If H is a parity-check matrix of the q-ary $[n,k]$-code C, then H is a generating matrix for the q-ary $[n, n-k]$-code $C^{\perp}$. Therefore, since $C = (C^{\perp})^{\perp}$,

$$C = \{ \underline{x} \in V(n,q) : \underline{x} H^T = \underline{0} \}$$

That is, $\underline{x}$ is a codeword of C if and only if $\underline{x} H^T = \underline{0}$.

The rows of a parity-check matrix H are therefore called the <u>parity checks</u> on the codewords of C, and the equations $\underline{x} H^T = \underline{0}$ are called the <u>parity-check equations</u>.

•<u>Example</u> Consider the binary code C with generator matrix $G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

Let $H = [1\ 1\ 1]$. Then, since

$$GH^T = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

H is a parity-check matrix for C.

Therefore $\underline{x} \in C$ if and only if

$\underline{x} H^T = \underline{0}$ if and only if $[x_1, x_2, x_3] \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = 0$

if and only if $x_1 + x_2 + x_3 = 0$.

So, C has $x_1 + x_2 + x_3 = 0$ as its only parity-check equation.

Given that G is a generator matrix of C, we can find a parity-check matrix of C by ...

Theorem 3.9 If $G = [I_k | A]$ is a standard form generator matrix of an $[n, k]$-code C, then a standard form parity-check matrix of C is given by $H = [-A^T | I_{n-k}]$.

Proof: H is clearly an $(n-k) \times n$ matrix with $n-k$ linearly independent rows, and it can be readily checked that $GH^T = \underline{0}$. Therefore H is a generator matrix for $C^\perp$, that is, H is a parity-check matrix for C. ∎

Definition Let C be a q-ary $[n, k]$-code with parity-check matrix H.

For $\underline{y} \in V(n, q)$, the <u>syndrome</u> of $\underline{y}$ is $S(\underline{y}) = \underline{y} H^T$.

If H has rows $\underline{h}_1, \underline{h}_2, \ldots, \underline{h}_{n-k}$, then

$$S(\underline{y}) = (\underline{y} \cdot \underline{h}_1, \underline{y} \cdot \underline{h}_2, \ldots, \underline{y} \cdot \underline{h}_{n-k})$$

and $S(\underline{y}) = \underline{0}$ if and only if $\underline{y} \in C$.

Lemma 3.10 Vectors $\underline{u}$ and $\underline{v}$ are in the same coset of C if and only if they have the same syndrome.

Proof: $\underline{u} + C = \underline{v} + C$ if and only if

$\underline{u} - \underline{v} \in C$ if and only if

$(\underline{u} - \underline{v}) H^T = \underline{0}$ if and only if

$\underline{u} H^T = \underline{v} H^T$ if and only if

$S(\underline{u}) = S(\underline{v})$

∎