Math 342 Problem set 7 (due 27/10/11)

Coding Theory: The Hamming Distance

Let Σ be a set ("alphabet"). Let $X = \Sigma^n$ be the set of sequences of length n ("words") consisting of elements of Σ. Given two words $\underline{w}, \underline{v} \in X$ we define their *Hamming distance* to be the number of positions at which they differ. That is, if $\underline{w} = (w_1, \ldots, w_n)$, $\underline{v} = (v_1, \ldots, v_n)$ we set:

$$d_{\mathrm{H}}(\underline{w}, \underline{v}) = \#\{i,\, 1 \leq i \leq n \mid w_i \neq v_i\} .$$

Example: if $\Sigma = \{0,1,2\}$, $n = 6$, $\underline{w} = 012212$, $\underline{v} = 022210$ then $d_{\mathrm{H}}(\underline{w}, \underline{v}) = 2$ (they differ in the 2nd and 6th letters).

1. Let $\Sigma = \{0,1\}$, $X = \Sigma^8$ (bit strings of length 8). Let $\underline{a} = 00000000$, $\underline{b} = 11110000$, $\underline{c} = 01001010$, $\underline{d} = 01001000$. Make a 4x4 table with rows and columns corresponding to these four vectors, and fill in each entry with the distance of the corresponding pair of vectors (there are 16 distances to find in total).

2. Going back to the general case of the Hamming distance on any $X = \Sigma^n$, show that d_{H} is a distance function:
   (a) Show that for any $\underline{w}, \underline{v} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{v}) = d_{\mathrm{H}}(\underline{v}, \underline{w})$.
   Hint: Convert the claimed assertion to words: "The number of positions at which $\underline{w}$ differs from $\underline{v}$ is equal to ..."
   (b) Show that for any $\underline{w}, \underline{v} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{w}) = 0$ but if $\underline{w} \neq \underline{v}$ then $d_{\mathrm{H}}(\underline{w}, \underline{v}) > 0$.
   Hint: Convert he assertions to words.
   (*c) (Triangle inequality) Show that for any $\underline{w}, \underline{v}, \underline{u} \in X$, $d_{\mathrm{H}}(\underline{w}, \underline{u}) \leq d_{\mathrm{H}}(\underline{w}, \underline{v}) + d_{\mathrm{H}}(\underline{v}, \underline{u})$.
   Hint: In what co-ordinates can $\underline{w}, \underline{u}$ differ?

Coding Theory: Repetition Coding

(Repetition coding) Alice and Bob can communicate through a channel which allows Alice to send one symbol at a time (in other words, Alice chooses a symbol from Σ, gives it to the channel, and Bob gets a symbol from the channel at the other end). Unfortunately, the channel is not perfect and sometimes Bob gets back a different symbol from the one transmitted by Alice. We assume however that the channel never loses symbols or creates new ones, so that Bob gets exactly one symbol for each symbol Alice transmits. In order to guard against errors, Alice and Bob agree that Alice send every letter of her message $2n+1$ times rather than just once.

3. Let's say Σ is the English alphabet and Alice will repeat every letter 5 times. Bob got HHHTH-EEUVE-LLLLL-LLRBL-OOOOK-WAWWW-YWWWW-OOOOO-RARRR-LALLL-DDDDD. Can you guess what message Alice wanted to send?

Of course, we'd like a computer to be able to make this "guess". Let's see how this is done.

4. Inside $X = \Sigma^{2n+1}$ let C be the set of "constant words": the set of words of the form $\sigma\sigma\sigma\ldots\sigma$ where $\sigma \in \Sigma$ (in problem 3, these would be: AAAAA to ZZZZZ).
   (a) Let $\underline{u}, \underline{v} \in C$ be distinct. What is $d_{\mathrm{H}}(\underline{u}, \underline{v})$?
   (b) Let $\underline{w} \in X$, and let $\underline{u}, \underline{v} \in C$ be both at distance at most n from $\underline{w}$. Use the triangle inequality to show $d_{\mathrm{H}}(\underline{u}, \underline{v}) \leq 2n$. Then use part (a) of this problem to show that $\underline{u} = \underline{v}$.

*5. Assume that the channel can corrupt at most n symbols out of any $2n+1$ it transmits. Show that Bob can unambiguously recover any message sent by Alice.

