An Introduction to Error Correcting Codes

Exercise 1.
Is the following binary code of length 4 linear?

$$C = \left\{ \begin{matrix} (0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1), \\ (0,1,1,0), (0,1,0,1), (0,0,1,1), (1,1,1,1) \end{matrix} \right\}$$

What is the minimal Hamming distance of C?

Exercise 2.
Let C be the linear binary code with generating matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Determine a parity check matrix and the minimal Hamming distance of C.

Exercise 3.
Let C be a linear binary (n, k, d) code. Prove the following bound for the minimal Hamming distance d, known as the *Plotkin bound*

$$d \leq \frac{n \cdot 2^{k-1}}{2^k - 1}.$$

Hint. Estimate the sum of Hamming weights $\sum w(c)$ over all code words $c \in C$ in two different ways. First show that at most 2^{k-1} code words in C may have a non-zero ith entry for any i and conclude that $\sum w(c)$ is at most $n \cdot 2^{k-1}$. On the other hand, the fact that $w(c) \geq d$ for any $c \in C \setminus \{0\}$ gives a lower bound for $\sum w(c)$.

An Introduction to Error Correcting Codes

(English-Japanese Dictionary)

channel	伝送路
code	符号
code length	符号語の長さ
code word	符号語
decode	復号
dimension	次元
encode	符号化
encryption	暗号化
finite field	有限体
forward error correction	前方誤り訂正
Hamming weight	ハミング重み
linear code	線型符号
linear dependent	線型従属
linear independent	線型独立
linear subspace	線型部分空間
matrix	行列
metric	距離函数
minimum distance decoding	最小距離復号
minimal Hamming distance	最小ハミング距離
noice	ノイズ
parity check	奇偶検査
perfect code	完全符号
rate	割合
standard basis	標準基底
syndrome decoding	シンドローム復号
systematic	系統的
vector space	ベクトル空間