Research Papers on 'oracle'

Google Scholar

Semantic Scholar

IEEE Xplore

PubMed

Paper 1:

Toward Optimal-Complexity Hash-Based Asynchronous MVBA with Optimal Resilience

Date: 2025-02-28

Time: 15:39:07

Authors:

Jovan Komatovic, Joachim Neu, Tim Roughgarden

Summary:

- Multi-valued validated Byzantine agreement (MVBA), a fundamental primitive of distributed computing, allows n processes to agree on a valid ℓ-bit value, despite t faulty processes behaving maliciously. Among hash-based solutions for the asynchronous setting with adaptive faults, the state-of-the-art HMVBA protocol achieves optimal $O(n^2)$ message complexity, (near-)optimal $O(n\ell+n^2 \lambda\log n)$ bit complexity, and optimal $O(1)$ time complexity. However, it only tolerates up to $t < \frac15 n$ adaptive failures. In contrast, the best known optimally resilient protocol, FIN-MVBA, exchanges $O(n^3)$ messages and $O(n^2\ell + n^3\lambda)$ bits. This highlights a fundamental question: can a hash-based protocol be designed for the asynchronous setting with adaptive faults that simultaneously achieves both optimal complexity and optimal resilience? In this paper, we take a significant step toward answering the question. Namely, we introduce Reducer, an MVBA protocol that retains HMVBA's complexity while improving its resilience to $t<\frac14 n$. Like HMVBA and FIN-MVBA, Reducer relies exclusively on collision-resistant hash functions. A key innovation in Reducer's design is its internal use of strong multi-valued Byzantine agreement (SMBA), a variant of strong consensus we introduce and construct, which ensures agreement on a correct process's proposal. To further advance resilience toward the optimal one-third bound, we then propose Reducer++, an MVBA protocol that tolerates up to $t < (\frac13-\epsilon)n$ adaptive failures, for any fixed constant $\epsilon > 0$. Unlike Reducer, Reducer++ does not rely on SMBA.

Instead, it employs a novel approach involving hash functions modeled as random oracles to ensure termination. Reducer++ maintains constant time complexity, quadratic message complexity, and quasi-quadratic bit complexity, with constants dependent on ϵ.

Click here for more

Paper 2:

SelectLLM: Query-Aware Efficient Selection Algorithm for Large Language Models

Date: 2025-02-28

Time: 13:23:56

Authors:

Kaushal Kumar Maurya, KV Aditya Srivatsa, Ekaterina Kochmar

Summary:

- Large language models (LLMs) have been widely adopted due to their remarkable performance across various applications, driving the accelerated development of a large number of diverse models. However, these individual LLMs show limitations in generalization and performance on complex tasks due to inherent training biases, model size constraints, and the quality or diversity of pre-training datasets. A promising direction is to efficiently harness the diverse capabilities of LLMs to overcome these individual limitations. To address these limitations, we introduce a novel LLM selection algorithm called SelectLLM, which efficiently directs input queries to the most suitable subset of LLMs from a large pool, ensuring that the selected models collectively provide accurate responses. SelectLLM employs a multi-label classifier and policy based on the classifier's predictions and confidence scores in selecting an optimal, query-aware, and lightweight subset of LLMs. Our findings indicate that the proposed model outperforms existing ensemble-based baselines and achieves competitive performance with similarly sized top-performing LLMs while maintaining efficiency. Specifically, it achieves a huge reduction in inference latency on two challenging reasoning benchmarks: 13% on GSM8K and 70% on MMLU, compared to the top-performing baseline. Also, we establish a theoretical upper bound by an Oracle with LLMs and perform an in-depth linguistic analysis to understand the performance gap between the Oracle and SelectLLM.

Click here for more

Paper 3:

Towards Reliable Vector Database Management Systems: A Software Testing Roadmap for 2030

Date: 2025-02-28

Time: 07:56:37

Authors:

Shenao Wang, Yanjie Zhao, Yinglin Xie, Zhao Liu, Xinyi Hou, Quanchen Zou, Haoyu Wang

Summary:

- The rapid growth of Large Language Models (LLMs) and AI-driven applications has propelled Vector Database Management Systems (VDBMSs) into the spotlight as a critical infrastructure component. VDBMS specializes in storing, indexing, and querying dense vector embeddings, enabling advanced LLM capabilities such as retrieval-augmented generation, long-term memory, and caching mechanisms. However, the explosive adoption of VDBMS has outpaced the development of rigorous software testing methodologies tailored for these emerging systems. Unlike traditional databases optimized for structured data, VDBMS face unique testing challenges stemming from the high-dimensional nature of vector data, the fuzzy semantics in vector search, and the need to support dynamic data scaling and hybrid query processing. In this paper, we begin by conducting an empirical study of VDBMS defects and identify key challenges in test input generation, oracle definition, and test evaluation. Drawing from these insights, we propose the first comprehensive research roadmap for developing effective testing methodologies tailored to VDBMS. By addressing these challenges, the software testing community can contribute to the development of more reliable and trustworthy VDBMS, enabling the full potential of LLMs and data-intensive AI applications.

