Corrections

- Slide IDC6-54:

$$
\begin{aligned}
&= \int_{\Re} f_X(x)\left[\frac{1}{2}\log_2(2\pi\sigma^2) + \log(2)\cdot\frac{(x-\mu)^2}{2\sigma^2}\right]dx \\
&= \int_{\Re} f_Y(x)\left[\frac{1}{2}\log_2(2\pi\sigma^2) + \log(2)\cdot\frac{(x-\mu)^2}{2\sigma^2}\right]dx
\end{aligned}
$$

should be

$$
\begin{aligned}
&= \int_{\Re} f_X(x)\left[\frac{1}{2}\log_2(2\pi\sigma^2) + \log_2(e)\cdot\frac{(x-\mu)^2}{2\sigma^2}\right]dx \\
&= \int_{\Re} f_Y(x)\left[\frac{1}{2}\log_2(2\pi\sigma^2) + \log_2(e)\cdot\frac{(x-\mu)^2}{2\sigma^2}\right]dx
\end{aligned}
$$

- Slide IDC 6-56: "$\lim_{\Delta 0}$" should be replaced by "$\lim_{\Delta\downarrow 0}$".
- Slide IDC 7-4: "retransmite" should be replaced by "retransmit".
- Slide IDC 7-8:

$$
= \begin{bmatrix} m_0 & m_1 & \cdots & m_{k-1} \end{bmatrix}
\begin{bmatrix}
g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\
g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\
ag_{0,0}+bg_{1,0} & ag_{0,1}+bg_{1,1} & \cdots & ag_{0,n-1}+bg_{1,n-1} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1}
\end{bmatrix}_{k\times n}
$$

$$
= \begin{bmatrix} \tilde{m}_0 & \tilde{m}_1 & \cdots & m_{k-1} \end{bmatrix}
\begin{bmatrix}
g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\
g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\
g_{3,0} & g_{3,1} & \cdots & g_{3,n-1} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1}
\end{bmatrix}_{(k-1)\times n}
$$

is better to be rewritten as

$$
= \begin{bmatrix} m_0 & m_1 & m_2 & m_3 & \cdots & m_{k-1} \end{bmatrix}
\begin{bmatrix}
g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\
g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\
ag_{0,0}+bg_{1,0} & ag_{0,1}+bg_{1,1} & \cdots & ag_{0,n-1}+bg_{1,n-1} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1}
\end{bmatrix}_{k\times n}
$$

$$
= \begin{bmatrix} \tilde{m}_0 & \tilde{m}_1 & m_3 & m_4 & \cdots & m_{k-1} \end{bmatrix}
\begin{bmatrix}
g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\
g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\
g_{3,0} & g_{3,1} & \cdots & g_{3,n-1} \\
\vdots & \vdots & \ddots & \vdots \\
g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1}
\end{bmatrix}_{(k-1)\times n}
$$

- Slide IDC 7-21: "$\boldsymbol{r}\mathbf{H}$" should be "$\boldsymbol{r}\mathbf{H}^T$". Two places.

1. (a) A lossy data compression scheme for source symbols in $\{0, 1\}$ is performed as follows.
   - First, the source sequence is segmented into blocks of 3 bits.
   - Then, the mapping below is performed.

$$\begin{aligned} 000 &\to 000 \\ 001 &\to 000 \\ 010 &\to 000 \\ 100 &\to 000 \\ 011 &\to 111 \\ 101 &\to 111 \\ 110 &\to 111 \\ 111 &\to 111 \end{aligned}$$

   Compress the input sequence $s_0 s_1 \ldots s_{17} = 001010100101011000$ to $v_0 v_1 \ldots v_{17}$ using the compression scheme above.

   (b) Use the Hamming distortion measure give by

$$d(s, v) = \begin{cases} 1, & s \neq v \\ 0, & s = v \end{cases}$$

   and suppose the distortion is additive, i.e.,

$$d(s_0 s_1 s_2 \ldots s_{n-1}, v_0 v_1 v_2 \ldots v_{n-1}) = \sum_{i=0}^{n-1} d(s_i, v_i).$$

   What is the average distortion of the **particular** input sequence in (a)?

