Dec-25

בפקולטה מתקיימים פרוייקטי מחקר רבים ולא כולם מפורטים בדף זה. ניתן ואף מומלץ
לפנות גם לחברי סגל שלא מופיעים כאן ועוסקים בנושאים שמעניינים אתכם:
https://www.cs.technion.ac.il/he/research-areas/

Title	Abstract	Advisor	Contact email
Identifying and Exploiting Symmetries in Formal Verification (Joint project with Apple)	I am looking for a Master's student interested in bridging the gap between theory and practice in formal verification. Our goal is to examine practical use-cases of formal verification, and try to alleviate some of their difficulty in various approaches. Concretely, we aim to prove properties about systems written in Verilog, using SAT solvers, and use those properties to add simplifying assumptions (called "symmetries") to the verification process. The project involves theoretical reasoning, practical implementation, and empirical testing. The project is in some collaboration with the formal verification group at Apple. Recommended background: - Some understanding of formal verification, LTL, etc. - Some understanding of logic, what a SAT solver does, etc.	Dr. Shaull Almagor	shaull@technion.ac.il
Enhancing Protocol Understanding Beyond Traditional Analysis	Protocol reverse engineering (PRE) is vital for understanding undocumented or proprietary communication protocols, with applications in cybersecurity, interoperability, and malware analysis. However, current PRE techniques based on static and dynamic analysis produce incomplete message grammars, reach limited state coverage, and overall achieve low precision. These limitations hinder accurate protocol modeling and increase the effort required for manual validation. Observing recent breakthroughs in LLM research we believe there is a significant opportunity to leverage LLM's comprehension and generation capabilities to enhance PRE In this project, we will investigate how LLMs can improve the precision and scope of PRE. We aim to develop data-driven methods that learn protocol structures and interaction patterns from network traces or binary samples. The project will involve designing LLM-based models to infer message formats and state transitions automatically, then evaluating their performance against traditional PRE approaches. The outcome will be a PRE framework prototype demonstrating the potential of LLM-Infused PRE frameworks.	Dr. Yaniv David	yanivmd@technion.ac.il

מנגנון caching עבור LLM-ים	מערכות LLM מחוללות מהפכה בעולם. מאידך, הן דורשות ביצוע כמויות עצומות של חישובים וצורכות כמויות גדולות של data, מה שמייקר את ההפעלה שלהן מאוד, מבזבז הרבה חשמל, ומגביל את השימוש בהן בסביבות עם משאבי חישוב מוגבלים (כדוגמת edge ו-embedded). מטרת מחקר זה הינה חקר ופיתוח של מנגנוני caching, שיכולים לשמור תוצאות חישוב קודמות, מלאות או חלקיות, ושליפה מהירה שלהן על מנת לחסוך ביצוע מחודש של שאילתות שהתשובה עבורן כבר חושבה בעבר.	Prof. Roy Friedman	roy@technion.ac.il
מקבול של ביצוע חוזים חכמים בבלוקצ'יין	חוזים חכמים עומדים בבסיס מהפכת ה- distributed finance (DeFi) והפוטנציאל לפיתוח אפליקציות מבוזרות כלליות מעל רשתות בלוקצ'יין. הבעיה היא שביצוע חוזים חכמים מהווה כיום צוואר בקבוק מרכזי בביצועיהן שח רשתות בלוקצ'יין. לאור העובדה שמחשבים כיום הן מקביליים, מיקבול הביצוע של אותם חוזים חכמים ניראה כמו כיוון מבטיח על מנת להאיץ את ביצועי המערכת. בפועל, האתגר הוא לשמר נכונות ולוודא שגם בריצות מקביליות של החוזים החכמים, כל ה-miners עדיין מגיעים לאותן תוצאות סופיות.	Prof. Roy Friedman	roy@technion.ac.il
מבני-מידע מבוזרים עם תכונות מתקדמות (concurrent data structures with non-rudimentary properties)	מבני-מידע מבוזרים מהווים את הבסיס למערכות מבוזרות, החל ממעבדים מרובי-ליבות ועד לשרתים מבוזרים. דוגמה אופיינית היא אובייקט מבוזר ל"צילום אטומי" של זיכרון משותף אשר מכיל אוסף של משתנים, כך שניתן לעדכן כל אחד בנפרד ולקרוא את כולם "בבת אחד". זאת, למרות שתהליכים שונים מבצעים פעולות אלה בו-זמנית וללא הפסקה. אובייקט זה מהווה רכיב מרכזי באלגוריתמים רבים לתיאום בין תהליכים, במיוחד במערכות מרובות-מעבדים עם זיכרון משותף, אבל גם (באופן לא ישיר) במערכות מבוזרות גיאוגרפית התומכות בשירותי web. בשנים האחרונות, מנסים להוסיף למבני-מידע מבוזרים תכונות נוספות, כגון אפשרות לעקוב מי משתמש בהם (auditing), והבטחות כמו העלמה של ההיסטוריה (history- independence) או הסתרה של פעולות שלא נצפו במפורש (non-leakage). מטרת המחקר היא לפתח דרכים לממש אובייקטים אלה ולשפר את הסיבוכיות שלהם, או להוכיח שזה בלתי אפשרי. מחקר זה יוביל לרכישה של הבנה עמוקה של תיאום במערכות מרובות-מעבדים. רקע נחוץ: קורסים באלגוריתמים וחישוביות	Prof. Hagit Attiya	hagit@cs.technion.ac.il
רובוטיקה נחילית	תחום הרובוטיקה הוא תחום מרתק ורחב מאד אשר כולל בתוכו כל מערכת מכאנית הפועלת במידת מה של עצמאות בעולם הפיזי, וכן כל מערכת מפוקחת למחצה או אוטונומית הפועלת במרחב הסייבר או בסימולציה של מציאות זו או אחרת. בקרה במערכות רובוטיות הינו תחום במדע ובהנדסה המאפשר שליטה במערכות. בתחום הרובוטיקה הנחילית אנו עוסקים בבקרה מבוזרת של המערכת הנחילית, שהיא מערכת של מערכות רובוטיות אוטונומיות, כאשר לכל מערכת אוטונומית המרכיבה את הנחיל אנו קוראים "סוכן". הבקרה המבוזרת של המערכת הנחילית באה לידי ביטוי בכך שאנחנו מצליחים להגיע למצב מערכתי רצוי של הנחיל באמצעות תכן של מערכת הבקרה של הסוכן הבודד. היתרונות של נחיל על פני מערכת מונוליטית היא שהנחיל מתמודד בצורה טובה עם כשלים של תתי מערכות, וכן בהרבה מקרים המערכת הנחילית מצליחה להתגבר על בעיות יותר גדולות (במובן קנה מידה – Scale) על ידי הגדלת מספר הסוכנים בנחיל בלבד, וכן טבעה המבוזר של המערכת הנחילית מאפשר פיזור של משאבים הדרושים לתפקודה כגון אנרגיה על פני רכיבי המערכת.	Prof. Alfred Bruckstein	freddy@cs.technion.ac.il

