ASSIGNMENT #2 SOLUTIONS

I. Let F be a field with $q = 2^n$ elements. For any non-zero element $\beta \in F$ we define

$$\mathrm{ord}(\beta) := \min\{i \text{ such that } \beta^i = 1\}.$$

From now on, set $0 \neq \beta \in F$.

(1) Show that $\mathrm{ord}(\beta)$ divides $q - 1$.

Solution. Let $m := \mathrm{ord}(\beta)$. Let us show a more general claim; namely, $\beta^i = 1$ if and only if $m|i$. The "if" direction is obvious. To show the "only if" direction, observe that $i \geqslant m$ (by definition of order), so consider

$$i = sm + r$$

where s and r are non-negative integers and $r < m$. Then we have

$$1 = \beta^i = \beta^{sm+r} = (\beta^m)^s \beta^r = \beta^r$$

But since m is the smallest positive integer such that $\beta^m = 1$, this forces $r = 0$. So m divides i.

Now, by Fermat's little theorem $\beta^{q-1} = 1$, so we have $m|(q-1)$. □

Remark. I found a few solutions which invoked Lagrange's theorem (from group theory). Indeed, the statement of this problem is precisely Lagrange's theorem for the multiplicative group F^*; in other words, the problem asks to prove Lagrange's theorem for F^*. So it feels a bit too strange for me to regard as correct those solutions which *use* Lagrange's theorem.

I do not prohibit solutions using some standard group theory or algebraic number theory, as far as everything is done correctly (though I may apply much stricter standard for correctness, to be fair). But as the instruction sheet says, you may use standard result unless "the result you assume is not a mere paraphrasing of the question itself. "

(2) Show that β is a primitive element if and only if $\mathrm{ord}(\beta) = q - 1$.

Solution. It is enough to show that $\beta \mathfrak{n} F$ is primitive if and only if $\{0, 1 = \beta^0, \beta^1, \beta^2, \cdots, \beta^{q-2}\} = F$. Let $\gamma \in F$ be any non-zero element. By definition of primitive element, there is some non-negative integer i such that $\beta^i = \gamma$. If $i \geqslant q - 1$, then consider

$$i = s(q-1) + r$$

where s and r are non-negative integers and $r < q - 1$. Then we have

$$\gamma = \beta^i = \beta^{s(q-1)+r} = (\beta^{q-1})^s \beta^r = \beta^r$$

This shows that any non-zero elements of F can be expressed as β^r for some integer $0 \leqslant r \leqslant q - 2$. But since there are exactly $q - 1$ non-zero elements in F, all β^r must be distinct for $r = 0, \cdots, q - 2$. □

(3) For any integer $d \geq 1$ show that

$$\mathrm{ord}(\beta^d) = \frac{\mathrm{lcm}(\mathrm{ord}(\beta), d)}{d},$$

where $\mathrm{lcm}(a, b)$ means the least common multiple of a and b.

Solution. Let $m := \mathrm{ord}(\beta)$. We've already showed in the solution of (1) that $\beta^i = 1$ if and only if $m|i$. Therefore $(\beta^d)^n = 1$ if and only if $m|nd$. The smallest such nd is precisely $\mathrm{lcm}(d, m)$, hence $\mathrm{ord}(\beta^d) = \mathrm{lcm}(d, m)/d$. □

(4) Assume that β is a primitive element. Show that β^d is a primitive element if and only if $\mathrm{hcf}(d, q-1) = 1$.

Solution. Note that $\mathrm{hcf}(d, q-1) = 1$ if and only if $\mathrm{lcm}(d, q-1) = d(q-1)$. So by (2) and (3), β^d is primitive if and only if $\mathrm{ord}(\beta^d) = q-1$ if and only if $\mathrm{hcf}(d, q-1) = 1$. □

(5) Now assume that $q = 2^4$ and $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. Find all primitive elements in F. (*Hint*: First, show that $\alpha \in F$ is a primitive element.)

Solution. To show α is primitive (or equivalently, $\mathrm{ord}(\alpha) = 15$), we need to show that $\alpha^3 \neq 1$ and $\alpha^5 \neq 1$ (since 3 and 5 are the only divisors of $15 = q-1$). But α^3 is clearly not equal to 1, and $\alpha^5 = \alpha^2 + \alpha$ is not equal to 1. So α is primitive.

Now, by (4) it is enough to find all integers between 1 and 14 which is coprime to 15. One can easily go through all 14 integers and check that 1, 2, 4, 7, 8, 11, 13, and 14 are coprime to 15. So primitive elements of F are α, α^2, α^4, α^7, α^8, α^{11}, α^{13}, and α^{14}. □

II. Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. For this question, "minimal polynomials" means minimal polynomials over $\mathbb{B}$.

(1) Find the minimal polynomial of each element of F. (*Hint*: You do *not* have to compute the minimal polynomials 16 times!)

Solution. Clearly, the minimal polynomial of 0 and 1 are respectively X and $X-1$. So it is left to find the minimal polynomials of $\beta \notin \mathbb{B}$.

We learned that the minimal polynomial of β is equal to the minimal polynomial of β^2. Therefore:

- α, α^2, α^4, and α^8 have the same minimal polynomials. (Note that $(\alpha^8)^2 = \alpha^{16} = \alpha$.)
- α^3, α^6, α^{12}, and α^9 have the same minimal polynomials. (Note that $(\alpha^9)^2 = \alpha^{18} = \alpha^3$.)
- α^5 and α^{10} have the same minimal polynomials. (Note that $(\alpha^{10})^2 = \alpha^{20} = \alpha^5$.)
- α^7, α^{14}, α^{13}, and α^{11} have the same minimal polynomials. (Note that $(\alpha^{11})^2 = \alpha^{22} = \alpha^7$.)

