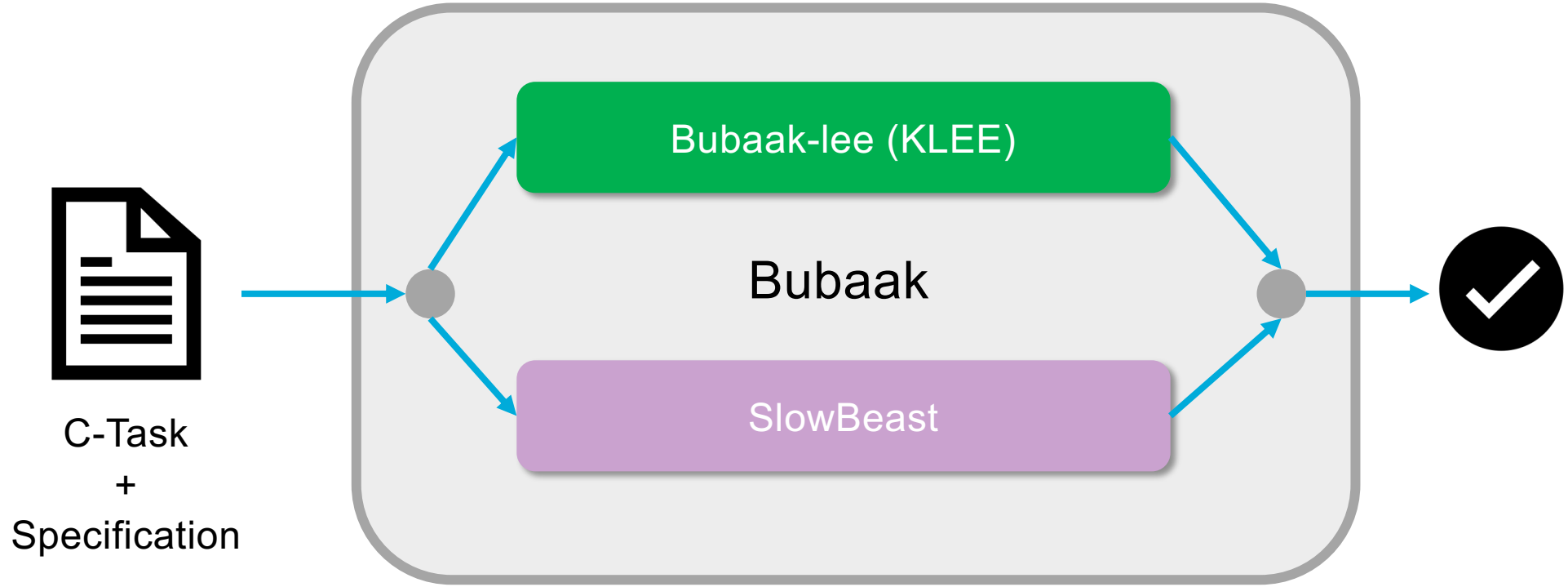
Carl von Ossietzky
Universität
Oldenburg

