

Expanding Specification Capabilities of a Gradual Verifier with Pure Functions

DORUK ALP MUTLU, Michigan State University, USA

Gradual verification soundly combines static checking and dynamic checking to provide an incremental approach for software verification. With gradual verification, programs can be partially specified first, and then the full specification of a program can be achieved in incremental steps. The first and only practicable gradual verifier based on symbolic execution, Gradual C0, supports recursive heap data structures. Despite recent efforts to improve the expressivity of Gradual C0's specification language, Gradual C0's specification language is still limited in its capabilities for complex expressions. This work explores an extension to Gradual C0's design with a common construct supported by many static verification tools, pure functions, which both extend the specification capabilities of Gradual C0 and increase the ease of encoding observer methods in Gradual C0. Our approach addresses the technical challenges related to the axiomatisation of pure functions with imprecise specifications.

1 Introduction

Static verification requires complete specifications to ensure that a program adheres to its specifications. Even though static verification can guarantee the correctness of a program given the specifications, this process burdens users by requiring detailed specifications. On the other hand, dynamic verification supports partial specifications of program properties through run-time checks. However, this comes at a significant cost of run-time overheads, and dynamic verification is limited to verifying a program during run-time. Combining these two techniques, gradual verification, first introduced by Bader et al.[2, 7], offers a smooth transition between static verification and dynamic verification. Gradual verification relies on imprecise specifications (conjoining precise formulas with $?$) to make this transition possible. In the presence of imprecise specifications, run-time checks are inserted in the original program where static information is not sufficient for static verification.

The current practicable implementation of a gradual verifier, Gradual C0[3], is based on symbolic execution and built on top of the Viper verification infrastructure[5]. Differing from various front-end modules such as VerCors[1], which rely on the Viper verification infrastructure, Viper's symbolic execution engine and intermediate language are modified to handle the imprecision introduced by imprecise specifications in gradual verification. Both Viper and by consequence Gradual C0 support the implicit dynamic frames logic for reasoning about heap manipulating programs, and recursive abstract predicates to reason about recursive heap data structures.

One of the current limitations of Gradual C0 is the expressivity of its specification language. Recent work by Gupta [4] introduced and implemented the design of unfolding expressions in the gradual setting for Gradual C0, which supports more intuitive specifications for recursive heap data structures. Pure functions, which are side-effect free constructs, enable intuitive specifications for recursive heap data structures as well. Pure functions enable this by making it possible to encode side-effect free observer methods and expressing refinements of existing predicates[5]. Also, pure functions often use unfolding expressions as well. A common example is unfolding a predicate in the function body to make the permissions required in the recursive function call available. One important detail here is that both the unfolding expressions and pure functions are side-effect free, meaning both can be used in specifications in various forms. By extending the design of gradual verification with pure functions, users can write specifications for recursive heap data structures more easily.

```

1  int pureFactorial(int n)
2    //@ pure;
3    //@ requires n >= 0;
4  {
5    return n == 0 ? 1 : n * pureFactorial(n-1);
6  }
7
8  int iterativeFactorial(int n)
9    //@ requires n >= 0;
10   //@ ensures \result == pureFactorial(n);
11  {
12    int result = 1;
13    int i = 1;
14
15    while (i <= n)
16      //@ loop_invariant 1 <= i && i <= n + 1;
17      /*@ loop_invariant result ==
18         pureFactorial(i - 1); @*/
19    {
20      result = result * i;
21      i = i + 1;
22    }
23
24    return result;
25  }

```

Fig. 1. Verifying an iterative factorial method in Gradual C0 using a pure function

consume, and exec. Eval is used for evaluating expressions and exec is used for executing statements. Producing a formula adds permissions, and constraints, while consuming a formula asserts constraints and removes permissions. As Gradual C0 extends the Viper verification infrastructure, pure functions in Gradual C0 are designed similarly to the pure functions in Viper. To better understand how our approach builds on the theory of verification of functions in Viper, we first explore how functions are verified in Viper.

