uOttawa

L'Université canadienne
Canada's university

# ELG 5372 Error Control Coding

## Lecture 8: Parity Check Matrices and Decoding of Linear Block Codes

Université d'Ottawa | University of Ottawa

# Parity Check Matrix

- Let $C$ be an $(n,k)$ linear block code over $F_q$.
- Let $\mathbf{G}$ be the generator matrix of $C$.
- Let $\mathbf{H}$ be the generator matrix of $C'$, which is the $(n,n-k)$ dual code of $C$.
- Let $\mathbf{c}$ be a codeword from $C$.
- Since $\mathbf{c} = \mathbf{mG}$, then $\mathbf{cH}^T = \mathbf{mGH}^T = \mathbf{0}_{1,(n-k)}$ where $\mathbf{0}_{i,j}$ is an $i \times j$ all zero matrix.
- The $\mathbf{H}$ matrix can be used to check that $\mathbf{c}$ is a valid codeword, hence it is called the parity check matrix of $C$.

# Example

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

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

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

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

# Parity check equations

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

- Parity check matrix gives rise to a set of parity check equations
- $c_0+c_2+c_3+c_4=0$, $c_0+c_1+c_2+c_5=0$, $c_1+c_2+c_3+c_6=0$
- Or $c_4=c_0+c_2+c_3$, $c_5=c_0+c_1+c_2$, $c_6=c_1+c_2+c_3$.

# Linear Block Code Theorem 1

- Let linear block code $C$ have parity check matrix $\mathbf{H}$. The minimum distance of the code is equal to the smallest positive number of columns of $\mathbf{H}$ which are linearly dependent.

  – Proof

  Let the column vectors of $\mathbf{H}$ be designated $\mathbf{h}_0^T$, $\mathbf{h}_1^T$, … $\mathbf{h}_{n\text{-}1}^T$, where $\mathbf{h}_i$ is a 1×n vector. Let codeword $\mathbf{c}=[c_0\ c_1\ \ldots\ c_{n\text{-}1}]$ be a $1\times n$ codeword of $C$. Then $\mathbf{cH}^T = c_0\mathbf{h}_0+c_1\mathbf{h}_1+\ldots c_{n\text{-}1}\mathbf{h}_{n\text{-}1} = \mathbf{0}_{1,(n\text{-}k)}$.

  Let $\mathbf{c}$ be a codeword of $C$ of minimum weight. Therefore $HW(\mathbf{c}) = d_{min}$. Further, let $\mathbf{c}$ be nonzero at indices $i_1$, $i_2$, …, $i_{dmin}$. Then

# Linear Block Code Theorem 1 cont'd

$c_{i1}\mathbf{h}_{i1}+c_{i2}\mathrm{h}_{i2}+\ldots+c_{idmin}\mathbf{h}_{idmin} = \mathbf{0}_{1,(n-k)}$. Therefore we know that we can find at least one linear combination of $d_{min}$ column vectors of H that add up to zero.

Consequently, if there were a linearly dependent set of column vectors of less than $d_{min}$ column vectors, then there would have to be a corresponding codeword of weight that is less that $d_{min}$.

# Example of LBC Theorem 1

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

$$
\begin{array}{ccccccc}
\uparrow & \uparrow & & \uparrow & & & \\
 & & \uparrow & \uparrow & & \uparrow & \\
\uparrow & & \uparrow & & & & \uparrow
\end{array}
$$

# Rank of a Matrix

- The rank of a matrix is the number of maximum number of linearly independent rows or columns of a matrix.
  - The column rank is the maximum number of linearly independent columns
  - The row rank is the maximum number of linearly independent rows
  - Row rank = column rank.
- For a $(n\text{-}k) \times n$ **H** matrix, the row rank is $(n\text{-}k)$.
- Therefore column rank = (n-k). Therefore we know that we cannot find a set of n-k+1 linearly independent column vectors in **H**.

# Singleton Bound

- We know that $d_{min}$ is the minimum number of linearly dependent column vectors in **H** and form the previous slide, we know that the maximum number of linearly independent column vectors in **H** is $n$-$k$.
  - $d_{min} \leq n-k+1$.
- Any code that satisfies the Singleton Bound with equality is called a maximum separable (MDS) code.

# Example (4,2) 4-ary code

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha \end{bmatrix}$$

| **m** | **c** | **m** | **c** |
|---|---|---|---|
| 00 | 0000 | $\alpha 0$ | $\alpha 0 1 \alpha^2$ |
| 01 | $011\alpha$ | $\alpha 1$ | $\alpha 101$ |
| $0\alpha$ | $0\alpha\alpha\alpha^2$ | $\alpha\alpha$ | $\alpha\alpha\alpha^2 0$ |
| $0\alpha^2$ | $0\alpha^2\alpha^2 1$ | $\alpha\alpha^2$ | $\alpha\alpha^2\alpha\alpha$ |
| 10 | $10\alpha^2\alpha$ | $\alpha^2 0$ | $\alpha^2 0\alpha 1$ |
| 11 | $11\alpha 0$ | $\alpha^2 1$ | $\alpha^2 1\alpha^2\alpha^2$ |
| $1\alpha$ | $1\alpha 11$ | $\alpha^2\alpha$ | $\alpha^2\alpha 0\alpha$ |
| $1\alpha^2$ | $1\alpha^2 0\alpha^2$ | $\alpha^2\alpha^2$ | $\alpha^2\alpha^2 10$ |

$$d_{min} = 3 = 4\text{-}2\text{+}1$$

# Example cont'd

$$\mathbf{H} = \begin{bmatrix} \alpha^2 & 1 & 1 & 0 \\ \alpha & \alpha & 0 & 1 \end{bmatrix}$$

$$\alpha \begin{bmatrix} \alpha^2 \\ \alpha \end{bmatrix} + \begin{bmatrix} 1 \\ \alpha \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

