

GOBPIE: AN IDE INTEGRATION FOR GOBLINT USING MAGPIEBRIDGE

Karoliine Holter, Software Engineering Master's

Supervisor: Vesal Vojdani, PhD



UNIVERSITY OF TARTU

Institute of Computer Science

GOBLINT

GOBLINT is a static analyzer for multi-threaded C programs, focusing primarily on data race detection [3]. Its analyses are based on abstract interpretation. The architecture of GOBLINT is designed to be modular so that the analyses are specified separately. It also has a flexible query- and event system for communication between analyses. The main application of this analyzer is to detect data races, which is done by checking that a common mutex protects all accesses to shared memory.

GOBLINT is developed in collaboration with the Technische Universität München's Chair of Formal Languages, Compiler Construction, Software Construction and the University of Tartu's Laboratory for Software Science [2].



GobPie



Goblint

Wettlaufweltmeister — Data Race World Champion

A *data race* is a situation in shared-memory concurrent systems where multiple threads may simultaneously access the same memory location. Data races can be avoided if

- whenever a thread may access the same memory location as another thread,
- both threads must acquire the same mutex.

The goal of data race analysis is to guarantee this condition. For example, consider the following two threads:

```
T1 : lock(&m1);
    g = g + 1;
    unlock(&m1);
```

```
T2 : lock(&m1);
    g = g + 1;
    unlock(&m1);
```



The analysis would *abstractly* evaluate the program and collect the list of accesses and the locks held at the time:

- $\langle g, \{m_1\}, \text{write}, \text{example.c} : 10 \rangle$
- $\langle g, \{m_1\}, \text{write}, \text{example.c} : 19 \rangle$

Taking the intersection of the held locksets, we conclude g is protected by $\{m_1\}$.

This is the GOBLINT organization mascot called Wettlaufweltmeister [Data Race World Champion].

GOBLINT takes part in SV-COMP, an International Competition on Software Verification. In year 2022, GOBLINT correctly verified the most programs as being data race free in the *NoDataRace* category, while stating no incorrect programs to be correct as seen in Figure 1.

Table 11: Results of verifiers in demonstration category *NoDataRace*

Verifier	Score	Correct true	Correct false	Incorrect true	Incorrect false
CSEQ	39	37	61	0	6
DARTAGNAN	-299	47	23	13	0
GOBLINT	124	62	0	0	0
LOCKSMITH ^{new}	34	17	0	0	0
UAUTOMIZER	120	49	54	1	0
UGEMCUTTER ^{new}	151	57	69	1	0
UKOJAK	0	0	0	0	0
UTAIPAN	139	56	59	1	0

Figure 1: GOBLINT successfully verified more cases than any other tool at SV-COMP [1].

MAGPIEBRIDGE

MAGPIEBRIDGE is a framework for integrating Static Analyses into IDEs and Editors with the Language Server Protocol [5]. The goal of MAGPIEBRIDGE is to make IDE integration easier for the static analyzers, making the $n \times m$ problem of developing a plugin for each static analyzer for each IDE a $n + m$ problem as seen in Figure 2.

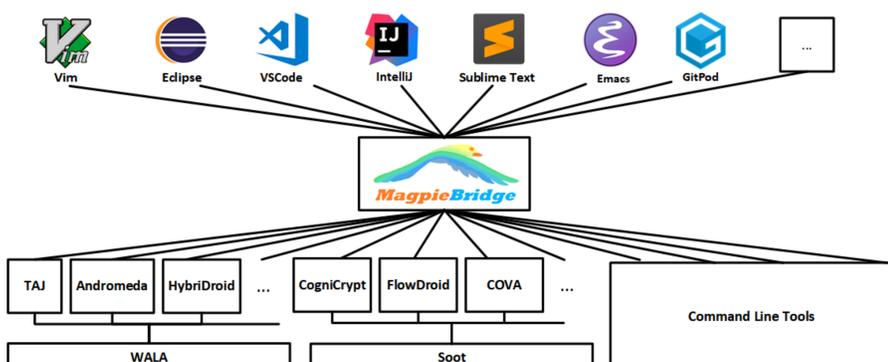


Figure 2: MAGPIEBRIDGE goal illustrated [5].

GOBPIE

GOBPIE is an interface that integrates GOBLINT into IDEs using MAGPIEBRIDGE [4]. It communicates with the GOBLINT server through a Unix domain socket. GOBPIE sends the server requests to analyze and converts the results into a format suitable for MAGPIEBRIDGE, which then sends the warnings to the IDE to visualize. The sequence diagram of a more detailed workflow is presented in Figure 3.

- This work is among the first to integrate a state-of-the-art software verifier within an IDE.
- It is an important contribution in the global race to create an Interactive Abstract Interpreter.
- GOBPIE is a notable external user of MAGPIEBRIDGE — invited to present at PRIDE 2022.