In Viper, before verification of any construct, functions have their body and postcondition checked with respect to the permissions and constraints provided in the precondition. This stage is also known as the stage for checking the well-definedness of functions. In this stage, axioms related to the functions are generated and emitted to the underlying SMT solver; this process is called axiomatisation. When the function calls need to be evaluated later, the axioms from the SMT solver are used. This prevents re-evaluation of functions in each function call. Emitted axioms reason about the values of heap locations through function snapshots, which are binary tree representations of the current values on the heap needed by the functions. During the evaluation of the function calls, function snapshots are computed during the consumption of function preconditions and passed to the symbolic function application[6].

The design of pure functions for Gradual C0 modifies both the axiomatisation algorithm and the eval rule for functions in Viper. The main challenge with the verification of pure functions in Gradual C0 arises from allowing pure function specifications to be imprecise. In the well-definedness stage of function verification, the function precondition is produced, during which the initial function snapshot is created. The mappings between the snapshot components and heap locations are recorded. During the evaluation of the function body and postcondition, heap accesses are related to the components of the function snapshot using the previously found mappings. However, the function precondition can be imprecise, which causes the function snapshot to be incomplete. An

An important motivation to support pure functions in Gradual C0 is to enable the specification of methods which are not possible to specify with the current constructs in Gradual C0. This is common with iterative methods, such as computing Fibonacci numbers or summations over a range. As given in Figure 1, we focus on the example of factorial computation. First, a recursive pure function (denoted with the pure tag) is given, which computes the factorial of a non-negative integer n . Then, an iterative method with the same goal is given. In this case, the given pure function enables the verification of the method. One critical detail here is that methods, which are impure, cannot be used in specifications, but pure functions can be used in specifications through function calls.

2 Approach

The symbolic execution engine for Gradual C0, called Gradual Viper, relies on the four major functions of Viper modified for gradual verification. The four functions are eval, produce,

incomplete function snapshot would result in a failure of the axiomatisation process. As a solution, when a precondition is imprecise and a heap access from the precondition, body, or postcondition of a function cannot be mapped to a component of the function snapshot, we attempt to extend the function precondition and the function snapshot with the missing permissions. This is done with respect to the branch conditions. If the function snapshot extension attempt results in failure, the user is informed of the reason. The major known reason is discussed later. For the later evaluations of the function in the function calls, we require the permissions related to the extended component of the function snapshot to be consumed in addition to the initial function precondition.

To illustrate how the previously defined axiomatisation strategy for Gradual C0 works, we now consider the example in Figure 2, which is a modified version of an example from the foundational work on function axiomatisation in Viper[6]. In the original example, $\text{acc}(x \rightarrow \text{val})$ is provided instead of $?$. During well-definedness check for this pure function in Gradual C0, when the body of the pure function is evaluated, the heap access $x \rightarrow \text{val}$ fails to find the corresponding snapshot. However, as the precondition is imprecise, we can optimistically assume the permission for $x \rightarrow \text{val}$ is provided in the precondition. Then, we can transform (assume) the third line of the pure function's precondition is $b ? \text{acc}(x \rightarrow \text{val}) \ \&\& \ z == x : z == y$ which is semantically equivalent to the full specification. The function snapshot is extended, and the accessibility predicate $\text{acc}(x \rightarrow \text{val})$ needs to be consumed during the eval of any function application.

The approach described above has shortcomings with imprecise recursive predicates. Attempting to make optimistic assumptions about the accessibility predicates used in imprecise recursive predicates would require a permanent change in the shape of the predicate snapshots. This case can be understood as follows: the client method folds the predicate P , but the function snapshot required by the pure function may have a different shape for predicate P rather than the shape of predicate P folded by the client method. This situation occurs because of the optimistic assumptions. Therefore, imprecise recursive predicates cannot be used with the pure functions in Gradual C0. Functions with such preconditions are rejected by equi-recursively checking the preconditions. Postconditions do not need to be checked, as the postconditions must be framed by the preconditions.

Another important part of our design for pure functions in Gradual C0 is evaluating the function calls. The rule used for eval (Figure 5, in Appendix) is modified to collect the run-time checks generated by consuming the function precondition. Also, $\text{is} - \text{imp}$ used in the rule checks if the pure function postcondition is imprecise. If the function postcondition is imprecise, we make the state imprecise. This exception is needed as the function postconditions are used in generated axioms, and imprecision is handled in symbolic execution at a level higher than the interactions with the SMT solver.

