UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR SOFTWARE ENGINEERING
AND PROGRAMMING LANGUAGES

isp

Development of Safety Critical Systems(Sichere Software) winter term 18
Martin Leucker, Grigory Markin, Felix Lange March 25, 2019

Exercise Sheet 5

Deadline: Sunday December 2, 2018 24:00

CPAchecker is a tool for configurable software verification. The tool is available as a local installation, download from `https://cpachecker.sosy-lab.org`, as well as a cloud service available at `https://cpachecker.appspot.com`. The cloud version of the tool has some limitations and can not be used for e.g. bit precise predicate analysis. The list of unavailable features can be found on the service page.

Task 5.1 Getting started with CPAchecker

- For local installation, please, follow the instruction at `https://github.com/sosy-lab/cpachecker/blob/trunk/INSTALL.md`. **It is highly recommend to use Linux for bit precise predicate analysis. If you use other OS, consider to run the tool inside e.g. a Virtualbox with Linux OS.**
- Read a "Getting started" guide at `https://github.com/sosy-lab/cpachecker/blob/trunk/README.md`

Task 5.2 Program 1

- Consider the following C program:

```
1  int x, y, z, w;
2
3  int main() {
4    do {
5      x = y;
6      if (w != 1) {
7        x++;
8      }
9      z = w - 1;
10   } while (x != y);
11
12   if (z) {
13   ERROR:
14     return 1;
15   }
16
17   return 0;
18 }
```

- Try to find out whether the ERROR location is reachable ?
- Copy the file "exercise-non-precise.properties" and "program1.c" into the CPAchecker directory.

- Verify the program using CPAchecker by executing the following command from the CPAchecker directory:

```
$ scripts/cpa.sh -config exercise-non-precise.properties program1.c
```

- Exemine the output located in the "CPAchecker/output" directory.
- Change the condition at line 6 to $w == 1$, run the tool again and check the report.

Task 5.3 Program 2

- Consider the following C program:

```
1  int __VERIFIER_assert(int cond) {
2    if (!(cond)) {
3    ERROR:
4      return 1;
5    }
6    return 0;
7  }
8
9  int glob_arr[] = {1, 2, 3, 4, 5};
10
11 int sum_arr(int *from, int *to) {
12   int result = 0;
13   while (from < to) {
14     result += *(from++);
15   }
16   return result;
17 }
18
19 int main() {
20   int sum = sum_arr(glob_arr, glob_arr + 5);
21   return __VERIFIER_assert(sum == 15);
22 }
```

- Copy the file "program2.c" into the CPAchecker directory.
- Verify the program using the same configuration file as before.
- Is the ERROR location rechable ? Are the results of the verification correct ?