16/3/10
Error Correcting Codes.

1. The q-ary Johnson’s bound appear in Sudan, Thm 8.17, page 8-76. It shows any \((n,k,d)\) code is \((\tau_0 n - 1, n)\) list-decodable for \(\tau_0 = c - \sqrt{c(c-\delta)}\), \(c = 1 - \frac{1}{q}\). Generalize it to show a bound on the list size for \(\tau < \tau_0\). In particular, for what \(\tau\) the list size is a constant independent of \(n\)? Compare your bounds with Sudan, Thm 12.5 and Sudan, Thm 12.7.

2. Show \(B(\lambda n, n) < 2^{H(\lambda)n}\) and \(\lim_{n \to \infty} \frac{1}{n} \log B(\lambda n, n) = H(\lambda)\).
   Hint: Expand \((\lambda + (1 - \lambda))^{\frac{1}{n}}\) and use Stirling’s formula.

3. Alice holds \(x \in \{0, 1\}^n\) and Bob holds \(y \in \{0, 1\}^n\) and they wish to verify that \(x = y\). The goal is to use as few communication bits as possible. We allow Alice and Bob to use private random coins, and allow one-sided error, i.e., if \(x = y\) Alice and Bob should always accept, whereas whenever \(x \neq y\) Alice and Bob should reject with probability (over their coins) at least \(1 - \epsilon\).
   Show a protocol with \(\epsilon\) one-sided error and \(\log(n) + O(\log(\frac{1}{\epsilon}))\) communication bits.

4. Read the Wikipedia articles for (all or a subset of) Singleton bound, Hamming bound, Hamming code, Plotkin bound, Gilbert-Varshamov bound, list-decoding, Justensen code and the missing Elias-Bassalygo bound, and suggest improvements.

2/5/10

5. Let \(F\) be a finite field. What is the expected number of roots of a random univariate polynomial of degree \(k\) over \(F\) ?

6. Let \(Q \in F[X_1, \ldots, X_m]\) and \((a_1, \ldots, a_m) \in F^m\) and \(I = (i_1, \ldots, i_m)\) some direction. Show that the constraint \(Q(I)(a_1, \ldots, a_m) = 0\) translates to one linear equation on the coefficients of \(Q\).

7. Analyze the Parvaresh-Vardy code with \(H = h\), \(deg(E) = k\), \(d_0 = (h - 1)(k - 1)\) and general multiplicity \(\ell\), and show that you can get a code with \((\gamma n, n/k)\) list-decoding for some \(\gamma \geq 1 - 2e(\frac{1}{m})^{\frac{1}{m+1}}\). What multiplicity \(\ell\) do you need for that?

8. Let \(C \subseteq \Sigma^n\). In the list recovery problem the input is a set \(\{(x_i, S_i)\}\) where \(x_i \in [n]\) and \(S_i \subseteq \Sigma\), and a number \(t\). We say \(f \in \Sigma^n\) (which we also view as a function \(f : [n] \to \Sigma\)) has \(k\) agreement with the input, if there are \(k\) values \(i\) for which \(f(x_i) \in S_i\). The output of the list recovery problem is a list of all codewords of \(C\) that have \(t\) agreement with the input.
   - Explain why the RS list decoding algorithm also solves the list recovery problem. What parameters does it give?
   - Give an example for RS, where for each \(i\), \(|S_i| = |\Sigma|/2\) and yet the size of the output list is exponential.
   - What parameters does the PV list recovery algorithm give?
What parameters does the GR list recovery algorithm give?
Can you find a bad example for the GR list-recovery algorithm?

1/6/10

9. Prove that \( I = \{ p(x, y) \mid \text{the free coefficient is 0} \} \) is an ideal but not a principal ideal.

10. Prove that \( K(x) \) does not have places other than \( P_\infty \) and \( P_q(x) \) for irreducible polynomials \( q \).

11. Let \( F/K \) be an algebraic function field, i.e., an algebraic extension of \( K(x) \). Let \( \bar{K} \) be the field of all elements of \( F \) that are algebraic over \( K \).

   • Prove that \( \bar{K} = \{ f \in F \mid \forall P \in P_F, v_P(f) = 0 \} \).
   • Let \( P \) a place of degree 1 belonging to the valuation ring \( O \), and \( F_P = O/P \). Prove that \( \bar{K} \subseteq F_P \).

12. (Stichtenoth, III.1.4) Let \( F' \) is an algebraic extension of \( F/K \). \( P \in P_F, P' \in P_{F'} \), \( P \subseteq P' \). Prove that \( O_P \subseteq O_{P'}, O_P^* \subseteq O_{P'}^* \) and that there exists a natural number \( e \geq 1 \) such that for every \( f \in F \), \( val_{O'}(f) = eval_O(f) \).

13. Let \( K = F_q, F_0 = K(x_0), F_{i+1} = F_i(x_{i+1}) \mod x_{i+1}^2 = \frac{x_i^2 + 1}{x_i} \) be the tower we defined in class. Denote \( u_i = \frac{x_i^2 + 1}{x_i} \). We found in class the valuations of \( x_0, u_0, x_1, u_1 \) in \( F_1 \).

   • Find the valuations of \( x_0, u_0, x_1, u_1, x_2, u_2 \) in \( F_2 \).
   • Find the valuations of \( x_0, u_0, x_1, u_1, x_2, u_2, x_3, u_3 \) in \( F_3 \).

14. Show that in the above tower:

   • all extensions are separable (easy once you understand what you need to prove).
   • Let \( K_n \) denote the field of elements in \( F_n \) that are algebraic over \( K \). Show that for every \( n \geq 0, F_n = K \) (You may use Stichtenoth, III.7.4).