

## Partial Solutions to Homework 12 for MATH 336

### Coding Supplement 4.5

We want to find the generator polynomial for a 16-ary  $[15, 11]$  Reed-Solomon code. So  $n = 15$ ,  $k = 11$ , and  $q = 16$ . By Theorem 4.3.7, this code will have a minimum distance  $d = n - k + 1 = 15 - 11 + 1 = 5$ .

Since  $q = 16$ , this Reed-Solomon code is constructed over the finite field  $GF(16)$ . Note that  $GF(16)$  is NOT  $\mathbb{Z}/16\mathbb{Z}$ , because 16 is composite and hence  $\mathbb{Z}/16\mathbb{Z}$  is not a field. Instead,  $GF(16) \simeq \mathbb{F}_2[x]/(x^4 + x + 1)$ , since  $x^4 + x + 1$  was previously shown to be irreducible. As shown in class,  $\alpha = [x]/(x^4 + x + 1)$  is a primitive element of  $\mathbb{F}_2[x]/(x^4 + x + 1)$ .

We now use the definition of a generator polynomial  $g(x)$  of a Reed-Solomon code, as found directly above Example 4.3.6 to see that:

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) \\ &= x^4 + (1 + \alpha^2 + \alpha^3)x^3 + (\alpha^3 + \alpha^2)x^2 + \alpha^3x + (\alpha^2 + \alpha + 1) \end{aligned}$$

where the last line follows after expanding and combining terms.