Linear Block Codes III

Qi Zhang

Aarhus University School of Engineering

14/02/2014

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

1 Minimum Distance of a Block Code

2 Error Detection & Correction Capability of a Block Code

3 Standard Array and Syndrome Decoding

4 Hamming Codes

Hamming weight

- **Definition 2.2**: The number of non-zero components $c_i \neq 0$ of a given vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ of size $(1 \times n)$ is called the weight, or Hamming weight, $w(\mathbf{c})$, of that vector.
- In the case of vector defined over the binary field GF(2), the weight is the number of "1"s in the vector.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Hamming distance

- **Definition 2.3**: The Hamming distance between two vectors $\mathbf{c}_1 = (c_{01}, c_{11}, \ldots, c_{n-1,1})$ and $\mathbf{c}_2 = (c_{02}, c_{12}, \ldots, c_{n-1,2})$, is denoted by $d(\mathbf{c}_1, \mathbf{c}_2)$. It is the number of component position in which the two vectors differ.
- e.g., $\mathbf{c}_1 = (0011010)$ and $\mathbf{c}_2 = (1011100)$, then $d(\mathbf{c}_1, \mathbf{c}_2) = 3$.
- According to the definitions, there is

$$d(\mathbf{c}_i, \mathbf{c}_j) = w(\mathbf{c}_i \oplus \mathbf{c}_j)$$

- Hamming distance of two code vectors is equal to the weight of addition of these two code vectors;

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Hamming distance

- **Property**: The Hamming distance is a metric function that satisfies the *triangle inequality*.

$$d(\mathbf{c}_i, \mathbf{c}_k) + d(\mathbf{c}_j, \mathbf{c}_k) \geq d(\mathbf{c}_i, \mathbf{c}_j)$$

- **Proof**: As

$$\begin{aligned} d(\mathbf{c}_i, \mathbf{c}_k) &= w(\mathbf{c}_i \oplus \mathbf{c}_k) \\ d(\mathbf{c}_j, \mathbf{c}_k) &= w(\mathbf{c}_j \oplus \mathbf{c}_k) \\ d(\mathbf{c}_i, \mathbf{c}_j) &= w(\mathbf{c}_i \oplus \mathbf{c}_j) \end{aligned}$$

It is easy to understand that $w(\mathbf{u}) + w(\mathbf{v}) \geq w(\mathbf{u} \oplus \mathbf{v})$
Let $\mathbf{u} = \mathbf{c}_i \oplus \mathbf{c}_k$ and $\mathbf{v} = \mathbf{c}_j \oplus \mathbf{c}_k$, then there is

$$w(\mathbf{c}_i \oplus \mathbf{c}_k) + w(\mathbf{c}_j \oplus \mathbf{c}_k) \geq w(\mathbf{c}_i \oplus \mathbf{c}_k \oplus \mathbf{c}_j \oplus \mathbf{c}_k) = w(\mathbf{c}_i \oplus \mathbf{c}_j)$$

Therefore

$$d(\mathbf{c}_i, \mathbf{c}_k) + d(\mathbf{c}_j, \mathbf{c}_k) \geq d(\mathbf{c}_i, \mathbf{c}_j)$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Minimum Distance of a Block Code

- Minimum distance of the code, d_{min}: the minimum value of the distance between any two of the the codewords.

$$d_{min} = \min\{d(\mathbf{c}_i, \mathbf{c}_j); \mathbf{c}_i, \mathbf{c}_j \in C_b; \mathbf{c}_i \neq \mathbf{c}_j\}$$

- As addition of any two code vectors becomes another code vector in linear block code, the Hamming distance of two code vectors is equal to the weight of another code vector.

$$\begin{aligned} d_{min} &= \min\{w(\mathbf{c}_i \oplus \mathbf{c}_j); \mathbf{c}_i, \mathbf{c}_j \in C_b; \mathbf{c}_i \neq \mathbf{c}_j\} \\ &= \min\{w(\mathbf{c}_m); \mathbf{c}_m \in C_b; \mathbf{c}_m \neq 0\} \end{aligned}$$

- Therefore, the minimum distance of a linear block code $C_b(n, k)$ is the minimum value of the weight of the non-zero codewords of that code.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Minimum distance and the structure of the H Matrix

- **Theorem 2.2**: Consider a linear block code $C_b(n, k)$ completely determined by its parity check matrix **H**, for each codeword of Hamming weight p_H, there exist p_H columns of the parity check matrix **H** whose sum is a all-zero vector.
  - In same way, if the parity check matrix **H** contains p_H columns whose sum is a all-zero vector, then there is a code vector of weigh p_H.

