CerCo: Certified Complexity

A FET project by the Università di Bologna, University of Edinburgh, and Université Paris-Diderot

The state of the art

How long will this code take to execute? How sure are you?

Compilation to assembly language
Completely untrusted

Does not preserve compositional cost models

Automatic/interactive static analysis on C source

Compilation

How are these related?

Static analysis on modern machines is imprecise

Cost model for assembly fragments

The CerCo approach

Complexity assertion
Body cost annotation

Loop complexity assertion
Loop body cost annotation

Complexity obligation (sketch)

/* Meme>0 time : time = \max(0, (\{v\}) - 1) + \max(0, (r - 1) \times 20 + 21) + e) */
void quick_recur(int l, int r) {
    if (l > r) {
        return;
    } else if (l == r) {
        return;
    } else {
        int m = (l + r) / 2;
        quick_recur(l, m - 1);
        quick_recur(m + 1, r);
    }
}

/* Meme>0 time : time = \max(0, (\{v\}) - 1) + \max(0, (r - 1) \times 20 + 21) + e) */
void quick_recur(int l, int r) {
    if (l > r) {
        return;
    } else if (l == r) {
        return;
    } else {
        int m = (l + r) / 2;
        quick_recur(l, m - 1);
        quick_recur(m + 1, r);
    }
}

The clock cycles spent in one iteration of the recursive function must be greater or equal than the sum of the clock cycles spent in the function body, in the whole loop and in the two recursive calls.

Program dependent, non-compositional cost model induced by compilation

Cost annotated C source

Proof checker (trusted)

CerCo compiler (certified)

Machine code output

Certificate

Certified reaction time bound for C source

Trusted code base: we trust the proof checker to be correctly implemented.

Certified code base: we prove in the Matita proof checker the following:
1) The semantics of source and target code is the same,
2) The C source level cost model fully agrees with the machine's execution timing.

For more information, please visit the CerCo project website at: http://cerco.cs.unibo.it

The project CerCo acknowledges the financial support of the Future and Emerging Technologies (FET) programme within the Seventh Framework Programme for Research of the European Commission, under FET-Open grant number: 245881.