1 Introduction

2 Preliminaries

2.1 LoRA

Among the different techniques for parameter-efficient fine-tuning of LLMs, one of the most relevant approaches of the last years has been LoRA (Low-Rank Adaptation of Large Language Models) [1]. The idea behind LoRA is

2.2 Incrementally Verifiable Computation

In a decentralized world, trust is a resource that is hard to achieve. In decentralized computation, we need to make sure the computation are being done, and are being correctly. In a seminal paper by Valiant (2008) [4], it was shown that proofs of knowledge can be used to assert the correct execution of general computations. That is, if M is a machine that runs for t steps producing a sequence of configurations $c_0, c_1, \ldots, c_t$, then there exist an efficient and effective way to produce a computationally sound proof for the computation $c_0 \xrightarrow{t} c_t$. This idea is referred to as Incrementally Verifiable Computation or IVC.

The main goal is IVC is to produce compact, updatable proofs of correctness for a sequence of computations, so that each new step in the computation can be verified on its own while building on the guarantees of the previous steps. This technique significantly reduces the verification overhead for long or evolving computations, which is invaluable in scenarios like decentralized networks, outsourced computation, and any application requiring frequent correctness checks.

Kumar et al. (2021) [3] introduced the proof system NOVA and the idea of recursive proofs, which are proofs that can "prove the correctness of other proofs." Recursive proof composition is key to IVC where each proof attests to the correctness of both a step's output and the validity of the previous step's proof.

HyperNova [2] is a novel recursive argument system optimized for customizable constraint systems (CCS) that generalizes and improves upon prior approaches like Nova. It achieves efficiency through a folding scheme where the prover's cryptographic costs are minimized and achieves zero-knowledge without relying on zkSNARKs.

An IVC system allows the construction of proofs in zero-knowledge where the proofs reveal no information about the underlying computation or its inputs beyond the validity of the claim [4].

3 ZKLoRA

4 Experiments

5 Concluding Remarks

References

[1] Edward J Hu, yelong shen, Phillip Wallis, Zeyuan Allen-Zhu, Yuanzhi Li, Shean Wang, Lu Wang, and Weizhu Chen. LoRA: Low-rank adaptation of large language models. In *International Conference on Learning Representations*, 2022.

[2] Abhiram Kothapalli and Srinath Setty. Hypernova: Recursive arguments for customizable constraint systems. In *Annual International Cryptology Conference*, pages 345–379. Springer, 2024.

[3] Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla. Nova: Recursive zero-knowledge arguments from folding schemes. In *Annual International Cryptology Conference*, pages 359–388. Springer, 2022.

[4] Paul Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. Proceedings 5*, pages 1–18. Springer, 2008.