Minimum distance and the structure of the $\mathbf{H}$ Matrix

- Assuming,
  - a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ has a weight p_H, then there are p_H non-zero components, i.e., $c_{i_1} = c_{i_2} = \ldots = c_{i_{p_H}} = 1$, $0 \leq i_1 < i_2 < \ldots < i_{p_H} \leq n-1$;
  - $\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-1}]$.
- Since $\mathbf{c} \circ \mathbf{H}^T = \mathbf{0}$, then

$$\begin{aligned} \mathbf{c} \circ \mathbf{H}^T &= (c_0, c_1, \ldots, c_{n-1}) \circ [\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-1}]^T \\ &= c_{i_1} \bullet \mathbf{h}_{i_1} \oplus c_{i_2} \bullet \mathbf{h}_{i_2} \oplus \ldots \oplus c_{i_{p_H}} \bullet \mathbf{h}_{i_{p_H}} \\ &= \mathbf{h}_{i_1} \oplus \mathbf{h}_{i_2} \oplus \ldots \oplus \mathbf{h}_{i_{p_H}} = \mathbf{0} \end{aligned}$$

Minimum distance and the structure of the H Matrix

- **Corollary 2.7.1**: For a linear block code $C_b(n, k)$ completely determined by its parity check matrix $\mathbf{H}$, the minimum weight or minimum distance of this code is equal to the minimum number of columns of parity check matrix whose sum is a all-zero vector.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Minimum distance and the structure of the H Matrix

- **Example 2.13**: For a linear block code $C_b(7,4)$, its parity check matrix is given below, determine the minimum distance of this code.

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

- Let's look at the column vector $\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_6$, we notice that e.g.,

$$\begin{aligned} \mathbf{h}_0 \oplus \mathbf{h}_1 \oplus \mathbf{h}_4 &= (100) \oplus (010) \oplus (110) = \mathbf{0} \\ \mathbf{h}_0 \oplus \mathbf{h}_2 \oplus \mathbf{h}_6 &= (100) \oplus (001) \oplus (101) = \mathbf{0} \end{aligned}$$

- The minimum distance of this code is $d_{min} = 3$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Error Detection Capability of a Block Code

- Due to the effect of noise, a number of positions changed their value in the original vector **c**;
- If the noise modifies d_{min} positions and in the worst case a code vector is transformed into another vector of the code, then undetectable error occurs.
- If $d_{min} - 1$ positions are changed by noise, it is guaranteed that the codeword cannot be converted into another codeword;
- The error-detection capability of a linear block code $C_b(n, k)$ with minimum distance d_{min} is $d_{min} - 1$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error Detection Capability of a Block Code

- Error-detection capability of a code can also be measured by means of the undetectable probability:
- As we know, $\mathbf{s} = \mathbf{r} \circ \mathbf{H}^T = (\mathbf{c} \oplus \mathbf{e}) \circ \mathbf{H}^T = \mathbf{c} \circ \mathbf{H}^T \oplus \mathbf{e} \circ \mathbf{H}^T = \mathbf{e} \circ \mathbf{H}^T$;
- If $\mathbf{s} = \mathbf{0}$ but $\mathbf{e} \neq \mathbf{0}$, then such error is not detectable.
- Therefore, the undetectable probability is equal to the probability of an error vector equal to a non-zero codeword.
- It can be expressed as:

$$P_U(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

  - where A_i is the number of codewords of weight i, called weight distribution.
  - p is the error probability of BSC.

