Math 512 Syllabus
Spring 2019, LIU Post

Week	Class Date	Material
1	1/28	ISBN, error-detecting codes HW: Exercises 1.1, 1.3, 1.5 Find the multiplicative inverse for all non-zero elements of $\mathbb{F}_{11}$ Show that ISBN-13 need not detect adjacent swaps
2	2/4	Error probability, Repetition Codes, Hamming square code HW: Exercises 1.7-1.9, 1.14-1.16 (linear part optional) Calculate the probabilities of transmitting strings error-free using the $[3, 1]$-repetition and the Hamming Square codes. (You may assume both correct 1 error.) For specific values of p, compare with sending strings with no encoding.
3	2/11	Linear Algebra over finite fields, the beginning of Linear Codes (§2.1, §2.3-2.6). HW: Problem written on board (list all codewords), and #1 and #10 from "Homework 3" handout.
4	2/19	Hamming $[7, 4]$ code (§1.7) Linear Codes (§2.1, §2.3-2.6) HW: 4, 5c, 6, and 7 from "Homework 3" handout.
5	2/25	Generator, Parity matrices Homework 5 handout
6	3/4	**Quiz 1** Weights, distances, and detection/correction. HW: Homework 6 handout
	3/11	Spring Break
7	3/18	Review, Probabilities HW: Updated HW 6 handout
8	3/25	**Quiz 2**, Polynomial Intro HW: Homework 7 handout
9	4/1	Galois Fields HW: Homework 8 handout
10	4/8	Polynomial Codes HW: Homework 9 handout
11	4/15	Cyclic Codes HW: Homework 10 handout
12	4/22	**Quiz 3**
13	4/29	Reed–Solomon Codes
	5/6	**Presentations of Final Projects**

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)

Example 0.2. $\mathbb{F}_p^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_p\}$.
More specifically, consdier the vectors $(0,1,2,0), (1,0,2,1) \in \mathbb{F}_3^4$. Then

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

Definition 0.3. 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 0.4. 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.

Definition 0.5. Given a linear map $T : V \to W$,

$$\textbf{Kernel} \quad \mathrm{Ker}(T) := \{\mathbf{v} \in V \mid T(\mathbf{v}) = \mathbf{0} \in W\} \subseteq V,$$

$$\textbf{Image} \quad \mathrm{Image}(T) := \{T(\mathbf{v}) \in W \mid \mathbf{v} \in V\} \subseteq W.$$

Proposition 0.6. *The Kernel and Image of a linear map are vector subspaces.*

Definition 0.7. Let V be a vector space over F. A finite collection of vectors $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$ is a **basis** of V if the induced linear map

$$F^n \longrightarrow V$$
$$(r_1, \ldots, r_n) \longmapsto r_1\mathbf{v}_1 + r_2\mathbf{v}_2 + \cdots r_n\mathbf{v}_n$$

is an *isomorphism.* In such a case, we say the dimension of V is $\dim(V) = n$.

Theorem 0.8 (Rank-Nullity)**.** *If $T : V \to W$ is a linear map (and V is finite-dimensional), then*

$$\dim \mathrm{Ker}(T) + \dim \mathrm{Image}(T) = \dim V.$$

Math 512 - "Homework 3"

~~Due February 19, 2019~~

1. Use row reduction/Gaussian elimination to solve the following system of linear equations over $\mathbb{R}$. Also, solve them over $\mathbb{F}_5$.

$$\begin{cases} x + 3y & = 0 \\ 3x + y + 2z & = 0 \end{cases}$$

2. 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.

3. (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.

4. 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) Construct the parity matrix H. Try to do this by writing the equations that any valid codeword must satisfy.
   (e) Using H, determine whether the following are valid codewords: $101101, 011010, 100011$.
   (f) Calculate the matrix product GH^T.

5. 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.
   (d) List all codewords of Hamming's $[7,4]$-code.

6. 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.

7. 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 $\mathbb{F}_2^2$.)

8. (optional) Consider working over the field $\mathbb{F}_5$. Which of the following two matrices would be a valid generating matrix G? Explain your answer. What problem would one of them cause?

$$G_1 = \begin{bmatrix} 1 & 3 & 0 \\ 3 & 1 & 2 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 3 \\ 3 & 1 \\ 0 & 2 \end{bmatrix}$$

9. Let G_{kn} be an $k \times n$ matrix with entries in $\mathbb{F}_q$. Show that the set of vectors $y \in \mathbb{F}_q^n$, satisfying $y = xG$ for some $x \in \mathbb{F}_q^k$, determines a linear code.

   (Hint: We need to show that $C = \{xG \in \mathbb{F}_q^n \mid x \in \mathbb{F}_q^k\}$ is a linear subspace of $\mathbb{F}_q^n$. To do this: assume $y_1, y_2 \in C$, and then prove $ay_1 + by_2 \in C$.)

10. 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?

11. 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 4, 2019

Next week's quiz will be, essentially, #1 parts a,b,c.

