quiz 07.1 Solution

(1) Efficiently compute the greatest common divisor of $x^8+x^5+x^4+x+1$ and $x^7+x^6+x^5+x+1$, as polynomials with coefficients in $\mathbf{F}_2 = GF(2)$.

Use the Euclidean algorithm applied to $x^8+x^5+x^4+x+1, x^7+x^6+x^5+x+1$: each step is a reduction algorithm step of the form $D - q \cdot d = r$. For each such line, the next replaces the previous dividend D by the previous divisor d, and replaces the divisor by the previous remainder r. The algorithm terminates when the right-hand side (remainder) is 0. The last non-zero remainder is the greatest common divisor.

$$(x^8+x^5+x^4+x+1) - (x+1)\cdot(x^7+x^6+x^5+x+1) = x^4+x^2+x$$

$$(x^7+x^6+x^5+x+1) - (x^3+x^2)\cdot(x^4+x^2+x) = x^3+x+1$$

$$(x^4+x^2+x) - (x)\cdot(x^3+x+1) = 0$$

Thus, the gcd of $x^8+x^5+x^4+x+1$ and $x^7+x^6+x^5+x+1$ is x^3+x+1. Since the last right-hand side before the 0 is always the gcd, the greatest common divisor of $x^8+x^5+x^4+x+1$, and $x^7+x^6+x^5+x+1$ is x^3+x+1.

(2) Find the multiplicative inverse of x^3+x+1 modulo x^5+x^3+1, as polynomials with coefficients in $\mathbf{F}_2 = GF(2)$.

Use the extended Euclidean algorithm applied to polynomials $g = x^3+x+1$ and $f = x^5+x^3+1$ to obtain polynomials a and b so that $af+bg = 1$. Looking at the latter relation modulo f gives b as a multiplicative inverse of g modulo f. Executing the extended Euclidean algorithm:

$$\begin{aligned}(x^5+x^3+1) + (x^2)(x^3+x+1) &= x^2+1\\ (x^3+x+1) + (x)(x^2+1) &= 1\\ (x^2+1) + (x^2+1)(1) &= 0\end{aligned}$$

$$\begin{aligned}1 &= (1)(x^3+x+1) + (x)(x^2+1)\\ &= (1)(x^3+x+1) + (x)[(x^5+x^3+1) + (x^2)(x^3+x+1)]\\ &= (x)(x^5+x^3+1) + (x^3+1)(x^3+x+1)\end{aligned}$$

Thus, by the earlier comment about expressions of the form $as+bt = 1$, the multiplicative inverse of x^3+x+1 modulo x^5+x^3+1 is x^3+1.

(3) Is it possible to find 32 binary codewords of length 10 with minimum distance at least 5?

A simple *necessary* condition for the existence of a binary code of (block) length n, with ℓ codewords, and correcting e errors, is the **Hamming bound**

$$\ell \cdot (1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{e}) \leq 2^n$$

In the present case, since e errors can be corrected if the minimum distance is $2e+1$, $e = 2$. The length is 10, and the number off codewords is $\ell = 32$. We compute the two sides of the Hamming bound in this case:

$$\text{left-hand side } = 1792 > 1024 = \text{ right-hand side}$$

That is, the Hamming inequality is contradicted, so there is no such code.

(4) Is there a (binary) [11,5] linear code with minimum distance 4?

Use the Gilbert-Varshamov bound, which says that for a binary $[n, k, d]$-code to exist we have the sufficient condition

$$2^{n-k} - 1 > \binom{n-1}{1} + \ldots + \binom{n-1}{d-2}$$

In the case at hand, plugging in $n = 11$, $k = 5$, $d = 4$, we ask whether or not it is true that

$$2^{11-5} - 1 > \binom{11-1}{1} + \binom{11-1}{2}$$

That is, we ask whether or not

$$63 > 55$$

Since this inequality holds, there does exist such a code.