

Error control coding: An introduction to linear block codes

Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

Mar. 28, 2016



Lecture #7B: Problem solving session-III



Linear block code

- **Problem #1:** Is it possible to have a linear $(16, 10, 8)$ binary block code? Justify your answer.

Linear block code

- **Problem #1:** Is it possible to have a linear $(16, 10, 8)$ binary block code? Justify your answer.
- **Solutions:** No, according to singleton bound $d_{\min} \leq n - k + 1$

Linear block code

- **Problem #2:** Is $(24,12,8)$ binary Golay code, a perfect code? Give reasons?

Linear block code

- **Problem #2:** Is $(24,12,8)$ binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.

Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right]$$

Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right]$$

- Perfect codes satisfy Hamming bound with equality.

Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right]$$

- Perfect codes satisfy Hamming bound with equality.
- (24, 12, 8) Golay code is a triple error correcting code.

Linear block code

- **Problem #2:** Is (24,12,8) binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right]$$

- Perfect codes satisfy Hamming bound with equality.
- (24, 12, 8) Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = 2325$$

Linear block code

- **Problem #2:** Is $(24,12,8)$ binary Golay code, a perfect code? Give reasons?
- **Solutions:** No, it doesn't satisfies Hamming bound with equality.
- **Hamming Bound:** For any binary (n, k) linear code with minimum distance $2t + 1$ or greater, the number of parity-check bits satisfies the following inequality:

$$2^{n-k} \geq \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right]$$

- Perfect codes satisfy Hamming bound with equality.
- $(24, 12, 8)$ Golay code is a triple error correcting code.
- R.H.S. of the Hamming bound =

$$1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 1 + 24 + 276 + 2024 = 2325$$

- However, L.H.S. of the Hamming bound is $2^{12} = 4096$.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ≡ ↺ 🔍 ↻

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ≡ ↺ 🔍 ↻

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ ($n - (n - k) + 1$).

Linear block code

- **Problem #3:** If C is maximum distance separable (MDS) code, its dual is also MDS code.
- **Solutions:** If C is a MDS code, then $d = (n - k + 1)$.
- This implies that no $(n - k)$ or fewer columns of $\mathbf{H}$ are linearly dependent.
- The dual code C_d has $\mathbf{H}$ as the generator matrix. So, the length of C_d is n and dimension $n - k$.
- To prove that the dual code is MDS, we have to show that the dual code has minimum distance of $k + 1$ ($n - (n - k) + 1$).
- Suppose there exists a codeword, $\mathbf{v}$ of weight $d' \leq k$. Then $\mathbf{v}$ has at most k ones and $(n - k)$ zero coordinates. Let's assume the last $(n - k)$ coordinates are zero.



Linear block code

- We can write the matrix $\mathbf{H}_{(n-k) \times n}$ as $[\mathbf{A}_{(n-k) \times k} \quad \mathbf{H}'_{(n-k) \times (n-k)}]$, where $\mathbf{H}'$ has $(n - k)$ independent columns, so invertible.



Linear block code

- We can write the matrix $\mathbf{H}_{(n-k) \times n}$ as $\begin{bmatrix} \mathbf{A}_{(n-k) \times k} & \mathbf{H}'_{(n-k) \times (n-k)} \end{bmatrix}$, where $\mathbf{H}'$ has $(n - k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H}'$ are also independent.

Linear block code

- We can write the matrix $\mathbf{H}_{(n-k) \times n}$ as $\begin{bmatrix} \mathbf{A}_{(n-k) \times k} & \mathbf{H}'_{(n-k) \times (n-k)} \end{bmatrix}$, where $\mathbf{H}'$ has $(n - k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H}'$ are also independent.
- To get zero in all the last $(n - k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H}'$. Therefore the entire codeword is zero. So $d' \geq k + 1$.

Linear block code

- We can write the matrix $\mathbf{H}_{(n-k) \times n}$ as $[\mathbf{A}_{(n-k) \times k} \quad \mathbf{H}'_{(n-k) \times (n-k)}]$, where $\mathbf{H}'$ has $(n - k)$ independent columns, so invertible.
- Hence the rows of $\mathbf{H}'$ are also independent.
- To get zero in all the last $(n - k)$ coordinates such as $\mathbf{v}$, is to use zero linear combination of the rows $\mathbf{H}'$. Therefore the entire codeword is zero. So $d' \geq k + 1$.
- But from singleton bound we know $d' \leq k + 1$. So we get $d' = k + 1$