3.2 Hamming code revisited

The Hamming code is best understood by the structure of its parity check matrix. This will also allow us to generalize Hamming codes to larger lengths.

We defined the $C_{\text{Ham}} = [7,4,3]_2$ Hamming code using generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

If we define the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

then one can check that $HG = \mathbf{0}$ and that H is a parity check matrix for C_{Ham}. Note that H has a rather nice structure: its columns are the integers 1 to 7 written in binary.

Correcting single errors with the Hamming code: Suppose that y is a corrupted version of some (unknown) codeword $c \in C_{\text{Ham}}$, with a single bit flipped. We know by the distance property of C_{Ham} that c is uniquely determined by y. In particular, a naive method to determine c would be to flip each bit of y and check if the resulting vector is in the null space of H.

A more slick (and faster) way to correct y is as follows. We know that $y = c + e_i$ where e_i is the column vector of all zeros except a single 1 in the i'th position. Note that $Hy = H(c + e_i) = Hc + He_i = He_i =$ the ith column of H. The ith column of H is the binary representation of i, and thus this method recovers the location i of the error.

Definition 10 (Syndrome) *The vector Hy is said to be the syndrome of y.*

Generalized Hamming codes: Define H_r to be the $r \times (2^r - 1)$ matrix where column i of H_r is the binary representation of i. This matrix must contain e_1 through e_r, which are the binary representations of all powers of two from 1 to 2^{r-1}, and thus has full row rank.

Now we can define the r'th generalized Hamming code

$$C^{(r)}_{\text{Ham}} = \{c \in \mathbb{F}_2^{2^r-1} \mid H_r c = \mathbf{0}\}.$$

to be the binary code with parity check matrix H_r.

Lemma 11 *$C^{(r)}_{\text{Ham}}$ is an $[2^r - 1, 2^r - 1 - r, 3]_2$ code.*

Proof: Since H_r has rank r, it follows that the dimension of $C^{(r)}_{\text{Ham}}$ equals r. By Lemma 9, we need to check that no two columns of H_r are linearly dependent, and there are 3 linearly dependent