Question 3

1. If \(a = b\), then the polynomials \(A(x), B(x)\) are equal, therefore, \(A(\alpha_i) = B(\alpha_i)\) for any choice of \(i\). Thus, the protocol always outputs 'equal'.

2. Solution 1. If \(a \neq b\), then the polynomials \(A(x), B(x)\) are distinct. These polynomials are of degree at most \(k - 1\), and therefore can be equal at at most \(k - 1\) points in \(\mathbb{F}\). Namely, there are at most \(k - 1\) values of \(i\) on which the protocol outputs 'equal'.

Solution 2. We look at \(a\) and \(b\) as messages that are encoded using a \([3k, k]\) RS code into the codewords \((A(\alpha_1), \ldots, A(\alpha_{3k}))\) and \((B(\alpha_1), \ldots, B(\alpha_{3k}))\) (resp.). We know that the distance of such code is \(d = 3k - k + 1 = 2k + 1\), meaning that there are at least \(2k + 1\) values of \(i\) on which the codewords differ, and at most \(k - 1\) values on which they agree.

3. The protocol outputs 'equal' if one of the \(k - 1\) 'bad' \(i\)'s were chosen. As \(i\) is chosen randomly from \([3k]\), this happens with probability \(\leq \frac{k - 1}{3k} < \frac{1}{3}\).

4. A single field member is sent, as well as \(\log(3k) + 1\) bits (representing \(i\) and the result).

Question 4

1. The equality was shown in class for any orthonormal basis of characters (the group is finite and abelian).

2. Every column in the matrix represents a vector \(a \in \mathbb{Z}_n^2\), and every row represents a subset \(S \subseteq [n]\). Following this notation, from section 1 we get

\[ H_n[S, a] = \overline{\chi_S(a)} = \chi_{S'}(a) \]

3. From definition,

\[ \chi_S(a) = (-1)^{\sum_{i \in S} a_i} \]

Denote

\[ s(S, a) = \sum_{i \in S} a_i \]

\[ s(S, a') = \sum_{i \in S} a'_i \]

\[ s(S', a) = \sum_{i \in S'} a_i \]

\[ s(S', a') = \sum_{i \in S'} a'_i \]

From definitions,

\[ s(S, a') = s(S, a) \quad s(S', a) = s(S, a) + a'_n = s(S, a) \quad s(S', a') = s(S, a) + a'_n = s(S, a) + 1 \]

And therefore,

\[ \chi_S(a') = (-1)^{s(S, a)} = \chi_S(a) \quad \chi_{S'}(a) = (-1)^{s(S, a)} = \chi_S(a) \quad \chi_{S'}(a') = (-1)^{s(S, a) + 1} = -\chi_S(a) \]
4. Let $\{\chi_S\}_{S \subseteq [n-1]}$ be the set of characters of $\mathbb{Z}_2^{n-1}$. We start with the observation that if $a \in \mathbb{Z}_2^n$ has a zero MSB, and if $S \subseteq [n]$ excludes $n$, then

$$\sum_{i \in S} a_i = \sum_{i \in S \setminus \{n\}} a_i \implies \chi_S(a) = \frac{1}{2} \chi'_S(a)$$

We divide the matrix into four quarters: columns corresponding to vectors with 0/1 MSB, and rows corresponding to subsets including/excluding $n$. The equality follows immediately from the observation and sections 2,3.

5. Divide and conquer. In every recursive iteration, we divide the matrix as described in section 4, make two recursive calls: one for the first $N/2$ coefficients, and one for the last $N/2$, then combine the results as follows from the division of the matrix.

**Protocol.**

$\text{HWT}(n, f)$:

(a) If $n = 1$, return

$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f(0) \\ f(1) \end{pmatrix}$$

(b) Otherwise, return

$$\frac{1}{2} \begin{pmatrix} \text{HWT}(n-1, f_0) + \text{HWT}(n-1, f_1) \\ \text{HWT}(n-1, f_0) - \text{HWT}(n-1, f_1) \end{pmatrix}$$

where $f_b(a_{n-1} \ldots a_1) = f(ba_{n-1} \ldots a_1)$ for $b \in \{0, 1\}$.

**Correctness.** Follows from the following equality.

$$H_n \begin{pmatrix} f(00 \ldots 0) \\ \vdots \\ f(11 \ldots 1) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} H_{n-1} \begin{pmatrix} f(00 \ldots 0) \\ \vdots \\ f(01 \ldots 1) \end{pmatrix} + H_{n-1} \begin{pmatrix} f(10 \ldots 0) \\ \vdots \\ f(11 \ldots 1) \end{pmatrix} \\ H_{n-1} \begin{pmatrix} f(00 \ldots 0) \\ \vdots \\ f(01 \ldots 1) \end{pmatrix} - H_{n-1} \begin{pmatrix} f(10 \ldots 0) \\ \vdots \\ f(11 \ldots 1) \end{pmatrix} \end{pmatrix}$$

**Complexity.** The complexity of the algorithm is (analysis similar to FFT)

$$T(N) = O(N) + 2T(N/2) = O(N \log N)$$

6. Use the algorithm from section 5 to tell whether the function is a character of $\mathbb{Z}_2^n$ by checking whether the result vector is a unit vector. If so, output 1, otherwise 0.