   (c) Suppose the input sequence $S_0 S_1 S_2 \ldots$ is i.i.d. with uniform marginal distribution. What is the expected value of the average distortion of the scheme in (a)?

   (d) Find the rate distortion function $R(D)$ for $D = \frac{1}{4}$. Can we find a lossy data compression scheme *better* than the one in (a) in the sense that the same distortion requirement can be fulfilled but a lower compression rate can be achieved?
   Hint: For i.i.d. binary source sequence,

$$R(D) = H_b(p) - H_b(D) \text{ bits/source symbol},$$

   where $\Pr[S_i = 0] = p$ and

$$H_b(p) = p \log_2 \frac{1}{p} + (1 - p) \log_2 \frac{1}{(1 - p)}.$$

Solution.

(a) $s_0 s_1 \ldots s_{17} = 001, 010, 100, 101, 011, 000 \to v_0 v_1 \ldots v_{17} = 000, 000, 000, 111, 111, 000$

(b) There are 18 source symbols. Hence, the average distortion of the **particular** input sequence is

$$\frac{d(s_0 s_1 \dots s_{17}, v_0 v_1 \dots v_{17})}{18} = \frac{1}{18} \underbrace{\sum_{i=0}^{17} d(s_i, v_i)}_{\substack{\text{distortion measure} \\ \text{is additive}}} = \frac{5}{18} \quad \text{(distortion per source symbol)}$$

(c) The expected value of the average distortion is

$$\begin{aligned}
\frac{1}{3}E[d(S_0S_1S_2, V_1V_2V_2)] &= \frac{1}{3}\Pr[S_0S_1S_2 = 000]d(000,000) + \frac{1}{3}\Pr[S_0S_1S_2 = 001]d(001,000) \\
&\quad + \frac{1}{3}\Pr[S_0S_1S_2 = 010]d(010,000) + \frac{1}{3}\Pr[S_0S_1S_2 = 011]d(011,111) \\
&\quad + \frac{1}{3}\Pr[S_0S_1S_2 = 100]d(100,000) + \frac{1}{3}\Pr[S_0S_1S_2 = 101]d(101,111) \\
&\quad + \frac{1}{3}\Pr[S_0S_1S_2 = 110]d(110,111) + \frac{1}{3}\Pr[S_0S_1S_2 = 111]d(111,111) \\
&= \frac{1}{3}\cdot\frac{1}{8}\cdot 0 + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 \\
&\quad + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 + \frac{1}{3}\cdot\frac{1}{8}\cdot 1 + \frac{1}{3}\cdot\frac{1}{8}\cdot 0 \\
&= \frac{1}{4} \text{ bits/source symbol}
\end{aligned}$$

(d)

$$\begin{aligned}
R(D) &= H_b(\tfrac{1}{2}) - H_b(\tfrac{1}{4}) \\
&= 1 - \left(\tfrac{1}{4}\log_2(4) + \tfrac{3}{4}\log_2(\tfrac{4}{3})\right) \\
&= \tfrac{3}{4}\log_2(3) - 1 \ (\approx 0.189 \text{ bits/source symbol})
\end{aligned}$$

The entropy rate (bits per source symbol) of the lossily compressed output sequence is

$$\begin{aligned}
\lim_{n\to\infty} \frac{H(V_0V_1\dots V_{n-1})}{n} &= \lim_{\ell\to\infty} \frac{1}{3\ell} \sum_{i=0}^{\ell-1} H(V_{3i}V_{3i+1}V_{3i+2}) \\
&\quad (\{V_{3i}V_{3i+1}V_{3i+2}\}_{i=0}^{\ell-1} \text{ are independent 3-tuples.} \\
&\quad \text{Note that } V_{3i} \text{ is actually strongly dependent on } V_{3i+1}. \\
&\quad \text{In fact, we have } \Pr[V_{3i} = V_{3i+1} = V_{3i+2}] = 1.) \\
&= \lim_{\ell\to\infty} \frac{1}{3\ell} \sum_{i=0}^{\ell-1} \left(\frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2\right) \\
&\quad (\text{Because } \Pr[V_{3i}V_{3i+1}V_{3i+2} = 000] = \Pr[V_{3i}V_{3i+1}V_{3i+2} = 111] = \frac{1}{2}) \\
&= \frac{1}{3} \text{ bits/source symbol.}
\end{aligned}$$

Since $R(\frac{1}{4}) \approx 0.189 < \frac{1}{3}$, according to Shannon's rate distortion theorem, there should exist a better lossy data compression scheme in the sense that a lower compression rate can be achieved subject to the expected value of the average distortion no larger than 1/4.