# Hamming Spheres

- Consider a $t$ error correcting code.
- A code can correct $t$ errors if $d_{min} \geq 2t+1$.
- A non-codeword has distance of $t$ or less from at least one codeword.
- The vectors of Hamming distance $t$ or less away from a codeword form a "sphere" of radius $t$ around the codeword. This is called a Hamming Sphere.
- There are $V_q(n,t)$ vectors of length $n$ within a Hamming sphere of radius $t$, where

$$V_q(n,t) = \sum_{i=0}^{t} (q-1)^i \binom{n}{i}$$

(this number includes the given codeword).

# Example

- Returning to the 4-ary example shown previously, let us consider codeword (0000).
  - Using this codeword as the center of the Hamming sphere, there are 13 vectors in a Hamming sphere of radius 1 around this codeword
  - 0000, 0001, 0010, 0100, 1000, $000\alpha$, $00\alpha0$, $0\alpha00$, $\alpha000$, $000\alpha^2$, $00\alpha^20$, $0\alpha^200$, $\alpha^2000$.
  - The above vectors also fall into a Hamming sphere of radius 2 around 0000. All vectors of weight 2 also fall into this sphere (0011, 0110 1100, $001\alpha$, …). There are 54 weight 2 length 4 vectors over GF(4). Therefore there are 67 vectors that fall into this sphere.

# Hamming Bound

- For hard decision decoding, we can express the received word as **r** = **c**+**e**, where **e** is called the error pattern.
- The codeword **c** is an element of *C* but **e** is an element of $V_q^n$ (of which *C* is a subspace), therefore **r** is an element of $V_q^n$.
- $V_q^n$ can be divided into Hamming spheres around codewords of C.
- For a *t* error correcting code, all error patterns of weight *t* or less can be corrected as long as $d_{min} \geq 2t+1$.
- We can divide the elements of $V_q^n$ into $M = q^k$ non-overlapping spheres of radius *t*. However, there may exist some elements in $V_q^n$ whose Hamming distance from every codeword in *C* is greater than *t*.

# Hamming Bound cont'd

- Therefore $MV_q(n,t) \le q^n$.
- $V_q(n,t) \le q^n/M \rightarrow \log_q V_q(n,t) \le n - \log_q M$
- For linear block codes, $M = qk$, therefore $n\text{-}k \ge \log_q V_q(n,t)$.
- The Hamming bound states that if we want to design a $t$ error correcting code, the amount of redundancy needed is greater than or equal to the log of the number of vectors in a Hamming sphere of radius $t$.
- Example Hamming (7,4) is a one error correcting code.
  - $V_2(7,1) = 1+7 = 8$
  - Then $n\text{-}k \ge 3$.
  - In the Hamming (7,4) case, $n\text{-}k = 3$.

# Hamming Bound example 2

- For our (4,2) 4-ary code, $d_{min} = 3$, therefore $t = 1$.
- For any general 1 error correcting code of length 4 over GF(4), we need $n\text{-}k \geq \log_4 V_4(4,1) = \log_4(13) = 1.85$.
- Therefore we need to choose $k = 1$ or 2. ($k$<2.15).

# Perfect Code

- A “perfect” code is a code that satisfies the Hamming bound with equality.
  - This title does not imply that the code is the best possible code.
  - It tells us that all elements in $V_q^n$ fall into a Hamming sphere. Therefore a *t* error correcting code corrects all error patterns of weight *t* but it cannot correct any of weight $t$+1.
- Most block codes (linear and nonlinear) are not perfect.
- Hamming codes, Golay (23,12)[1] and odd length repetition codes are examples of perfect codes. See page 89 of text for complete list of perfect codes.

[1] this is a binary 3 error correcting code.

# Error Detection and Error Correction with Hard Decisions

- Error detection
  - $\mathbf{r} = \mathbf{c}+\mathbf{e}$
  - $\mathbf{S} = \mathbf{r}\mathbf{H}^T$ (this is called the syndrome).
  - $\mathbf{S} = (\mathbf{c}+\mathbf{e})\mathbf{H}^T = \mathbf{c}\mathbf{H}^T+\mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$.
  - When the error pattern is all zero (no error has occurred, then the syndrome is all zero).
  - If the syndrome is not all zero, an error is detected.
  - In automatic repeat request (ARQ) schemes, if the syndrome is non-zero, the receiver requests that the sender resend the codeword.