Bubaak-SpLit

Split what you cannot verify

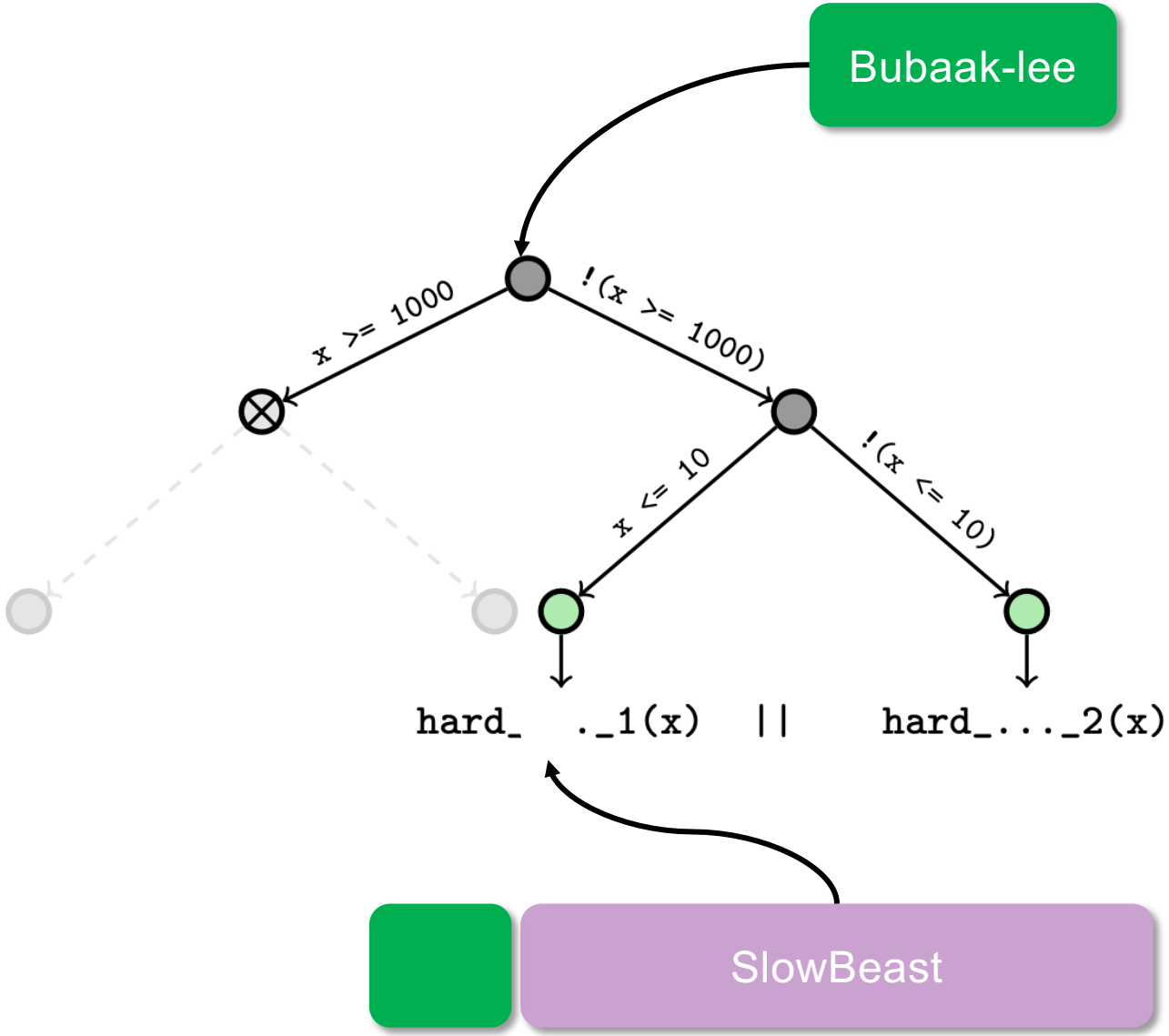
Marek Chalupa and **Cedric Richter**,
08.04.2024

Bubaak

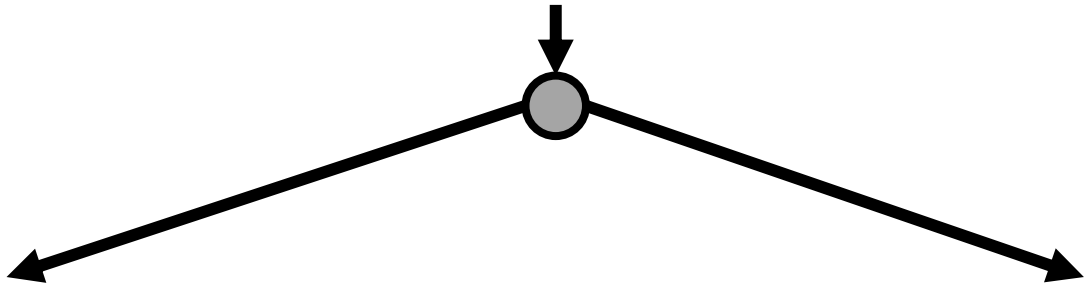


Bubaak-SpLit

```
1  int main(void) {
2    int x = nondet();
3    if( x >= 1000 ) abort();
4
5    if( x <= 10 ){
6      hard_to_verify_1(x);
7    } else {
8      hard_to_verify_2(x);
9    }
10 }
```



Control Flow Splitting



```
1 int main(void) { // P+
2   int x = nondet();
3   assume( x >= 1000 );
4   abort();
5 }
```

```
1 int main(void) { // P-
2   int x = nondet();
3   assume( !(x >= 1000) );
4   if( x <= 10 ) ...
5 }
```

„Scaling Formal Verification to Realistic Code with Appplication to DeFi“, Mooly Sagiv, ETAPS 2023

Task Rewriting System

$$\textbf{Split}(P): \quad P^+, P^- := \texttt{split}(P) \rightarrow \wedge \begin{cases} \rightarrow CCAndCheckWeak(P^+) \\ \rightarrow CCAndCheckWeak(P^-) \end{cases}$$

$$\textbf{CCAndCheckWeak}(P): \quad bc := \texttt{compile}(P) \longrightarrow CheckWeak(bc, P)$$

Software Systems (Second Place)