Programming Languages: Imperative Program Construction 0. Introduction

Shin-Cheng Mu

Autumn Term, 2022

National Taiwan University and Academia Sinica

Can you Implement Binary Search?

Given a sorted array of N numbers and a key, either locate the position where the key resides in the array, or report that the key does not present in the array, in $O(\log N)$ time.

- You would not expect it to be a hard programming task.
- Jon Bentley, however, noted:

> *"I've assigned this problem in courses at Bell Labs and IBM. Professional programmers had a couple of hours to convert the above description into a program in the language of their choice; ...90% of the programmers found bugs in their programs.*
>
> *...Knuth points out that while the first binary search was published in 1946, the first published binary search without bugs did not appear until 1962."*

Give It a Try?

- Bentley: “The only way you’ll believe this is by putting down this column right now and writing the code yourself.”
- Given: an array $a\ [0..N)$ of N elements,
- that is sorted: $\langle \forall i, j : 0 \leqslant i < j < N : a[i] \leqslant a[j] \rangle$.
- Find i such that $a[i] = K$, or report that K is not in the array.

Programming is Hard

We have heard about plenty of "horror story" about software errors.

- NASA's Mars Climate Orbiter, 1998.
  - Conversion from imperial units to metric.
- Ariane 5 explosion, 1996.
  - Cramming a 64-bit number into a 16-bit space.
- Baggage handling system in Heathrow Terminal 5, 2008.
  - Cannot cope with "real world" situation.
- Patriot Missile system failed to detect an attack, 1991.
  - Rounding error caused a delay of $1/3$ second after 100 hours.

But today let us look at a more recent bug caused by a tiny piece of code.

The Zune Bug

- **Zune**: a line of portable media players and software, produced by Microsoft.
- “First-generation Zunes — those with 30-gigabyte disk drives — went silent everywhere on December 31. The cause was soon traced to calendrical code in the device’s firmware. The bug is an interesting one, if only because all the details, including the source code, immediately came to light.” .

The Task

- The variable `days` is set to the number of days since January 1, 1980.
- The task: **what is the current year**?
- Each common year has 365 days; each leap year has 366 days.
- The predicate `IsLeapYear(year)` yields true if `year` is a leap year.

The Code That Caused All the Trouble

```
year = 1980;
while (days > 365) {
    if (IsLeapYear(year)) {
        if (days > 366) {
            days -= 366;
            year += 1;
        }
    }
    else {
        days -= 365;
        year += 1;
    }
}
```

Fix?

- A reader at Zuneboards.com suggested a fix: replace `(days > 366)` with `(days >= 366)`.
- The program returns the wrong year on the last day of every leap year.

A Program That Works

```
year = 1980;
while (days > 365) {
    if (IsLeapYear(year)) {
        if (days > 366) {
            days -= 366;
            year += 1;
        }
        else break;
    }
    else { days -= 365;
           year += 1;
    }}
```

"... but the logic is anything but perspicuous."

How To Ensure That a Program is Correct?

Programming is more than producing the code. At the very least we should produce code *that is correct*.

But how do we ensure that the code is correct?

How To Ensure That a Program is Correct?

Programming is more than producing the code. At the very least we should produce code *that is correct*.

But how do we ensure that the code is correct?

- Testing.
- Verification.
- Derivation.

A technique widely used in industry. A matured discipline in its own right, which I cannot claim I know very well.

Due to its very nature, however, testing can never be complete.

Dijkstra: "Today a usual technique is to make a program and then to test it. But: program testing can be a very effective way to show the **presence** *of bugs, but is hopelessly inadequate for showing their* **absence**."

— The humble programmer, 1972.

Dijkstra: *"Today a usual technique is to make a program and then to test it. But: program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence. The only effective way to raise the confidence level of a program significantly is to* **give a convincing proof of its correctness.**"

Formal Verification

To *prove* that a program is correct, via formal/mathematical means.

Also a matured discipline, used for software whose correctness is of vital importance.

The main difficulties:

- programs written without proofs in mind are often hard to prove;
- programmers don't bother to prove their code once it is written.

Dijkstra: "The only effective way to raise the confidence level of a program significantly is to give a convincing proof of its correctness. But one should not first make the program and then prove its correctness, because then the requirement of providing the proof would only increase the poor programmer's burden. On the contrary: the programmer should ..."

"...[let] correctness proof and program grow hand in hand: with the choice of the structure of the correctness proof one designs a program for which this proof is applicable."

Program Derivation

Program Derivation: developing a program and its correctness proof at the same time.

Why?

- Programs developed with proofs in mind are easier to prove.
- Programming is easier too! In fact, “how to prove the program” may give you hints on “how the program can be written.”

Goals This Term

Formal approaches to (imperative) program construction — constructing programs with sufficient confidence that they are correct.

- We will start with learning an imaginary programming language: the *Guarded Command Language*.
- Starting with: given a program, how to prove that it is correct?
  - Tools: Hoare logic, weakest precondition, predicate logic...
- Then we move on to learn about *deriving* programs.
  - Most of the tricks will be about constructing loops.
- If time allows, we will talk about reasoning about heaps and pointers using *separation logic*.

We will emphasise on program derivation when possible, and switch to program verification when we have to.

Testing, Verification, and Derivation

We will emphasise on program derivation when possible, and switch to program verification when we have to.

While early debates sometimes positioned testing, verification, and derivation as rivaling techniques, I tend to see them as related disciplines sharing common theories. People in these disciplines can communicate and learn from each other.

Textbook and Homepage

- We will not follow any textbook completely, but most of this course are adapted from Kaldewaij 90.
- Other highly recommended materials include: Dijkstra 76, Gries 81, Morgan 90, Backhouse 11.
- Some materials are borrowed from "(In)formal Methods" a very recommended course given by Prof. Carroll Morgan.
- Prof. Yih-Kuen Tsay's course on Software Specification and Verification tells the verification side of the story.
- Course homepage: https://scmu.github.io/plip/. We might use NTU COOL too.