2. Finding the source distribution that maximizes **entropy** or **differential entropy** (i.e., richest in information content) is important in certain applications such as data analytics. Here are some examples.

   (a) (Maximal differential entropy) Prove that among all continuous random variables of mean μ and variance σ^2 (i.e., of the same "dc and ac energy"), Gaussian random variable has the largest differential entropy.

   (b) (Maximal differential entropy) Prove that among all continuous random variables of support $[a, b)$, the uniform random variable has the largest differential entropy.

   (c) (Maximal discrete entropy) Among all **discrete** random variables of finite support, say $\{0, 1, 2, \ldots, K-1\}$, what distribution gives the largest entropy? Justify your answer.

   (d) (Maximal discrete entropy) Prove that of all probability mass functions for a non-negative integer-valued random variable with mean μ, the geometric distribution given by

$$P_X(x) = \frac{1}{1+\mu}\left(\frac{\mu}{1+\mu}\right)^x, \quad \text{for } x = 0, 1, 2, \ldots,$$

   has the largest entropy.

Solution.

   (a) See Slide IDC 6-54.

   (b) See Slide IDC 6-55.

   (c) From Slide IDC 6-18, we know the uniform distribution over $\{0, 1, \ldots, K-1\}$ gives the largest entropy. Proof can be found in Slide IDC 6-18 and hence we omit it.

   (d) Let X be geometric distributed with mean μ, and let Y represent any other non-negative integer-valued random variable with the same mean. Then

$$\begin{aligned}
H(X) &= \sum_{x=0}^{\infty} P_X(x) \log_2 \frac{1}{P_X(x)} \\
&= \sum_{x=0}^{\infty} P_X(x) \left[\log_2(1+\mu) - x \cdot \log_2 \frac{\mu}{1+\mu}\right] \\
&= \log_2(1+\mu) - E[X] \cdot \log_2 \frac{\mu}{1+\mu} \\
&= \log_2(1+\mu) - E[Y] \cdot \log_2 \frac{\mu}{1+\mu} \\
&= \sum_{x=0}^{\infty} P_Y(x) \left[\log_2(1+\mu) - x \cdot \log_2 \frac{\mu}{1+\mu}\right] \\
&= \sum_{x=0}^{\infty} P_Y(x) \log_2 \frac{1}{P_X(x)}.
\end{aligned}$$

Hence,

$$
\begin{aligned}
H(X) - H(Y) &= \sum_{x=0}^{\infty} P_X(x) \log_2 \frac{1}{P_X(x)} - \sum_{x=0}^{\infty} P_Y(x) \log_2 \frac{1}{P_Y(x)} \\
&= \sum_{x=0}^{\infty} P_Y(x) \log_2 \frac{1}{P_X(x)} - \sum_{x=0}^{\infty} P_Y(x) \log_2 \frac{1}{P_Y(x)} \quad \text{(Change } P_X \text{ to } P_Y\text{.)} \\
&= \sum_{x=0}^{\infty} P_Y(x) \log_2 \frac{P_Y(x)}{P_X(x)} \quad \text{(Gather all log terms.)} \\
&= \sum_{x=0}^{\infty} P_Y(x) \log_2(e) \left(\ln \frac{P_Y(x)}{P_X(x)} \right) \quad \text{(Change to natural logarithm.)} \\
&\geq \sum_{x=0}^{\infty} P_Y(x) \log_2(e) \left(1 - \frac{P_X(x)}{P_Y(x)} \right) \quad \text{(Fundamental ineq. } y \geq 1 - \frac{1}{y} \ \forall y > 0.\text{)} \\
&= \sum_{x=0}^{\infty} \log_2(e) \left(P_Y(x) - P_X(x) \right) = \log_2(e) \left(\sum_{x=0}^{\infty} P_Y(x) - \sum_{x=0}^{\infty} P_X(x) \right) = 0,
\end{aligned}
$$

with equality holding iff $P_Y = P_X$.

