

ESE532 Project P2 Report

Ritika Gupta, Taylor Nelms, and Nishanth Shyamkumar

November 6, 2019

1 Design Space Axes

1. **Axis:** S , Number of SHA-256 hardware units

Challenge: Improving throughput of hashing step

Opportunity: Send chunks to rotating SHA unit index to allow for parallel execution

Continuum: Anywhere from 1 to however many of our hardware SHA units will fit on the FPGA

Equation for Benefit: $\text{Throughput}(S) = S * \text{singleSHAUnitThroughput}$

2. **Axis:** L , Number of LZW hardware units

Challenge: Improving throughput of LZW step

Opportunity: Send chunks to rotating LZE unit index to allow for parallel execution

Continuum: Anywhere from 1 to however many of our hardware LZW units will fit on the FPGA (BRAM likely limiting factor)

Equation for Benefit: $\text{Throughput}(L) = S * \text{singleLZWUnitThroughput}$

3. **Axis:** Z , Design choice for LZW hash table unit

Challenge: Allow for efficient access of code-table for LZW step while fitting within hardware specifications

Opportunity: Use trees or associative memories (or both) to allow for low cycle count for finding relevant table entry

Continuum: $Z \in \{\text{Tree with Dense RAM, Tree with Fully Associative Memory, Tree with Tree, Tree with Hybrid}\}$

Equation for Benefit: Slide 65 from Day 17 has the relevant tradeoff chart, with implied `implementation_complexity` parameter to consider.

4. **Axis:** H , Number of bits in hash of SHA value for storing SHA values

Challenge: Effectively storing mapping between SHA values of previous chunks and the chunk index

Opportunity: Tune hash table size to reduce conflicts but also remain compact

Continuum: Could be any small number of bits (call it 5 as a low value) through 256 for the full SHA value.

Equation for Benefit:

$$\begin{aligned} \text{numRows } C &= 2^H \\ \text{probCollision} &= \binom{N}{m} \left(\frac{1}{C}\right)^m \left(1 - \frac{1}{C}\right)^{N-m} \end{aligned}$$

5.

6.

7.

8.

9.

10.

11.

12.

2 Teamwork