Error Detection Capability of a Block Code

- **Example 2.14**: To calculate the undetectable error probability of the linear block code $C_b(7,4)$, the weight distribution of this code is listed below:

$$A_0 = 1, \quad A_1 = A_2 = 0, \quad A_3 = 7, \quad A_4 = 7, \quad A_5 = A_6 = 0, \quad A_7 = 1$$

- **Solution**:

$$\begin{aligned} P_U(E) &= \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \\ &= 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7 \approx 7p^3 \end{aligned}$$

- If $p = 10^{-2}$, $P_U(E) \approx 7 \times 10^{-6}$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Maximum Likelihood Decoding.

- Let t be a positive integer. As d_{min} is either odd or even, there is

$$2t+1 \leq d_{min} \leq 2t+2$$

- A transmitted codeword $\mathbf{c}_1$ is transformed into $\mathbf{r}$. With respect of another codeword $\mathbf{c}_2$, there is

$$d(\mathbf{c}_1, \mathbf{r}) + d(\mathbf{c}_2, \mathbf{r}) \geq d(\mathbf{c}_1, \mathbf{c}_2)$$

- As $\mathbf{c}_1$ and $\mathbf{c}_2$ are codewords, there is

$$d(\mathbf{c}_1, \mathbf{c}_2) \geq d_{min} \geq 2t+1$$

- Suppose an error pattern of t' errors occurs during transmission of $\mathbf{c}_1$. Then $d(\mathbf{c}_1, \mathbf{r}) = t'$. And $d(\mathbf{c}_2, \mathbf{r}) \geq 2t+1-t'$. If $t' \leq t$, then $d(\mathbf{c}_2, \mathbf{r}) > t$.
- It shows that if an error pattern of t or fewer errors occur, the received vector $\mathbf{r}$ is closer to the transmitted codeword $\mathbf{c}_1$ than any other codeword $\mathbf{c}_2$ in C
- For a BSC, it means the probability $P(\mathbf{r}|\mathbf{c}_1)$ is higher than $P(\mathbf{r}|\mathbf{c}_2)$.
- This is the process of maximum likelihood decoding.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error Correction Capability of a Block Code

- In contrast, the code is not capable of correcting all the error pattern of error with $l > t$, for there is at least one case in which an error pattern of l errors results in a received vector that is closer to an incorrect codeword than to the transmitted codeword.
- Proof: Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be two codewords in C such that $d(\mathbf{c}_1, \mathbf{c}_2) = d_{min}$
  - Let $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{c}_1 + \mathbf{c}_2$.
  - $\mathbf{e}_1$ and $\mathbf{e}_2$ do not have nonzero components in common place.
  - Hence, $w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{c}_1 + \mathbf{c}_2) = d_{min}$
  - suppose that $\mathbf{c}_1$ is transmitted and is corrupted by $\mathbf{e}_1$, the received vector $\mathbf{r} = \mathbf{c}_1 + \mathbf{e}_1$;
  - Hence, $d(\mathbf{c}_1, \mathbf{r}) = w(\mathbf{c}_1 + \mathbf{r}) = w(\mathbf{e}_1)$.
  - There is $d(\mathbf{c}_2, \mathbf{r}) = w(\mathbf{c}_2 + \mathbf{r}) = w(\mathbf{c}_2 + \mathbf{c}_1 + \mathbf{e}_1) = w(\mathbf{e}_2)$
  - suppose $\mathbf{e}_1$ contains more than t errors $(w(\mathbf{e}_1) \geq t + 1)$, thus $w(\mathbf{e}_2) \leq t + 1$
- Hence there is $d(\mathbf{c}_1, \mathbf{r}) \geq d(\mathbf{c}_2, \mathbf{r})$. This inequality shows there exists an error pattern of $(l > t)$ errors that results in a received vector is closer to an incorrect codeword than to the transmitted codeword.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Error Correction Capability of a Block Code

- In summary, a block code with minimum distance d_{min} *guarantees* correction of all the error patterns of $t = \lfloor (d_{min} - 1)/2 \rfloor$ or fewer errors.
- The parameter $t = \lfloor (d_{min} - 1)/2 \rfloor$ is called the random-error-correcting capability of the code.
- The code is referred to as a t-error-correcting code.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Error Correction Capability of a Block Code

