Mathematics 392 – Seminar in Coding Theory
Selected Solutions – Midterm Problem Set
March 7, 2002

I B) It *is possible* for a binary code to contain two words u and v such that if u is transmitted, then any error of weight at most 2 can be corrected, while if v is transmitted, then there is some error of weight 1 that cannot be corrected. The idea, in rough terms, is that u can be *far away from all the other words in the code, while v is close to some other codeword w.* Specifically, in order for all errors of weight at most 2 to be correctable if u is transmitted, we want $d(u, x) \geq 5$ for all $x \in C$, $x \neq u$ (since then if two errors are introduced in u, the resulting word will still be closer to u than to any other codeword). On the other hand, we want some $v, w \in C$ such that $d(v, w) = 1$ (say). An example here is:

$$C = \{u = 000000, v = 111110, w = 111101\}.$$

Comment: Our theorem on the relation of the minimum distance and error-correction capacity deals with the *code as a whole*, not with individual codewords. It says: If $d = 2t+1$ or $2t+2$ then any error of weight t or less can be corrected by finding the closest codeword, no matter which codeword is transmitted. But the error-correction capacity of a code is *not necessarily uniform* across the whole code.

II. For both parts of this question, we want to consider the operation of deleting a fixed position from all words in some set. Deleting the ith position can be considered as a function

$$\begin{aligned} \Pi_i : K^n &\to K^{n-1} \\ (x_1, \ldots, x_n) &\mapsto (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \end{aligned}$$

The key observation you need to write "slick" proofs that punctured and shortened codes of linear codes are linear is this: If $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then $x + y = (x_1 + y_1, \ldots, x_n + y_n)$, so:

$$\begin{aligned} \Pi_i(x + y) &= (x_1 + y_1, \ldots, x_{i-1} + y_{i-1}, x_{i+1} + y_{i+1}, \ldots, x_n + y_n) \\ &= (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) + (y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n) \\ &= \Pi_i(x) + \Pi_i(y) \end{aligned}$$

That is, Π_i is a *linear mapping.*

A) Linearity: If C is linear and $C' = \Pi_i(C)$ is the punctured code, then C' contains the zero word. Moreover, for all $x', y' \in C'$, $x' = \Pi_i(x)$ for some $x \in C$, and $y' = \Pi_i(y)$ for some $y \in C$. Hence

$$x' + y' = \Pi_i(x) + \Pi_i(y) = \Pi_i(x + y)$$

by the above. Since C is assumed linear, $x + y \in C$. Hence, $x' + y' = \Pi_i(x + y)$ is in C'.

Dimension: For any word $z \in K^{n-1}$, there are two different words $x \in K^n$ such that $\Pi_i(x) = z$ (the deleted entry could be either a 0 or a 1). Hence the number of words in the image of C under Π_i is between $|C| = 2^k$ and $|C|/2 = 2^{k-1}$. The second case would happen only when every word in C' was the image of two distinct words in C. Thus $k - 1 \leq k' \leq k$.

Minimum distance: Since C' is linear, the minimum distance is the same as the minimum weight of a nonzero codeword in C'. We will assume $d > 1$, so no nonzero word in C punctures to the zero word in C'. Let $x' \in C'$. By definition, $x' = \Pi_i(x)$ for some $x \in C$. The weight of x' is $\geq d - 1$ since the weight of x is $\geq d$. This shows $d' \geq d - 1$. On the other hand, $d' \leq d$, since if we take a nonzero word of smallest weight d in C, then its image under the mapping Π_i is nonzero and has weight d at most (if the deleted entry is a 0).

B) The shortened code C'' is the same as $\Pi_i(C \cap H_i)$, where $H_i = \{x \in K^n : x_i = 0\}$.

Linearity: If C is linear and $C'' = \Pi_i(C \cap H_i)$ is the shortened code, then C'' contains the zero word. Moreover, for all $x'', y'' \in C'$, $x'' = \Pi_i(x)$ for some $x \in C \cap H_i$, and $y'' = \Pi_i(y)$ for some $y \in C \cap H_i$. Hence

$$x'' + y'' = \Pi_i(x) + \Pi_i(y) = \Pi_i(x + y)$$

by the above. Since C is assumed linear, $x + y \in C$. Moreover, since $x, y \in H_i$, $x + y \in H_i$ as well. Hence, $x'' + y'' = \Pi_i(x + y)$ is in C''.

Dimension: Π_i restricted to $C \cap H_i$ is one-to-one. Hence $|C''| = |C \cap H_i|$. Since an intersection of subspaces of a vector space is a subspace, $C \cap H_i$ is also a linear code. Its dimension is the same as $\dim(C)$ if $C \subset H_i$; otherwise $\dim(C \cap H_i) = \dim(C) - 1$. One way to see this is to think of making a parity check matrix for $C \cap H_i$ – you need one extra column containing the ith standard basis vector if not every word in C has a 0 in the ith position. Hence $k - 1 \leq k'' \leq k$.

Minimum distance. Since only zero entries are deleted to get words in C'', the minimum weight of a nonzero word in C'' is the same as the minimum weight of a nonzero word in $C \cap H_i$. Since $C \cap H_i$ is contained in C, we have $d'' \geq d$. But, $d'' > d$ is certainly possible if the only words of weight d in C all have 1's in position i. An example: $C = \{0000, 1100, 0111, 1011\}$, with $i = 2$. We have $C'' = \{000, 111\}$, so $d'' = 3$, but $d = 2$.

V.

B) Without working out the whole SDA for this code, you can see the required statements as follows. We have $n = 7, k = 4$. Hence there are $2^{n-k} = 2^3 = 8$ different cosets. On the other hand, by part A, $d = 3$, so every error of weight 1 can be corrected by finding the closest codeword. From a theorem proved in class (also see proof of 1.11.14 in text), this means that each word of weight ≤ 1 will be the unique leader in its coset. There are exactly $1 + 7 = 8$ words of weight ≤ 1 with $n = 7$. Hence every coset has a unique leader, since there are only 8 different cosets in all.

The words in each Hamming ball of radius 1, $B_1(x)$, $x \in C$, are the words of the form: codeword + error of weight ≤ 1. There are exactly 8 of these for each $x \in C$. Hence each ball contains exactly one word from each of the 8 cosets.

C) Following the reasoning in part B, the desired property holds only when the number of words in $B_1(x)$ is the same as the number of cosets: $1 + n = 2^{n-k}$. Letting $n - k = r$, we see that this means $n = 2^r - 1$, and $k = n - r = 2^r - r - 1$. (These are the parameters for the Hamming codes – the perfect codes with $d = 3$.)