Note: Now you shall sense what the shape of the source distribution that maximizes entropy or differential entropy looks like.

3. The (7,4) Hamming code can be generated via generator matrix

$$
\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \\ \mathbf{g}_4 \end{bmatrix}
$$

Its corresponding parity-check matrix is given by

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

(a) List all 2^4 codewords of the (7,4) Hamming code. What is the error correcting capability of this code?

(b) Is the parity-check matrix unique for the given generator matrix $\mathbf{G}$? If affirmative, prove it; if negative, give another parity-check matrix.
Hint: The parity-check matrix can be formed by three linearly independent row vectors that are orthogonal to the linear subspace spanned by $\mathbf{g}_1$, $\mathbf{g}_2$, $\mathbf{g}_3$ and $\mathbf{g}_4$.

(c) Give another generator matrix of the (7,4) Hamming code.
Hint: $\mathbf{G}$ can be formed by any k (non-zero) linearly independent $(1 \times n)$ codewords.

(d) List all the cosets of the (7,4) Hamming codes. There are eight of them.

(e) Find the coset leaders of the eight cosets.

Solution.

(a)

$$\underbrace{\begin{bmatrix}0&0&0&0\\0&0&0&1\\0&0&1&0\\0&0&1&1\\0&1&0&0\\0&1&0&1\\0&1&1&0\\0&1&1&1\\1&0&0&0\\1&0&0&1\\1&0&1&0\\1&0&1&1\\1&1&0&0\\1&1&0&1\\1&1&1&0\\1&1&1&1\end{bmatrix}}_{\text{all 16 possible inputs}}\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{bmatrix}=\begin{bmatrix}0&0&0&0&0&0&0\\1&0&1&0&0&0&1\\1&1&1&0&0&1&0\\0&1&0&0&0&1&1\\0&1&1&0&1&0&0\\1&1&0&0&1&0&1\\1&0&0&0&1&1&0\\0&0&1&0&1&1&1\\1&1&0&1&0&0&0\\0&1&1&1&0&0&1\\0&0&1&1&0&1&0\\1&0&0&1&0&1&1\\1&0&1&1&1&0&0\\0&0&0&1&1&0&1\\0&1&0&1&1&1&0\\1&1&1&1&1&1&1\end{bmatrix}$$

The smallest Hamming weight (i.e., the number of 1's in non-zero codewords) is 3. Hence, the error correcting capability is $\lfloor\frac{3-1}{2}\rfloor = 1$. So, this code guarantees to correct 1 bit error.

Note: I mark four rows by color red for later use.

(b) Writing

$$\mathbf{H} = \begin{bmatrix}\mathbf{h}_1\\\mathbf{h}_2\\\mathbf{h}_3\end{bmatrix},$$

we require $\mathbf{h}_i \cdot \mathbf{g}_j = 0$ for all i and j. Apparently,

$$\tilde{\mathbf{H}} = \begin{bmatrix}\mathbf{h}_1\\\mathbf{h}_1+\mathbf{h}_2\\\mathbf{h}_1+\mathbf{h}_2+\mathbf{h}_3\end{bmatrix}$$

can also serve as a parity-check matrix since we can easily prove that

$$\tilde{\mathbf{H}}\mathbf{G}^T = \mathbf{0} \text{ if, and only if } \mathbf{H}\mathbf{G}^T = \mathbf{0}.$$

Note: You are free to choose your own $\tilde{\mathbf{H}}$ via linearly combination as long as the three rows remain linearly independent.

(c) We can take four linear independent codewords in (a) (e.g., the four in color red) to form a new generator matrix:

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

(d) The seven cosets other than the codebook itself can be obtained by adding respectively the error patterns (listed below) to each of the codewords:

$$(0,0,0,0,0,0,1),(0,0,0,0,0,1,0),(0,0,0,0,1,0,0),(0,0,0,1,0,0,0),$$

$$(0,0,1,0,0,0,0),(0,1,0,0,0,0,0) \text{ and } (1,0,0,0,0,0,0).$$

As a result, the eight cosets are:

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

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

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

(e) The coset leader is on top of each coset in (d), which are $(0,0,0,0,0,0,0)$, $(0,0,0,0,0,0,1)$, $(0,0,0,0,0,1,0)$, $(0,0,0,0,1,0,0)$, $(0,0,0,1,0,0,0)$, $(0,0,1,0,0,0,0)$, $(0,1,0,0,0,0,0)$ and $(1,0,0,0,0,0,0)$.