Click here for more

Paper 4:

Grover's search meets Ising models: a quantum algorithm for finding low-energy states

Date: 2025-02-28

Time: 05:28:38

Authors:

Andrey Zhukov, Andrey Lebedev, Walter Pogosov

Summary:

- We propose a methodology for implementing Grover's algorithm in the digital quantum simulation of disordered Ising models. The core

concept revolves around using the evolution operator for the Ising model as the quantum oracle within Grover's search. This operator induces phase shifts for the eigenstates of the Ising Hamiltonian, with the most pronounced shifts occurring for the lowest and highest energy states. Determining these states for a disordered Ising Hamiltonian using classical methods presents an exponentially complex challenge with respect to the number of spins (or qubits) involved. Within our proposed approach, we determine the optimal evolution time by ensuring a phase flip for the target states. This method yields a quadratic speedup compared to classical computation methods and enables the identification of the lowest and highest energy states (or neighboring states) with a high probability $\lesssim 1$.

Click here for more

Paper 5:

Learning and Computation of Φ-Equilibria at the Frontier of Tractability

Date: 2025-02-28

Time: 00:45:49

Authors:

Brian Hu Zhang, Ioannis Anagnostides, Emanuel Tewolde, Ratip Emin Berker, Gabriele Farina, Vincent Conitzer, Tuomas Sandholm

Summary:

- Φ-equilibria -- and the associated notion of Φ-regret -- are a powerful and flexible framework at the heart of online learning and game theory, whereby enriching the set of deviations Φ begets stronger notions of rationality. Recently, Daskalakis, Farina, Fishelson, Pipis, and Schneider (STOC '24) -- abbreviated as DFFPS -- settled the existence of efficient algorithms when Φ contains only linear maps under a general, d-dimensional convex constraint set $\mathcal{X}$. In this paper, we significantly extend their work by resolving the case where Φ is k-dimensional; degree-ℓ polynomials constitute a canonical such example with $k = d^{O(\ell)}$. In particular, positing only oracle access to $\mathcal{X}$, we obtain two main positive results: i) a $\text{poly}(n, d, k, \text{log}(1/\epsilon))$-time algorithm for computing ϵ-approximate Φ-equilibria in n-player multilinear games, and ii) an efficient online algorithm that incurs average Φ-regret at most ϵ using $\text{poly}(d, k)/\epsilon^2$ rounds. We also show nearly matching lower bounds in

the online learning setting, thereby obtaining for the first time a family of deviations that captures the learnability of Φ-regret. From a technical standpoint, we extend the framework of DFFPS from linear maps to the more challenging case of maps with polynomial dimension. At the heart of our approach is a polynomial-time algorithm for computing an expected fixed point of any $\phi : \mathcal{X} \to \mathcal{X}$ based on the ellipsoid against hope (EAH) algorithm of Papadimitriou and Roughgarden (JACM '08). In particular, our algorithm for computing Φ-equilibria is based on executing EAH in a nested fashion -- each step of EAH itself being implemented by invoking a separate call to EAH.

Click here for more

Paper 6:

HELENE: An Open-Source High-Security Privacy-Preserving Blockchain Based System for Automating and Managing Laboratory Health Tests

Date: 2025-02-27

Time: 19:28:29

Authors:

Gabriel Fernández-Blanco, Pedro García-Cereijo, David Lema-Núñez, Diego Ramil-López, Paula Fraga-Lamas, Leire Egia-Mendikute, Asís Palazón, Tiago M. Fernández-Caramés

Summary:

- In the last years, especially since the COVID-19 pandemic, precision medicine platforms emerged as useful tools for supporting new tests like the ones that detect the presence of antibodies and antigens with better sensitivity and specificity than traditional methods. In addition, the pandemic has also influenced the way people interact (decentralization), behave (digital world) and purchase health services (online). Moreover, there is a growing concern in the way health data are managed, especially in terms of privacy. To tackle such issues, this article presents a sustainable direct-to-consumer health-service open-source platform called HELENE that is supported by blockchain and by a novel decentralized oracle that protects patient data privacy. Specifically, HELENE enables health test providers to compete through auctions, allowing patients to bid for their services and to keep the control over their health test results. Moreover, data exchanges among the involved stakeholders can be performed in a trustworthy, transparent and standardized way to ease software

integration and to avoid incompatibilities. After providing a thorough description of the platform, the proposed health platform is assessed in terms of smart contract performance. In addition, the response time of the developed oracle is evaluated and NIST SP 800-22 tests are executed to demonstrate the adequacy of the devised random number generator. Thus, this article shows the capabilities and novel propositions of HELENE for delivering health services providing an open-source platform for future researchers, who can enhance it and adapt it to their needs.

Click here for more