

Resource Usage Contracts for .NET

Jonathan Tapicer, Diego Garbervetsky and Martin Rouaux
Departamento de Computación, FCEyN, UBA
Buenos Aires, Argentina
{jtapicer, diego, mrouaux}@dc.uba.ar

ABSTRACT

CODE CONTRACTS [2] is a tool that allows the specification and verification of contracts (pre, post-condition, invariants) in all .NET based programming languages. RESOURCE CONTRACTS is an extension of this language to specify resource usage in .NET programs. The new annotations, initially focussed on dynamic memory, enable modular analysis of both memory consumption and lifetime properties. They are checked by relying on the own CODE CONTRACTS static verifier and a points-to analysis. This approach is implemented as a VISUAL STUDIO extension¹, providing facilities such as autocompletion and verification at build time.

Categories and Subject Descriptors

D.2.4 [Software Engineering]: Software/Program Verification—*Programming by contract*

General Terms

Verification, documentation

Keywords

Resource usage annotations, static verification

1. MEMORY USAGE ANNOTATIONS

The annotations provide means for quantifying object allocation as well as lifetime information in a simple and modular fashion. Fig. 1 presents some of the annotations and exhibits how our tool is able to detect an issue with one annotation concerning object lifetime. `Tmp` is used to specify the amount of *temporary* objects, used for auxiliary computation within the method and no longer needed when it finishes its execution. In contrast, `Rsd` is used for *residual* objects, that may be used by a client method and, therefore, should live longer. These annotations must be placed at the beginning of a method and are part of the method interface.

¹Available at: <http://lafhis.dc.uba.ar/resourcecontracts>.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

TOPI '11, May 28, 2011, Waikiki, Honolulu, HI, USA
Copyright 2011 ACM 978-1-4503-0599-0/11/05 ...\$10.00.

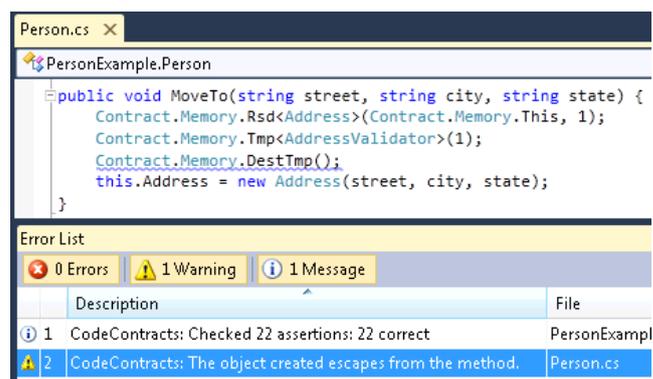


Figure 1: Verifying annotations the tool. `Rsd` annotations require identifiers. They are meant to group objects that may have similar lifetimes (e.g., they are part of the same data structure). For instance, the identifier `Contract.Memory.This` states that objects may be reachable by the receiver. In that regard the `DestRsd(t)` declares an allocation as residual consumption and associates the object with one of the identifier already mentioned in the contract. `DestTmp` is used for declaring a temporary object. They are not part of the method interface. The full list of annotations as well as a discussion of related work can be found at [3]. **Verification:** Lifetime annotations (e.g., `DestTmp`) are verified using a points-to and escape analysis [3]. Then, the program is transformed into a functionally equivalent one but using only CODE CONTRACTS annotations in such a way that a successful verification of the transformed program implies the correctness of the resource usage annotations.

2. FUTURE WORK

We plan to automatically infer quantitative and lifetime annotations in order to relieve some of the annotation burden. In this matter we plan to port our previous work on memory consumption inference for Java [1] to .NET. We will also extend the technique to deal with polymorphic method calls, which are not currently handled by the tool.

3. REFERENCES

- [1] V. Braberman, F Fernández, D. Garbervetsky, and S Yovine. Parametric prediction of heap memory requirements. In *ISMM'08*. ACM, jun 2008.
- [2] M. Fähndrich, M. Barnett, and F. Logozzo. Embedded contract languages. In *SAC 2010*, pages 2103–2110. ACM, 2010.
- [3] D. Garbervetsky, M. Rouaux, and J. Tapicer. SEIF project: ResourceContracts.NET. <http://lafhis.dc.uba.ar/resourcecontracts/files/report.pdf>.