Exam Review Session Notes: Outline of Topics

We list the topics from the error-correcting codes material that will be possibly on the exam. The exam is cumulative; the topics from earlier parts of the course appear on the earlier posted outlines. Certain of those topics will be excluded, see the end of this outline for this listing.

1) Examples:
   - Repetition codes
   - Parity check code
   - 2D parity check
   - Hamming [7,4]: encoding and decoding.

2) Generalities
   - Definition of a q-ary \((n,M,d)\) code
   - Definition of Hamming distance and \(d(C)\).
   - Proof of triangle inequality
   - Proof of Theorem 1 from page 400.
     \[ (\text{Detect } s \text{ errors } \iff d(C) \geq s+1, \]
     \[ \text{Correct } 2s \text{ errors } \iff d(C) \geq 2s+1) \]
   - Definition of code rate: \( R = \frac{\log_2 M}{n} \) and interpretation as ratio of message symbols to \(n\) transmitted symbols.
3) Linear codes

- Definition of a linear q-ary \([n, k, d]\)-code.
- Definition of Hamming weight.
- Proof that \(d(C) = \text{minimum nonzero Hamming weight}\).
- Definition of generating matrix \(G\), parity-check matrix \(H\).
- Definition of these matrices in systematic form (i.e.: \(G = [I_k, P]\), \(H = [-P^T, I_{n-k}]\)).
- Definition of information symbols/check symbols.
- Proof that if \(G = [I_k, P]\), \(H = [-P^T, I_{n-k}]\), then \(vH^T = 0\) for every \(v \in C\). (Other direction of this will not be on test.)
- Definition of coset, coset leader, syndrome.
- Syndrome decoding algorithm, explanation of how this works (i.e.: \(vH^T = vH^T + cH^T = vH^T\), where \(v\) = received word, \(v \in \text{coset leader}, c \in C\), so by minimality of \(\text{wt}(v)\) in coset, \(d(C, r)\) is minimized.)
- Definition of dual codes.
- Know how Hamming codes are defined in general.
  (Explain how the parity check matrix \(H\) can be defined, then write it as \([-P^T, I_{n-k}]\) in order to define \(G = [I_k, P]\).)
- Know how correcting 1 error works in this example.
3) Cyclic codes

- Definition of cyclic codes; how to think of them in \( \mathbb{F}[X] \mod (X^n - 1) \).

*Proof that if \( C \subseteq \mathbb{F}[X] \mod (X^n - 1) \) is closed under multiplication by polynomials, it is cyclic, and vice-versa. (Remember: this is easy, since multiplication by \( X \) is the same as cycling the letters in a code word.)*

- Statement of the main theorem on page 429 including definition of the generating polynomial \( g \) of a cyclic code \( C \) and, given \( g \), the fact that
  \[
  C(g) = \{ g(x) f(x) \mid \deg(f) \leq n-1 - \deg(g) \} \quad \text{(by Part 3 of theorem)}
  \]

  \[
  = \{ g(x) f(x) \mid f(x) \in \mathbb{F}[X] \}.
  \]

- Proof of main theorem given strong hints. (I will tell you which division equation is used; you will also be given the needed other parts of the main theorem 3: the lemma * above.)

- Definition of \( h(x) \), the generating matrix \( G \), and the parity check matrix \( H \) for the cyclic code. You do not need to know the proof that \( H \) is a parity check matrix.

- Understand examples of cyclic codes.

4) BCH codes (extra credit problems only)

- Definition of \( n^{th} \) root of unity, primitive \( n^{th} \) root of unity.

- Statement of BCH bound

- Definition of BCH code, including definition of the \( f_i ' s \) and \( g_i ' s \).

- Understand how to compute the example of \( \mathbb{F}_2[X] \mod (X^7 - 1) \).
Remarks on earlier material 3. regular vs. extra credit problems.

There will be no question about Pohlig-Hellman on the final.
The birthday paradox 3 related material won't be on the final.
The following material will only appear in the extra credit problems if at all:

- Coin-Flipping
- Zero-knowledge proofs
- BCH codes (will definitely appear)