3 Conclusion

Extending Gradual C0 with the pure functions allows the development of more straightforward specifications. This extension involves introducing a new strategy for axiomatising pure functions in a gradual setting as well as modifying the existing formal rule for functions in Viper for Gradual C0. Future work will explore implementing the gradual parts of this approach in Gradual C0 and soundness proof for pure functions based on the formalization introduced by Zimmerman et al. [8].

```

1 struct Node { int val; };
2 typedef struct Node Node;
3 int double(bool b, Node* x, Node* y, Node* z)
4     //@ pure;
5     //@ requires ? && acc(y->val);
6     //@ requires b ? z == x : z == y;
7 {
8     return b ? x->val + z->val : y->val + z->val;
9 }

```

Fig. 2. Pure function example in Gradual C0 with imprecise specifications

References

- [1] Afshin Amighi, Stefan Blom, and Marieke Huisman. 2016. VerCors: A Layered Approach to Practical Verification of Concurrent Software . In *2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*. IEEE Computer Society, Los Alamitos, CA, USA, 495–503. doi:10.1109/PDP.2016.107
- [2] Johannes Bader, Jonathan Aldrich, and Éric Tanter. 2018. Gradual Program Verification. In *International Conference on Verification, Model Checking, and Abstract Interpretation*. Springer, 25–46.
- [3] Jenna DiVincenzo, Ian McCormack, Conrad Zimmerman, Hemant Gouni, Jacob Gorenburg, Jan-Paul Ramos-Dávila, Mona Zhang, Joshua Sunshine, Éric Tanter, and Jonathan Aldrich. 2025. Gradual C0: Symbolic Execution for Gradual Verification. *ACM Trans. Program. Lang. Syst.* 46, 4, Article 14 (Jan. 2025), 57 pages. doi:10.1145/3704808
- [4] Priyam Gupta. 2025. Increasing the Expressiveness of a Gradual Verifier. arXiv:2507.13533 [cs.PL] <https://arxiv.org/abs/2507.13533>
- [5] P. Müller, M. Schwerhoff, and A. J. Summers. 2016. Viper: A Verification Infrastructure for Permission-Based Reasoning. In *Verification, Model Checking, and Abstract Interpretation (VMCAI) (LNCS, Vol. 9583)*, B. Jobstmann and K. R. M. Leino (Eds.). Springer-Verlag, 41–62.
- [6] Malte H Schwerhoff. 2016. *Advancing automated, permission-based program verification using symbolic execution*. Ph. D. Dissertation. ETH Zurich.
- [7] Jenna Wise, Johannes Bader, Cameron Wong, Jonathan Aldrich, Éric Tanter, and Joshua Sunshine. 2020. Gradual verification of recursive heap data structures. *Proc. ACM Program. Lang.* 4, OOPSLA, Article 228 (Nov. 2020), 28 pages. doi:10.1145/3428296
- [8] Conrad Zimmerman, Jenna DiVincenzo, and Jonathan Aldrich. 2024. Sound Gradual Verification with Symbolic Execution. *Proc. ACM Program. Lang.* 8, POPL, Article 85 (Jan. 2024), 30 pages. doi:10.1145/3632927

A Appendix

$\text{verify}(\text{decl}) : MDECL \cup PDECL \longrightarrow RESULT$

$\text{verify}(\text{function } \text{fun}(\overline{x:T}) : T_r) =$

$\text{well-formed}(\sigma_0\{\gamma := \sigma_0.\gamma[\overline{x \mapsto \text{fresh}}]\}, \text{func}_{pre}, \text{fresh}, (\lambda \sigma_1 .$
 $\text{well-formed-e}(\sigma_1\{\gamma := \sigma_1.\gamma[\overline{\text{result} \mapsto \text{fresh}}]\}, \text{func}_{post},$
 $(\lambda _ . \text{success()}))$
 \wedge
 $\text{eval}(\sigma_1, \text{func}_{body}, (\lambda \sigma_2, \text{body}.$
 $\text{consume}(\sigma_2\{\gamma := \sigma_2.\gamma[\overline{\text{result} \mapsto \text{fresh}}]\}, \text{func}_{post}, (\lambda \sigma_3, _ .$
 $; \text{success()}))))))$

■ Handles imprecision

Fig. 3. Rule defining a valid pure function in a Gradual Viper program

$\text{well-formed}(\sigma, \tilde{\phi}, \delta, Q) : \Sigma \longrightarrow \widetilde{FORMULA} \longrightarrow SNAPSHOT \longrightarrow (\Sigma \longrightarrow RESULT) \longrightarrow RESULT$

$\text{well-formed-e}(\sigma, \tilde{\phi}, Q) : \Sigma \longrightarrow FORMULA \longrightarrow (\Sigma \longrightarrow RESULT) \longrightarrow RESULT$

$\text{well-formed}(\sigma_1, \tilde{\phi}, \delta, Q) = \text{produce}(\sigma_1, \tilde{\phi}, \delta, (\lambda \sigma_2 .$
 $\text{produce}(\sigma_1\{\pi := \sigma_2.\pi\}, \tilde{\phi}, \delta, Q))$
 $\text{well-formed-e}(\sigma_1, \phi, Q) = \text{eval}(\sigma_1\{\text{isImprecise} := \text{false}\}, \phi, Q)$
 $\text{well-formed-e}(\sigma_1, ?\&\&\phi, Q) = \text{eval}(\sigma_1\{\text{isImprecise} := \text{true}\}, \phi, Q)$

Fig. 4. Well-formed formula function definition

In Gradual Viper, $\sigma \in \Sigma$ is used to denote a symbolic state, which is a 6-tuple given by $(\text{isImprecise}, h_?, h, \gamma, \pi, \mathcal{R})$ where isImprecise is a Boolean denoting if the state is imprecise, $h_?$ is the optimistic heap containing the optimistically assumed heap chunks for accessibility predicates, h is the symbolic heap, γ is the symbolic store, π is the path condition, and \mathcal{R} is the collection of the runtime checks. Q denotes the remainder continuation which is the remaining symbolic execution that needs to be performed.

Each pure function in a Gradual Viper program is checked for well-formedness alongside with the methods and predicates. In Figure 3, well-formedness rule for functions in Gradual Viper is given. Well-formedness check for functions in Viper has been modified for Gradual Viper. In Figure 4, well-formed formula function definitions are given. Well-formed formula function definitions have been modified for checking the well-formedness of function postconditions. Since the function postconditions are expressions and not assertions, eval must be used with the function postconditions instead of produce .

$$\text{eval}(\sigma, e, Q) : \Sigma \longrightarrow \text{EXPR} \longrightarrow (\Sigma \longrightarrow \text{SVALUE} \longrightarrow \text{RESULT}) \longrightarrow \text{RESULT}$$

$$\text{eval}(\sigma_1, \text{func}(\bar{e}), Q) = \text{eval}(\sigma_1, \bar{e}, (\lambda\sigma_2, \bar{e}'.{$$

$$\mathcal{R}' := \sigma_2.\mathcal{R}\{\text{origin} := (\sigma_2, \bar{z} := \text{func}(\bar{e}), \bar{e}')\}$$

$$\text{consume}(\sigma_2\{\mathcal{R} := \mathcal{R}'\}, \text{func}_{pre}[\bar{x} \mapsto \bar{e}'], (\lambda\sigma_3, s.$$

$$\text{if } (\text{is-imp}(\text{func})) \text{ then}$$

$$\sigma_4 := \sigma_3\{h := \sigma_2.h, h? := \sigma_2.h?, \text{isImprecise} := \text{true}\}$$

$$\text{else } \sigma_4 := \sigma_3\{h := \sigma_2.h, h? := \sigma_2.h?, \text{isImprecise} := \sigma_2.\text{isImprecise}\}$$

$$Q(\sigma_4\{\mathcal{R} := \sigma_4.\mathcal{R}\{\text{origin} := \text{none}\}, \text{func}(\bar{e}', s))))$$

where func_{pre} does not transitively contain another application of func

■ Handles imprecision ■ Handles run-time check generation and collection

Fig. 5. Rule for symbolically executing a pure function in a Gradual Viper program

In Figure 5, the eval rule for functions in Gradual Viper is given in continuation-passing style. Yellow and blue colors denote the differences from the eval rule for functions in Viper. Yellow highlighted eval and consume denote the Gradual Viper versions of the CPS rules for eval and consume rather than the Viper rules. Blue highlighted part ensures that where the runtime checks are originated from is tracked.