1 Generator and Parity Check Matricies

1.1 Recall: Linear Code

We say that $C \subseteq \Sigma^n$ is a linear code if C is a linear subspace of Σ^n where Σ is a finite field. i.e.:

1. $0 \in C$
2. $\forall a, b \in C, a + b \in C$

"a linear code is an error-correcting code for which any linear combination of codewords is also a codeword"

1.2 Definition: Generator Matrix

Given some linear code $C \subseteq \Sigma^n$, we can create a basis that spans C. Let G be a generator matrix, who's rows form a basis for C. We can use $G \in \mathbb{R}^{k \times n}$ to generate codewords given a message $m \in \Sigma^k$:

$$\underbrace{c}_{1 \times n} = \underbrace{m}_{1 \times k} \underbrace{G}_{k \times n}$$

Where c is some codeword.

1.3 Definition: Parity Check Matrix

Given some linear code $C \subseteq \Sigma^n$, a parity check matrix H can be used to check if a codeword $c \in C$.

$$\underbrace{H}_{(n-k) \times n} \underbrace{c^T}_{n \times 1} = \mathbf{0} \iff c \in C$$

2 Hamming Codes

”Hamming was interested in two problems at once: increasing the distance as much as possible, while at the same time increasing the code rate as much as possible.”

2.1 Definition: Parity Bit

A parity bit is a bit, it’s added to a string of bits to ensure the total number of 1’s in a string is even or odd.

e.g. Even parity bit is added to make the total number of 1’s even.

string	number of 1’s	even parity bit
0001000	1	1
0001111	4	0
0101010	3	1