RECAPITULATION OF LINEAR CODES

A code of length n with k symbols of information is **linear** when we can verify a codeword $\mathbf{x}$ using a system of homogeneous[1] linear equations, called **check equations**,

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1k}x_k + x_{k+1} \qquad &= 0 \\ &\vdots \\ a_{n-k,1}x_1 + \cdots + a_{n-k,k}x_k \qquad + x_n &= 0. \end{aligned}$$

Without loss of generality, these equations are linearly independent. (If not, we can discard equations that give no useful information.)

As usual, we can rewrite this linear system as a matrix equation,

$$H\mathbf{x}^T = 0.$$

We call H the **parity check matrix**. Since the equations are linearly independent, the rows of H are likewise linearly independent. Another way of saying this is that H is **full rank**. Notice that H has a block structure, $(A \mid I_{n-k})$.

We can rewrite the check equations by solving for the check digit variables,

$$\begin{aligned} x_{k+1} &= -a_{11}x_1 - \cdots - a_{1k}x_k \\ &\vdots \\ x_n &= -a_{n-k,1}x_1 - \cdots - a_{n-k,k}x_k. \end{aligned}$$

To this system we prepend some "obvious" equations,

$$\begin{aligned} x_1 &= x_1 \\ &\vdots \\ x_k &= x_k \\ x_{k+1} &= -a_{11}x_1 - \cdots - a_{1k}x_k \\ &\vdots \\ x_n &= -a_{n-k,1}x_1 - \cdots - a_{n-k,k}x_k. \end{aligned}$$

This matrix has a block structure $\left(\frac{I_k}{-A}\right)$ that is similar to the one above. We'll call G the transpose of this matrix, $G = \left(I_k \mid -A^T\right)$.

A useful relationship between these two matrices is that $GH^T = 0$. Inasmuch as the block dimensions match, block multiplication makes this plain,

$$GH^T = \left(I_k \mid -A^T\right)\left(\frac{A^T}{I_{n-k}}\right) = \left(A^T - A^T\right) = 0.$$

[1]A linear system is **homogeneous** when the constants are all zero.

This shows that any row $\mathbf{r}$ of G is a codeword, since $GH^T = 0$ implies $\mathbf{r}H^T = 0$, and

$$\mathbf{r}H^T = 0 \quad \Longrightarrow \quad \left(\mathbf{r}H^T\right)^T = 0^T \quad \Longrightarrow \quad \left(H^T\right)^T \mathbf{r}^T = 0 \quad \Longrightarrow \quad H\mathbf{r}^T = 0.$$

Recall now the definition of the code: $\mathbf{x} \in C$ iff $H\mathbf{x}^T = 0$.

In addition, the left block of G is the identity matrix, which is linearly independent, so the rows of G itself must be linearly independent.

The rank of G is k, which is also the dimension of C (the first k symbols of a codeword are free; the rest are determined by the check equations).

This tells us that the rows of G form a basis of C, and we are justified in calling G a **generator matrix**.