Rings and maps

6. (Injectivity and kernels: exercise in reading definitions) Let R, S be rings, and $f: R \to S$ a ring homomorphism. (The precise meaning is Definition 69 in the notes).
   (a) Assume that f is injective (also called $1-1$), that is that if $r, r' \in R$ are distinct then $f(r), f(r')$ are distinct elements of S. Show that if $r \in R$ satisfies $r \neq 0_R$ then $f(r) \neq 0_S$. *Hint*: What is $f(0_R)$?
   (b) Assume that f has the property that $f(r) = 0_S$ only if $r = 0_R$. Show that f is injective. *Hint:* Use $f(r) - f(r') = f(r - r')$.

7. (Scalar matrices) Let R be a ring, and let $S = M_n(R)$ be the ring of $n \times n$ matrices with entries in R. Let $\iota: R \to S$ be the map where $\iota(r)$ is the diagonal matrix with r along the diagonal and zeroes elsewhere) (if $n = 2$ then $\iota(r) = \begin{pmatrix} r & 0_R \\ 0_R & r \end{pmatrix}$).
   (a) Show that ι is a homomorphism of rings.
   (b) Show that ι is *injective*.
   (c) Let $T \subset S$ be the set of scalar matrices. Show that $\iota: R \to T$ is an isomorphism.

8. Let R be a ring. Call $a \in R$ *invertible* if there is $b \in R$ such that $ab = 1_R$, a *zero-divisor* if there is $b \in R$, $b \neq 0_R$, such that $ab = 0_R$. Let S be the ring R^X for some non-empty set X.
   (a) Let $f: \{0,1,2\} \to \mathbb{Z}/11\mathbb{Z}$ be the function $f(i) = [i]_{11}$. Is f a zero-divisor? If so find a non-zero $g \in (\mathbb{Z}/11\mathbb{Z})^{\{0,1,2\}}$ such that $fg = 0$.
   (b) Show that $f \in R^X$ is invertible in the ring R^X exactly when $f(x)$ is invertible in R for all x. What is the inverse?

Supplementary Problems

A. (The boolean ring) Let X be a set, $\mathcal{P}(X)$ the *powerset* of X, that is the set of subsets of X.
   (a) For $A, B \in \mathcal{P}(X)$ (that is, for two subsets of X) show that
   $$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$
   and that this is the set of elements of X that belong to *exactly one* of A, B. Call the set the *symmetric difference* and denote it $A \Delta B$.
   (b) Show that the symmetric difference is an associative and commutative operation on $\mathcal{P}(X)$. Show that the empty set is an netural element for this operation, and find an inverse to every set (for every A find B so that $A \Delta B = \emptyset$).
   (c) Show that the intersection opreation $(A, B \mapsto A \cap B)$ is an associative and commutative operation on $\mathcal{P}(X)$. Show that the set X is a neutral element for this operation.
   (d) (de Morgan's law) Show the distributive law $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
   (e) Conclude that $\mathcal{A} = (\mathcal{P}(X), \emptyset, X, \Delta, \cap)$ is a commutative ring.

B. (Characteristic functions) Consider the map $\chi \colon \mathcal{P}(X) \to (\mathbb{Z}/2\mathbb{Z})^X$ which associates to every $A \subset X$ the function $\chi_A \colon X \to \mathbb{Z}/2\mathbb{Z}$ where:
   $$\chi_A(x) = \begin{cases} [1]_2 & x \in A \\ [0]_2 & x \notin A \end{cases}.$$
   Show that χ is an isomorphism of the boolean ring $\mathcal{A}$ and the ring of functions from X to $\mathbb{Z}/2\mathbb{Z}$ with pointwise addition and multiplication.

C. Let $C(\mathbb{R})$ denote the ring of continuous real-valued functions defined on the entire real line. Let $\varphi \colon C(\mathbb{R}) \to \mathbb{R}$ be the *evaluation map* $\varphi(f) \stackrel{\text{def}}{=} f(0)$. In other words, φ is the rule that associates to each function $f \in C(\mathbb{R})$, the real number $f(0)$.
   (a) Show that φ is a ring homomorphism.
   (b) Did your proof use the continuity of f?
   (c) Let X be a set, R a ring. Choose a point $x \in X$, and consider the evaluation map $e_x \colon R^X \to R$ given by $e_x(f) \stackrel{\text{def}}{=} f(x)$ (recall that R^X is the ring of functions from X to R). Show that e_x is a ring homomorphism.