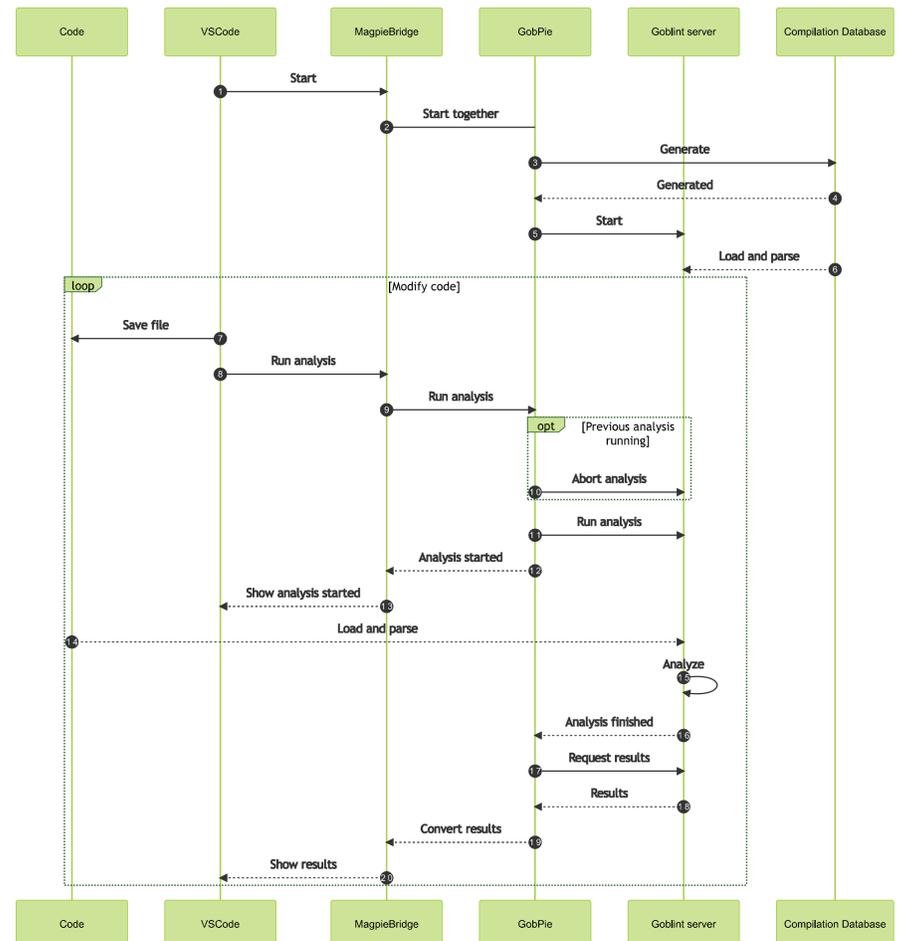


Figure 3: The sequence diagram of GOBPIE.

The program in Figure 4 conflicts with the condition presented above, and therefore a warning for a possible race, detected by GOBLINT, is shown.

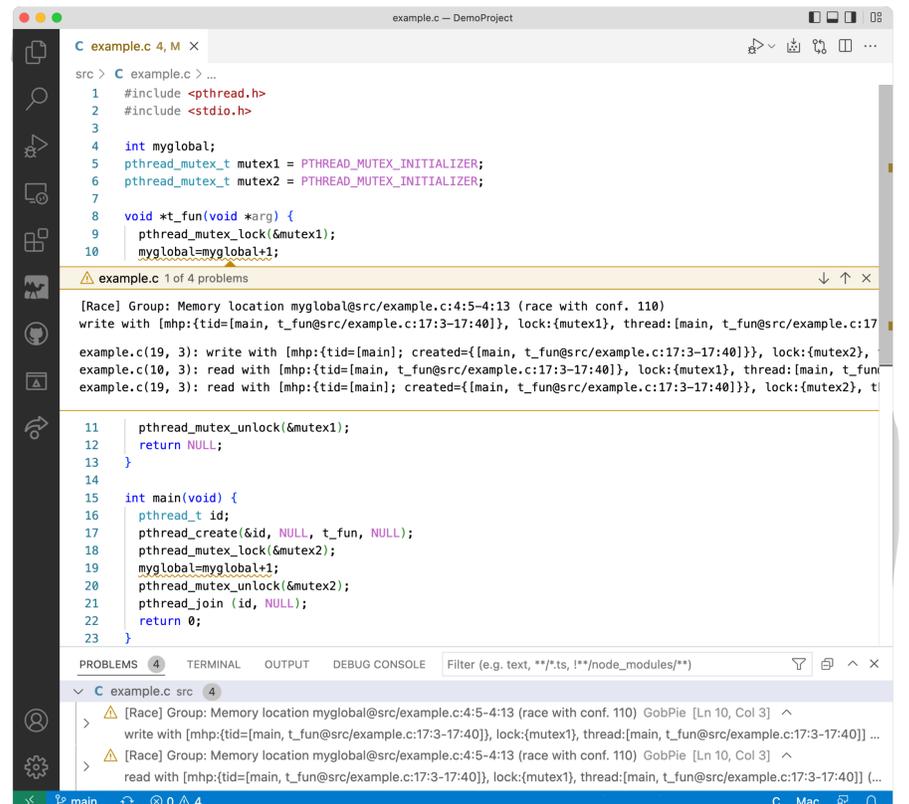


Figure 4: GOBLINT race warnings in VS Code IDE.

References

- [1] Dirk Beyer. "Progress on Software Verification: SV-COMP 2022". In: *Tools and Algorithms for the Construction and Analysis of Systems*. Ed. by Dana Fisman and Grigore Rosu. Springer International Publishing, 2022, pp. 375–402.
- [2] *Goblint Github*. URL: <https://github.com/goblint/analyzer>.
- [3] *Goblint Webpage*. URL: <https://goblint.in.tum.de>.
- [4] *GobPie Github*. URL: <https://github.com/goblint/GobPie>.
- [5] *MagpieBridge Github*. URL: <https://github.com/MagpieBridge/MagpieBridge>.