Mathematics 392 – Seminar in Coding Theory
Selected Solutions – Discussion 2
February 18, 2002

C) The general formula relating the dimensions of C, D, E is

$$\dim(E) = k + \ell = \dim(C) + \dim(D).$$

To prove this, let $\gamma = \{u_1, \ldots, u_k\}$ be a basis for C and $\delta = \{v_1, \ldots, v_\ell\}$ be a basis for D. Then we claim that the set

$$\beta = \{(u_1|u_1), \ldots, (u_k|u_k), (0|v_1), \ldots, (0|v_\ell)\}$$

is a basis for E. Since $|\beta| = k + \ell$, this will prove our claim.

To show that β is a basis for E, we must show that β spans E and that β is linearly independent.

To see that β spans E, note that a general vector in E has the form $(u|u+v) = (u|u) + (0|v)$, where $u \in C$ and $v \in D$. Since γ is a basis for C, there exist scalars $c_i \in K$ such that $u = c_1u_1 + \cdots + c_ku_k$. Hence $(u|u) = c_1(u_1|u_1) + \cdots + c_k(u_k|u_k)$. Similarly, since δ is a basis for D, there exist scalars $d_j \in K$ such that $v = d_1v_1 + \cdots + d_\ell v_\ell$. Hence $(0|v) = d_1(0|v_1) + \cdots + d_\ell(0|v_\ell)$. Putting all this together, we have

$$(u|u+v) = (u|u) + (0|v) = c_1(u_1|u_1) + \cdots + c_k(u_k|u_k) + d_1(0|v_1) + \cdots + d_\ell(0|v_\ell)$$

This shows that $(u|u+v)$ is in the span of β.

To see that β is linearly independent, consider a linear combination of vectors in β that adds up to the zero word of length $2n$:

$$c_1(u_1|u_1) + \cdots + c_k(u_k|u_k) + d_1(0|v_1) + \cdots + d_\ell(0|v_\ell) = (0|0). \tag{1}$$

We can also write this as

$$(c_1u_1 + \cdots + c_ku_k|(c_1u_1 + \cdots + c_ku_k) + (d_1v_1 + \cdots + d_\ell v_\ell)) = (0|0). \tag{2}$$

Looking at the first half of the word, we see that $c_1u_1 + \cdots + c_ku_k = 0$. Since γ is a basis for C, the vectors u_i are linearly independent. Hence $c_1 = \cdots = c_k = 0$. Substituting this into (2), we have

$$(0|d_1v_1 + \cdots + d_\ell v_\ell) = (0|0).$$

Since δ is a basis for D, the vectors v_j are linearly independent, so $d_1 = d_2 = \cdots = d_\ell = 0$. Hence β is linearly independent as well, since all the coefficients in the linear combination in (1) must be zero.

D) The minimum distance of E is $2d$. To prove this, note that if the word $(u|u+v)$ is not zero, then $u \neq 0$, or $u = 0$ but $v \neq 0$. If the vector $u \in C$ is not zero, it has weight at least d by hypothesis. Say $wt(u) = d + r$, where $r \geq 0$. Similarly, if $v \neq 0$, then by hypothesis

$wt(v) \geq 2d$. In the word $(u|u+v)$, the first half has $d+r$ 1's, while the second half has *at least* $2d-(d+r)$ 1's. (There would be exactly this many if all the 1's in u canceled 1's in v. Note also that the inequality is still true if $2d-(d+r)<0$.) Hence the total weight is at least $d+r+2d-(d+r)=2d$. On the other hand if $u=0$, then $(0|v)$ has weight $\geq 2d$ by hypothesis (and some words achieve this minimum). This shows that every nonzero word in E has weight at least $2d$, and some words have weight exactly $2d$. Since E is linear this shows the claim about the minimum distance.

E) The general statement along these lines is that if H is a parity check matrix for C and H has the property that *every set of $d-1$ rows of H is linearly independent, but some set of d rows of H is linearly dependent*, then the minimum distance of C is d.

Proof: By the definition of a parity check matrix, $uH=0$ if and only if $u \in C$. Let $u=(u_1,\ldots,u_n) \in K^n$ be any vector, and let $H_1,\ldots,H_n$ be the rows of H. Then the matrix product uH is the same as the linear combination $u_1H_1+\cdots+u_nH_n$ of the rows of H. If every set of $d-1$ rows is linearly independent, but some set of rows of H is linearly dependent, then we have some linear combination

$$u_{i_1}H_{i_1}+\cdots+u_{i_d}H_{i_d}=0,$$

where not all $u_{i_j}=0$. Moreover, all the u_{i_j} must equal 1, or else we would have a linear dependence on $<d$ rows of H. By the above, the word u with 1's in positions $i_1,\ldots,i_d$ and zeros elsewhere satisfies $uH=0$. Hence u is a codeword of weight d, and there are no codewords of smaller weight. Since C is linear, the minimum distance is d.