Coding Techniques and Algorithms for DNA-based Storage Systems	Our research mission is to advance both the theoretical foundations and practical implementations of DNA-based data storage systems. We draw on a wide range of disciplines, such as coding theory, information theory, algorithms, discrete mathematics, algebra, machine learning, and more, to develop and adapt new theoretical schemes. These ideas are then implemented and tested using tools developed in our lab, including SOLQC and the DNA-Storalator, as well as through hands-on wet-lab experiments in DNA synthesis and sequencing. Our goal is to design novel coding methods and techniques that address the unique structure and error behaviors of DNA as an information channel. Using an analytical framework tailored to the challenges of synthesis, storage, and sequencing, we develop solutions such as clustering codes, trace-reconstruction techniques, error-correction codes, and constrained codes. Together, these approaches enable reliable long-term storage and recovery of digital information encoded in DNA, while overcoming the distinctive challenges that arise throughout the DNA storage pipeline.	Prof. Eitan Yaakobi	yaakobi@cs.technion.ac.il
Utilizing Strong Proof Systems in Automated Reasoning	Proof systems provide formal proofs for the validity of statements under a given set of axioms and are powerful tools for applying logic in automated reasoning. The strength of a proof system is typically measured by the length of the shortest proof it admits for valid statements: stronger proof systems allow shorter proofs. However, there is an inherent trade-off between the strength of a proof system and the feasibility of implementing efficient proof-search algorithms for it. As the strength of the system increases, the search space grows accordingly, often making proof search computationally intractable. Model Checking is an automatic formal verification technique used to establish the correctness of computerized systems. Given a model and a specification, it determines whether the specification holds in the model and, in doing so, effectively constructs a proof. Intuitively, model checking can be viewed as a proof-search algorithm operating within a particular proof system. Our research focuses on developing the theory and algorithms that enable the use of strong proof systems in automated reasoning in general, and in Model Checking in particular.	Dr. Yakir Vizel	yvizel@cs.technion.ac.il