1. 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 (eg $3 = 0011, 4 = 0100$ etc), and encode each of them.
   (c) You receive the following message: $1001011, 0101111, 1101001, 1110010$. Correct and decode the message.
   (d) List all codewords of Hamming's $[7,4]$-code.

2. Let C be a binary linear code with generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$
   Write a parity matrix H for the code.

3. Write the generator matrix and parity matrix for the ISBN-10 code.

4. Write the generator and parity matrix for the Hamming $[9,4]$ square code.

5. (optional) Consider working over the field $\mathbb{F}_5$. Which of the following two matrices would be a valid generating matrix G? Explain your answer. What problem would one of them cause?
$$G_1 = \begin{bmatrix} 1 & 3 & 0 \\ 3 & 1 & 2 \end{bmatrix}, \quad G_2 = \begin{bmatrix} 1 & 3 \\ 3 & 1 \\ 0 & 2 \end{bmatrix}$$

Math 512 - Homework 6
Due March 18, 2019

(Additional problems for Homework 7 are added with a * on them. For probabilities, assume we are transmitting across a noisy memoryless symmetric binary channel with symbol error p.)

1. Calculate the minimum distance of the Hamming $[9, 4]$ square code (the one where you input a 2x2 matrix and output a 3x3 matrix). Since there are only $2^4 = 16$ codewords, you can just explicitly list them and determine their weights. How many errors can you detect/correct? Write the weight enumerator polynomial.
   * What is the probability that a codeword is received with no errors? What is the probability that a codeword, after the error-correction procedure, is the original codeword sent? What is the probability there is an undetected error?

2. Compute the weight enumerator for the $[n, 1]$-repetition code. How many errors can you detect? How many errors can you correct?
   * What is the probability that a codeword is received with no errors? What is the probability that a codeword, after the error-correction procedure, is the original codeword sent? What is the probability there is an undetected error?

3. The weight enumerator for the $[4, 2]$-repetition code is related to the weight enumerator for the $[2, 1]$-repetition code. How? Can you guess how this generalizes?

4. Consider the $[5, 2]$-code given in class (the one where I handed out the standard array; you can use that table).
   (a) Correct the message $01010, 11011, 11101$.
   (b) Give an example (or multiple) of introducing 2 errors to a valid codeword, using the standard array to correct, and producing a different codeword than what you started with.
5. Consider the binary $[6, 3]$ linear code with

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

   We have already determined its minimal distance is $d = 3$.
   (a) Construct the parity matrix H. (You did this in HW 3; you can just recopy if you want.)
   (b) Set up a table for *syndrome decoding*. (Note that to do syndrome decoding, you only have to list the coset leaders (elements in row with minimal weight) and their syndrome.)
   (c) Using your table, correct the message $011010, 001110, 100001, 011110, 101111$.
   * Calculate the weight enumerator polynomial for this code. What is the probability of there being an undetected error? Suppose that, any time we receive a word that doesn't have a unique closest word (i.e. it is not in the "correctable" portion of our syndrome decoding table) we ask for it to be retransmitted. What is the probability a word will have to be retransmitted?

Math 512 - Homework 7
Due April 1, 2019

1. Show the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ has no roots by plugging in in $x = 0$ and $x = 1$.

2. Perform the following multiplication: $(x^3 + x^2 + 1)(x + 1) \in \mathbb{F}_2[x]$.

3. In $\mathbb{F}_2[x]$, $x^5 + x^2 + x + 1 = (x^2 + 1)g(x)$. Find $g(x)$.

4. In $\mathbb{F}_2[\alpha]$, use polynomial division to write α^7 as $f(\alpha)(\alpha^4 + \alpha + 1) + g(\alpha)$, where $\deg(g) \leq 3$.
   Hint: Compute $\dfrac{\alpha^7}{\alpha^4 + \alpha + 1}$

Math 512 - Homework 8
Due April 8, 2019

1. Let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined by
$$x \sim y \quad \text{if } y - x = 2n \text{ for some } n \in \mathbb{Z}.$$
Prove that $\sim$ is reflexive ($x \sim x$ for all $x \in \mathbb{Z}$) and symmetric (if $x \sim y$ then $y \sim x$).

2. Let $g = g(x) \in \mathbb{Z}[x]$ be a polynomial. Define an equivalence relation $\sim$ on $\mathbb{Z}[x]$ by
$$f_1 \sim f_2 \quad \text{if } f_2 - f_1 = g \cdot h \text{ for some } h = h(x) \in \mathbb{Z}[x].$$
Prove that $\sim$ is transitive. (The proof follows the exact same logic and format as the proof of transitivity we did in class.)

3. Make a chart (as described in class) that calculates α^k in
$$\mathbb{F}_8 = \mathbb{F}_2[\alpha] / \left(1 + \alpha + \alpha^3\right).$$
You can stop when you reach $\alpha^n = 1$ for some $n > 1$.

4. Make a chart (as described in class) that calculates α^k in
$$\mathbb{F}_{16} = \mathbb{F}_2[\alpha] / \left(1 + \alpha + \alpha^4\right).$$
You can stop when you reach $\alpha^n = 1$ for some $n > 1$.

