Research Statment

Alex Sanchez-Stern

Software has become more and more pervasive in our world in recent decades, but building high-quality software quickly is still a major challenge. Advances in example-based program synthesis and large language models for code have enabled more and more programmers to automate parts of their development process. These advances have already started to impact industrial practices; in 2018, Meta started using automatically generated program patches in their development [9], and recently Google has been using ML-based code-generation models in the workflow of more than ten thousand developers [19]. However, the results of such tools still need programmer analysis and review, due to their error rate and the fundamental ambiguities of example- and natural language-based specifications. Github's Copilot, one of the most powerful and popular of these modern tools, acknowledges this, saying "the code [Copilot] suggests may not always work, or even make sense... code suggested by GitHub Copilot should be carefully tested, reviewed, and vetted, like any other code" [1].

More worrisome than obviously wrong code which "doesn't make sense" is code which appears to be correct, and even might pass some tests, but fails in unexpected ways during deployment. In fact, in security settings Copilot-generated code has been shown to have vulnerabilities 40% of the time [12]. Thus, as these tools become more and more powerful, the burden of writing software becomes more and more focused on the review and analysis of software.

Formal verification of software promises to reduce the burden of human review and increase program reliability, by connecting programs to formal specifications through machine-checkable proof. This, in theory, would allow the programmer to review only the specification and not the implementation of already-written verified code. Formal verification is used by Firefox and Chrome to produce high-reliability cryptography code [20, 3], and by the Airbus airplane manufacturer for compiling airplane control software [18]. However, the labor-intensive nature of foundational verification today prevents it from being viable for the vast majority of software projects. Since analyzing code for correctness can be quite labor-intensive, how do we combine the benefits of machine-learned code synthesis, namely allowing code to be written more easily, with wide-scale code correctness and reliability?

Enter machine-learned *proof* synthesis. While machine-learned *code* synthesis can try to produce code which is likely correct, machine-learned *proof* synthesis can produce proofs which are **machine-checkable**. That means that the proofs of correctness that are produced can be independently checked by a small proof-checker kernel in well studied proof theories, such as Coq [4] or Isabelle/HOL [11]. When proof synthesis succeeds, this amounts to automatically and foundationally checking the correctness of the target code. And, unlike in machine-learned code synthesis, if the system fails to find a correct proof, the proof checker will always reject the proof, *never* producing false confidence in an incorrect result.

To bring machine-learned proof synthesis to the scale of tools like Copilot, we need three things: highly-effective proof search systems, techniques for specifying the many parts of a software system, and embeddings of common languages into a unified proof system.

Proof Search Systems Proof search systems are software systems that take a logical statement to be proven, and try to produce a proof of that statement. These logical statements can be statements about programs, such as "the sort function always returns a sorted permutation of its input", by using a mathematical model of program code. In simple mathematical domains, such as linear integer arithmetic, proof search can be done deterministically, with procedures that guarantee success for any true statement within the domain. In general though, proof search systems need to heuristically search an infinite space of possible proofs to find a proof which correctly proves the target theorem.

Proof search systems using machine learning have been explored by many in recent years, including teams at Google [2, 10], UMass Amherst [6, 5], University of Innsbruck [7], OpenAI [8], and others. The current state of the art in proof synthesis, in terms of number of proof scripts correctly synthesized, is my dissertation work Proverbot9001, originally published at MAPL 2020 [15]. Proverbot9001 works by using a novel neural architecture to model proof contexts and proof scripts in the Coq proof assistant, one of the oldest and most commonly used proof languages for verifying software. The proof scripts generated control

smaller, lower-level proof search procedures called "tactics" which manipulate the machine-checkable proof terms.

There's still much to do in order to bring these proof search systems to the threshold of wide applicability though, and here my collaborations have yielded many advantages. In my postdoc at UMass Amherst I've been working with Emily First and Yuriy Brun to understand and integrate tree structured models for understanding proof contexts, and proof-history sequence models for accurately predicting next steps. This work has already yielded Passport [16] (currently under submission to TOPLAS), a new way to model identifiers in proof terms to improve proof search. And I've been collaborating with Talia Ringer at UIUC, bringing in her deep knowledge of proof semantics and sound transformations. With REPLICA [14], we conducted the first user-study of proof engineers, in order to understand what kinds of changes they make to proofs during development, and where their time is spent.