Filament winding over Freeform Surfaces	Nowadays, a common technology for fabricating very strong yet lightweight artifacts is via the exploitation of composite materials. A relatively recent variant of such technology employs filament winging – a multi-axis robot is continuously pasting a continuous strip of a composite fiber (e.g., glass) over the freeform surface of the manufactured artifact. For simple artifacts, like cylinders, a pasting plan for the placement path that covers the entire geometry could be relatively simple to deduce. For general freeform shapes, however, possibly with cavities, this is a much more challenging open geometric question, which would likely entail a global optimization search. See also: • Hang Li, Shinjiro Sueda, John Keyser, “Computation of Filament Winding Paths with Concavities and Friction”, Computer-Aided Design, Volume 141, 2021. • Haisheng Li, Mingkun Li, “Constant Winding Angle Curve on Revolution Surface and its Application”, Computer-Aided Design, Volume 144, 2022.	Prof. Gershon Elber	gershon@cs.technion.ac.il
Geometric Modeling of Mechanical Kinematic Devices via Learning	Algorithms are known for designing a specific motion of a kinematic mechanism, even freeform motion. However, given a desired freeform motion (e.g., the trace of the foot of a human leg, while walking), the creation of a kinematic device to trace the path is quite challenging. Yet, one can synthesize numerous kinematic devices with the aid of geometric modeling tools and study their traces, only to try and learn from them and oUer a good kinematic approximation, given a newly desired trace. See also: • Michael Barton, Nadav Shragai, and Gershon Elber. ``Kinematic Simulation of Planar and Spatial Mechanisms Using a Polynomial Constraints Solver''. CAD09, Reno, Nevada, USA, June 2009. • Yong-Joon Kim, Gershon Elber, and Myung-Soo Kim. ``Precise Continuous Contact Motion for Planar Freeform Geometric Curves.'' The Journal of Graphical Models, Vol 76, pp 580-592, 2014.	Prof. Gershon Elber	gershon@cs.technion.ac.il
Mechanical Lattices of Logical Expressions	While VLSI of microchips is an amazing success, electronic devices have the deficiency that they require power to operate. Mechanical devices that could function as logic gates are already known to a limited extent (see below), with the major advantage that they require no power to function or to store a state. With highly unique abilities of the Technion group to design heterogeneous lattices (see also below), we seek to explore the ability to design arbitrary tangible artifacts, of arbitrary global shape, that could satisfy any given logical expression. • Song, Y., Panas, R.M., Chizari, S. et al. “Additively manufacturable micro-mechanical logic gates.” Nat Commun 10, 882 (2019). • Gershon Elber. “A Review of a B-spline based Volumetric Representation: Design, Analysis and Fabrication of Porous and/or Heterogeneous Geometries.” Computer Aided Design, Vol 163, 2023, 103587.	Prof. Gershon Elber	gershon@cs.technion.ac.il

Trade-Offs Between Fast and Slow Paths in Distributed Algorithms	In this project we aim to bridge the gap between theory and practice in distributed algorithms. In particular, we will examine the likelihood of various executions in a distributed system, and study trade-offs in the performance and robustness of algorithms in good executions vs challenging executions (those with failures and slowdowns). Our focus will be on distributed consensus and transactional systems. This project will involve theoretical reasoning, algorithm design, and possibly also an implementation and experimental evaluation portion, depending on the directions explored and the student's interests and strengths. Recommended background: - Strong grasp of theoretical reasoning and algorithm analysis - Some familiarity with distributed systems and consensus algorithms	Dr. Naama Ben-David	bendavidn@technion.ac.il
Error-Correcting Codes for Reliable Computation	Error correcting codes is widely used in communication and storage. However, it can also be used for enhancing the reliability and efficiency of *computation*. While this had already been suggested 70 years ago by Moore, Shannon, and von Neumann, it is only fairly recently that the topic has gained a revived attention. One motivation for the renewed interest is the need to improve reliability of nanoscale hardware accelerators that perform certain computational tasks, such as analog vector--matrix multipliers. This research aims at proposing and analyzing coding techniques that can be utilized in such applications. Prerequisite: 02360309 Introduction to Coding Theory (מבוא לתורת הצפינה)	Prof. Ronny Roth	ronny@cs.technion.ac.il

Stochastic online algorithms	I'm looking for Master's students interested in online decision-making under uncertainty. In these problems, algorithms must make irrevocable decisions based on information revealed so far, without knowing the future, but sometimes with statistical predictions about it, for example learned from prior data. One (ambitious) objective is to obtain good approximation guarantees compared to an algorithm with perfect knowledge of the future. Another goal is to approximate efficiently the best (computationally unbounded) online algorithm for such problems. Such questions are motivated by applications such as ride-hailing, online advertising, and labor-market platforms, and connect to game theory and mechanism design, which we may also explore. Background (the more the merrier, but not all required): You do not need all of the following. A good match is usually someone with strong proof-based foundations, curiosity, and creativity. •Algorithms seminar 236813 ("prophets, secretaries and philosophers") (taking it concurrently is fine) •Background in advanced (especially randomized) algorithms •Comfort with at least one of: probability, linear programming/duality, combinatorial structures (e.g., matroids) •Enjoy tackling open-ended problems / mathematical puzzles	Dr. David Wajc	wajc@technion.ac.il
Dynamic graph algorithms	I'm looking for Master's students interested in dynamic graph algorithms, where the input graph changes over time (via edge/vertex insertions and deletions) and we want to maintain answers to graph problems much faster than recomputing from scratch. Typical questions include maintaining (perhaps approximate) shortest paths, matchings, cuts/flows, connectivity, and more under updates. These problems are motivated by real-world networks that evolve continuously (transportation networks, communication networks, social graphs etc), and have theoretical motivation (beyond the basic question of understanding computation under changing inputs) in the context of speeding up static algorithms, similarly to how basic data structures speed up classic algorithms. Background (the more the merrier, but not all required): You do not need all of the following. A good match is usually someone with strong proof-based foundations, curiosity, and creativity. •Advanced Dynamic Graph Algorithms course (236011) (taking it concurrently is fine) •Background in advanced (especially randomized) algorithms •Comfort with probability theory and graph theory •Competitive programming experience •Enjoy tackling open-ended problems / mathematical puzzles	Dr. David Wajc	wajc@technion.ac.il