Quiz 6

111550057 資工15 莊婷馨

Problem 1

(a) The provided pseudocode is an iterative implementation of Walsh-Hadamard Transform. To implement the recursive process, set a function. In each call of the function, split the length of signal x into half and call on the function again. The base case is reached when length=2, then return Hadamard matrix of the smallest size (in this case, `np.array([[1, 1], [1, -1]])`). Then we can use Kronecker product to construct larger Hadamard matrices. The process stops when Hadamard matrix reaches the wanted size.

Pseudocode of the process:

```
def WHT(x):
    x = np.array(x)
    if (len(x.shape) < 2):  # make sure x is 1D array
        if (len(x) > 3):  # accept x of min length of 4 elements (M=2)
            # check length of signal, adjust to 2**m
            n = len(x)
            M = math.trunc(math.log(n, 2))
            x = x[0:2 ** M]
            H = Hadamard(2 ** M)
            return (np.dot(H, x) / 2. ** M, x, M)

def Hadamard(leng):
    h2 = np.array([[1, 1], [1, -1]])
    if leng == 2:
        return np.kron(h2, h2)
    h = Hadamard(leng // 2)
    return np.kron(h,h2)
```

(b) Applications include

1. Image processing : Includes image denoising, edge detection, texture analysis, etc. It can efficiently capture the spatial frequency content of the image, making it suitable for analyzing textures and patterns. Additionally, the orthogonality property of the WHT ensures that the transformed image can be reconstructed without loss of information.
2. Cryptography : Includes secure key generation, data encryption, digital signatures, secure communication protocols, etc. The advantage of WHT comes from its property of orthogonality, invertibility, and randomness.
3. Data compression : Includes image compression, audio compression, etc. Since the Walsh functions are orthogonal, they can be used to efficiently represent the signal

with fewer coefficients. This property leads to compression with minimal loss of data.

4. Signal processing : Includes speech processing, radar and sonar signal processing, etc.The WHT can efficiently represent signals in terms of their frequency content. It is particularly useful for analyzing signals with discontinuities or non-sinusoidal characteristics.

Problem 2

(a) It is highly likely that pq can be recognized as a composite. However, since the Miller-Rabin Test is a probabilistic algorithm, it is also possible (with low probability) that pq is recognized as "possibly prime."

(b) No, we cannot break RSA with it. We can only know that a number is composite with the Miller-Rabin Test, but we cannot factor the number into its large prime factors. Since breaking RSA requires knowing the factors, it is not possible to break RSA with the Miller-Rabin Test alone.