quiz6

111550076楊子羿

notion link:

quiz6

Problem 1

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

The Walsh-Hadamard Transform is applied to a one-dimensional real-valued signal, effectively decomposing it into a sequence of simpler signals whose combined effects reconstruct the original signal. This is particularly useful in various fields such as signal processing, data compression, and error correction.

1. **Input Validation and Preparation**:
    a. The input `x` is converted into a numpy array to ensure it's in the correct format for operations that follow.
    b. It further checks if the length of `x` is at least 4 elements long (a requirement since we need a minimum length of 2^2 for the transformation process to be meaningful). If it's longer, the length is adjusted to be a power of 2 (2^M), which is crucial for the recursive structure of the transform.
2. **Matrix Construction for Transformation**:
   The Walsh-Hadamard transform starts with a simple matrix h_2=$[[1,1],[1,-1]]$ and iteratively expands it through the Kronecker product. Initially, the transform matrix H is h_2 Kronecker-multiplied by itself, doubling in size. This process repeats, doubling H's size each time, until it matches the required dimensions for the input signal's transformation. This expansion is determined by $M-1$ iterations, where M is the logarithm base 2 of the input length.

3. **Transformation**:

   After constructing the matrix H, the Walsh-Hadamard Transform is applied to the input signal x by calculating the dot product of H and x. The resulting transformed signal is then scaled by dividing by 2^M, where M is the exponent that aligns with the adjusted input signal's length.

4. **Output**:
   The function returns a tuple containing the transformed signal, the adjusted input signal, and the power
   M.

The pseudocode illustrates a recursive approach to implement the Walsh-Hadamard Transform (WHT) by expanding the transformation matrix H using the Kronecker product. While straightforward, this method may not be the most efficient for large signals due to the recursive nature of the matrix construction and the potential for H to become very large.

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

The Walsh-Hadamard Transform (WHT) is a non-sinusoidal, orthogonal transformation technique used in various fields such as signal processing, communications, image processing, and data compression. Its properties, such as simplicity, speed, and the ability to operate with binary (-1, 1) operations, provide distinct advantages in several applications:

1. **Signal Processing and Analysis**

   - **Application**: In signal processing, WHT is used for noise filtering, signal analysis, and feature extraction.
   - **Advantage**: WHT's binary nature allows for efficient implementation in digital systems, making it suitable for real-time signal processing tasks. The transform can efficiently distinguish between signal and noise components, improving signal clarity.

2. **Image Compression and Processing**

- **Application**: WHT is applied in image compression algorithms to reduce the amount of data required to represent an image without significantly degrading its quality. It's also used in edge detection and image enhancement techniques.
- **Advantage**: Due to its fast computation and the ability to concentrate image energy into fewer coefficients, WHT facilitates efficient image compression, resulting in faster transmission and reduced storage space. For image processing, its simplicity allows for quick transformations, essential for real-time applications.

3. **Error Correction Codes**
   - **Application**: In the field of error correction, WHT plays a crucial role in constructing and decoding error-correcting codes, such as Hadamard codes, which are used to improve the reliability of digital communications.
   - **Advantage**: The transform's orthogonal properties ensure that the codes have high error detection and correction capabilities, crucial for maintaining data integrity in noisy communication channels.
4. **Data Encryption and Cryptography**
   - **Application**: WHT is utilized in certain cryptographic algorithms for data encryption, providing security for digital communications.
   - **Advantage**: Its ability to rapidly transform data into a seemingly random sequence makes it valuable for creating cryptographic keys that are difficult to predict, enhancing security.

Conclusion

The Walsh-Hadamard Transform, known for its computational ease, efficiency, and binary operation, serves a wide array of technological applications. It enhances data transmission speed and reliability, bolsters digital security, and optimizes system efficiency, underlining its vast applicability and importance in contemporary technology.

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?

The Miller-Rabin test is a probabilistic algorithm that typically identifies composite numbers like pq (where p and q are primes) as composite. While it's generally reliable, there's a small chance it could falsely identify such a number as prime (a false positive). The likelihood of a false positive reduces with more iterations of the test.

b) Can we break RSA with it?

No, the Miller-Rabin test cannot be used to break RSA encryption. RSA relies on the difficulty of factoring the product of two large prime numbers (the public key), not on finding whether a number is prime or not. The Miller-Rabin test is only used to check the primality of a number, which could be part of the process of generating RSA keys, where one needs to find large prime numbers. However, it does not help in the factorization of a large composite number, which is the problem that needs to be solved to break RSA encryption. The security of RSA is based on the fact that no efficient algorithm is currently known for factoring such large products of primes in a reasonable amount of time, which is a different problem than primality testing.