Mathematics Department Stanford University
Math 61DM Homework 5

Due at TA section, Friday Oct. 28

1. Suppose A is an $m \times n$ real matrix. Prove:

   (a) $A^{\mathrm{T}}A$ is positive semi-definite, and

   (b) $A^{\mathrm{T}}A$ is positive definite if $N(A) = \{\underset{\sim}{0}\}$.

Here we use the following terminology: an $n \times n$ matrix $B = (b_{ij})$ is positive semi-definite if $\underset{\sim}{x}^{\mathrm{T}}B\underset{\sim}{x} \geq 0$ for all $\underset{\sim}{x} \in \mathbb{R}^n$ and B is positive definite if $\underset{\sim}{x}^{\mathrm{T}}B\underset{\sim}{x} > 0$ for all $\underset{\sim}{x} \in \mathbb{R}^n \setminus \{\underset{\sim}{0}\}$. Notice that $\underset{\sim}{x}^{\mathrm{T}}B\underset{\sim}{x} = \sum_{i,j=1}^n b_{ij}x_ix_j$; such an expression is called a *quadratic form.* Similarly, for a linear map $T \in \mathcal{L}(V,V)$ where V is a finite dimensional inner product space, one says that T is positive semi-definite if $Tx \cdot x \geq 0$ for all $x \in V$, and one says that T is positive definite if $Tx \cdot x > 0$ for all $x \in V \setminus \{0\}$.

2. Suppose V is a finite dimensional real inner product space, $e_1, \ldots, e_n$ is an orthonormal basis for V, and suppose that $A \in \mathcal{L}(V,V)$. (i) Show that $\operatorname{trace} A = \sum_{j=1}^n e_j \cdot Ae_j$ is independent of the choice of the orthonormal basis of V. (ii) Define the inner product of $A, B \in \mathcal{L}(V,V)$ by $\langle A, B\rangle = \operatorname{trace}(B^{\mathrm{T}}A)$. Show that this *is* an inner product, and the corresponding squared norm is $\|A\|^2 = \sum_{i,j=1}^n a_{ij}^2$ where a_{ij} is the ij matrix entry of A in some orthonormal basis (in particular this sum is independent of the choice of orthonormal basis).

Note for (i): $e_j \cdot Ae_j$ is the jj entry of the matrix of A in the basis $e_1, \ldots, e_n$, so the trace is the sum of the diagonal entries of the matrix. Note for (ii): this norm is called the Hilbert-Schmidt norm, and it is discussed in Section 1.6 of the book in the setting of $\mathbb{R}^n$.

3. For each of the following permutations, find the parity (i.e. evenness or oddness) by two methods: (i) by directly calculating the number N of inversions, and (ii) by representing the permutation by a sequence of transpositions applied to the trivial permutation $(1, 2, \ldots, n)$:

$$\text{(a) } (4,3,1,5,7,2,6), \quad \text{(b) } (2,3,1,8,5,4,7,6).$$

4. For a point $x \in \mathbb{F}_2^n$ and a nonnegative integer r, the Hamming ball $B_r(x)$ of radius r around x is the set of all points y of distance at most r from x.
(i) Prove that $|B_r(x)| = \sum_{k=0}^r \binom{n}{k}$.
(ii) Prove that any code C that corrects for t errors has at most $2^n / \sum_{k=0}^t \binom{n}{k}$ elements.

5. Let $\ell \geq 2$ be an integer, $n = 2^\ell - 1$, and $k = n - \ell$. Recall that generalized Hamming code $\mathbb{F}_2^n$ has 2^k elements and can correct for a single error. Prove that any code in $\mathbb{F}_2^n$ with more than 2^k elements cannot correct for a single error.

6. Suppose that if a word is sent along a channel, the chance of an error in any given bit of the word is $1/10$, independent of the other bits in the word. Why would it not make sense to use the generalized Hamming code with $\ell = 10$ (so $n = 2^{10} - 1 = 1023$ and $k = n - \ell = 1013$)?

Hint: How likely is it that at most one error is made?

7. Suppose I wanted to send you a message which is just a nonnegative integer that is at most 15. I first convert it to binary as $abcd$ with $a, b, c, d \in \{0, 1\}$, which I then view as an element of $\mathbb{F}_2^4$. Next, using the Hamming code, I encode it as a seven bit codeword in $\mathbb{F}_2^7$. I then transmit it to you along a channel. In the message you receive, at most one error might occur in which one of the bits is misinterpreted. The received word is 1100010.
(i) How many errors occured in the received word?
(ii) What was the sent code word?
(iii) What was the integer I wanted to send you?

Show your work.