0, 2, 1, 0), \quad 0(0, 1, 2, 0) = (0, 0, 0, 0).$$

Math 512 - Homework 4
Due March 2, 2015

1. Consider the $[6,3]$ linear code (given on p. 12 of "Error-correcting codes" and discussed in class) with
$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$
   (a) Construct the parity matrix H. Try to do this by writing the equations that any valid codeword must satisfy.
   (b) Using H, determine whether the following are valid codewords: 101101, 011010, 100011.
   (c) Calculate the matrix product GH^T.

2. Consider the q-ary repetition code code of type $[6,2]$, given by taking 2 elements of $\mathbb{F}_q$ and repeating each of them 3 times.
   (a) Write the generator matrix G and a parity matrix H.
   (b) Calculate GH^T.

3. Let C be a binary linear code with generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$
   List all the codewords in C. (You can do this by encoding all vectors in $\mathbb{F}_2^2$.)

4. Solve the system of linear equations over $\mathbb{R}$. (Do row reduction/Gaussian elimination if you can.)
$$\begin{cases} x + 3y & = 0 \\ 3x + y + 2z & = 0 \end{cases}$$

5. Write down specific matrices A and B such that AB is defined (they can be simple). Check that $(AB)^T = B^T A^T$.

6. Let H_{mn} be an $m \times n$ matrix with entries in $\mathbb{F}_q$. Show that the set of vectors $y \in \mathbb{F}_q^n$ satisfying $Hy^T = 0$ determines a linear code.
   (Hint: We need to show that $C = \{y \in \mathbb{F}_q^n \mid Hy^T = 0\}$ is a linear subspace of $\mathbb{F}_q^n$. To do this: assume $y_1, y_2 \in C$, and then prove $ay_1 + by_2 \in C$.)

7. For your edification, read the brief story of transmission of photographs from deep-space, taken from Hill's "A first course in coding theory," which you can see by clicking here. (You don't have to do the Exercises.)

Math 512 - Homework 5
Due March 16, 2015

1. Compute the weight enumerator for the $[n, 1]$-repetition code. How many errors can you detect/correct?

2. The weight enumerator for the $[4, 2]$-repetition code is related to the weight enumerator for the $[2, 1]$-repetition code. How? Can you generalize?

3. Calculate the minimum distance of the Hamming $[9, 4]$ square code (the one where you input a 2x2 matrix and output a 3x3 matrix). How many errors can you detect/correct?

4. Consider the binary $[7, 4]$-code with generating matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

   Determine whether this code is equivalent to Hamming's $[7, 4]$-code. (Hint: Write down the generating matrix for Hamming's $[7, 4]$-code, and use row reduction to put both generating matrices in standard form.)

Math 512 - Homework 6
Due March 23, 2015

1. Consider the binary $[n, 1]$-repetition code. Calculate the weight enumerator polynomial. What is the probability that an error goes undetected? If we are not correcting errors, what is the probability of asking for retransmission?

2. Consider the binary $[6, 3]$ linear code with
$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$
   (a) Calculate the weight enumerator polynomial. What is the probability that an error goes undetected? If we are not correcting errors, what is the probability of asking for retransmission?
   (b) Using appropriate row/column operations, show that the dual code given by H is equivalent to the code given by G.
   (c) Use the MacWilliams identity, along with part (a), to find the weight enumerator of $C^{\perp}$. (You should get the same polynomial.)

3. Let C be the binary Hamming $[7, 4]$-code. Calculate the weight enumerator polynomial of $C^{\perp}$. Using this, calculate the probability of an undetected error in C.

Test Format

1. In a binary symmetric channel (i.e. each symbol has probability p of being error) transmitting n bits, calculate the probability that .... For example, probability that the kth slot has an error, the probability there are exactly 2 errors, the probability there are at least 2 errors, ...

2. Write the parity matrix H for Hamming's $[7, 4]$-code. Correct/Decode a message. Write the generating matrix G. Encode a message.

3. You are given a generating matrix G (possibly over $\mathbb{F}_3$ or $\mathbb{F}_5$). Encode a message. Write a parity matrix H. Determine if a word is a valid codeword. If a message is error-free, decode it. Write the weight enumerator polynomial. Determine how many errors can be detected/corrected.

4. Suggestions?

Math 512 - Homework 7
Due March 30, 2015

1. Consider the $[5, 2]$-code given in class (the one where I handed out the standard array; you can use this table). Correct the message $01010, 11011, 11101$. Give an example (or multiple) of introducing 2 errors to a valid codeword, and the standard array correction producing a different codeword than what you started with.

2. Consider the binary code $C = \{0000, 1011, 0101, 1110\}$. Construct a standard array for this code. Give an example (or multiple) of introducing 1 error to a valid codeword, and the standard array correction producing a different codeword than what you started with.

3. Set up a table for *syndrome decoding* with the binary $[6, 3]$ generated by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

   Correct the message $011010, 001110, 100001, 011110, 101111$. (*Note that to do syndrome decoding, you only have to list the coset leaders and their syndrome.*)

4. Suppose you have a binary $[31, 26]$ code. How many rows and columns would be in this array? How many vectors would be listed?

Math 512 - Homework 8
Due April 6, 2015

1. Using the definition of C^+, C^-, C' given in class, determine whether or not the following are equivalent to C in general: $(C^+)^-, (C^-)^+, (C^+)'$.

2. Suppose C is a binary code with parity-check matrix H. Show that the parity-check matrix H^+ of the parity extension code C^+ is given by

$$H^+ = \left[\begin{array}{ccc|c} & & & 0 \\ & H & & 0 \\ & & & 0 \\ \hline 1 & \cdots & & 1 \end{array}\right]$$

3. Let C be the Hamming $[7, 4]$ code with parity check extension C^+. Determine the minimum distance of C^+.

4. Calculate the minimum distance of $RM(1, m)$ codes.
(Reed-Muller codes $RM(r, m)$ can be defined inductively in the following way: $RM(0, m)$ is the $[2^m, 1]$ repetition code, $RM(m, m) = \mathbb{F}_2^{2^m}$, and
$RM(r, m) = RM(r, m-1) * RM(r-1, m-1)$ for $0 < r < m$.)

5. Bonus: Show that $RM(1, 3)$ is equivalent to the dual code of the parity extension of the Hamming $[7, 4]$-code.

Math 512 - Homework 9
Due April 13, 2015

1. Show that if C is a binary linear $[5, k]$-code with $d(C) = 3$, then $k \leq 2$.

2. Determine the smallest n such that $k = 3$ bits can be encoded in a string of length n and have 1 error corrected. Answer the same problem for $k = 4$ bits.

3. Check that Ham(2) is equivalent to the $[3, 1]$-repetition code.

4. In the "Hat Puzzle" with 3 people, we had a strategy that only lost when everyone had a 0 or everyone had a 1. Show that with more than 3 people, there is no such strategy.

5. In the "Hat Puzzle" with 4 people, use the optimal strategy from the 3-player game. What percent of the time will the team win? What about with 5 people? Is there a better strategy with 5 people?

6. Try to figure out the best strategy for the "Hat Puzzle" with 7 players. Hint: Try rewriting the 3-player strategy in terms of linear codes.