Information and Coding Theory

Mahdi Cheraghchi

Friday 18 Nov 2016

m.cheraghchi@imperial.ac.uk

Minimum distance and parity checks

- Minimum distance *d(C)* is equal to

$$\begin{aligned} d(C) &= 1 + \max\{t\text{: every } t \text{ columns of } H \text{ are linearly independent}\} \\ &= \min\{t\text{: there are } t \text{ linearly dependent columns of } H\} \end{aligned}$$

- Why? If $d(C) = d + 1$, then
  - Every *d* columns of *H* must be linearly independent. Otherwise, there would be a non-zero vector $\vec{c}$ of weight at most *d* such that $H \cdot \vec{c} = 0$. This means $\vec{c}$ would be a non-zero codeword of weight less than $d(C)$, a contradiction.
  - There is a non-zero codeword $\vec{c}$ of Hamming weight *d*+1. Since $H \cdot \vec{c} = 0$, this defines a linear dependence between *d*+1 of the columns of *H*.

Example

- What is the best (that is, largest) binary linear code of length ***n*** that can detect any one-bit error? ($d(C) \geq 2$)
- Every 2-1=1 column of ***H*** must be linearly independent.
- => Every column of ***H*** must be nonzero.
- ***H*** with smallest number of rows (to make ***C*** largest) is
  - H = (1, 1, …, 1).
  - Dimension k = n-1, d(C) = 2 => [n, n-1, 2] code.
  - Parity code of length ***n***.

Example

- What is the best (that is, largest) binary linear code of length ***n*** that can *correct* any one-bit error? ($d(C) \geq 3$)
- Every 3-1=2 columns of ***H*** must be linearly independent.
- => Every column of ***H*** must be nonzero, AND no two columns equal.
- Suppose $n = 2^r - 1$.
- ***H*** with smallest number of rows (to make ***C*** largest) is such that the columns enumerate all non-zero ***r***-bit strings.
- Example for ***n***=7: $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$. The code is [7,4,3].
- This is called the ***Hamming code***. In general it's $[2^r - 1, 2^r - r - 1, 3]$.

Error correction of Hamming codes

- Suppose $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.
- Let $\vec{c} = x \cdot G$ be the sent codeword.
- Recipient receives $\vec{y} = \vec{c} + \vec{e}$ where $\vec{e}$ is the ***error vector***.
- The decoder first calculates $\vec{s} = H \cdot \vec{y} = H \cdot (\vec{c} + \vec{e}) = H \cdot \vec{c} + H \cdot \vec{e} = H \cdot \vec{e}$.
- If there has been no errors, $\vec{e} = \vec{0}$ and $\vec{s} = \vec{0}$, so the received word is correct.
- Else, $\vec{e} = (0,0, \dots, 1, \dots, 0)$ where the 1 is at, say, the ith position. The goal is to find i.
- In this case, $\vec{s}$ is the ith column of ***H***, which is actually the *binary expansion* of the integer i. ☺

Syndrome decoding

- What we saw is an example of ***syndrome decoding*****.**
- For any linear code with parity check matrix ***H***, the ***syndrome*** of a received word $\vec{y}$ is the (n-k)-dimensional vector $\vec{s} = H \cdot \vec{y}$.
- If $\vec{y} = \vec{c} + \vec{e}$ for some codeword $\vec{c}$ and error vector $\vec{e}$, it it ***always*** possible to uniquely identify $\vec{e}$ (and therefore, $\vec{c}$, and the correct sent message) as long as the Hamming weight of $\vec{e}$ is at most $\lfloor \frac{d(C)-1}{2} \rfloor$.
- Why? Suppose there are two distinct solutions $\vec{e}$ and $\overrightarrow{e'}$, each of weight at most $\lfloor \frac{d(C)-1}{2} \rfloor$, such that $H \cdot \vec{e} = H \cdot \overrightarrow{e'} = \vec{0}$. Then, $H \cdot (\vec{e} - \overrightarrow{e'}) = \vec{0}$. But $(\vec{e} - \overrightarrow{e'})$ is a non-zero vector of Hamming weight less than *d(C)*, a contradiction.

Orthogonality of *G* and *H*

- Any choice of ***G*** and ***H*** **must be** orthogonal: $G\ H^\top = \vec{0}$ (that is, the inner product of every row of ***G*** and every rows of ***H*** must be zero).
  - *[Exercise: Check this for the formula of **H** from systematic **G**.]*
- Why? Every row of ***G*** is a codeword, so it must satisfy the system of linear equations defined by ***H*** ☺
- In linear-algebraic terms, rows of ***H*** span the orthogonal space of the code (orthogonal space of a linear space is the set of vectors that are orthogonal to *every vector* in the linear space).
- This orthogonal space is called the ***dual code*** (shown as $\mathcal{C}^\perp$).
- Dual of $\mathcal{C}^\perp$ is $\mathcal{C}$.

The dual code

- If $\mathcal{C}$ is determined by a generator matrix *G* and parity check matrix *H*, then $\mathcal{C}^{\perp}$ is determined by generator matrix ***H*** and parity check matrix ***G*** (that is, the role of G and H interchanged).
- The dual code is of length *n* and dimension *r* = *n*-*k*.
- Dual of an MDS code must be an MDS code.
  - If $\mathcal{C}$ is MDS, every $k \times k$ submatrix of *G* must have rank *k* (that is, every *k* columns of *G* must be linearly independent).
  - Therefore, the minimum distance of $\mathcal{C}^{\perp}$ must be at least (in fact exactly) *k*+1 = *n*-*r*+1.
  - Therefore, $\mathcal{C}^{\perp}$ is MDS.

The dual code: example

- Parity code of length 5: $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, H = (1\ 1\ 1\ 1\ 1)$.
- Dual will have: $G = (1\ 1\ 1\ 1\ 1)\ and\ H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$.
- => Dual of the parity code is the repetition code!
- Parity code: [5, 4, 2], Repetition code: [5, 1, 5] (both MDS).