Math 342 Midterm 2 syllabus.
Spring 2018

The midterm will be held in class on Thursday, March 15. Calculators, laptops, notes, “cheat sheets,” etc. will NOT be allowed.

The midterm will cover Chapters 1-7 in the text, excluding the material on block designs in Chapter 2 and on the probability of correction/detection in Chapter 6. The emphasis will be on the topics covered after Midterm 1. Here is a quick summary of these topics.

Linear algebra basics

Definition, first properties and examples of vector spaces (particularly over finite fields).

Subspaces. A linear code is a subspace of $V(n, q) = F_q^n$

Basic concepts in linear algebra

• linear independence
• linear dependence
• spanning set,
• basis
• dimension

Some facts about these concepts, such as

• any spanning set of a subspace contains a basis for the subspace (Theorem 4.2)
• any element of a subspace can be expressed as a unique linear combination of a basis for the subspace (Theorem 4.3(i))
• any subspace of $V(n, q)$ has size $q^k$ for some $0 \leq k \leq n$ (Theorem 4.3(ii))
• all bases for the same subspace have the same size, namely $q^k$ where $k$ is the dimension of the subspace.

Matrices over finite fields. The row space of a matrix.

• Row operations, row echelon form (REF), reduced row echelon form (RREF), standard form.
• Using row reduction/Gaussian elimination to determining linear independence, find a basis in $V(n, q)$. 

1
Linear Codes

Definition and Notation: A $q$-ary linear code is a subspace of $V(n, q) = GF(q)^n$. A $q$-ary $[n, k]$-code is a $k$-dimensional subspace of $V(n, q)$. A $q$-ary $[n, k, d]$-code is an $[n, k]$-code with minimum distance $= d$.

Generator matrices:
- A generator matrix for a linear code is a matrix whose rows form a basis for the code.
- How to find a generator matrix from a spanning set for a code: use elementary row operations to find reduced row echelon form and then delete the all-zero rows.
- A generator matrix $G$ for an $[n, k]$-code can be used for encoding arbitrary strings of length $k$ into codewords: $u \mapsto uG$.
- The standard form of a generator matrix for an $[n, k]$-code is a matrix of the form $[I_k | A]$ where $I_k$ is the $k \times k$ identity matrix. Up to equivalence, every linear code has a generator matrix in standard form. The standard form can be constructed from a given generator matrix by elementary row and column operations.

Dual codes and parity check matrices
- For a linear code $C$ in $V(n, q)$, the dual code $C^\perp = \{ x \in V(n, q) : x \cdot u = 0 \; \text{for every} \; u \in C \}$.
- The sum of the dimensions of $C$ and $C^\perp$ code is always $n$.
- A parity check matrix for $C$ is, by definition, a generator matrix for $C^\perp$.

<table>
<thead>
<tr>
<th>code</th>
<th>generator matrix</th>
<th>parity check matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C$</td>
<td>$G$</td>
<td>$H$</td>
</tr>
<tr>
<td>$C^\perp$</td>
<td>$H$</td>
<td>$G$</td>
</tr>
</tbody>
</table>

- A generator matrix $G$ for a linear code $C$ can be transformed to parity check matrix $H$ for $C$. If $G$ is in standard form $G = [I_k | A]$, then $H = [-A^T | I_{n-k}]$ is a parity check matrix for $C$.

The minimal distance of a linear code $C$
- $d(C)$ is the minimal weight of a non-zero word in $C$ (Theorem 5.2).
- $d(C)$ is the minimal number of linearly dependent columns in a parity check matrix for $C$.

Decoding with a linear code

Cosets of $C$.
- A $k$-dimensional linear code in $V(n, q)$ has $q^{n-k}$ cosets.
• Each coset has \( q^k \) words.
• Costs of \( C_p \) partition \( V(n, q) \).
• Coset leader is an element of a coset of \( C \) with minimum weight.

Standard array
• the array consists of all elements of \( V(n, q) \)
• each row of the array is a coset of \( C \)
• the first row consists of the code itself
• the first column consisting of the coset leaders
• The rows are ordered so that the weights of coset leaders are non-decreasing as you pass from top to bottom

Standard array decoding
• If the received word in \( y \), find \( y \) in the standard array.
• Decode \( y \) to the top element in its column. Equivalently, subtract from \( y \) the coset leader of \( y + C \).
• Incomplete standard array decoding: decode a received word \( y \) if and only if the coset leader of \( y + C \) has weight at most \( \lceil (d - 1)/2 \rceil \); otherwise, declare an error.

The syndrome
• The syndrome of a word \( y \) in \( V(n, q) \) is \( S(y) = yH^T \).
• \( S(y) = 0 \) if and only if \( y \in C \).
• More generally, two words are in the same coset if and only if they have the same syndrome.

Syndrome decoding (a more practical version of standard array decoding): Let \( H \) be a parity check matrix for \( C \).
• For a received vector \( y \), compute the syndrome of \( y \)
• Find the coset leader \( e \) such that \( S(e) = S(y) \).
• Decode \( y \) as \( x = y - e \).