

Answers to review problems for 2nd Midterm

1. (a) Since any code vector \mathbf{y} is the sequence of values of a polynomial of degree at most 3, it must satisfy $\Delta^4 \mathbf{y} = \mathbf{0}$. Calculate $\Delta^4 \mathbf{r} = [2 \ 3]$. Since this is not zero, there is an error.
 (b) $[1 \ 0]$, $[3 \ 1]$, $[6 \ 3]$, $[3 \ 6]$, $[1 \ 3]$, $[0 \ 1]$.
 (c) $\Delta^4 \mathbf{r} = [2 \ 3] \equiv 3[3 \ 1] = 3\Delta^4 \mathbf{e}_2$, where $e_2 = [0 \ 1 \ 0 \ 0 \ 0 \ 0]$. Adding $-3e_2 \equiv [0 \ 4 \ 0 \ 0 \ 0 \ 0]$ to \mathbf{r} will therefore produce a vector $\mathbf{y} = [4 \ 2 \ 2 \ 6 \ 2 \ 6]$ with $\Delta^4 \mathbf{y} = \mathbf{0}$. This \mathbf{y} is the desired code vector. The error was in the second symbol.

2. (a)

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 \end{bmatrix}$$

- (b) $[4 \ 4 \ 10 \ 0 \ 7 \ 9 \ 6 \ 9 \ 7]$.

- (c) Three, since $2e = n - m$ for a Reed-Solomon code.

- (d) Yes, it's better. Both codes have the same number of message symbols and code symbols. The redundancy code can sometimes correct three errors, if they happen to be distributed one in each group of three symbols, but in the worst case it can only correct one error. The Reed-Solomon code can correct any three errors.

3. (a) Let $E(t) = u_0 + u_1 t + u_2 t^2$. Use the difference table method to obtain equations for the unknown coefficients:

$$\begin{bmatrix} 1 & 10 & 8 \\ 1 & 6 & 6 \end{bmatrix} [u_0 \ u_1 \ u_2] = \mathbf{0}.$$

Setting $u_2 = 1$, solve to find $u_0 = 8$, $u_1 = 5$, $E(t) = t^2 + 5t + 8$.

- (b) Calculate to find $E(i) \equiv 0$ for $i \equiv 2$ and $i \equiv 4 \pmod{11}$. The errors are in r_2 and r_4 , the third and fifth positions (since the first position is r_0).

4. Solve the linear system using arithmetic (mod 5) to get the message vector $[2 \ 0 \ 2 \ 1]$.

5. Method 1: There are eight cases: $n \equiv 1, 3, 5, 7, 9, 11, 13, \text{ or } 15 \pmod{16}$. Compute n^4 and verify that the result is $\equiv 1$ in each case.

Method 2: Let $n = 2k + 1$. A bit of algebra gives $n^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1$, which is congruent to $8k^2 + 8k + 1 \pmod{16}$. Now $8k^2 + 8k = 8k(k + 1)$ is divisible by 16 no matter whether k is even or odd, so $n^4 \equiv 1 \pmod{16}$ in either case.

6. Suppose to the contrary that p_1, \dots, p_l is a list of all the primes of the form $3k + 2$. Let $Q = 3p_1 \cdots p_l - 1$. Then $Q \equiv -1 \pmod{p_i}$ for every p_i , so no p_i is a factor of Q . The only possible prime factors of Q are then 3 and primes congruent to 1 (mod 3), which implies that $Q \equiv 0$ or $Q \equiv 1 \pmod{3}$. But $Q \equiv 2 \pmod{3}$ by construction, so we have a contradiction.

7. Let $P = n(n + 1)(n + 2)(n + 3)$ be the product of four consecutive integers. At least one of the integers $n, n + 1, n + 2, n + 3$ is divisible by 3, so P is divisible by 3. Two of them are even, and one of those is divisible by 4, so P is divisible by 8. Since 3 and 8 are relatively prime, P is divisible by their product, 24.

8. Proof by induction on n . Basis step is $n = 4$. Then $2^4 = 16 < 24 = 4!$, so $2^n < n!$ in this case. For the induction step, assume $2^n < n!$. Clearly $2 \leq n + 1$, so multiplying $2^n < n!$ by 2 on the left and by $n + 1$ on the right shows that $2^{n+1} < (n + 1)!$.

9. Proof by induction on n . Basis step is $n = 1$, where both sides of the identity reduce to 1. For the induction step assume

$$1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6.$$

Add $(n+1)^2$ to both sides and do a little algebra to get

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= n(n+1)(2n+1)/6 + (n+1)^2 \\ &= (n+1)(n+2)(2(n+1)+1)/6. \end{aligned}$$

10. Proof by induction on n . The basis step $n = 1$ is obvious. For the induction step, assume

$$\mathbf{A}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

and multiply both sides by \mathbf{A} to get

$$\mathbf{A}^{n+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}.$$