Math 55: Discrete Mathematics, Fall 2008
Homework 11 Solutions

* 9. We are to show that every word belongs to the Hamming ball of radius one around some codeword. Since the code corrects 1 error, these Hamming balls are disjoint, so it suffices to show that number of codewords times the size of each Hamming ball is equal to the total number of words, *i.e.*,

$$2^m(1+\binom{n}{1}) = 2^n,$$

where $n = 2^k - 1$ and $m = 2^k - k - 1$. The equation holds since

$$2^{2^k-k-1}(1+2^k-1) = 2^{2^k-k-1}2^k = 2^{2^k-1}$$

11 (a)

$$C = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{bmatrix}$$

(b) Compute $\begin{bmatrix} 2 & 3 & 4 \end{bmatrix} C \equiv \begin{bmatrix} 2 & 2 & 3 & 5 & 1 & 5 & 3 \end{bmatrix} \pmod 7$.

12. Express the received vector as $\mathbf{r} = \begin{bmatrix} \mathbf{x} & | & \mathbf{y} \end{bmatrix}$, where $\mathbf{x}$ consists of the first m entries of $\mathbf{r}$ and $\mathbf{y}$ consists of the remaining $n-m$ entries.

For any $1 \times m$ vector $\mathbf{x}$, we have $\mathbf{x}C = \begin{bmatrix} \mathbf{x} & | & \mathbf{xP} \end{bmatrix}$, hence $\mathbf{r}$ is a codeword if and only if $\mathbf{y} = \mathbf{xP}$.

On the other hand, $\mathbf{rS} = \mathbf{xP} - \mathbf{y}$, so this is equal to zero if and only if the same condition $\mathbf{y} = \mathbf{xP}$ holds.

* 13. Let $E(x) = x + u$, $Q(x) = ax^3 + bx^3 + cx + d$. The key equations $E(i) = R_iQ(i)$ (mod 11) for $i = 0, 1, 2, 3, 4$ give

$$\begin{aligned} 10d + 9u &= 0 \\ 10a + 10b + 10c + 10d + 2u + 2 &= 0 \\ 3a + 7b + 9c + 10d + 9u + 7 &= 0 \\ 6a + 2b + 8c + 10d + u + 3 &= 0 \\ 2a + 6b + 7c + 10d + 7u + 6 &= 0 \end{aligned}$$

Solving these in arithmetic mod 11, we find $E(x) = x - 2$, $Q(x) = 4x^3 + 3x^2 + 9x + 4$, and the message polynomial is $Q(x)/E(x) = 4x^2 + 9$.

The original message vector was therefore $\begin{bmatrix} 9 & 0 & 4 \end{bmatrix}$. It encodes to $\begin{bmatrix} 9 & 2 & 3 & 1 & 7 \end{bmatrix}$. The error was in the middle position (corresponding to $i = 2$, as we can also see from the fact that $E(2) = 0$).

* 14. To correct $e = n/3$ errors, a Reed-Solomon code should have $m = n - 2e = n/3$ message symbols. So its data rate is $1/3$, the same as for a triple-redundancy code. But

the Reed-Solomon code is better because its error-correcting power is greater. For example, suppose your code has 10 message symbols and 30 code symbols. In the redundancy code, the 30 code symbols will be 10 triplets xxx, each encoding one message symbol x. This code can only correct 10 errors if just one error occurs in each triplet. If 2 errors occur in the same triplet, it will fail. The Reed-Solomon code of the same length, by contrast, will correct 10 errors no matter where they occur in the 30 code positions.