Review Week 07: Calculating a check matrix. The Distance Theorem. Hamming codes

2022-11-07

The inner product. The dual code

- **If $C \subset \mathbb{F}_q^n$ is a linear code, the dual code $C^\perp$ is** $\{\underline{v} \in \mathbb{F}_q^n : \underline{v} \cdot \underline{c} = 0 \text{ for all } \underline{c} \in C\}$ **(that is: $C^\perp$ consists of all vectors orthogonal to C).**

The check matrix H. The syndrome of a vector. The use of H for error detection

- **A generator matrix H for $C^\perp$ is called a check matrix for C.**
- **Can be used to detect errors and to correct errors.**

The use of H for error correction - syndrome decoding.

A2. Let C be the binary linear code with parity check matrix $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$.

(a) Construct a table of syndromes for C.

(b) Use your table of syndromes to decode the received vectors 11110 and 10011.

How to calculate a check matrix

Example: find a check **matrix** for code generated by $\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$.

gen. matr. for $C^\perp$ = check matrix for C

gen. matr. for $\underbrace{(C^\perp)^\perp}_{= C}$ = check matrix for $C^\perp$

THM Generator $G = [\underbrace{I_k}_{k \text{ columns}} \mid \underbrace{A}_{n-k \text{ columns}}]\}k \Longrightarrow$ A possible check matrix $H = [\underbrace{-A^T}_{k \text{ columns}} \mid \underbrace{I_{n-k}}_{n-k \text{ columns}}]\}n-k$

$k = \dim C \Rightarrow \dim C^\perp = n-k$

$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$. Use row operations to bring G to standard form:

$r_1 \leftrightarrow r_3$

$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \boxed{0} & 1 & 1 \end{bmatrix}$ No standard form for this matrix.

We need to pass to a code linearly equivalent to C.

DEF Column operations: (C1) swap column i and column j;

(C2) Scale a column: $\lambda \in \mathbb{F}_q \setminus \{0\}$,

column $i \longmapsto \lambda$(column i)

Codes which can be obtained from C using these operations are linearly equivalent to C.

Properties: ① $C' \sim C \Rightarrow$ parameters of C' are the same as for C.

② Permuting columns leads to a code with a gen. matrix in standard form:

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \xrightarrow{C_1 \leftrightarrow C_4} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \xleftrightarrow{C_3 \leftrightarrow C_4} \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \underbrace{1 \quad 1}_{} \end{array}\right]$$

generates C'; $C' \sim C$

A check matrix for C':

$$G' = [I_3 \mid A] \Rightarrow H' = [-A^T \mid I_2]$$

$$= \left[\begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right]$$

A check matrix for C is $\left[\begin{array}{ccc|cc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{array}\right]$

$C_3 \leftrightarrow C_4$, $C_1 \leftrightarrow C_4$

The Distance Theorem

Example: what is the *weight* of a ternary code with check matrix $\boxed{H = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 2 & 0 & 1 & 1 \end{bmatrix}}$ **?**

d(C) is the minimum number of columns of H which form a linearly dependent set.

① No zero columns in H $\Rightarrow d(C) \geq 2$

② Check pairs of columns: no proportional pairs of columns, $d(C) \geq 3$

③ $\begin{bmatrix} 0 \\ 2 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ so $d(C) = 3$.

OR: $1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

~~The~~ Hamming code Ham(r,q)

Idea: design a check matrix H (with r rows) such that H has no pairs of proportional columns (so that $d \geq 3$) and # columns is as large as possible.

$\boxed{q = 2}$ Ham$(r, 2)$ check matrix:

$$H = \underbrace{\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}}_{\text{all distinct non-zero columns of } r \text{ bits}} \Big\} r \text{ rows}$$

(example for $r = 3$) $\quad$ # columns $= 2^r - 1$