

1. Prove the following interesting facts about binary polynomials:

- (a) If $p(x)$ is a binary polynomial, then $(p(x))^2 = p(x^2)$.
- (b) If $\alpha \in GF(2^r)$ is a root of the binary polynomial, then so are $\alpha^2, \alpha^4, \alpha^8$, etc.

2. Build the Galois field $GF(2^4)$ using the following irreducible polynomials. For each construction, determine the minimal polynomials for each of the field elements. (*Hint*: You should see the same set of polynomials in both tables since there is only one $GF(2^4)$!)

- (a) $g_1(x) = x^4 + x + 1$.
- (b) $g_2(x) = x^4 + x^3 + x^2 + x + 1$.

3. Let the Galois field $GF(2^4)$ be built by adjoining to the base field $\mathcal{F} = \{0, 1\}$ a root α of the primitive polynomial $g(x) = x^4 + x^3 + 1$. Express the following elements γ in terms of the basis elements $\{1, \alpha, \alpha^2, \alpha^3\}$.

(a) $\gamma = 1 + \alpha^{-1} + \alpha^{-2} + \alpha^{-3}$.

(b) $\gamma = \frac{\alpha^5(1 + \alpha^{-11})}{1 + \alpha^{-2}}$.

(c) $\gamma = \sum_{\beta \in GF(2^4)} \beta$.

(d) $\gamma = \prod_{\beta \in GF(2^4) - \{0\}} \beta$.

4. Duals of BCH codes.

- (a) Let \mathcal{C} be the primitive, narrow-sense BCH code of length $n = 15$ and design distance $d = 3$. Show that \mathcal{C}^\perp is also a BCH code. What does the BCH bound tell you about the minimum distance of \mathcal{C}^\perp ?
- (b) Let \mathcal{C} be the primitive, narrow-sense BCH code of length $n = 15$ and design distance $d = 5$. Show that \mathcal{C}^\perp is *not* a BCH code.