MATH 2568H: Project 1

Liam Schmidt

10/3/2025

Q1: Most Likely Transmitted Codeword

When Bob recieves a message $y \in \{0,1\}^n$, the codeword that was most likely sent by Alice was the one that differs from y by the fewest bits. The hamming distance $d_H(x,y)$ counts the number of differing bits.
Therefor the codeword in C that is most likely to be the codeword transmitted by Alice is the one with the minimum hamming distance.

Q2: Maximum Bit Flips

The maximum number of bit flips that can occur in a code with a minimum distance d is

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

For example, given a code that is a subset of $\{0,1\}^1$ the two options are $\{0\}$ and $\{1\}$. Using the formula above, the maximum number of bits allowed to be flipped is 0. If any one bit is flipped, the message is unable to be deciphered. Because the minimum distance is the minimum distance between any two codewords in the code, a codeword can not have more than $d/2$ bits flipped without the noisy codeword being closer to a different codeword.

Q3: Codes with largest min distance

Two code words: {000,111}. Since there are only three bits and two codewords, the largest the minimum distance can be is three bits.
Three code words: {000, 101, 011}. Since there are only three bits and three codewords, it is impossible for the minimum distance to be 3. If you add any element of $\{0,1\}^3$ to the set of two codewords, the distance must be less than 3.
Four code words: {000, 101, 011, 110}. For same reason as three code words, the minimum distance can not be three, but this combination has a minimum distance of two which is the largest it could be.

Q4: Min distance in code C

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \; x_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \; ...x_{16} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Since the first four by four square of G is an identity map, Gx = $\begin{bmatrix} x \\ Px \end{bmatrix}$ where P is the bottom 3 x 4 rectangle of G.

Px $= x_1p_1 + x_2p_2 + x_3p_3 + x_4p_4$ where p_i is the ith column of P. Weight$(p_1) = 2$, Weight$(p_2) = 2$, Weight$(p_3) = 2$, Weight$(p_4) = 3$. If the weight of x is 0, then the corresponding weight of Gx is also 0. If the weight of x is 1, then the weight of Px $\geq$ weight$(p_i) \geq 2$.Therefor the weight of Gx when x has a weight of 1 is $\geq 1 + 2 = 3$

For x with a weight of 2, then Px $= p_i + p_j$ where i and j are two columns of P corresponding to where x has 1's. Since no two columns of P are exactly identical, $p_i + p_j$ must have atleast a one in the resulting vector. Therefor, weight(Px) when x has a weight of 2 is atleast one. The total weight of x in this case is $\geq 2 + 1 = 3$.

When x has a weight of 3, the total weight of Gx is already atleast 3.

When x has a weight of 4, the total weight of Gx is already atleast 4.

The distance between any two codewords x_i and x_j is equivalent to the number of different bits. The number of different bits is the same as weight$(x_i + x_j)$. Since the code is linear, it is closed under addition. This means that $x_i + x_j \in C$. Therefor the minimum distance would be equivalent to the minimum non-zero weight of the 16 codewords. Since the minimum weight as shown above is three, this means the minimum distance is also three.

Q5: Determing the original message

As stated in Q4, the first four by four box of G is an identity map. This means that to determine a message x from the linear encoding Gx, you look at the first four rows of Gx.

Q6: ker(H)

The kernel of a matrix is the set of all vectors that when multiplied by the matrix result in the zero vector. This means that for any codeword c ∈ C, H(c) = 0. Since c = Gx, H(x) = H(G(x)) = (H * G)x. If H * G is 0, this means that the kernel of H is equal to C.

$$\begin{bmatrix}1 & 1 & 0 & 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 1 & 0 & 0 & 1\end{bmatrix} * \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\end{bmatrix}$$

Row one column one: $1(1) + 1(0) + 0(0) + 1(0) +1(1) + 0(1) + 0(0) = 1 + 0 + 0 + 0 + 1 + 0 + 0 = 1 + 1 = 0$

