Homework 15

Arkworks R1CS tutorial part 1

Work through the Merkle Tree tutorial
You will need to clone the repo or setup a codespace.

We will work through this in stages, initially we look at the normal implementation of a merkle tree outside a circuit, then will implement this in a circuit.
At this stage we just need to familiarise ourselves with the code and the process.

Part 1 - API without constraints

Look at the test code in lib.rs
see function `test_merkle_tree()`
Line 40 creates a simple tree.
There are 2 types of hash functions

- CRH is used for a Leaf Hash. - a single hash
- TwoToOneCRH is used to hash pairs

Part 2 - creating a circuit

Look at the implementation and tests in constraints.rs
Before looking at the code implementing the constraints, have a look at the test `merkle_tree_constraints_correctness` starting on line 69, to get an idea of the process.
Note that we also have a test to show the soundness.

We will look at this further in the next lesson.