- Q: If we know a linear block code $C_b(n,k)$ can correct all the errors with weight t or less, what is the undecoded probability? Assuming the error probability of BSC is p.
- A: The undecoded probability is equal to the probability that more than t errors occur:

$$P_e = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

Error Detection & Correction Capability of a Block Code

- In a hybrid system, where errors are in part corrected and in part detected.
  - Error pattern of weight λ or less can be corrected;
  - Error pattern of weight is larger than λ but less than $l+1$, the system can detect it; $(\lambda < l)$
  - Such a system is possible if $d_{min} \geq l + \lambda + 1$.
- e.g., a liner block code $C_b(n, k)$ has minimum distance $d_{min} = 7$, this code can be used for correcting error pattern of weight $\lambda = 2$ or less and detecting error pattern of weight $l = 4$ or less.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Standard array

- For a (n, k) linear block code C.
- Any decoding scheme at the receiver is a rule to partition the 2^n possible received vectors into 2^k disjoint subsets D_1, D_2, ..., D_{2^k}.
- Each subset D_i is one-to-one correspondence to a codeword $\mathbf{c}_i$.
- If the received vector $\mathbf{r}$ is found in the subset D_i, $\mathbf{r}$ is decoded into $\mathbf{c}_i$.
- Decoding is correct if and only if the received vector $\mathbf{r}$ is in the subset D_i that corresponds to the codeword transmitted.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Standard array

- A method to partition is *standard array*:

$$
\begin{array}{cccccc}
\mathbf{c}_1 = \mathbf{0} & \mathbf{c}_2 & \dots & \mathbf{c}_i & \dots & \mathbf{c}_{2^k} \\
\mathbf{e}_2 & \mathbf{c}_2 \oplus \mathbf{e}_2 & \dots & \mathbf{c}_i \oplus \mathbf{e}_2 & \dots & \mathbf{c}_{2^k} \oplus \mathbf{e}_2 \\
\mathbf{e}_3 & \mathbf{c}_2 \oplus \mathbf{e}_3 & \dots & \mathbf{c}_i \oplus \mathbf{e}_3 & \dots & \mathbf{c}_{2^k} \oplus \mathbf{e}_3 \\
\vdots & & & & \vdots & \\
\mathbf{e}_j & \mathbf{c}_2 \oplus \mathbf{e}_j & \dots & \mathbf{c}_i \oplus \mathbf{e}_j & \dots & \mathbf{c}_{2^k} \oplus \mathbf{e}_j \\
\vdots & & & & \vdots & \\
\mathbf{e}_{2^{n-k}} & \mathbf{c}_2 \oplus \mathbf{e}_{2^{n-k}} & \dots & \mathbf{c}_i \oplus \mathbf{e}_{2^{n-k}} & \dots & \mathbf{c}_{2^k} \oplus \mathbf{e}_{2^{n-k}}
\end{array}
$$

  - A standard array has 2^{n-k} rows and 2^k columns.
  - The 2^{n-k} rows is called *cosets* of the code C. The first vector $\mathbf{e}_j$ at each row is called *coset leader* (or coset representative).
  - The 2^k columns correspond to the 2^k disjoint subsets D_1, D_2, ..., D_{2^k}.
  - Note that any vector in a coset can be used as its coset leader, which does not change the vectors of the coset.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Standard array

- **THEOREM**: No two vectors in the same row of a standard array are identical. Every vector appears in one and only one row.
- **THEOREM**: Every (n, k) linear block code is capable of correcting 2^{n-k} error patterns.
  - To minimize the probability of a decoding error, the error patterns that are most likely to occur for a given channel should be chosen as the coset leaders.
  - For a BSC, an error pattern of smaller weight is more probable than an error pattern of larger weight.
  - Therefore, each coset leader should be chosen to be a vector of least weight from the remaining available vectors.
  - The decoding based on the standard array is the *minimum distance decoding* (i.e., the maximum likelyhood decoding)