I plan to continue improving proof search strategies, models for evaluating proof states, and models for predicting proof steps over the cominb years. While proof-search systems today can synthesize proofs for about a third of theorem statements in large software projects, I expect these improvements to lead to proof search systems which can synthesize upwards of ninety percent of proofs for software projects.

Specifying Components In contrast to proof search systems, less work has been done on easing the burden of creating *formal specifications* for the many parts of a software system. While proofs of a particular theorem or specification can be automatically checked for correctness, mistakes in the specification itself are much harder to discover. Indeed, as proof search systems get better, writing precise, modular specifications may become the hardest part of verifying large software systems.

Fortunately, there is one way to check the correctness of specifications for the majority of software components: correct component specifications are those that allow proving correctness theorems of the software taken as a whole. From this perspective, the challenge becomes taking a top-level correctness theorem for a piece of software, and decomposing it into specifications for various components.

As a first step towards this problem, with some coauthors at UCLA and UCSD I've developed LFind, a data-driven lemma synthesis tool published at OOPSLA 2022 [17]. LFind takes a theorem and a partial proof, and uses the proof state to search for a helper lemma which will allow the proof to progress. It does so with a mix of term generalization and data-driven program synthesis, then uses QuickChick and Proverbot9001 to check that the lemma holds, and to rank lemmas which can lead to more automated proving higher.

While LFind can help produce helper lemmas in conjunction with a human prover, I expect this technology to combine with proof search tools in the coming years to produce tools which can specify parts of software systems with little to no human input. These tools will eventually even define their own data structures and propositions to assist with proving correctness.

Embedding Languages Finally, to bring the benefits of machine-learned proof synthesis to the code that makes up the majority of codebases, we need to be able to reason about code written in popular languages. Most verified software that exists today is written in specialized languages like Coq or Dafny that exist to be verifiable using particular tools. But moving all software development to these languages is not viable. Instead, we need to meet developers where they are by building tools which allow programs in popular languages, like Python, Javascript, or Rust, to be verified.

This presents unique challenges for the different features of each language, like duck-typing, reflection, and ownership types. Each of these features must be carefully modeled to avoid marking incorrect programs as correct, or visa-versa. However, this work can be done incrementally: first, by modeling a useful subset of a language, and checking the correctness of code that only uses that subset, and then gradually expanding the allowed features to maximize the amount of verifiable code. My own work has involved creating verifyable domain specific languages in the past [13]; in the future these techniques can be expanded to create verifiable models of these common languages.

Conclusion With highly-effective proof search, techniques for specifying software at scale, and embeddings of common languages into a unified proof system, I plan to make software correctness scale as fast as software implementation.

First, developers will write down an overall specification of a software system, much like requirement engineers do today. Then, they will write a natural language or example-based description of some software component they wish to implement. From there, software will attempt to automate the rest of the development process.

Tools like Github's Copilot will use the user-provided description to generate candidate implementations, and the code of these implementations will be embedded into a unified proof system. Then a specification of the target component will be derived from the specification of the overall software system, and a proof that the candidate implementations match that specification will be searched for using proof search systems. This search will reject incorrect implementations until a correct implementation is found, and presented to the user. For code which is too difficult to automatically write, the system can safely return to the user without a solution, preventing any falsely-correct implementations.

With this new workflow, developers will be able to focus on the high-level and complex aspects of programming, drastically increasing programmer productivity.

References

[1] Github copilot - your ai pair programmer.

[2] Kshitij Bansal, Sarah M. Loos, Markus N. Rabe, Christian Szegedy, and Stewart Wilcox. Holist: An environment for machine learning of higher-order theorem proving (extended version). *CoRR*, abs/1904.03241, 2019.

[3] Andres Erbsen, Jade Philipoom, Jason Gross, Robert Sloan, and Adam Chlipala. Simple high-level code for cryptographic arithmetic — with proofs, without compromises. In *IEEE Symposium on Security and Privacy (S&P)*, pages 1202–1219, 2019.

