EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2010

Solutions to Assignment 4 — Prepared by Arun Mukundan and Sravan Kumar

---

1. The generator matrix

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

can be brought to a systematic form by adding the first row to the second row and the second row to the third row. Since the rows of the generator matrix are linearly independent, these operations do not change the code. The resulting generator matrix is

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

So a parity check matrix can be readily obtained as

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

2. Suppose $\mathbf{v} \in C$. Then $\mathbf{v}$ is orthogonal to every vector in $C^\perp$. In particular, it is orthogonal to basis vectors of $C^\perp$ (rows of H)

Hence $\mathbf{v}.H^T = 0$

Suppose $\mathbf{v}.H^T = 0$

$\Rightarrow \mathbf{v}.h^T = 0 \; \forall \; h \in C^\perp$ (as $h \in C^\perp \Rightarrow h = H^T\lambda$ for some vector λ)

$\Rightarrow \mathbf{v} \in (C^\perp)^\perp$

Every vector in C is orthogonal to every vector in $C^\perp$

So $C \subseteq (C^\perp)^\perp$

But if dimension of C is k, we know that the dimension of $C^\perp$ is $n-k$.
Hence dimension of $(C^\perp)^\perp$ is k.

So C and $(C^\perp)^\perp$ have same finite dimension and hence $C = (C^\perp)^\perp$

And as $\mathbf{v}.H^T = 0 \Rightarrow \mathbf{v} \in (C^\perp)^\perp$, it means $\mathbf{v} \in C$

So, $\mathbf{v} \in C \Leftrightarrow \mathbf{v}.H^T = 0$.

3. Let dimension of C be k. Then dimension of $C^\perp$ is $n-k$.

   But if $C = C^\perp$, then $k = n - k$

   $\Rightarrow n = 2k$, an even number

   And dimension of C is $k = \frac{n}{2}$

4. Let $\mathbf{v} \in C$. Since $C = C^\perp$, $v \in C^\perp$. Then $\mathbf{v} \cdot \mathbf{v}^T = 0$.

   But $\mathbf{v} \cdot \mathbf{v}^T = w_H(\mathbf{v}) \mod 2$ where $w_H(\cdot)$ is the Hamming weight function.

   So $\mathbf{v} \cdot \mathbf{v}^T = 0 \Rightarrow \mathbf{v}$ has even weight.

   Also, if $\mathbf{1} = (1\ 1\ 1\ 1 \ldots 1)$, then $\mathbf{v} \cdot \mathbf{1}^T$ is the same as $w_H(\mathbf{v}) \mod 2$ which is 0 for all $\mathbf{v} \in C$. So $\mathbf{1}$ will belong to $C^\perp$ which means it belongs to C.

5. Let C_i be the set of all codewords in C with weight i

   Then, we show that $f : C_i \to C_{n-i}$ defined as f($\mathbf{v}$)=1+$\mathbf{v}$ $\forall \quad \mathbf{v} \in C_i$ is a one-one correspondence between C_i and C_{n-i}

   f is one-one

   suppose $f(\mathbf{v}_1) = f(\mathbf{v}_2)$ for some $\mathbf{v}_1 \neq \mathbf{v}_2$

   $\Rightarrow 1 + \mathbf{v}_1 = 1 + \mathbf{v}_2$

   $\Rightarrow \mathbf{v}_1 = \mathbf{v}_2$, a contradiction

   so f is one-one

   f is onto

   Let $\mathbf{v} \in C_{n-i}$ Then $\mathbf{v}$ has weight $n-i$

   As $1 \in C and \quad \mathbf{v} \in C$, $1 + \mathbf{v}$ also is in C

   And $1 + \mathbf{v}$ will have weight i

   $\Rightarrow 1 + \mathbf{v} \in C_i$

   $\Rightarrow f$ is onto

   Hence f is a one-one correspondence and so $|c_i| = |c_{n-i}|$

   $$i.e., A_i(c) = A_{n-i}(c)$$

6. Let A be the set of all positions at which u and v differ

   $(A = \{i : u(i) \neq v(i)\})$

   Let w be any n-tuple.

   Let B be the set of positions among A,where

   u,w differ $(B = \{i : i \in A, u(i) \neq w(i)\})$

   so $B \subseteq A$.

   And u and w have equal values at $A \cap B^c$ positions.

