Results:

The accuracy of a Bloom filter refers to its ability to correctly determine set membership. In the context of Bloom filters, accuracy is typically measured in terms of false positive rate, which is the probability that the Bloom filter incorrectly reports an element as a member of the set when it is not.

Since Bloom filters can produce false positives but not false negatives, their accuracy is inherently probabilistic. The accuracy depends on the size of the filter (number of bits), the number of elements inserted, and the number of hash functions used. A larger filter and more hash functions generally result in a lower false positive rate.

The false positive rate (FPR) can be estimated using the formula:

FPR ≈ (1 - e^(-kn/m))^k

Where:

- k: Number of hash functions
- n: Number of elements inserted
- m: Number of bits in the filter

For example, if you have inserted 1000 elements into a Bloom filter with 10,000 bits and used 5 hash functions, the estimated false positive rate would be approximately:

FPR ≈ (1 - e^(-5*1000/10000))^5 ≈ 0.043

This means that the Bloom filter would produce false positives about 4.3% of the time.

It's important to note that Bloom filters are designed for applications where a low false positive rate is tolerable. The trade-off for their memory efficiency is the probability of false positives. The choice of Bloom filter parameters, such as the number of bits and hash functions, should be based on the acceptable false positive rate for a given use case.

Keep in mind that Bloom filters are not suitable for scenarios where false positives must be strictly avoided (e.g., cryptographic applications). In such cases, alternative data

structures like cryptographic hash tables or cryptographic data structures should be used.