4. Let the generator polynomial of a polynomial code of length $n = 5$ be $g(X) = X^3 + X + 1$.

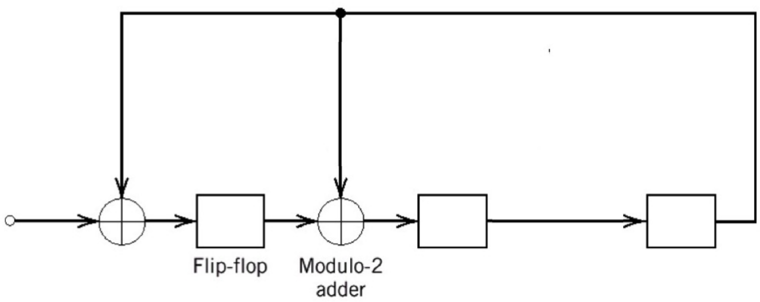
(a) List all the code polynomials of this polynomial code via

$$c(X) = a(X)g(X).$$

(b) List all the code polynomials of this polynomial code via

$$\bar{c}(X) = X^3 a(X) - X^3 a(X) \bmod g(X).$$

(c) For the division circuit below for the calculation of $X^3 a(X) \bmod g(X)$, indicate how many clock cycles are needed to complete the division and where the remainder is.



(d) Find the syndrome polynomial for received word polynomial $r(X) = 1 + X + X^2 + X^4$. In addition, determine the coset leader polynomial for this syndrome polynomial.

Solution.

(a) $c(X) = (a_0 + a_1 X)(1 + X + X^3)$ implies

$c(X)$	$(a_0 + a_1 X)(1 + X + X^3)$
$0 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4$	$(0 + 0 \cdot X)(1 + X + X^3)$
$0 + 1 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 1 \cdot X^4$	$(0 + 1 \cdot X)(1 + X + X^3)$
$1 + 1 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 + 0 \cdot X^4$	$(1 + 0 \cdot X)(1 + X + X^3)$
$1 + 0 \cdot X + 1 \cdot X^2 + 1 \cdot X^3 + 1 \cdot X^4$	$(1 + 1 \cdot X)(1 + X + X^3)$

(b) $\bar{c}(X) = X^3 a(X) - X^3 a(X) \bmod g(X)$ implies

$\bar{c}(X)$	$X^3 a(X)$	$X^3 a(X) \bmod g(X)$
$0 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4$	$0 \cdot X^3 + 0 \cdot X^4$	$0 + 0 \cdot X + 0 \cdot X^2$
$0 + 1 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 1 \cdot X^4$	$0 \cdot X^3 + 1 \cdot X^4$	$0 + 1 \cdot X + 1 \cdot X^2$
$1 + 1 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 + 0 \cdot X^4$	$1 \cdot X^3 + 0 \cdot X^4$	$1 + 1 \cdot X + 0 \cdot X^2$
$1 + 0 \cdot X + 1 \cdot X^2 + 1 \cdot X^3 + 1 \cdot X^4$	$1 \cdot X^3 + 1 \cdot X^4$	$1 + 0 \cdot X + 1 \cdot X^2$

(c) The input to this division circuit is $X^3 a(X)$, i.e., $000 a_0 a_1$ (a_1 should be entered first). We need $n = 5$ clocks to complete the division. The remainder is the content of the shift registers after $n = 5$ clocks.

(d) We derive

$$s(X) = r(X) \bmod g(X) = (1 + X + X^2 + X^4) \bmod (1 + X + X^3) = 1.$$

The coset contains $\{e(X) = c(X) + s(X) = c(X) + 1\}$ for all $c(X)$. Thus from the table in (a), we obtain

$e(X)$
$1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4$
$1 + 1 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 1 \cdot X^4$
$0 + 1 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 + 0 \cdot X^4$
$0 + 0 \cdot X + 1 \cdot X^2 + 1 \cdot X^3 + 1 \cdot X^4$

The coset leader polynomial is $1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4 = 1$.