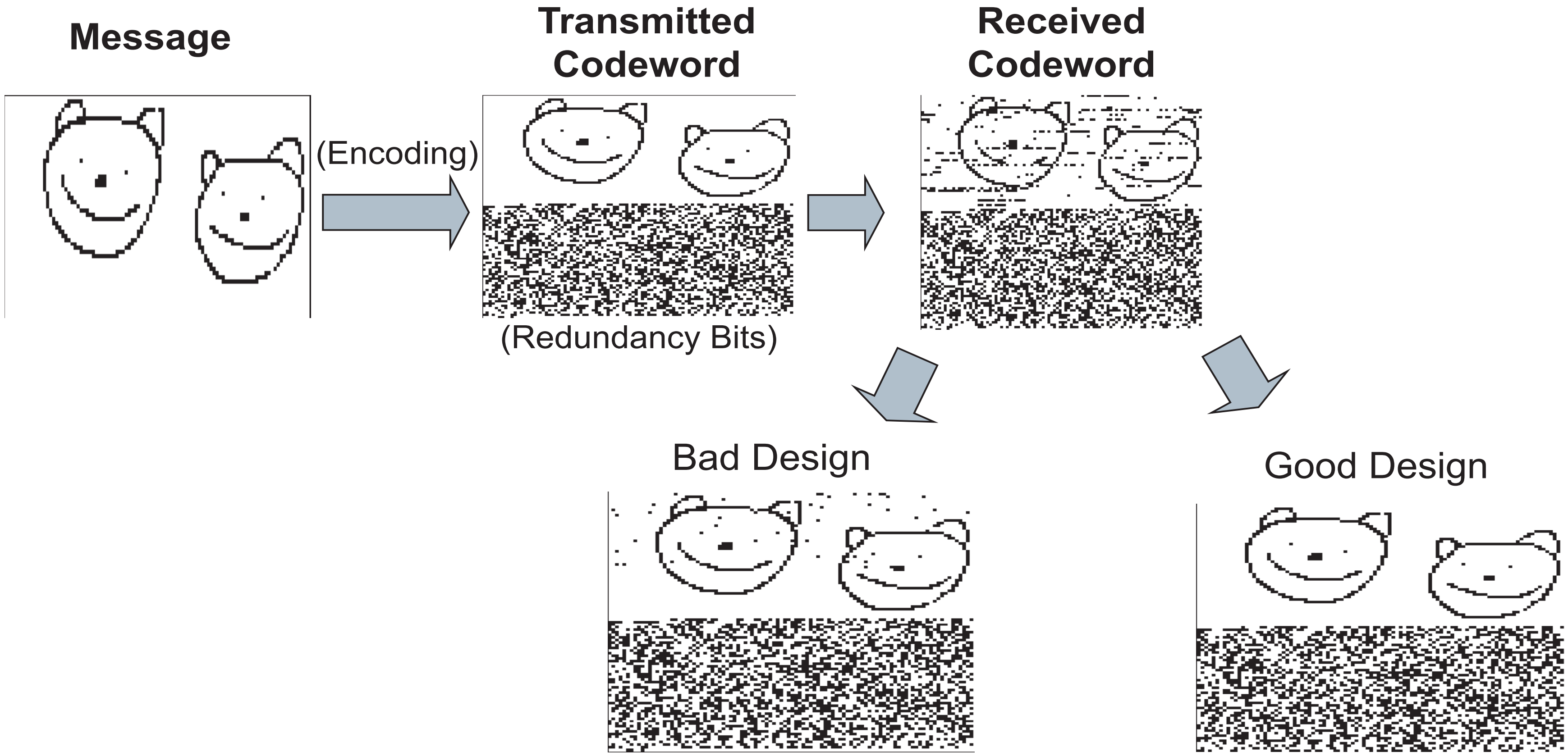
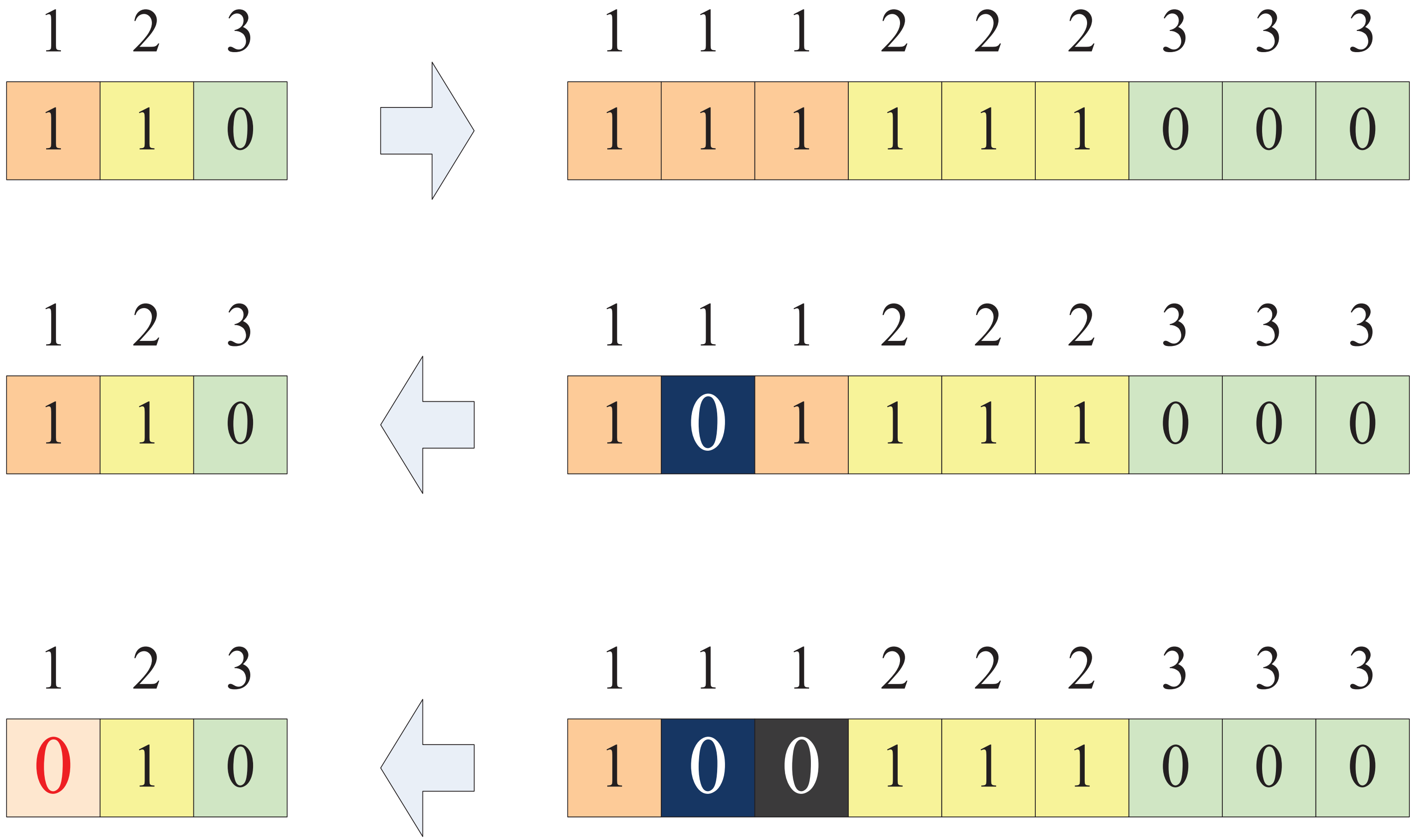
# Lecture 1 : Linear block codes