5. Using the model of $\mathbb{F}_{16}$ from the previous problem, calculate
$$\alpha^4 + \alpha^8 \text{ and } (\alpha^2 + \alpha^3)(1 + \alpha^2).$$

Math 512 - Homework 9
Due April 15, 2019

1. Consider the generating polynomial $g(x) = 1+x^2+x^3 \in \mathbb{F}_2[x]/(x^7+1)$. This is the example we did in the first half of class (though I didn't write the quotient part until later).
   (a) Encode the "message" $1+x^2$.
   (b) By considering the polynomial code as a linear $[7,4]$-code over $\mathbb{F}_2$ (as we did in class), encode the message 1001.
   (c) You receive the polynomial message $x+x^3+x^4+x^5$. Use polynomial division to determine if there is some $f(x)$ such that $f(x) \cdot g(x) = x+x^3+x^4+x^5$. Can you "decode" the message?
   (d) Use polynomial division to find $h(x)$ such that $g(x)h(x) = x^7+1 \in \mathbb{F}_2[x]$.

2. Consider the polynomial code over $\mathbb{F}_8$, given by the generating polynomial
$$g(x) = (x+\alpha^5)(x+\alpha^6) \in \mathbb{F}_8[x].$$
Here we use the explicit model $\mathbb{F}_8 := \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1)$. This determines a $[7,5]$-code over $\mathbb{F}_8$, or a $[21,15]$-code over $\mathbb{F}_2$. Note: The polynomial $g(x)$ is different than the one used in class, but the concepts and the code behavior is the same.
   (a) Use $g(x)$ to encode the following string of 15 bits in a string of 21 bits:
$$000\,010\,000\,101\,100.$$
   (b) Determine the generator matrix G of the corresponding linear $[7,5]$-code over $\mathbb{F}_8$.
   (c) Determine the generator matrix of the corresponding linear $[21,15]$-code over $\mathbb{F}_2$.

Math 512 - Homework 10 (really 11)
Due April 22, 2019

1. Let $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$, where $\mathbb{F}$ is some field (e.g. $\mathbb{R}, \mathbb{F}_2, \mathbb{Q}$; This assures us polynomial division will work well). Prove that $(x-a)$ divides f in $\mathbb{F}[x]$ if and only if $f(a) = 0$.
Hint: We proved the if direction in class. To show the only if direction, use the fact that the polynomial division algorithm will provide polynomials $Q(x), R(x) \in \mathbb{F}[x]$ with $\deg(R) < \deg(x-a)$ such that $f(x) = Q(x) \cdot (x-a) + R(x)$.

2. Consider the polynomial code in $R_7 = \mathbb{F}_2[x]/(x^7+1)$ generated by $g(x) = x+1$.
   (a) Write a generator matrix G for the induced cyclic $[7,6]$ code.
   (b) Perform row reduction on the generator matrix G. (Note that while this changes how one might perform the encoding, the set of all codewords does not change under these row operations. Your row reduced generator matrix is still a generator matrix for the same code.)
   (c) Show the induced cyclic code is the same as the $[7,6]$ code given by adding a parity bit to every codeword.

3. Consider the cyclic code generated by $g(x) = 1 + x + x^3 \in R_7 = \mathbb{F}_2[x]/(x^7+1)$.
   (a) Write a generator matrix G for the induced cyclic $[7,4]$ code.
   (b) Swap the columns in the generator matrix G in the following way:
   $$1 \mapsto 3, \quad 2 \mapsto 1, \quad 3 \mapsto 4, \quad 4 \mapsto 2.$$
   In other words, the third column in the new matrix will be the first column in the original matrix. The new generating matrix from the previous part gives a code that is *equivalent, but not equal* to the original code.
   (c) Show this new code is the Hamming $[7,4]$ code. You can do this by performing row reduction on the generator matrix from (b) and the generator matrix for the Hamming $[7,4]$ code. Conclude that the Hamming code is equivalent to a cyclic code.

4. Consider $g(x) = x^2 \in \mathbb{F}_2[x]/(x^3-1) = R_3$.
   (a) Suppose we created a $[3,1]$ code C by using the corresponding generator matrix
   $$G = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}.$$
   Show the induced code C is not cyclic.
   (b) Show that x^2 does not divide $x^3 - 1$ in $\mathbb{F}_2[x]$.
   (c) Optional: In fact, show that x^2 is a unit in R_3, i.e. that $x^2 \cdot f(x) = 1 \in R_3$ for some $f(x)$. Conclude that the ideal generated by x^2 in R_3 is equal to all of R_3.
   (d) Does this example contradict the following theorem that was stated in class?
   Assume q is a power of p, and $p \nmid n$. A linear code $C \subset \mathbb{F}_q^n$ is cyclic if and only if C is induced by a generating polynomial $g(x) \in \mathbb{F}_q[x]$ such that $g(x)h(x) = x^n - 1$ for some $h(x) \in \mathbb{F}_q[x]$.