MAT 312 Spring 2009 Review for Midterm 1

1.1 Understand Theorem 1.1 (A parity check bit allows the detection of all single errors). Understand how Example 1.6 is an error-correcting code.

1.2 Be able to calculate the Hamming distance $H(\mathbf{a}, \mathbf{b})$ between two code words $\mathbf{a}$ and $\mathbf{b}$. Understand why the Hamming distance satisfies the triangle inequality. Be able to calculate the *minimum distance* d for a code whose code words are binary n-tples. Be able to prove Theorem 1.3 (If d is greater than or equal to 3, then the maximum likelihood decoding scheme corrects all single errors). Understand why this cannot work if $d = 2$.

1.3 Understand "addition" of binary n-tples as vector addition mod 2, and the definition of a *Group code* as one where the set of code words is closed under addition (Definition 1.4). Be able to prove Theorem 1.5 ($\mathbf{0}$ is a code word in any group code). Understand the *weight* $W(\mathbf{a})$ of a code word $\mathbf{a}$ and be able to prove $H(\mathbf{a}, \mathbf{b}) = W(\mathbf{a} + \mathbf{b})$ (Proposition 1.7). Be able to prove Theorem 1.8 (d of a code is the minimum weight of a nonzero code word).

1.4 Understand the *inner product* on the set of binary n-tples (Definition 1.6), and the relation between inner products and matrix multiplication (Definitions 1.8, 1.9). Be able to calculate matrix products as in Example 1.37, and understand that matrix product is distributive with respect to vector addition (Theorem 1.9). Be able to prove Theorem 1.11 (Given an $r \times n$ matrix H, the set of n-tples $\mathbf{a}$ such that $H\mathbf{a}^t = 0$ is a group code). This set is also called the *null-space* of H. Understand the definition of a *canonical parity-check matrix*.

1.5 Understand that if $\mathbf{e}_i$ is the n-tple with a 1 in the ith place and other entries 0, then multiplying $\mathbf{e}_i^t$ by an $r \times n$ matrix H yields the ith column of H. (Proposition 1.13). Be able to prove Theorem 1.14 (The null-space of H is a single-error-detecting code if and only if no column of H is $\mathbf{0}$). Be able to prove Theorem 1.15 (The null-space of H is a single-error-correcting code if and only if no column of H is $\mathbf{0}$ and no two columns of H are equal). Understand Example 1.54: how to construct an efficient single-error detecting group code encoding 2^m symbols. You need r check bits, where r is big enough for $2^r - r - 1 \geq m$. Then a canonical parity check matrix with r rows will do the trick.

Information theory. Be able to calculate the *entropy* $-\sum_i p_i \log_2 p_i$ for a

set of probabilities p_1,... p_N. Be able to make up an optimal code (lowest average cost in bits/character) for an alphabet of N characters x_1,... x_N ocurring with probabilities p_1,... p_N. Understand that the average cost in bits/character is always greater than the entropy.