Lecturer: Yen-Ming Chen, National Sun Yat-sen University.

★ Error correcting code:



★ Example: Repetition code for BSC channel



★ A binary block code of length $n$ with $2^k$ codewords is called an $(n,k)$ linear block code iff its $2^k$ codewords form a $k$ dimensional subspace of the vector space $V$ of all the $n$-tuples over $GF(2)$.

★ For a binary $(n,k)$ linear block code $C$, there exists $k$ linear independent basis $\mathbf{g_0}, \mathbf{g_1}, \ldots, \mathbf{g_{k-1}}$ such that every codeword $\mathbf{v}$ in $C$ is a linear combination of these $k$ linearly independent basis.

★ Example: Systematic (7,4) Hamming code

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

, For a length-4 message vector $\mathbf{u}$, the corresponding codeword $\mathbf{v} = \mathbf{u} \cdot \mathbf{G}$

★ Let $\mathbf{u} = (u_0, u_1, ..., u_{k-1})$ be the message to be encoded. The codeword $\mathbf{v} = (v_0, v_1, ..., v_{n-1})$ for this message is given by

$$\mathbf{v} = u_0\mathbf{g_0} + u_1\mathbf{g_1} + \cdots + u_{k-1}\mathbf{g_{k-1}}$$

$$= \mathbf{u} \cdot \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \mathbf{u} \cdot \mathbf{G}$$

where $\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$

is a generator matrix of $\mathbf{C}$.