   $\Rightarrow w$ and v differ at $A \cap B^c$ positions

   $(i \in A \cap B^c \Rightarrow w(i) \neq v(i))$

so $d(u, w) \geq |B|$ and $d(w, v) \geq |A \cap B^c| = |A| - |B|$

so $d(u, w) + d(w, v) \geq |B| + (|A| - |B|) = |A| = d(u, v)$

7. As the channel is a BSC with $p < 1/2$, minimum distance decoding is the optimal decoding. So we choose the error patterns(correctable) to be of least Hamming weight.

000000	011100	101010	110001	110110	101101	011011	000111
000001	011101	101011	110000	110111	101100	011010	000110
000010	011110	101000	110011	110100	101111	011001	000101
000100	011000	101110	110101	110010	101001	011111	000011
001000	010100	100010	111001	111110	100101	010011	001111
010000	001100	111010	100001	100110	111101	001011	010111
100000	111100	001010	010001	010110	001101	111011	100111
010010	001110	111000	100011	100100	111111	001001	010101

$G = [KI]$, with

$$K = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

So parity check matrix

$$H = [I \quad K^T] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$Error \rightarrow$	000000	000001	000010	000100	001000	010000	100000
$Syndrome \rightarrow$	000	110	101	011	001	010	100

Error $\rightarrow$ 010010
Syndrome $\rightarrow$ 111

All weight 1 errors can be detected,(and corrected) but only one weight 2 error can be corrected.

8. Let e_i denote $\underbrace{00\ldots0}_{\text{(n-i)times}}\underbrace{11\ldots1}_{\text{i times}} \qquad 0 \leq i \leq n$

For a linear code to decode all error patterns e_i correctly, we need their syndrome to be distinct

i.e., if H is the parity check matrix of the code,

then $H.e_i^T \neq H.e_j^T$ whenever i $\neq$ j $0 \leq i, j \leq n$.

i.e., $H.(e_i^T - e_j^T) \neq 0$

i.e., $\underbrace{00\ldots0}_{p}\underbrace{11\ldots1}_{q}\underbrace{00\ldots0}_{r} \notin C$ for any p,q,r $\neq 0$.

So no m consecutive columns of H can add upto zero, for all $1 \leq m \leq n$.

Any H satisfying above condition, will give a code that can correct all given error patterns

Let r be smallest integer such that $(n+1) \leq 2^r$.

We need the code to correct all errors e_i $0 \leq i \leq n$.

So $(n+1) \leq 2^{(n-k)}$. So, for largest rate we need $(n-k) = r$.

We now show that such a H ($r \times n$ matrix) can be constructed.

We construct H by gradually adding columns (n times) from the end.

The first column can be any random r-tuple

Whenever we add a new column, we ensure that any m consecutive columns,starting with this new column, do not add upto zero, for all m i.e., let there be t columns $C_1, C_2, ..., C_t$ and we are adding a new column C_{t+1}

then $\sum_{i=m}^{t+1} C_i \neq 0 \; \forall \; 1 \leq m \leq (t+1)$

So $C_{t+1} \neq \sum_{i=m}^{t+1} C_i \; \forall \; 1 \leq m \leq t$ and $C_{t+1} \neq 0$

So there atmost $(t+1)$ vectors that are not permitted to be used as C_{t+1}

But $(t+1) \leq n < 2^r$

So there will always exist an r-tuple satisfying above conditions.

So, starting with any random non-zero column, we can keep adding columns, while ensuring above conditions to finally give a $(r \times n)$ matrix. From the construction, we can see that this matrix will satisfy condition 1 and hence a code with this as positive check matrix can correct the given error patterns.

For n=7, n+1=8 $\leq 2^3$ So r=3.

We construct a 3×7 matrix by adding 3-tuples, satisfying conditions given before

We start with $C_1 = (0\ 0\ 1)^T$

$C_2 \neq (0\ 0\ 1)^T$ or $(0\ 0\ 0)^T$. So let $C_2 = (0\ 1\ 0)^T$

Now, $C_3 \neq C_2$ or $C_1 + C_2$ or 0

So $C_3 \neq (0\ 1\ 0)^T$ or $(0\ 1\ 1)^T$ or $(0\ 0\ 0)^T$

So, let $C_3 = (1\ 0\ 0)^T$

And $C_4 \neq C_3$ or $C_3 + C_2$ or $C_3 + C_2 + C_1$ or 0

So, let $C_4 = (0\ 0\ 1)^T$

Proceeding similarly, we finally get

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