MATH 342—Quiz #1
May 17, 2006

No notes, books, or calculators allowed; put away all cell phones, pages, etc. and make sure that they won't beep. Show all your work and justify all of your responses fully, unless otherwise stated in the problem. You may write on the backs of pages if necessary. Do not remove the staple or any of the pages.

Name: Suggested Solutions **Student ID:** _____

1. For this problem, you only have to write the answers down—you don't have to prove anything.

(a) **[5 pts]** Describe precisely what it means for a code to be a q-ary (n, M, d)-code.

(b) **[5 pts]** Explain in words what the equality $A_2(10, 5) = 12$ means.

(a) q-ary (n, M, d)-code is a set of M codewords, where each codeword is a sequence of n symbols, each symbol chosen from a set $F_q = \{\lambda_1, \lambda_2 \dots \lambda_q\}$ of q distinct elements, with d being the smallest Hamming distance among the codewords

(or. a code 1. using an alphabet of q symbols.
2. every codeword has length n
3. there are exactly M codewords.
4. $d(x,y) \geq d$ $\forall$, $x, y \in C$, $x \neq y$, and $\exists$ $x, y \in C$ s.t. $d(x,y) = d$.)

(b) The maximal size of a binary code of length 10 and minimum distance 5, is 12 codewords.

(or all binary $(10, M, 5)$-code have $M \leq 12$, and there exists a binary $(10, 12, 5)$-code).

2. Consider the two codes

$$C_1 = \begin{matrix} \text{AAAAAAA} \\ \text{ABBBBBB} \\ \text{CCACBCC} \\ \text{CDDADBC} \end{matrix} \quad \text{and} \quad C_2 = \begin{matrix} 01111110 \\ 01100001 \\ 10011001 \\ 10000110 \end{matrix}.$$

C_1 is a $(7, 4, 5)$-code and C_2 is a binary $(8, 4, 5)$-code (you don't have to prove either of those statements).

(a) **[5 pts]** "Puncture" the code C_1 to produce a $(6, 4, 4)$-code. Explain the choices you make.

(b) **[5 pts]** "Lengthen" the code C_2 to produce a $(9, 4, 6)$-code. Explain how you calculated what bits to add.

(a) The only two codewords at distance 5 are the last two, (distance between any other pair is 6).

So deleting any columns where CCACBCC & CDDADBC are different. therefore puncturing any but the first or last column will result in a (6,4,4)- code.

(b). The weights of the codewords are 6, 3, 4, 3 respectively, use theorem 2.7 in the book, and add (0,1,0,1) column at the right as the overall parity check digits.

Example:

(a) delete the 4th column: new code is

AAAAAA
ABBBBB
CCABCC
CDDDBC

(b) answer is

011111100
011000011
100110010
100001101

3.

(a) **[3 pts]** Consider the ternary, length-5 word $\mathbf{x} = 21021$. ("Ternary" means that the possible symbols are "0", "1", and "2".) Compute the number of ternary words of length 5 whose Hamming distance from $\mathbf{x}$ is less than or equal to 2.

(b) **[7 pts]** There is an upper bound of the form

$$A_q(n, 2t+1) \leq \cdots$$

called the *sphere-packing bound.* Write down the sphere-packing bound and *briefly* describe how it was proved.

(a) $d=0$, only 1 word (itself).

$d=1$, $\binom{5}{1}(3-1) = 5\times 2 = 10$ words.

$d=2$, $\binom{5}{2}(3-1)^2 = 10\times 4 = 40$ words.

$\therefore 1+10+40 = 51$.

(b). $A_q(n, 2t+1) \leq \dfrac{q^n}{1+\binom{n}{1}(q-1)+\cdots+\binom{n}{t}(q-1)^t}$ is the bound.

Proof: (see book P19~20)

① $d(C) \geq 2t+1$, then the sphere of radius t centred on codeword c are disjoint. Otherwise if $y \in S(x,t)$, $y \in S(x',t)$, $x, x' \in C$, then $d(x,x') \leq d(x,y)+d(y,x') \leq t+t = 2t$

contradiction to $d(C) \geq 2t+1$.

② A sphere of radius t contains exactly $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i$ vectors. If $x \in C$ is the centre of sphere, then the # of vectors(y) with $d(x,y)=k$ is $\binom{n}{k}(q-1)^k$, since there are $\binom{n}{k}$ ways of choosing where x & y differ, and $(q-1)$ ways to choose how they differ at each position.

③. There are in total q^n vectors in $(\mathbb{F}_q)^n$

④. For $(n, M, 2t+1)$-code, $M\left\{\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\right\} \leq q^n$.

4. [10 pts] Let C be a code with $d(C) = 4$. Describe a "scheme" using C that simultaneously corrects single errors and detects double errors. (That is, describe how you would tell a computer to deal with received words that weren't necessarily codewords of C.) Prove that your scheme really does correct single errors and detect double errors.

Scheme:

given $\underline{v}$ is the received word, find the nearest neighbour $\underline{y}$ from C.

if $d(\underline{v}, \underline{y}) \leq 1$, decode as $\underline{y}$

if $d(\underline{v}, \underline{y}) \geq 2$, ERROR

Proof: $\underline{x}$ is sent, $\underline{v}$ is received. $x \in C$.

① by contradiction, assume the scheme incorrectly corrects single error.

so, it corrects to $\underline{y} \in C$ s.t. $\underline{y} \neq \underline{x}$. Since we used nearest neighbour correcting, we must have $d(\underline{y}, \underline{v}) \leq d(\underline{x}, \underline{v}) \overset{(=)}{\leq} 1$.

$\therefore d(x, y) \leq d(x, v) + d(v, y) = 2$ (*) by triangle inequality

contradiction to $d(c) = 4$ since $\underline{x}, \underline{y} \in C$.

②. Same idea, by contradiction.

Assume the scheme can fail to detect double errors,

which means there exist $\underline{y} \in C$, s.t. $d(\underline{v}, \underline{y}) \leq 1$,

And we know that $d(\underline{x}, \underline{v}) = 2$,

$\therefore d(x, y) \leq d(x, v) + d(v, y) \leq 1 + 2 = 3$. (*)

contradiction to $d(c) = 4$ since $x, y \in C$.

A direct proof is also fine, but (*) is important to be mentioned.