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Minimum distance decoding

- Let $\mathbf{r}$ be the received vector. Assume $\mathbf{r}$ is found in the ith column D_i and lth coset of the standard array.
- Then $\mathbf{r}$ is decoded into the codeword $\mathbf{c}_i$.
- As $\mathbf{r} = \mathbf{e}_l \oplus \mathbf{c}_i$, the distance between $\mathbf{r}$ and $\mathbf{c}_i$ is

$$d(\mathbf{r}, \mathbf{c}_i) = w(\mathbf{r} \oplus \mathbf{c}_i) = w(\mathbf{e}_l \oplus \mathbf{c}_i \oplus \mathbf{c}_i) = w(\mathbf{e}_l)$$

- If consider the distance between $\mathbf{r}$ and any other codeword $\mathbf{c}_j$.

$$d(\mathbf{r}, \mathbf{c}_j) = w(\mathbf{r} \oplus \mathbf{c}_j) = w(\mathbf{e}_l \oplus \mathbf{c}_i \oplus \mathbf{c}_j)$$

  as $\mathbf{c}_i$, $\mathbf{c}_j$ are two different codewords, the sum of them is a nonzero codeword, say $\mathbf{c}_s$, thus

$$d(\mathbf{r}, \mathbf{c}_j) = w(\mathbf{e}_l \oplus \mathbf{c}_s)$$

- As $\mathbf{e}_l$ and $\mathbf{e}_l \oplus \mathbf{c}_s$ are in the same coset and there is $w(\mathbf{e}_l) \leq w(\mathbf{e}_l \oplus \mathbf{c}_s)$, we can say

$$d(\mathbf{r}, \mathbf{c}_i) \leq d(\mathbf{r}, \mathbf{c}_j)$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

- We can conclude that a linear block code $C_b(n,k)$ can correct 2^{n-k} error patterns and can detect $2^n - 2^k$ error patterns.
- For a linear block code $C_b(n,k)$ with minimum distance d_{min}, all the vectors of weight equal to $t = \lfloor \frac{d_{min}-1}{2} \rfloor$ or less can be used as coset leaders.
- Not all the error patterns of weight $t+1$ can be corrected, even though some of them maybe can be corrected.
- **Example**: The standard array of a linear block code $C_b(6,3)$:

000000	011100	101010	110001	110110	101101	011011	000111
100000	111100	001010	010001	010110	001101	111011	100111
010000	001100	111010	100001	100110	111101	001011	010111
001000	010100	100010	111001	111110	100101	010011	001111
000100	011000	101110	110101	110010	101001	011111	000011
000010	011110	101000	110011	110100	101111	011001	000101
000001	011101	101011	110000	110111	101100	011010	000110
100100	111000	001110	010101	010010	001001	111111	100011

Syndrome decoding

- All the vectors of the same coset have the same syndrome. Assuming $\mathbf{e}_i$ is a coset leader, another vector in this coset can be denoted as $\mathbf{c}_j \oplus \mathbf{e}_i$, the syndrome of the non-coset header vector is

$$(\mathbf{c}_j \oplus \mathbf{e}_i) \circ \mathbf{H}^T = \mathbf{c}_j \circ \mathbf{H}^T \oplus \mathbf{e}_i \circ \mathbf{H}^T = \mathbf{e}_i \circ \mathbf{H}^T$$

  The syndrome of any vector in the coset is equal to the syndrome of the leader of this coset.
- Syndrome is a $(n-k)$-component vector, there are 2^{n-k} different syndrome vectors which are allocated to different coset. In other words, for each correctable error pattern, there is a different syndrome vector.
- So it is possible to decode by constructing a table with correctable error patterns and their corresponding syndrome vectors.
- The decoder can correct the received vector simply by adding error pattern to the received vector.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Syndrome decoding

- **Example 2.16**: For the linear block code $C_b(7,4)$ with parity check matrix:

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

  The received vector $\mathbf{r} = (1010011)$. Please determine the codeword $\mathbf{c}$.
- There are $2^4 = 16$ codewords and $2^{7-4} = 8$ cosets or correctable error patterns, each correctable error pattern has a unique syndrome vector.
- Error patterns and their corresponding syndrome vectors table:

Error patterns							Syndromes		
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0	0	1
0	0	0	1	0	0	0	1	1	0
0	0	0	0	1	0	0	0	1	1
0	0	0	0	0	1	0	1	1	1
0	0	0	0	0	0	1	1	0	1

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Syndrome decoding

continue...

