4. Fountain Codes

(a)

This transmission can recover from at most 3 lost symbols, and it could **always** recover from losing 1 symbol at most.

However, there are cases where it can't handle even just two lost symbols. For example, a specific pattern like losing both of the "a"s (the 1^{st} and 4^{th} symbols) – similarly, any loss that contains both "b"s (2^{nd} and 5^{th} symbols) or both "c"s (3^{rd} and 6^{th}) – can't be handled by this transmission.

4.

(b)

$$\vec{k} = \begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \\ \alpha_4 & \beta_4 & \gamma_4 \\ \alpha_5 & \beta_5 & \gamma_5 \\ \alpha_6 & \beta_6 & \gamma_6 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

(c) $\vec{V_1}^T = [1\ 0\ 0]$ $\quad \vec{V_2}^T = [0\ 1\ 0]$ $\quad \vec{V_3}^T = [0\ 0\ 1]$

$\vec{V_4}^T = [1\ 0\ 0]$ $\quad \vec{V_5}^T = [0\ 1\ 0]$ $\quad \vec{V_6}^T = [0\ 0\ 1]$

(d) Since $k_i = \vec{V_i}^T \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}$ and with the information given on $\vec{k}$ and $\vec{V_i}^T$

so. we only have:

$$\begin{aligned} 1a + 0\cdot b + 0\cdot c &= 7 \\ 1\cdot a + 1\cdot b + 0\, c &= 3 \\ 1\cdot a + 0\cdot b + 1\cdot c &= 4 \end{aligned} \quad \overset{\star}{\Leftrightarrow} \quad \left[\begin{array}{ccc|c} 1 & 0 & 0 & 7 \\ 1 & 1 & 0 & 3 \\ 1 & 0 & 1 & 4 \end{array}\right]$$

Row 2: Subtract Row 1 ; Row 3: Subtract Row 1, and this leads to:

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 7 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & -3 \end{array}\right]$$

So we have the solution $a=7,\ b=-4,\ c=-3$.

Thus, Yes, I can and the message was $\begin{bmatrix} 7 \\ -4 \\ -3 \end{bmatrix}$.

P.S.

(To justify the transformation $\star$, the system of linear equation can be expressed as

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 7 \\ 3 \\ 4 \end{bmatrix}$$

which leads to the augmented matrix)

(e)

The maximum loss is **four** symbols.

This is because that any 3 equations of the method in part (d) is linearly independent, which means that any 3 equations would give a unique solution, which could be used to recover the message. In other words, As long as the loss is less than or equal to 4 symbols, Bob can still recover the message.

(f)

Alice should use the strategy in part **(d)**.

Let Alice use the strategy in part (d). Since any three equations could help Bob recover the message, so it doesn't matter which linear combination gets lost as long as other 3 are sent through. Suppose only the second linear combination is lost – with "b" being lost and the value of "a" and "c" being sent through – then her fourth linear combination would contain the value of "$a + b$". Since Bob knows the value of "a", the fourth linear combination would give him enough information to recover the entire message.

Let Alice use the strategy in part (a). Again, if only the second linear combination is lost – in this case, with "b" being lost and the value of "a" and "c" being sent through – then her fourth linear combination is useless for Bob as it only provides information for "a", which means that he can't recover the entire message.

Thus, Alice should use the strategy in part (d).