Mathematics 392 – Seminar in Coding Theory
Discussion 2 – The "$(u|u+v)$" Code Construction,
And an Important Theorem on Minimum Distance
February 8, 2002

Background

The "$(u|u+v)$ construction" (and other variants of the same idea) is sometimes used to produce longer codes from known shorter codes, with reasonable control over the resulting minimum distance. It works like this: Let C be a linear (n,k,d) code and let D be a linear (n,l,d') code. We construct a new code E (of block length $2n$) whose codewords are of the form $(u|u+v)$ where $u \in C$ and $v \in D$. Today, we will explore this construction and relate the parameters of E to those of C and D.

Discussion Questions

A) Show first that E is always a linear code.

B) If $C = \langle\{101110, 010110, 110011\}\rangle$ and $D = \langle\{111001, 011011\}\rangle$, what is E? Find a basis (i.e. a generator matrix). Also determine the minimum distances of C, D, E.

C) Describe in general how to produce a generator matrix for E if you know generator matrices for C and D. (Hint: $(u|u+v) = (u|u) + (0|v)$.) Find and prove a formula for $\dim(E)$.

D) Suppose that $d' = 2d$. What is the minimum distance of E? Prove your assertion.

E) *The Important Theorem (this question is not related to A,B,C above)* – Suppose you knew a parity check matrix H for a linear code C with the property that *every set of four rows of H was linearly independent, but some set of five rows was linearly dependent*. Would this imply something about the minimum distance of C? Explain. State and prove a general result along these lines.

Assignment: Group write-ups due in class Friday, February 15.