Math 512 Syllabus
Spring 2017, LIU Post

Week	Class Date	Material
1	1/23	ISBN, error-detecting codes HW: Exercises 1.1, 1.3, 1.5, 1.8, 1.14, 1.15 If $\vec{x}, \vec{y}$ satisfy ISBN-10 check, then so does $\overrightarrow{x+y}$.
2	1/30	Hamming [7,4] code HW: Exercises 1.19-1.24. Bonus: Generalize Hamming $[7, 4]$ code to a code with r check bits.
3	2/6	Linear Algebra over finite fields HW: Homework 3 handout.
4	2/13	**Quiz 1** Weights, distances, and detection/correction. HW: Homework 4 handout
5	2/21	Error correction (§3.2) Probabilities (§3.4) HW: Homework 5 handout
6	2/27	Sphere packing (Hamming) bound and Perfect codes (§2.8) HW: Study for Quiz 2
7	3/6	**Quiz 2** Polynomials and finite fields Optional HW handout
	3/13	**Spring Break**
8	3/20	Polynomial codes (§4-5) HW: Homework 7 Handout
9	3/27	Principal ideals, cyclic codes
10	4/3	Error-correction in cyclic codes Field extensions and minimal distances HW: Homework 8 Handout
11	4/10	Arithmetic in Galois Fields Reed–Solomon codes HW: Homework 9 Handout
12	4/17	**Quiz 3** Reed–Solomon codes continued
13	4/24	Review
	5/1	**Final Exam**

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

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

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 $T : V \to W$,

$$\textbf{Kernel} \quad \operatorname{Ker}(T) := \{\mathbf{v} \in V \;\big|\; T(\mathbf{v}) = \mathbf{0} \in W\} \subseteq V,$$

$$\textbf{Image} \quad \operatorname{Image}(T) := \{T(\mathbf{v}) \in W \;\big|\; \mathbf{v} \in V\} \subseteq W.$$

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*

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

Math 512 - Homework 3
Due February 13, 2017

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. Use row reduction/Gaussian elimination to solve the following system of linear equations over $\mathbb{R}$. Also, solve them over $\mathbb{F}_5$.
$$\begin{cases} x + 3y & = 0 \\ 3x + y + 2z & = 0 \end{cases}$$

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

6. (optional) 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 $ay_1 + by_2 \in C$.)

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 4
Due February 20, 2017

1. Let C be a binary linear code with generator matrix
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$
(as in problem 3 from HW 3). Construct the parity check matrix H.

2. 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.

3. In Homework 2, Exercise 1.19 asked you to list all the codewords in the Hamming $[7, 4]$ code. Using your previous results, write the weight enumerator polynomial, determine the minimal distance of this code, and determine how many errors it successfully detects/corrects.

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

5. 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?

Math 512 - Homework 5
Due February 27, 2017

In the following, assume that transmission occurs across a memoryless binary symmetric channel, which just means that the probability of error in any single bit is p. This is what we assumed in class.

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, using the standard array to correct, and producing a different codeword than what you started with.

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. How many errors can we detect/correct?
   (b) What is the probability that an error goes undetected?
   (c) If we were to just send the 3-bit strings directly, instead of encoding them as 6-bit strings, what would be the probability of having an undetected error?
   (d) Create a small table for the answers to (b) and (c) for the specific values of $p = .4, .1, .01, .001$.
   (e) Construct the parity matrix H. (You did this in HW 3.)
   (f) Set up a table for *syndrome decoding*, and correct the message $011010, 001110, 100001, 011110, 101111$.
   (*Note that to do syndrome decoding, you only have to list the coset leaders (elements in row with minimal weight) and their syndrome.*)

3. Let C be the binary Hamming $[7, 4]$-code. In last homework, we calculated the weight enumerator polynomial.
   (a) Calculate the probability of an undetected error in C.
   (b) In this code, we correct any 7-bit string. What is the probability that our corrected word is not the originally transmitted codeword? Hint: If 0 or 1 errors are made during transmission, then our corrected word will equal the original codeword.

4. Suppose you have a binary $[31, 26]$ code, and you constructed the entire decoding table. How many rows and columns would be in this array? How many words would be listed? If you only construct the syndrome table, how many rows, columns, and words do you need?

Quiz 2
March 6, 2017

In the following, assume that transmission occurs across a memoryless binary symmetric channel, which just means that the probability of error in any single bit is p. This is what we assumed in class.

Consider the binary $[n, k]$ code given by the following generator matrix G (to be given on quiz).

1. Encode the following message.
2. List all codewords and calculate the weight enumerator polynomial.
3. How many errors can we detect? How many errors can we correct?
4. What is the probability that an error goes undetected?
5. Construct the parity matrix H.
6. Set up a table for *syndrome decoding*.
7. Correct the following message. Then decode it.