- $\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (111)$
- Look up the decoding table and find the error pattern $\mathbf{e} = (0000010)$.
- Hence, the codeword is
  $\mathbf{c} = \mathbf{r} + \mathbf{e} = (1010011) + (0000010) = (1010001)$

Syndrome decoding summary

- Syndrome decoding or table-lookup decoding scheme consists of three steps:
  1. Compute the syndrome of $\mathbf{r}$, $\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T$.
  2. Locate the coset leader $\mathbf{e}_l$ whose syndrome is equal to $\mathbf{r} \cdot \mathbf{H}^T$. Then $\mathbf{e}_l$ is assumed to be the error pattern caused by the channel.
  3. Decode the received vector $\mathbf{r}$ into the codeword $\mathbf{c} = \mathbf{r} + \mathbf{e}_l$.
- In principle, table-lookup decoding can be applied to any (n, k) linear code, however, for large $n - k$, the implementation of this decoding scheme becomes impractical, either a large storage or a complicated logic circuitry is needed.
- Other variations of table-lookup decoding exist but each of these decoding schemes requires additional properties of a code other than the linear structure.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Linear block codes examples

- One class of linear block codes was discovered by Richard W. Hamming in 1950.
  - Hamming codes have a minimum distance of 3 and capable of correcting any single error
  - Hamming code can be decoded easily by table-lookup scheme.
- One class of linear block codes is the calss of Reed-Muller codes discovered by David E. Muller in 1954 and reformulated by Irwin S. Reed in the same year.
  - Reed-Muller codes form a large class of codes for multiple random error correction.

Hamming codes

- For any integer $m \geq 3$, there exists a Hamming code with the following characteristics:

length	$n = 2^m - 1$
Number of message bits	$k = 2^m - m - 1$
Number of parity check bits	$n - k = m$
Error correction capability	$t = 1$, $(d_{min} = 3)$

- For example:

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

$$\begin{aligned} n &= 2^3 - 1 = 7 \\ k &= 2^3 - 3 - 1 = 4 \\ n - k &= m = 3 \\ t &= 1 \ (d_{min} = 3) \end{aligned}$$

Hamming codes

- The parity check matrix **H** of a Hamming code is formed of non-zero m elements column vectors, its systematic form:

$$\mathbf{H} = \left[\mathbf{I}_m \mathbf{Q}\right]$$

  - Identity submatrix $\mathbf{I}_m$ of size $m \times m$;
  - Submatrix $\mathbf{Q}$ consists of $k = 2^m - m - 1$ columns formed with vectors of weight 2 or more.

- The systematic form of the generator matrix of Hamming code:

$$\mathbf{G} = \left[\mathbf{Q}^T \mathbf{I}_{2^m - m - 1}\right]$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Hamming codes

- The weight distribution of a Hamming code of length $n = 2^m - 1$ can be expressed by

$$A(z) = \frac{1}{n+1}\{(1+z)^n + n(1-z)(1-z^2)^{(n-1)/2}\}$$

  - The number of code vectors of weight i, A_i is the coefficient of z^i in the above polynomial

- This polynomial is the weight enumerator for Hamming codes.
- For example, the weight enumerator for the $(7, 4)$ Hamming code is

$$A(z) = \frac{1}{8}\{(1+z)^7 + 7(1-z)(1-z^2)^3\} = 1 + 7z^3 + 7z^4 + z^7$$

Hence, the weight distribution for the $(7, 4)$ Hamming code is $A_0 = 1$, $A_3 = 7$, $A_4 = 7$ and $A_7 = 1$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Homework

- The rest subproblems in 2.4 and 2.6
- The problem 2.5, 2.7 and 2.8
- Preparation reading Chapter 3.1 - 3.6.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN