Xin Zhang — Achievement 1

My thesis research proposed a user-centric approach to program analysis, a new paradigm that adapts a given analysis to different needs of individual usage scenarios and thereby improves its soundness, accuracy, and scalability. Existing program analysis tools rely on an expert designer to carefully choose a design that they deem suitable for all possible usage scenarios. However, such a uniform design often fails to meet the needs of individual scenarios, and thereby greatly hinders the effectiveness of the analysis. I addressed this challenge in multiple research papers by adapting a given analysis to different targets in a usage scenario, which I outline below:

1. In the paper "On Abstraction Refinement for Program Analyses in Datalog", which won a Distinguished Paper Award at PLDI'14, we proposed an approach that improves the accuracy and scalability of a given analysis by adapting it to individual assertions of interest in a program. This approach enables pointer analysis, a foundational analysis for analyzing any program using pointers, to resolve twice as many assertions as existing approaches and consume significantly less time on large programs of the order of hundreds of thousands of lines of code.

2. In the paper "Hybrid Top-down and Bottom-up Interprocedural Analysis", which was also published at PLDI'14, we proposed an approach to improve the scalability of an analysis by adapting it to patterns of procedure reuse in a program. This approach yields speedups upto 60× over conventional approaches on large Java programs for a type-state analysis, an analysis that is widely used to the check library API usages.

3. Finally, in the paper "A User-Guided Approach to Program Analysis", which won a Distinguished Paper Award at FSE'15, we proposed an approach that reduces the number of false alarms by adapting a given analysis to user feedback. This approach is able to suppress 70% of the false alarms by incorporating user feedback on 5% of the bug reports for a pointer analysis and a datarace analysis, a foundational analysis for analyzing concurrent programs.