8 a) The answer is 1

Proof: First we will prove the following lemma:

Lemma: If $n$ is odd and $a \in \widehat{\mathbb{F}_{2^n}}$, then $a^2 + a \in \widehat{\mathbb{F}_{2^n}}$.

Proof: Since $a \in \widehat{\mathbb{F}_{2^n}}$, there is a polynomial $P(x) \in \mathbb{F}_2[x]$ degree $n$ such that $P$ is irreducible and has $a$ as its root. This come from the fact that $x^{2^n} - x$ is the product of all irreducible polynomials in $\mathbb{F}_2[x]$ such that their degree divides $n$. Let $t = a^2 + a$, then $t \in \widehat{\mathbb{F}_{2^d}}$ with $d \mid n$. Let $Q(x) \in \mathbb{F}_2[x]$ such that $Q$ is irreducible and has $t$ as its root. Then $\deg(Q) = d$. It is easy to see that $a$ is a root of $Q(x^2+x)$. This means $P(x) \mid Q(x^2+x)$. However $\deg(P) = n$ and $\deg(Q(x^2+x)) = 2d$, this means $d = n$ since $d \mid n$. Thus we proved the lemma.

Now, we compute $|\widehat{\mathbb{F}_{2^n}}|$. We see that:

$$\sum_{d \mid n} |\widehat{\mathbb{F}_{2^d}}| = 2^n$$

Thus $|\widehat{\mathbb{F}_{2^n}}| = \sum_{d \mid n} 2^d \mu\left(\frac{n}{d}\right)$, where $\mu$ is the mobius function.

By the lemma above, we have:

$$|B_n^1| = \#\{x^2 + x \mid x \in \widehat{\mathbb{F}_{2^n}}\}$$

We see that $x^2 + x = y^2 + y \iff \left[\begin{array}{l} x = y \\ x = y + 1 \end{array}\right.$, therefore

$$\#\{x^2 + x \mid x \in \widehat{\mathbb{F}_{2^n}}\} = \frac{1}{2} |\widehat{\mathbb{F}_{2^n}}|$$

Thus $|B_n^0| / |B_n^1| = 1$

$\mathbb{F}_2[x]$

at

$d \mid n$.

b) Answer:

When $n$ is odd, then $|B_n^0| = |B_n^1| = \frac{1}{2}\sum_{d\mid n} 2^d \mu\left(\frac{n}{d}\right)$

When $n$ is even, if $n = 2^k t$, $t$ is odd, then

$$G(n) = \sum_{d\mid t} 2^{2^{k-1}d}\mu\left(\frac{t}{d}\right)$$

We have $|B_n^1| = \frac{1}{2}\left(\sum_{d\mid n} 2^d \mu\left(\frac{n}{d}\right) - G(n)\right)$

$$|B_n^0| = \frac{1}{2}\left(\sum_{d\mid n} 2^d \mu\left(\frac{n}{d}\right) + G(n)\right)$$

Currently, I do not know an explicit fomula for $G(n)$.

<u>Proof</u>: We just need to consider even $n$, sine we proved everything for odd $n$ in a).

Let $C_n = \{ t \in \widehat{\mathbb{F}_{2^{n/2}}} \mid t = x^2 + x$ for some $x \in \widehat{\mathbb{F}_{2^n}} \}$

From a), we see that if $x \in \widehat{\mathbb{F}_{2^n}}$, then $x^2 + x$ is in $\widehat{\mathbb{F}_{2^n}}$ or $\widehat{\mathbb{F}_{2^{n/2}}}$ since $n$ is even.

Thus: $|B_n^1| = \# \{ x^2 + x \mid x \in \widehat{\mathbb{F}_{2^n}} \} - \# C_n$

* For $n \in \mathbb{N}$, <u>let $A(n) = \{ P(x) \in \mathbb{F}_2[x] \mid P$ is irreducible and $\deg(P) = n \}$</u>

Note that, if $t \in C_n$, then consider $Q \in A\left(\frac{n}{2}\right)$ that has $t$ as its root, then $Q(x^2+x) \in A(n)$, because $t = a^2 + a$ for some $a \in \widehat{\mathbb{F}_{2^n}}$ and $a$ is a root of $Q(x^2+x)$.

In the other hand, if $Q \in A\left(\frac{n}{2}\right)$ and $Q(x^2+x) \in A(n)$, then if $t$ is a root of $Q$ then $t \in C_n$.

From this observation, each $Q \in A\left(\frac{n}{2}\right)$ and $Q(x^2+x) \in A(n)$ gives us $\frac{n}{2}$ values in $C_n$.