[4] Jean-Christophe Filliâtre, Hugo Herbelin, Bruno Barras, Bruno Barras, Samuel Boutin, Eduardo Giménez, Samuel Boutin, Gérard Huet, César Muñoz, Cristina Cornes, Cristina Cornes, Judicaël Courant, Judicael Courant, Chetan Murthy, Chetan Murthy, Catherine Parent, Catherine Parent, Christine Paulin-mohring, Christine Paulin-mohring, Amokrane Saibi, Amokrane Saibi, Benjamin Werner, and Benjamin Werner. The coq proof assistant - reference manual version 6.1. Technical report, 1997.

[5] Emily First and Yuriy Brun. Diversity-driven automated formal verification. In *Proceedings of the 44th International Conference on Software Engineering (ICSE)*, Pittsburgh, PA, USA, May 2022.

[6] Emily First, Yuriy Brun, and Arjun Guha. Tactok: Semantics-aware proof synthesis. *Proc. ACM Program. Lang.*, 4(OOPSLA), November 2020.

[7] Thibault Gauthier, Cezary Kaliszyk, and Josef Urban. Tactictoe: Learning to reason with hol4 tactics. In Thomas Eiter and David Sands, editors, *LPAR-21. 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, volume 46 of *EPiC Series in Computing*, pages 125–143. EasyChair, 2017.

[8] Daniel Huang, Prafulla Dhariwal, Dawn Song, and Ilya Sutskever. Gamepad: A learning environment for theorem proving. *CoRR*, abs/1806.00608, 2018.

[9] Yue Jia, Ke Mao, and Mark Harman. Finding and fixing software bugs automatically with sapfix and sapienz, Sep 2018.

[10] Aditya Paliwal, Sarah M. Loos, Markus N. Rabe, Kshitij Bansal, and Christian Szegedy. Graph representations for higher-order logic and theorem proving. *CoRR*, abs/1905.10006, 2019.

[11] Lawrence C. Paulson. Natural deduction as higher-order resolution. *CoRR*, cs.LO/9301104, 1993.

[12] Hammond Pearce, Baleegh Ahmad, Benjamin Tan, Brendan Dolan-Gavitt, and Ramesh Karri. An empirical cybersecurity evaluation of github copilot's code contributions. *CoRR*, abs/2108.09293, 2021.

[13] John Renner, Alex Sanchez-Stern, Fraser Brown, Sorin Lerner, and Deian Stefan. Scooter & sidecar: A domain-specific approach to writing secure migrations. In *Programming Languages Design and Implementation*. ACM SIGPLAN, June 2021.

[14] Talia Ringer, Alex Sanchez-Stern, Dan Grossman, and Sorin Lerner. Replica: Repl instrumentation for coq analysis. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2020, New York, NY, USA, 2020. Association for Computing Machinery.

[15] Alex Sanchez-Stern, Yousef Alhessi, Lawrence Saul, and Sorin Lerner. Generating correctness proofs with neural networks. In *Machine Learning in Programming Languages*. ACM SIGPLAN, June 2020.

[16] Alex Sanchez-Stern, Emily First, Timothy Zhou, Zhanna Kaufman, Yuriy Brun, and Talia Ringer. Passport: Improving automated formal verification using identifiers, 2022.

[17] Aishwarya Sivaraman, Alex Sanchez-Stern, Bretton Chen, Sorin Lerner, and Todd Millstein. Data-driven lemma synthesis for interactive proofs. *Proc. ACM Program. Lang.*, 6(OOPSLA2), oct 2022.

[18] Jean Souyris. Industrial use of compcert on a safety-critical software product, 2014.

[19] Maxim Tabachnyk and Stoyan Nikolov. Finding and fixing software bugs automatically with sapfix and sapienz, July 2022.

[20] Jean Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, and Benjamin Beurdouche. Hacl*: A verified modern cryptographic library. Cryptology ePrint Archive, Paper 2017/536, 2017. `https://eprint.iacr.org/2017/536`.