STARKNET

STARK proofs ELI5

November 12th 2024

@henrlihenrli

Agenda

The agenda

What is proving

Arithmetization: Turning computation into polynomials

Execution trace: Turning execution into polynomials

Applying error correcting code to detect mismatches

Using the result to convince the verifier of integrity

Let’s go

What is proving

Proving is a process in which a **prover** wishes to **executes a computation** and convince a **verifier** that the result is correct and the computation was done correctly, **without the verifier executing the program**.

There are several proof systems and today I'll talk about STARKs.

Arithmetization: From computation to polynomials

Arithmetization is converting a computational problem into an algebraic form by representing program operations and logical steps as polynomials over finite fields

These polynomials capture the behavior of that specific program mathematically

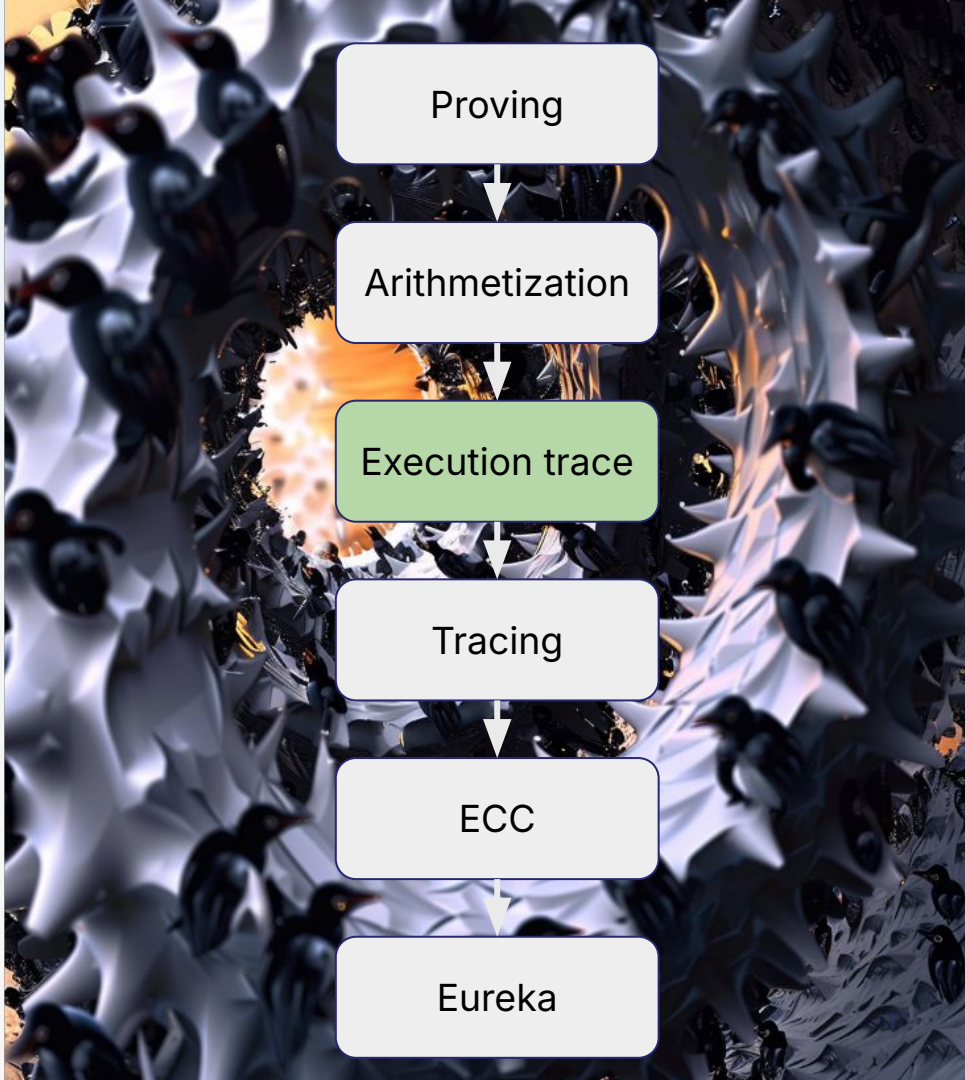
Let’s call it the expected polynomial

What is an execution trace

The execution trace is a sequence of states (or "steps") that the program goes through, from start to finish.

It’s like a log of every CPU instruction executed, register values, memory accesses etc, at each step.