Thus, if we let:

$D_n = \{ Q(x) \in \mathbb{F}_2[x] \mid Q \in A(\frac{n}{2})$ and $Q(x^2+x) \in A(n)$

then we have $|C_n| = \frac{n}{2} |D_n|$

To compute $|D_n|$, we consider the polynomial:

$Z_n(x) = x^{2^{n/2}-1} - 1$

Then $Z_n(x^2+x) = (x^2+x)^{2^{n/2}-1} - 1$

We claim that, the set of irreducible divisor of $Z_n$ is $E_n \cup F_n$, where:

$E_n = \{ P(x) \in \mathbb{F}_2[x] \mid P$ is irreducible and $P \mid Z_n(x) \}$

$F_n = \{ P(x^2+x) \mid P \in A(d)$ and $P(x^2+x) \in A(2d)$ for some $d$ such that $d \mid \frac{n}{2}$ and $2d \nmid \frac{n}{2} \}$

Proof of claim:

Note that $x^{2^{n/2}-1} - 1 = \prod_{P(x) \in E_n} P(x)$. Thus $(x^2+x)^{2^{n/2}-1} - 1 = \prod_{P(x)\in E_n} P(x^2+x)$. Consider $Q \in E_n \cup F_n$. If $Q \in E_n$ not that $Q \mid \frac{x^{2^{n/2}-1}-1}{x-1}$, and $(x^2+x)^{2^{n/2}-1} - 1 \equiv (x+1)^{2^{n/2}-1} - 1 \equiv x \cdot \frac{x^{2^{n/2}-1}-1}{x-1} \equiv 0 \pmod{\frac{x^{2^{n/2}-1}-1}{x-1}}$, thus $Q \mid Z_n(x^2+x)$.

If $Q \in F_n$, then $Q = P(x^2+x)$ for $P \in A(d)$ with $d \mid \frac{n}{2}$ thus $P \mid x^{2^{n/2}-1} - 1$, and therefore $P(x^2+x) \mid (x^2+x)^{2^{n/2}-1} -$

Conversely, if $Q$ is an irreducible divisor of $(x^2+x)^{2^{n/2}-1} - 1$. If $Q \in E_n$ we are done. Otherwise, $Q \mid P(x^2+x)$ for some $P \in E_n$. Suppose $P \in A(d)$, then $P(x^2+x) \in A(2d)$, or $P(x^2+x)$ is the product of 2 polynomials in $A(d)$. If it is the latter case, then

$Q(x) \in A(d)$, but since $d \mid \frac{n}{2}$, we have $Q \mid x^{2^{n/2}-1} - 1$, contradiction. Thus $Q = P(x^2+x)$. Since $Q \nmid x^{2^{n/2}-1} - 1$ we have $2d \nmid \frac{n}{2}$, this means $Q \in F_n$, and thus we proved our claim.

Back to the problem, we see that $Z_n(x^2+x)$ does not have multiple root since $Z'(x^2+x) = (x^2+x)^{2^{n/2}-2}$. From this, we see that $(x^2+x)^{2^{n/2}-1} - 1 = \frac{x^{2^{n/2}-1}-1}{x-1} \cdot \prod_{Q \in F_n} Q(x)$

Let $n = 2^k t$, where $t$ is odd.

Let $G_d = \{ Q(x^2+x) \mid Q \in A(d) \text{ and } Q(x^2+x) \in A(2d) \}$

Then $F_n = F_{2^k t} = \bigcup_{d \mid t} G_{2^{k-1} d}$ and $|D_n| = |D_{2^k t}| = |G_{2^{k-1} t}|$

We have: $(x^2+x)^{2^{n/2}-1} - 1 = \frac{x^{2^{n/2}}-1-1}{x-1} \cdot \prod_{d \mid t} \cdot \prod_{Q \in G_{2^{k-1} d}} Q(x)$

By comparing the degree, we have:

$$2^{2^{k-1} t + 1} - 2 = 2^{2^{k-1} t} - 2 + \sum_{d \mid t} 2^k d \cdot |G_{2^{k-1} d}|$$

By using Mobius inversion fomula, we have:

$$2^k t \, |G_{2^{k-1} t}| = \sum_{d \mid t} 2^{2^{k-1} d} \mu\left(\frac{t}{d}\right)$$

Let $G(n) = \sum_{d \mid t} 2^{2^{k-1} d} \mu\left(\frac{t}{d}\right)$, then $|C_n| = 2^{k-1} t \, |D_{2^k t}| =$

$$2^{k-1} t \, |G_{2^{k-1} t}| = \frac{1}{2} G(n)$$

Finally, $|B_n^1| = \frac{1}{2}\left(\sum_{d \mid n} 2^d \mu\left(\frac{n}{d}\right) - G(n)\right)$

$|B_n^0| = \frac{1}{2}\left(\sum_{d \mid n} 2^d \mu\left(\frac{n}{d}\right) + G(n)\right)$, when $n$ is even

When $n$ is odd, as we proved in a)

**VKA**

$|B_n^0| = |B_n^1| = \frac{1}{2}\left(\sum_{d \mid n} 2^d \mu\left(\frac{n}{d}\right)\right)$