MATH 525
Section 2.7: Parity-Check Matrices

September 30, 2020

Goal: Introduce the parity-check matrix of a linear code, which is useful for decoding. In later chapters we will design a code from its parity-check matrix.

Definition

Let C be a linear code. We say that H is a parity-check matrix for C if the columns of H form a basis for $C^\perp$, the dual code of C.

Remarks:

1. The columns of a parity-check matrix of a linear code are linearly independent.
2. H is a parity-check matrix for a linear code C if and only if H^T is a generator matrix for $C^\perp$.
3. If C is an (n, k) linear code then – as we already saw – $C^\perp$ is an $(n, n-k)$ linear code. So H is an $n \times n-k$ matrix. It follows from the definition that $GH = O$ where G is a generator matrix for C.
4. $(C^\perp)^\perp = C$.

- Starting from a generator matrix G for a code C, we already learned an algorithm for constructing a matrix H whose columns form a basis for $C^\perp$. Note that H is then a parity-check matrix for C. In the particular case where $G = [I_k|X]$, we have $H = \left[\begin{array}{c} X \\ \hline I_{n-k} \end{array}\right]$.
- Now, starting from the parity-check matrix H_C for C, we can form H_C^T, which is then the generator matrix for $C^\perp$. Denote the latter matrix by $G_{C^\perp}$. From $G_{C^\perp}$, we can use the same algorithm as above to construct a parity-check matrix for $C^\perp$, namely, $H_{C^\perp}$. The transpose of the latter matrix is a generator matrix for $(C^\perp)^\perp = C$. That is, $G_C = H_{C^\perp}^T$.

$$\begin{tikzcd}
H_{C^\perp} \arrow[d, "\text{Transpose}"'] & G_{C^\perp} = H_C^T \arrow[l] \\
G_C = H_{C^\perp}^T \arrow[r] & H_C \arrow[u, "\text{Transpose}"']
\end{tikzcd}$$

- **Main Point**: Given G we can produce H and vice-versa. Either matrix can be used to completely define a linear code.

Example

Let

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

be a generator matrix for a linear code.

(a) Find $G_{C^\perp}$, a generator matrix for the dual of C.

(b) Find $H_{C^\perp}$, a parity-check matrix for the dual of C.

The example will be worked out during the lecture.

Consider the following observations:

1. Assume that $\mathrm{v} \in C$. Then $\mathrm{v} = \mathrm{u}G$ for some $\mathrm{u} \in K^k$. Hence, $\mathrm{v}H = \mathrm{u}GH = 0$ where 0 is the all-zero vector consisting of $n-k$ zeroes.

2. On the other hand, assume that $\mathrm{v}H = 0$ for some vector (word) $\mathrm{v} \in K^n$. This implies that v is orthogonal to every vector in the basis of $C^\perp$, whence v is orthogonal to all vectors in $C^\perp$. This in turn means that $\mathrm{v} \in (C^\perp)^\perp = C$, that is, v must be a codeword in C.

The two observations constitute a proof for the following

Theorem

Let H be a parity-check matrix for a linear code C. Then:

$$\mathrm{v}H = 0 \text{ if and only if } \mathrm{v} \in C.$$

The latter theorem is very useful from the decoder's point of view as the decoder can use the result stated there to quickly decide whether a received word $\mathrm{r} \in K^n$ is a codeword:

If $\mathrm{r}H = 0$, declare that r is a codeword (actually, the most likely codeword to have been sent);

If $\mathrm{r}H \neq 0$, declare that r is not a codeword. From here, either ask for retransmission or decode r.

Theorem

Matrices $G = (g_{ij})_{k\times n}$ and $H = (h_{ij})_{n\times n-k}$ are generator and parity-check matrices, respectively, of an (n, k) linear code C if and only if:

(i) Rank $G = k$ *and* Rank $H = n - k$, *and*

(ii) $GH = O$.