★ A code $\mathbf{C}$ can be regarded as the row space of $\mathbf{G}$.

★ A generator matrix of a given $(n, k)$ linear block code is not unique. Any choice of a basis of $C$ gives a generator matrix of $C$. The rank of a generator matrix of $C$ is equal to the dimension of $C$.

★ Since a binary $(n, k)$ linear block code $C$ is a $k$-dimensional subspace of the vector space $\mathbf{V}$ of all the $n$-tuples over $GF(2)$, its null (or dual) space, denoted $C_d$, is an $(n-k)$-dimensional subspace of $\mathbf{V}$ given by $C_d = \{\mathbf{w} \in V\colon \mathbf{w}\mathbf{v}^\top = 0$ for all $\mathbf{v} \in C\}$.

1. $C_d$ may be regarded as a binary $(n, n-k)$ linear block code and is called the dual code of $\mathbf{C}$.
2. Let $\mathbf{h_0}, \mathbf{h_1}, ..., \mathbf{h_{n-k-1}}$ be the $n-k$ linearly independent codewords of $C_d$ Form the following $(n-k) \times n$ matrix over $GF(2)$.

$$
\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{bmatrix}
= \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix}
$$

Then $\mathbf{H}$ is a generator matrix of $C_d$.

★ $\mathbf{H} \cdot \mathbf{G}^\top = \mathbf{0}_{(n-k)\times k}$

★ $C$ is also unquely specified by the $\mathbf{H}$ matrix as follows:
$C = \{\mathbf{v} \in V : \mathbf{H}\mathbf{v}^\top = \mathbf{H}\mathbf{G}^\top\mathbf{u}^\top = \mathbf{0}\}$
$\mathbf{H}$ is called a parity-check matrix (PCM) of $C$ and
$C$ is said to be the null space of $\mathbf{H}$.

★ In general, encoding of a linear block code is based on a generator matrix of the code and decoding is based on a parity-check matrix of the code.

★ A parity-check matrix $\mathbf{H}$ is said to be a full-rank matrix if its rank is equal to the number of rows of $\mathbf{H}$.

★ A linear systematic $(n, k)$ block code is completely specified by a $k \times n$ generator matrix of the following form

$$\mathbf{G} = [\mathbf{I}_k \ \mathbf{P}_{k\times(n-k)}]$$

The $\mathbf{P}$ submatrix of $\mathbf{G}$ is called the parity submartix of $\mathbf{G}$. A generator matrix in this form is said to be systematic form.

★ Given a $k \times n$ generator matrix $\mathbf{G}^{'}$ of an $(n, k)$ linear block code $C^{'}$ not in systematic form, a generator matrix $\mathbf{G}$ in the systematic form can always be obtained by performing elementary row operations on $\mathbf{G}^{'}$ and then possibly taking column permutations. The $k \times n$ matrix $\mathbf{G}$ is called a combinatorially equivalent matrix of $\mathbf{G}^{'}$.

★ The systematic $(n, k)$ linear block code $\mathbf{C}$ generated by $\mathbf{G}$ is called a combinatorially equivalent code of $\mathbf{C}^{'}$. Two combinatorially equivalent $(n, k)$ linear block codes give the same error performance.

★ If a generator matrix of an $(n, k)$ linear block code $\mathbf{C}$ is given by $\mathbf{G} = [\mathbf{I}_k \quad \mathbf{P}]$, then its corresponding PCM in systematic form is given by $\mathbf{H} = [\mathbf{P}^\top \quad \mathbf{I}_{n-k}]$. It can be easily shown that $\mathbf{H}\mathbf{G}^\top = 0$.

★ Example:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \Rightarrow \mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [\mathbf{I}_k \ \mathbf{P}_{k\times(n-k)}]$$

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [\mathbf{P}^{\top}_{(n-k)\times k} \ \mathbf{I}_{n-k}]$$

★ Syndrom decoding:

Let $\mathbf{u} = \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}$

Encoding: $\mathbf{v} = \mathbf{u} \cdot \mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$

If one bit error happens under BSC channel, and the received signal vector

$$\mathbf{z} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} = \mathbf{v} + \mathbf{n} = \mathbf{v} + \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\mathbf{H} \cdot \mathbf{z}^\top = \mathbf{H} \cdot (\mathbf{v} + \mathbf{n})^\top = \mathbf{H} \cdot \mathbf{G}^\top \cdot \mathbf{u}^\top + \mathbf{H} \cdot \mathbf{n}^\top = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^\top$$

$\Rightarrow$ the third column of $\mathbf{H}$.