quiz 10.3 Solution

(1) Determine the dimension and minimum distance of the BCH code of length 48 constructed with designed distance 9 using the field extension $GF(7^2)$ of the finite field $GF(7)$.

There is an efficient approach (below) which in effect does the following. First, the Frobenius automorphism $x \to x^p$ (over the finite field $GF(p)$) is applied repeatedly to the rows of the initial check matrix H for the BCH code, making a larger check matrix, called the Frobenius-stable check matrix (after all the different possibilities are included, but without repetition). The row rank of this Frobenius-stable check matrix is the 'true' row rank, in the sense that

$$\text{dimension of BCH code} = \text{length} - \text{ row rank of Frob-stable check matrix}$$

Further, a better estimate of the minimum distance can be obtained from the Frobenius stable check matrix: let t' be the largest integer so that contiguous exponents $1, 2, 3, \ldots, t'-2, t'-1$ appear as exponents (of the primitive root) in the second column of the Frobenius-stable check matrix. Then the minimum distance is *at least* t'. (We cannot easily reach a stronger conclusion about minimum distance since we have only the Vandermonde determinant criterion for linear independence of columns.)

More efficiently, given the set of exponents (of the primitive root) in the second column of the usual check matrix for a length n BCH code using $GF(p^m)$ over $GF(p)$, to determine the set of such exponents in the Frobenius-stable version we repeatedly multiply these exponents by p (reducing modulo $p^m - 1$). Let r be the number of exponents in the Frobenius-stabilized set: then the actual dimension k of the code is $k = n - r$. That is, there is no need to write the whole rows of any check matrix, but only the exponents occurring in the second column, since that exponent determines the whole row.

Here, the inital set of exponents in the second column of the check matrix is $1, 2, 3, \ldots, 8$ (going up to design distance t less 1). Repeatedly multiplying by 7 (effectively applying the Frobenius) gives the Frobenius-stable set

$$1, 2, 3, 4, 5, 6, 7, 8, 14, 21, 28, 35, 42$$

which has 13 elements. Thus, the row rank of the Frobenius-stable check matrix is 13, and the dimension of the BCH code is (with length 48)

$$48 - 13 = 35$$

The largest t' so that continguous exponents $1, 2, \ldots, t' - 1$ is visibly 9. Thus, we can conclude that the actual minimum distance is *at least* 9.

(2) Is the cubic $p(x) = x^3 + x^2 + 3x + 6$ irreducible, or not, in $\mathbf{F}_7[x]$?

We do trial division. Since the polynomial is of degree 3 and we need only test for divisibility by *monic* polynomials $d(x)$ of degree $\leq$ degree$/2 = 3/2$, and since degrees are integers, we need only test for divisibility by monic *linear* polynomials. And a linear factor $x - \alpha$ divides $p(x)$ if and only if $p(\alpha) = 0$, so we need only evaluate $p(\alpha)$ for $\alpha = 0, 1, \ldots, 7 - 1$. If any of these values is 0, then the cubic is *reducible*. If none is 0, then it is *irreducible*. Evaluate, successively:

$$p(0) = 6 \neq 0 \bmod 7$$

$$p(1) = 4 \neq 0 \bmod 7$$

$$p(2) = 3 \neq 0 \bmod 7$$

$$p(3) = 2 \neq 0 \bmod 7$$

But then

$$p(4) = 0 = 0 \bmod 7$$

so the polynomial is *reducible*, with linear factor $x - 4$.

(3) Is the cubic $x^3 + 3x^2 + x + 1$ irreducible or not in $\mathbf{F}_5[x]$?

We do trial division. Since the polynomial is of degree 3 and we need only test for divisibility by *monic* polynomials $d(x)$ of degree $\leq$ degree$/2 = 3/2$, and since degrees are integers, we need only test for divisibility by monic *linear* polynomials. And a linear factor $x - \alpha$ divides $p(x)$ if and only if $p(\alpha) = 0$,

so we need only evaluate $p(\alpha)$ for $\alpha = 0, 1, \ldots, 5-1$. If any of these values is 0, then the cubic is *reducible*. If none is 0, then it is *irreducible*. Evaluate, successively:

$$p(0) = 1 \neq 0 \bmod 5$$

$$p(1) = 1 \neq 0 \bmod 5$$

$$p(2) = 3 \neq 0 \bmod 5$$

$$p(3) = 3 \neq 0 \bmod 5$$

$$p(4) = 2 \neq 0 \bmod 5$$

Thus, having failed to find a monic linear factor, the polynomial is *irreducible*.

(4) The cubic polynomial $x^3 + 3x^2 + 2$ is irreducible in $\mathbf{F}_5[x]$. (Do it not recheck the irreducibility.) Let $\alpha = x\text{-mod-}(x^3 + 3x^2 + 2)$ be one root in $\mathbf{F}_{5^3}$ of the cubic equation $x^3 + 3x^2 + 2 = 0$. (Note that the root α is not $\mathbf{F}_5$, but in the larger field $\mathbf{F}_{5^3}$.) Find it another root and express it in the form

$$c + b \cdot \alpha + a \cdot \alpha^2$$

for some c, b, a in F_5.

Generally, if α is a root of an equation $g(x) = 0$ with $g(x) \in \mathbf{F}_q[x]$, then α^q (the image of α under the Frobenius automorphism) is another root. Thus, here, α^5 is another root. But we need to *reduce* this expression, by computing

$$x^5 \,\%\, (x^3 + 3x^2 + 2) = x^2 + x + 2$$

(perhaps simply by division.) Thus, one other root is $\alpha^2 + \alpha + 2$. Another root will be α^{5^2} which we compute in the desired form (probably by fast modular exponentiation), by computing, in successive states $(X, E, Y) = (x, 25, 1), (x, 24, x), (x^2, 12, x), (4x^2 + 3x + 1, 6, x), (4x^2 + 4x + 4, 3, x), (4x^2 + 4x + 4, 2, 2x^2 + 4x + 2), (x^2 + 3, 1, 2x^2 + 4x + 2), (x^2 + 3, 0, 4x^2 + 3x)$, so

$$x^{5^2} \,\%\, (x^3 + 3x^2 + 2) = 4x^2 + 3x$$

Thus, the third root is $4\alpha^2 + 3\alpha$. The complete list of roots is $\alpha,\ \alpha^2 + \alpha + 2,\ 4\alpha^2 + 3\alpha$.