Decoding Hamming Codes

1 Decoding

Encoding is easy: use the generator matrix G

Decoder problem:

- Input: a vector $v \in F^n$
- Output: The unique codeword c at Hamming distance $\leqslant 1$ from v

Remarkable property of the Hamming code: a vector $v \in F^n$ either is a codeword, or is at Hamming distance 1 from a unique codeword

1.1 Example

The source and destination use the (7,4,3)-Hamming code

The source wants to transmit the four bit message

$$m = (0, 0, 1, 1)$$

The source encodes the message

$$c = mG = (1, 0, 0, 0, 0, 1, 1)$$

During transmission on the channel, the sixth bit is flipped, the reciever then obtains

$$v = (1, 0, 0, 0, 0, 0, 1)$$

$$\mathbf{m} = (0, 0, 1, 1) \overset{\text{encoding}}{\longrightarrow} \mathbf{c} = (1, 0, 0, 0, 0, 1, 1)$$
$$\overset{\text{channel}}{\longrightarrow} \mathbf{v} = (1, 0, 0, 0, 0, 0, 1)$$

2 Decoding

2.1 Brute force

First method: Brute force

Denote the vectors of F^k as:

$$\mathbf{m}_0 = (0, 0, \ldots, 0), \mathbf{m}_1 = (0, 0, \ldots, 1), \ldots, \mathbf{m}_{2^k-1} = (1, 1, \ldots, 1)$$

Description: Compute the Hamming distance between the received vector v and the ith codeword m_iG until it is no more than 1.
Remark: For the brute force algorithm, we need G. It will be given in your practicals.

2.1.1 Example

For the (7,4,3)-Hamming code. Recieve $v = (1, 0, 0, 0, 0, 0, 1)$

$$\begin{aligned}
\mathbf{m}_0\mathbf{G} &= (0, 0, 0, 0, 0, 0, 0) : d_H(\mathbf{m}_0\mathbf{G}, \mathbf{v}) = 2 \\
\mathbf{m}_1\mathbf{G} &= (1, 1, 0, 1, 0, 0, 1) : d_H(\mathbf{m}_1\mathbf{G}, \mathbf{v}) = 2 \\
\mathbf{m}_2\mathbf{G} &= (0, 1, 0, 1, 0, 1, 0) : d_H(\mathbf{m}_2\mathbf{G}, \mathbf{v}) = 5 \\
\mathbf{m}_3\mathbf{G} &= (1, 0, 0, 0, 0, 1, 1) : d_H(\mathbf{m}_3\mathbf{G}, \mathbf{v}) = 1
\end{aligned}$$

Then the codeword is $c = m_3G = (1, 0, 0, 0, 0, 1, 1)$

2.2 Local Search

We know that the codeword c must be either v or of the form v with one bit flipped.

For $1 \leqslant i \leqslant n$ define $e_i = (0, ..., 0, 1, 0, ..., 0)$ were 1 is in the position i, then either c=v or $c = v + e_i$ for some i

Description: Check whether v is a codeword. If not, then flip each bit until we obtain a codeword.

This decoding algorithm does not require you to compute G

To check if a vector is a codeword, multiply by H^T, if the result is zero, then it is a codeword

2.2.1 Example

For the (7,4,3) - Hamming code. Recieve v=(1,0,0,0,0,0,1)

$$\begin{aligned}
\mathbf{v}\mathbf{H}^\top &= (1,1,0) \\
(\mathbf{v}+\mathbf{e}_1)\,\mathbf{H}^\top &= (1,1,1) \\
(\mathbf{v}+\mathbf{e}_2)\,\mathbf{H}^\top &= (1,0,0) \\
(\mathbf{v}+\mathbf{e}_3)\,\mathbf{H}^\top &= (1,0,1) \\
(\mathbf{v}+\mathbf{e}_4)\,\mathbf{H}^\top &= (0,1,0) \\
(\mathbf{v}+\mathbf{e}_5)\,\mathbf{H}^\top &= (0,1,1) \\
(\mathbf{v}+\mathbf{e}_6)\,\mathbf{H}^\top &= (0,0,0)
\end{aligned}$$

Then the codeword is $c = v + e_6 = (1, 0, 0, 0, 0, 1, 1)$

2.3 Syndrome - The best one to use and implement

The received word v is either a codeword or of the form $c + e_i$ for some i.

If v is a codeword, we have $vH^T = 0$. Otherwise

$$\begin{aligned}
\mathbf{v}\mathbf{H}^\top &= (\mathbf{c}+\mathbf{e}_i)\,\mathbf{H}^\top \\
&= \mathbf{c}\mathbf{H}^\top + \mathbf{e}_i\mathbf{H}^\top \\
&= \mathbf{e}_i\mathbf{H}^\top \\
&= i^{th} \text{ column of } \mathbf{H}
\end{aligned}$$

Description: Compute the **syndrome** vH^T to obtain i, and hence the correct codeword $v + e_i$

2.3.1 Example

For the $(7, 4, 3)$-Hamming code. Receive v=(1,0,0,0,0,0,1)
Compute

$$vH^T = (1, 1, 0)$$

Then $i = 1 \times 4 + 1 \times 2 + 0 \times 1 = 6$
The codeword is $c = v + e_6$=(1,0,0,0,0,1,1)

2.3.2 Example

Case 1: $vH^T = 0 \Rightarrow v = c$
Case 2 $vH^T \neq 0 \Rightarrow v = c + e_i$
$vH^T = (c + e_i)H^T = cH^T(0) + e_iH^T = e_iH^T$ = ith column of H=The number i in binary

vH^T gives 6 in binary, so the 6th bit is an error

3 Recovering the original message

Once we get the codeword c, we still need to get the original message m.

This is very easy with our choice of generator matrix: remove the positions $1, 2, 4, ..., 2^{r-1}$ from c.

E.g.: C=(1,0,**0**,0,**0,1,1**) means that the original message is $m = (0, 0, 1, 1)$