Dr. A. Betten Spring 06

M460 Information and Coding Theory

practice exam for Midterm # 2

not graded, no solutions!

Exercise # 1 (0 points)
Show that in a linear code over $\mathbb{F}_q$ either all codewords begin with 0, or exactly half of them begin with 0 and half of them begin with 1.

Exercise # 2 (0 points)
Define the "intersection" of two binary vectors u and v to be the vector

$$u \wedge v := (u_0 v_0, \ldots, u_{n-1} v_{n-1})$$

which has ones only where both u and v have ones. Also, let

$$u \vee v := (1 - (1 - u_0)(1 - v_0), \ldots, 1 - (1 - u_{n-1})(1 - v_{n-1}))$$

be the "union" of u and v, i.e. the vector which is one if at least one of u or v is one. Show that

$$\mathrm{wt}(u + v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2\mathrm{wt}(u \wedge v) = \mathrm{wt}(u \vee v) - \mathrm{wt}(u \wedge v).$$

Exercise # 3 (0 points)
Let u, v and w be binary vectors which are pairwise at distance d. Show that d is even and that there exists exactly one vector which is at distance $d/2$ from u, v, w. If u, v, w and x are binary vectors which are pairwise at distance d, show that there exists at most one vector at distance $d/2$ from u, v, w and x.

Exercise # 4 (0 points)
Evaluate the minimum distances of the binary codes which are generated by

a)

$$G := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

b)

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Exercise # 5 (0 points)

Let C be a binary, self-orthogonal code.

a) Show that each word of C is even (i.e., has even weight) and that $C^\perp$ contains the all-one vector $\mathbf{1}$.

b) Assume in addition that the length n of C is odd and that the dimension of C is $(n-1)/2$. Show that

$$C^\perp = C \cup (\mathbf{1} + C).$$

Exercise # 6 (0 points)

Show that a code with check matrix $H = (I_k \mid A)$ is self-dual if and only if A is a square matrix with $A \cdot A^\top = -I_k$.

Exercise # 7 (0 points)

Show the following:

a) If $u, v \in \mathbb{F}_2^n$, then $\langle u, v\rangle \equiv \mathrm{wt}(u \wedge v) \bmod 2$.

b) If $u \in \mathbb{F}_2^n$, then $\langle u, u\rangle \equiv \mathrm{wt}(u) \bmod 2$.

c) If $u \in \mathbb{F}_3^n$, then $\langle u, u\rangle \equiv \mathrm{wt}(u) \bmod 3$.

Exercise # 8 (0 points)

If C is a binary, self-orthogonal code, show that every codeword has even weight. Furthermore, if each row of the generator matrix G of C has weight divisible by 4, then so does every codeword.

Exercise # 9 (0 points)

Let C be a ternary, self-orthogonal code. Show that $\mathrm{wt}(c) \equiv 0 \bmod 3$ for every codeword $c \in C$.

Exercise # 10 (0 points)

A (n, k, d) code is perfect if the balls of radius $\lfloor (d-1)/2 \rfloor$ centered around codewords cover the whole space $\mathbb{F}_q^n$. Show that this is the case if and only if

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i = q^{n-k}.$$

Show that the $(7, 3)$-Hamming code is perfect. Verify that the following parameter sets describe perfect codes (which may or may not exist) $(n, k, d, q) = (23, 12, 7, 2)$, $(11, 6, 5, 3)$, $(90, 78, 5, 2)$.

Exercise # 11 (0 points)

Show that for any (n, k, d) code, we have $d \leq n - k + 1$.

Exercise # 12 (0 points)

Verify that the extended binary Hamming code is self-orthogonal.