This sequence is also turned into polynomials. Let’s call it the execution polynomials



Execution trace: From execution to polynomial

Any correct run of the expected program will generate an execution trace with points that all fall on the expected polynomial

Who does the prover convince the verifier that all points of the execution trace fall on the expected polynomial, without checking all of them?

Applying error correcting code to detect mismatches

ECC are a set of techniques used in telecommunications to transmit data.

They allow to detect and correct errors.

In STARK proofs, they are used to DETECT errors. They allow checking that the execution polynomials and the expected polynomials are the same

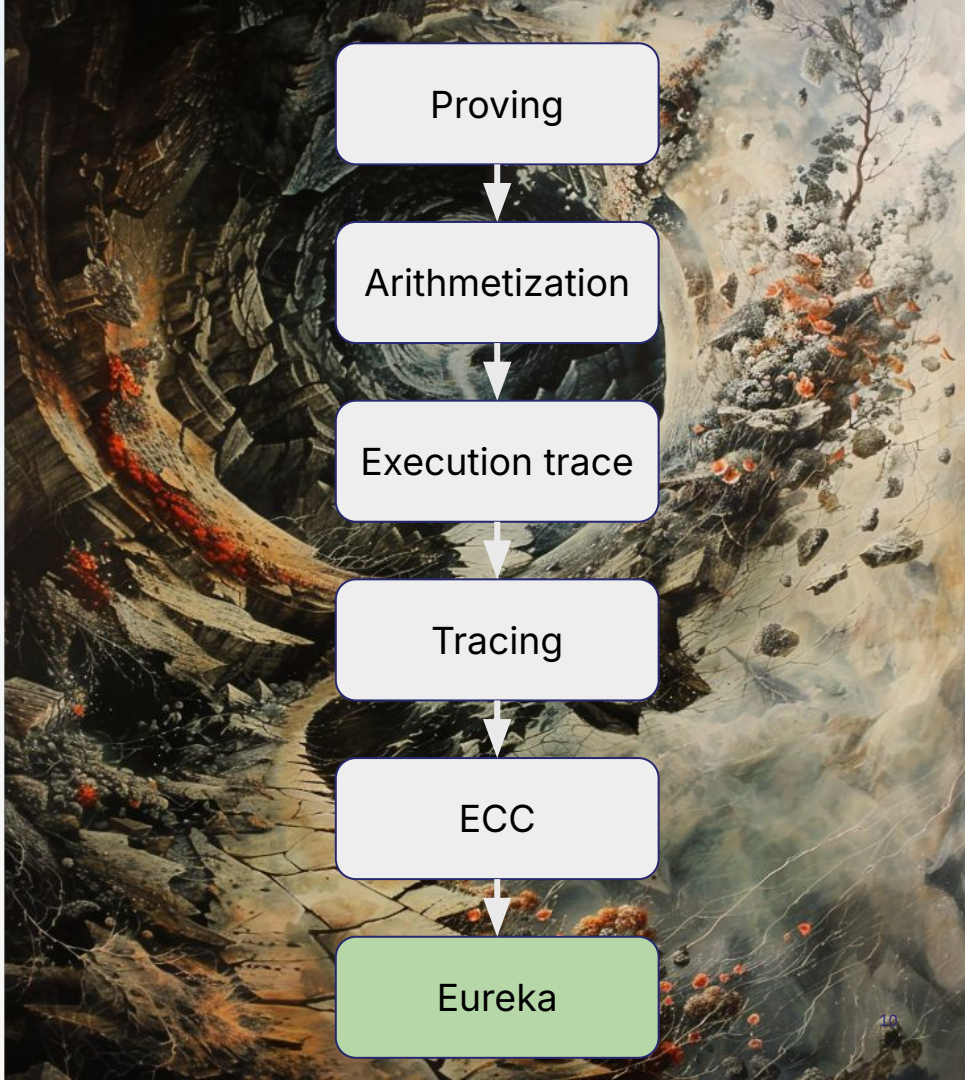
Using the result to convince the verifier of integrity

The verifier doesn’t have to retrieve and analyse the ECC output.

He can sample only a few parts, and check for errors

Any error, anywhere in the execution trace, will appear in most places in the ECC output

After a few samples, the verifier is convinced



STARKNET

The End

The Starknet documentation

All you ever wondered about Starknet

- November 2024

@henrli