EE/Ma 127a Error-Correcting Codes - Homework Assignment 1

Ling Li, ling@cs.caltech.edu

October 3, 2000

## 1.1 Three Erasures

We can use the positions of the erasures to denote the pattern of three erasures. That is, $(i, j, k)$ is a pattern with $x_i$, $x_j$ and $x_k$ erased and unknown.

The only way to determine $x_i$, $x_j$ and $x_k$ is to solve the equation

$$Hx^T = 0 \tag{1}$$

where

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

is the parity-check matrix and $x$ is the code word. Using $h_i$ as the $i$th column of $H$, we can rewrite (1) as

$$x_i h_i + x_j h_j + x_k h_k = c \tag{2}$$

where $c$ can be calculated by known bits of $x$ and $H$.

$x_i$, $x_j$ and $x_k$ can be determined by (2) if and only if $h_i$, $h_j$ and $h_k$ are linearly independent. In $GF(2)$, $h_i$, $h_j$ and $h_k$ are linearly independent if and only if $h_i + h_j + h_k \neq 0$, since they are non-zero and already different with each other. Here's the conclusion:

**Theorem:** Pattern $(i, j, k)$ of three erasures can be corrected if and only if $h_i + h_j + h_k \neq 0$.

For $\begin{pmatrix} 7 \\ 3 \end{pmatrix} = 35$ patterns of three erasures, we can find that only $(1, 2, 4)$, $(1, 3, 7)$, $(1, 5, 6)$, $(2, 3, 6)$, $(2, 5, 7)$, $(3, 4, 5)$, and $(4, 6, 7)$ cannot be corrected. Other 28 patterns can be corrected.

## 1.2 Basis for the Nullspace

For any information code $x$, $xG$ is a valid code word. The nullspace for the code space is defined as

$$\left\{ y \,\middle|\, (\forall x)\ (xG)y^T = 0 \right\} = \left\{ y \,\middle|\, Gy^T = 0 \right\}.$$

Since

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

has a very good structure, we can easily find out that $y$ in the nullspace should be

$$y = (y_1, y_2, y_3, y_4, y_2 + y_3 + y_4, y_1 + y_3 + y_4, y_1 + y_2 + y_4, y_1 + y_2 + y_3)$$

where $y_{1,2,3,4}$ can be 0 or 1. So one basis for the nullspace is the four row vectors of

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

(In fact, the four row vectors of $G$ can also be a basis for the nullspace since $GG^T = 0$.)

### 1.3 $G$ and $H$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{1+2\to 2} \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow{2+3\to 2} \begin{pmatrix} \underline{1} & 0 & 1 & 0 & 1 & 1 \\ 0 & \underline{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & \underline{1} & 1 & 1 \end{pmatrix}$$

One parity-check matrix can be

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

### 1.4 Gaussian $q$-binomial Coefficient

From the definition, we know

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{k-i} - 1} = \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{i+1} - 1} \tag{3}$$

So for $1 \leq k < n$,

$$\begin{bmatrix} n \\ k+1 \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot \frac{q^{n-k} - 1}{q^{k+1} - 1} \tag{4}$$

which makes the computation easier:

| $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $\begin{bmatrix} 7 \\ k \end{bmatrix}_2$ | 127 | 2667 | 11811 | 11811 | 2667 | 127 | 1 |

For $m \neq 0$, since $\lim_{q \to 1} q^n - 1 = \lim_{q \to 1} q^m - 1 = 0$, we have

$$\lim_{q \to 1} \frac{q^n - 1}{q^m - 1} = \lim_{q \to 1} \frac{(q^n - 1)'}{(q^m - 1)'} = \lim_{q \to 1} \frac{nq^{n-1}}{mq^{m-1}} = \frac{n}{m}.$$

Thus from (3)

$$\lim_{q\to 1}\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1}\lim_{q\to 1}\frac{q^{n-i}-1}{q^{k-i}-1} = \prod_{i=0}^{k-1}\frac{n-i}{k-i} = \begin{pmatrix} n \\ k \end{pmatrix}. \tag{5}$$

(We can define $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$. Thus for $k = 0$, (4) and (5) still hold.)

### 1.5 $(39, 32)$

Consider the error-check matrix $H$ for this $(n, k)$ linear block code. $H$ is an $(n-k)\times n$ matrix with each column $h_i$ $(i = 1..n)$ that

- $h_i$ should not be 0 and
- $h_i$ should be different from each other, in order to correct all single bit errors;
- $h_1 + h_j$ should not be one of $h_i$ or 0, where $j = 2..n$, in order to detect all double bit errors; or we can not distinguish some double bit error with some one bit error.

Thus, we have $h_i$, $h_1 + h_j$, and 0 are $[n + (n-1) + 1]$ different[1] vectors with dimension $(n-k)$. That is

$$n + (n-1) + 1 \le 2^{n-k}$$

Since $n > k = 32$, we have

$$2^{n-k} \ge 2n > 2k \Rightarrow n > k + \log 2k = 38$$

So $n$ is at least 39. We will design a $(39, 32)$ code below capable of correcting all single bit errors and detecting all double bit errors. So the smallest value of $n$ *is* 39.

For convenience, we can write $h_i$ as a binary number, like this

$$\left\langle \begin{pmatrix} 2^{n-k-1} & 2^{n-k-2} & \dots & 1 \end{pmatrix} \cdot h_i \right\rangle$$

A $(38, 32)$ linear code with parity-check matrix $H' = (\langle 1\rangle, \langle 2\rangle, \cdots, \langle 38\rangle)$ is capable of correcting all single bit errors but not detecting all double bit errors. We 'extend' the code to $(39, 32)$ with parity-check matrix

$$H = (\langle 1\rangle, \langle 3\rangle, \langle 5\rangle, \cdots, \langle 77\rangle)$$

Then it can both correct all single bit errors and detect all double bit errors.

[1] $i \ne j \Leftrightarrow h_i \ne h_j \Leftrightarrow h_1 + h_i \ne h_1 + h_j$.