Quiz 6

110550108 施柏江

Problem 1

a) Please showcase the recursive process of the Walsh-Hadamard Transform using the pseudocode provided above.

Ans:

In this recursive version, the build_Hadamard function recursively constructs the Hadamard matrix of order M by repeatedly applying the Kronecker product with the Hadamard matrix of order 2 (h2).

```
def  WHT(x):
    x = np.array(x)
    if len(x.shape) < 2:
        if len(x) > 3:
            n = len(x)
            M = math.trunc(math.log(n, 2))
            x = x[0:2 ** M]
            h2 = np.array([[1, 1], [1, -1]])

            def  build_Hadamard(M):
                if M == 1:
                    return h2
                else:
                    H_lower = build_Hadamard(M - 1)
                    return np.kron(H_lower, h2)

            H = build_Hadamard(M)
            return (np.dot(H, x) / 2. ** M, x, M)
```

b) Examine different applications of the Walsh-Hadamard Transform, highlighting how its properties offer advantages in each specific application.

Ans:

1. Signal Processing:

The WHT is used in signal compression due to its ability to concentrate signal energy into a few coefficients. Unlike the Discrete Fourier Transform, which tends to spread the energy across all coefficients, the WHT often results in a sparse representation of the signal, making it efficient for compression.

2. Digital Communication:

In digital communication systems, WHT is utilized due to its orthogonality property. Orthogonal codes generated using WHT can be employed for channel multiplexing, allowing multiple signals to be transmitted simultaneously without interference.

3. Image Processing:

WHT can be applied for feature extraction. By transforming image blocks using WHT, certain features or patterns can be enhanced, aiding in tasks like object recognition or image classification.

Problem 2

a) What happens when we apply the Miller-Rabin test to numbers in the format pq, where p and q are large prime numbers?

Ans:

For large primes, the Miller-Rabin test is typically more efficient than traditional primality tests. This is because the time complexity of the Miller-Rabin test is usually logarithmic, whereas traditional primality tests may have higher time complexity. When p and q are large primes, $n = pq$ is also a very large number. According to the design of the Miller-Rabin test, it can usually efficiently and quickly detect composites when n is large. Therefore, even for very large n, the Miller-Rabin test can provide reliable results in determining whether n is composite or possibly prime.

b) Can we break RSA with it?

Ans:

Breaking RSA with the Miller-Rabin test alone is not feasible because RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors. While the Miller-Rabin test can identify composite numbers efficiently, it doesn't provide a method for efficiently factoring large composites. Breaking RSA typically involves factoring the modulus n into its prime factors p and q, which is a separate problem from primality testing. Although the Miller-Rabin test can identify composite numbers efficiently, it does not directly facilitate the factorization of the modulus n.