Row one column two: $1(0) + 1(1) + 0(0) + 1(0) +1(1) + 0(0) + 0(1) = 0 + 1 + 0 + 0 + 1 + 0 + 0 = 1 + 1 = 0$

Row one column three: $1(0) + 1(0) + 0(1) + 1(0) +1(0) + 0(1) + 0(1) = 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$

Row one column four: $1(0) + 1(0) + 0(0) + 1(1) +1(1) + 0(1) + 0(1) = 0 + 0 + 0 + 1 + 1 + 0 + 0 = 1 + 1 = 0$

Row two column one: $1(1) + 0(0) + 1(0) + 1(0) + 0(1) + 1(1) + 0(0) = 1 + 0 + 0 + 0 + 0 + 1 + 0 = 1 + 1 = 0$

Row two column two: $1(0) + 0(1) + 1(0) + 1(0) + 0(1) + 1(0) + 0(1) = 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$

Row two column three: $1(0) + 0(0) + 1(1) + 1(0) + 0(0) + 1(1) + 0(1) = 0 + 0 + 1 + 0 + 0 + 1 + 0 = 1 + 1 = 0$

Row two column four: $1(0) + 0(0) + 1(0) + 1(1) + 0(1) + 1(1) + 0(1) = 0 + 0 + 0 + 1 + 0 + 1 + 0 = 1 + 1 = 0$

Row three column one: $0(1) + 1(0) + 1(0) + 1(0) + 0(1) + 0(1) + 1(0) = 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$

Row three column two: $0(0) + 1(1) + 1(0) + 1(0) + 0(1) + 0(0) + 1(1) = 0 + 1 + 0 + 0 + 0 + 0 + 1 = 1 + 1 = 0$

Row three column three: $0(0) + 1(0) + 1(1) + 1(0) + 0(0) + 0(1) + 1(1) = 0 + 0 + 1 + 0 + 0 + 0 + 1 = 1 + 1 = 0$

Row three column four: $0(0) + 1(0) + 1(0) + 1(1) + 0(1) + 0(1) + 1(1) = 0 + 0 + 0 + 1 + 0 + 0 + 1 = 1 + 1 = 0$

Therefor the resulting matrix is $\begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}$ HG = 0_{3x4} therefor ker(H) = C

Q7: Using H to determine element of C

Since ker(H) = c, that means that for any given $y \in \mathbb{F}_2^7$. Therefor if we multiply y by H and get a result of $\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$ then y resides in C. Any other result means that y is not a codeword in C.

Q8: Inverting steps

To invert the steps, we start with the noisy version of the linear encoding of a codeword c. This can have either 0 or 1 bit flips. To determine if there is a bit flip, you multiply the noisy version by H. If you do not get an output of all zero's, you then know that there was a bit flip. To determine which element of c was flipped, you must first understand that the noisy version of the c is equal to $c + (0, ...c_i, ..., 0)$ where 0¡=i¡=6,c_1=1 and c_i is the ith bit of c. Therefor, when you multiply the noisy version by H, this is the same as H * $(c + (0, ...c_i, ..., 0))$ which equals H*c + H * $(0, ...c_i, ..., 0)$ = $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ + the ith column of H. This means to identify where the bit was flipped, you determine which column of H is the result of the multiplication of H and the noisy bit, and you then flip that element in c. Now that you have the intended codeword c, you can get the original message by just looking at the first four bits of c. This works because the first four rows of G are an identity map, meaning that a 4 bit message would be equivalent to the first four bits of a codeword. Now that you have the original four bit message, you can combine it with the message after it to create an 8-bit binary sequence. The next step is to convert from binary to decimal numbers. So for every non-zero element in the 8-bit sequence, sum together $2^{indexofnon-zeroelement}$. Now for each decimal number, you will use an ascii table to find the character relating to that value. The final step is to concatenate every character that you decoded into one string.

Q9: Decoding the message

”Dear Bob, How is the linear algebra homework coming along? Love, Alice”