Group Assignment 3.1

Niv Adam, David Kaufmann, Casper Kristiansson, Nicole Wijkman

December 14, 2023

1 E-Level Problem (3.1)

The objective is to create an algorithm that can verify that the sum of n-bit integers from m computers equals an n-bit integer. This means we want to confirm if the sum $\sum_{i=1}^{m} x_i = y$ holds true where x_i is the n-bit number from the i-th computer. The constraint is that the solution with a probability of at least 0.9 is the sum of the integers of the computers with a complexity that requires $O(m \log^{10} n)$ bits of communication.

To achieve the required complexity of $O(m \log^{10} n)$, we employ a fingerprinting technique based on the selection of primes. The algorithm leverages the Prime Number Theorem, which allows us to make probabilistic statements about the equality of fingerprints $h_p(x)$ and $h_p(y)$, where h_p is the fingerprint function associated with a prime p.

The fingerprinting algorithm involves the selection of a prime p.

Based on the Prime Number Theorem we can determine that if $x \neq y$, then the probability of the fingerprint functions $h_p(x)$ and $h_p(y)$ being equal, denoted as $\Pr[h_p(x) = h_p(y)]$, is bounded by $\frac{1}{2}$. This probabilistic property forms the foundation of our algorithm and provides a means to distinguish between different inputs.

$$\Pr[h_p(x) = h_p(y)] \leq \frac{1}{2}$$

We then need to establish a bound for the prime so that we can sample specific primes within a range of [2, M] where M is a value large enough to ensure a low probability of collision. This means that for example by setting $M = K \times n \times ln(n)$, where K ...

Let us look at the L different fingerprints the server received from each computer. For each prime $p \in L$ it holds that

$$((x_1 \mod p) + (x_2 \mod p) + ...) \mod p = (x_1 + x_2 + ...) \mod p$$

Then

$$((x_1 \mod p) + (x_2 \mod p) + ...) \mod p = y \mod p$$

holds if $x_1 + x_2 + ... = y$ holds. In case it does not, we know from the theorem in the lecture that the probability $Pr[((x_1 \mod p) + (x_2 \mod p) + ...) \mod p = (x_1 + x_2 + ...) \mod p] \leq 0.5$.