EE/Ma 127b Error-Correcting Codes - Homework Assignment 3

Ling Li, ling@cs.caltech.edu

February 15, 2001

3.1 *Extended R-S Code.* The generator matrix is

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_0^{k-2} & \alpha_1^{k-2} & \cdots & \alpha_{n-1}^{k-2} & 0 \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \cdots & \alpha_{n-1}^{k-1} & 1 \end{pmatrix},$$

and the codeword is

$$xG = (I_0, I_1, \dots, I_{k-1})G.$$

Thus this is a linear code with codeword length $(n+1)$. Consider the matrix G' formed from the left-most $(k-1)$ columns and the right-most column of G. From Vandemonde determinant theorem, we have

$$\det(G') = \det \begin{pmatrix} 1 & \cdots & 1 & 0 \\ \alpha_0 & \cdots & \alpha_{k-2} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_0^{k-2} & \cdots & \alpha_{k-2}^{k-2} & 0 \\ \alpha_0^{k-1} & \cdots & \alpha_{k-2}^{k-1} & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_0 & \cdots & \alpha_{k-2} \\ \vdots & \vdots & \vdots \\ \alpha_0^{k-2} & \cdots & \alpha_{k-2}^{k-2} \end{pmatrix} = \prod_{0 \le i < j \le k-2} (\alpha_j - \alpha_i),$$

which is non-zero. Thus the dimension of the code is k.

If $I_{k-1} \neq 0$, the polynomial $P(x) = I_0 + I_1 + \cdots + I_{k-1}x^{k-1}$ has at most $(k-1)$ roots; If $I_{k-1} = 0$, then $P(x)$ has at most $(k-2)$ roots. In either case,

$$(P(\alpha_0), P(\alpha_1), \dots, P(\alpha_{n-1}), P(\infty))$$

has at most $(k-1)$ zeros, if not all the elements are zeros. So the minimum nonzero weight is no less than $(n+1)-(k-1) = n-k+2$. However, we know that $d_{\min} \le r+1 = n-k+2$. Thus for this code, the equality holds. So it is an $(n+1, k)$ MDS code.

3.2 Wicker Theorem 8.5 says

$$A_w = \binom{n}{w}(q-1)\sum_{i=0}^{w-d_{\min}} (-1)^i \binom{w-1}{i} q^{w-i-d_{\min}}. \tag{1}$$

Note that for MDS code, $d_{\min} = n - k + 1$. Since we use $t = n - w$, we have $w - d_{\min} = n - d_{\min} - t = k - t - 1$. Thus (1) is

$$\begin{aligned}
A_w &= \binom{n}{w}(q-1)\sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}q^{k-t-1-i} \\
&= \binom{n}{w}\left[\sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}q^{k-t-i} - \sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}q^{k-t-1-i}\right] \\
&= \binom{n}{w}\left[\sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}\left(q^{k-t-i}-1\right) - \sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}\left(q^{k-t-1-i}-1\right)\right] \\
&= \binom{n}{w}\left[\sum_{i=0}^{k-t-1}(-1)^i\binom{w-1}{i}\left(q^{k-t-i}-1\right) + \sum_{i=1}^{k-t}(-1)^i\binom{w-1}{i-1}\left(q^{k-t-i}-1\right)\right] \\
&= \binom{n}{w}\left[\left(q^{k-t}-1\right) + \sum_{i=1}^{k-t-1}(-1)^i\left[\binom{w-1}{i}+\binom{w-1}{i-1}\right]\left(q^{k-t-i}-1\right)\right] \\
&= \binom{n}{w}\sum_{i=0}^{k-t-1}(-1)^i\binom{w}{i}\left(q^{k-t-i}-1\right).
\end{aligned}$$

Thus we get the version in the problem.

3.3 *Frequency domain.* $n = 31$, $k = 15$, $r = 16$, $t = 8$. $\sigma(x) = 1$ means $\sigma_i = 0$ for $i > 0$. Since we use $S_j = \sum_{i=1}^{d}\sigma_i S_{j-i}$ to calculate S_j for $2t < j < n$ and $j = 0$, we get $S_j = 0$ for those j. If the decoding algorithm verifies the S by calculating S_j for t more times,[1] it would know that the received word is not decodable — the number of errors exceeds $r/2$. However, if the decoder doesn't verify S and continue the decoding, we will get (see the footnote for why j is from 1 to t.)

$$E_i = \sum_{j=0}^{n-1} S_j\alpha^{-ij} = \sum_{j=1}^{t}\sum_{k=0}^{n-1}R_k\alpha^{(k-i)j} = \sum_{k=0}^{n-1}R_k\sum_{j=1}^{t}\alpha^{(k-i)j}$$

and $C = R - E$. However, this is a decoder error and C is not the correct codeword.

3.4 Decoding error. $n = 31$, $k = 15$, $r = 16$. Received word R.

(a) $e_0 = 16$, $e_1 = 1$. Since any subset of k columns in an MDS code is independent, the decoder would consider this case as $e_1' = 0$ and recover the whole codeword from R (15 unerased symbols). Thus the decoder error always happens and the probability therefore is 1.

(b) $e_0 = 15$, $e_1 = 1$. The decoder error happens if the decoder returns a codeword with $e_1' \le \frac{r-e_0}{2} = \frac{1}{2}$. That is, there's an error iff the decoder returns a codeword exactly the same as R (in the 16 unerased positions). However, since $e_1 = 1$ and the codeword can be decided by the 15 correct symbols, there's no codeword exactly the same as R. Thus the possibility of decoder error is 0.

[1] Since we now get the whole S, we can calculate $S_1 \sim S_t$ by other part of S and then we can compare these calculated $S_1 \sim S_t$ with those we have already got. If they do not match, we say the verification fails. For this problem, $\sigma(x)S(x) \equiv \omega(x) \pmod{x^{2t}}$ and $\deg\omega(x) \le t-1$ gives $\deg S(x) \le t-1$. And $S(x) \neq 0$, since the algorithm would exit and say "no errors occurred" if $S(x) = 0$. However, the calculated $S_1 \sim S_t$ will be all zeros. So the verification must fail.

(c) $e_0 = 14$, $e_1 = 2$. $e_1' \le \frac{r-e_0}{2} = 1$. Consider a codeword C' that differs from R by only 1 position. (We know it is impossible to have a codeword that exactly the same as R.) Let C be the real codeword for R. From $d(C,C') \le d(C,R) + d(C',R) \le e_0 + e_1 + e_1' = 17$, and the minimum distance between different codewords is $r + 1 = 17$, we know C and C' have exactly 14 positions in common, and the position where R differs from C' is not among the positions where R differs from C (i.e., not among the error positions), if we don't consider the erasures.

We want to find out what kind of errors in R will result a C'. For any given C and e_0 erasure and e_1 error positions, R has $(p-1)^{e_1}$ choices, where p is the size of the field. (In our project, $p = 32$.) C' can be constructed by: replacing an arbitrary symbol out of the 15 correct positions of C by any other symbol and using it together with other 14 correct symbols to decide C'. The two symbols of C' with positions that have errors in R are those can result a decoder error. The number of different C' is $(p-1) \times 15$, and this is also the number of different two symbols that can result decoder errors.[2] So the possibility of decoder error is

$$\frac{15}{p-1} = \frac{15}{31}.$$

[2]If two codewords C' and C'' are the same in the two error positions, and either of them has only 1 symbol different from C in the 15 correct positions, the number of common positions of C' and C'' is no less than $(15-1-1)+2 = 15$. This shows $C' = C''$.