Math 512 - Optional Homework 6
Due March 20, 2017

1. Show the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ has no roots (hint: you only have to plug in $x = 0$ and $x = 1$). Write all elements in $\mathbb{F}_2[x]/(x^2 + x + 1)$, and compute addition and multiplication tables (we did this in class).

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

Math 512 - Homework 7
Due March 27, 2017

1. In class, we obtained a generating matrix G corresponding the polynomial $g(x) = 1+x+x^3 \in \mathbb{F}_2[x]/(x^7-1)$, and we recalled the generating matrix G_{Ham} for the Hamming $[7,4]$-code. Use row operations *and* swapping of columns to transform one of the matrices to the other. This proves that the code given by $1+x+x^3$ is *equivalent* to Hamming $[7,4]$.

2. Consider the generating polynomial $g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]/(x^7+1)$.
   (a) Encode the "message" $1+x$.
   (b) Find $h(x)$ such that $g(x)h(x) = x^7 + 1 \in \mathbb{F}_2[x]$. In fact, factor x^7+1 as completely as you can.
   (c) The polynomial $g(x)$ will determine and $[n,k]$ code. What are n, k?
   (d) You receive the polynomial $x + x^3 + x^5 + x^6 \in \mathbb{F}_2[x]/(x^7+1)$. Use polynomial division to determine if it is valid.
   (e) Construct the generating matrix G for the linear code corresponding to $g(x)$.

3. Consider $g(x) = x^2 \in \mathbb{F}_2[x]/(x^3-1)$ generating a polynomial code.
   (a) List all of the codeword polynomials.
   (b) What linear code is this equivalent to?
   (c) Extra: What is happening? Hint: Show that x^2 is a unit in R_3, i.e. that $x^2 \cdot f(x) = 1 \in R_3$ for some $f(x)$.

Math 512 - Homework 8
Due April 10, 2017

1. Determine all possible binary cyclic codes of length 5.

2. (a) Show $(1+x)(1+x+x^2)(1+x^3+x^6) = (x^9+1) \in \mathbb{F}_2[x]$.
   (b) Consider the code C in R_9 generated by $g(x) = 1+x^3+x^6$. Write a remainder table for this code.
   (c) Determine whether $1+x+x^3+x^4+x^6+x^7$ is valid in C.
   (d) Determine whether $1+x^2+x^3+x^6+x^8$ is valid in C. If not, can you correct it?

3. In class, we used $(1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4) = x^{15}+1 \in \mathbb{F}_2[x]$. We considered $\alpha \in \mathbb{F}_{2^4}$, viewed as one of the roots of $(1+x+x^4)$. We showed that α^3 is a root of $(1+x+x^2+x^3+x^4)$. Determine the minimal polynomial for which α^5 is a root. Then, use this to write $g(x)$ for a binary cyclic code of length 15 with minimal distance at least 7.

Math 512 - Homework 9
Due April 17, 2017

1. Consider the finite field $\mathbb{F}_{16}$, given by the explicit model
$$\mathbb{F}_{16} := \mathbb{F}_2[\alpha]/(\alpha^4 + \alpha + 1).$$
Calculate $\alpha^4 + \alpha^8$ and $(\alpha^2 + \alpha^3)(1 + \alpha^2)$.

2. Consider the Reed–Solomon code over $\mathbb{F}_8$, discussed in class, 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 $\mathbb{F}_2$. Use $g(x)$ to encode the following string of 15 bits in a string of 21 bits:
$$000\,010\,000\,101\,100.$$

3. Consider the finite field $\mathbb{F}_{2^8}$. We call an element of $\mathbb{F}_{2^8}$ a *byte*, and one byte is composed of eight bits. Consider the Reed–Solomon codes $RS(8, t) \subset \mathbb{F}_{2^8}[x]/(x^{255} - 1)$ generated by $(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2t})$.
   (a) Let $t = 3$. Then $RS(8, 3)$ would be a $[?, ?]$-code over $\mathbb{F}_{256}$, and it would be a $[?, ?]$-code over $\mathbb{F}_2$. How many random byte errors can be corrected? Error bursts of ? bits can be corrected.
   (b) What would t need to be in order to ensure successful correction of error bursts of length 4000 bits?

Practice Quiz 3

(Taken from HW 7)
Consider the generating polynomial $g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]/(x^7 + 1)$.

1. Encode the "message" $1 + x$.
2. Find $h(x)$ such that $g(x)h(x) = x^7 + 1 \in \mathbb{F}_2[x]$. In fact, factor $x^7 + 1$ as completely as you can.
3. The polynomial $g(x)$ will determine and $[n, k]$ code. What are n, k?
4. You receive the polynomial $x + x^3 + x^5 + x^6 \in \mathbb{F}_2[x]/(x^7 + 1)$. Use polynomial division to determine if it is valid.
5. Construct the generating matrix G for the linear code corresponding to $g(x)$.