So it is enough to find the minimal polynomials of α, α^3, α^5 and $\alpha^{14} = \alpha^{-1}$.

The minimal polynomial of α is clearly $X^4 + X + 1$ because α is its zero and it is irreducible.

The minimal polynomials of α^3, α^5, and α^{14} are respectively $X^4 + X^3 + X^2 + X + 1$, $X^2 + X + 1$, and $X^4 + X^3 + 1$. There are a few ways to obtain this. One (rather inefficient) way to find minimal polynomial of any element $\beta \in F$ is to search for $\mathbb{B}$-linear relations between $\{1, \beta, \cdots, \beta^i\}$ as you increase i. An alternative and slicker way to find the minimal polynomials.

- Since $(\alpha^3)^5 = 1$ by Fermat's little theorem, α^3 is a zero of $X^5 - 1$. But since $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$ and $\alpha^3 \neq 1$, we see that α^3 is a zero of $X^4 + X^3 + X^2 + X + 1$. Now note that $X^4 + X^3 + X^2 + X + 1$ is irreducible. One can similarly proceed to obtain the minimal polynomial of α^5 using $(\alpha^5)^3 = 1$.

- Since $\alpha^4 + \alpha + 1 = 0$, we obtain
$$0 = \alpha^{-4}(\alpha^4 + \alpha + 1) = 1 + (\alpha^{-1})^3 + (\alpha^{-1})^4.$$
Therefore, α^{-1} is a zero of X^4+X^3+1. And X^4+X^3+1 is irreducible.

□

Remark. I found a few solutions which proves the minimal polynomial for α^{-1} is $X^4 + X^3 + 1$ *using* the isomorphism
$$\mathbb{B}[\beta]/\beta^4 + \beta^3 + 1 \xrightarrow{\sim} \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1,$$
defined by sending β to α^{-1}. Indeed, this solution is *circular* for the following reason; the reason why the aforementioned map is a well-defined ring homomorphism is precisely because the minimal polynomial of α^{-1} is $X^4 + X^3 + 1$.

(2) Factorise *all* the polynomials which are minimal polynomials of some $\beta \in F$ into linear polynomials with coefficients in F. (*Remark*: You can solve this problem *without* doing any computation!)

Solution. Note that X and $X - 1$ are already linear polynomials.

For $X^4 + X + 1$, we know all four zeroes of it; namely, α, α^2, α^4, and α^8. (Note that $X^4 + X + 1$ is the common minimal polynomial of these elements.) So
$$X^4 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$$

For the same reason, we obtain
$$\begin{aligned} X^4 + X^3 + X^2 + X + 1 &= (X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})(X - \alpha^9) \\ X^2 + X + 1 &= (X - \alpha^5)(X - \alpha^{10}) \\ X^4 + X^3 + 1 &= (X - \alpha^7)(X - \alpha^{14})(X - \alpha^{13})(X - \alpha^{11}) \end{aligned}$$

□

(3) Using *Fermat's little theorem*, factorise $X^{16} - X$ into linear polynomials with coefficients in F.

Solution. By Fermat's little theorem, any 16 elements $\beta \in F$ are zeroes of $X^{16} - X$. Since we've found all 16 zeroes, we have
$$X^{16} - X = \prod_{\beta \in F} (X - \beta).$$

□

(4) Combining all the previous parts, factorise $X^{16} - X$ into *irreducible* polynomials in $\mathbb{B}[X]$.

Solution. Recall from the previous part that
$$X^{16} - X = \prod_{\beta \in F} (X - \beta) = (X - 0) \prod_{i=0}^{14} (X - \alpha^i).$$

Using (2), we may regroup the factorisation of $X^{16} - X$ as follows:
$$X^{16} - X = (X - 0)(X - 1)(X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1) \\ (X^2 + X + 1)(X^4 + X^3 + 1).$$

□

III. Is BCH$(4,3)$ r-perfect for any r?

Solution. Note that the dimension of BCH$(4,3)$ is 5. So one needs to look for a positive integer r such that $2^{10} = 1024 = \sum_{i=0}^{r} \binom{15}{i}$. Note that the formula on the right hand side is the number of vectors $w \in \mathbb{B}^{15}$ such that $d(w,0) \leqslant r$.

But when $r = 3$ and $r = 4$, we have

$$\begin{aligned} \sum_{i=0}^{3} \binom{15}{i} &= 1 + 15 + 105 + 455 < 1024 \\ \sum_{i=0}^{4} \binom{15}{i} &= 1 + 15 + 105 + 455 + 1365 > 1024. \end{aligned}$$

Note that $\sum_{i=0}^{r} \binom{15}{i}$ increases as r increases, so it cannot equal 1024. So BCH$(4,3)$ is not r-perfect for any r. □

Remark. It turns out that the minimal distance of BCH$(4,3)$ is precisely 7 (not just at least 7). I mentioned this in lecture, but I did not prove it. Indeed, the proof is rather some exhaustive search in the spirit of Question 4 of Assignment#1 (i.e., something not straightforward). This is why I bother to rule out r-perfectness for $r \geqslant 4$.