Prof. Dr. A. Poetzsch-Heffter
Dipl.-Inf. P. Michel
Dipl.-Inf. C. Feller

University of Kaiserslautern
Department of Computer Science
Software Technology Group

Exercise Sheet 10: Specification and Verification with Higher-Order Logic (Summer Term 2012)

Date: 06.07.2012

Exercise 1 Hoare Calculus

Consider the following while program `prog`, which calculates the nth Fibonacci number in linear time:

```
f0 := 0;
f1 := 1;
i  := 0;

WHILE i < n INV ? DO
  f1 := f0 + f1;
  f0 := f1 − f0;
  i  := i + 1
END;

result := f0
```

As a postcondition we would like to have that `result` is fib n, where fib is specified as usual:

$$\text{fib } n = \begin{cases} 0 & n \leq 0 \\ 1 & n = 1 \\ \text{fib } (n-1) + \text{fib } (n-2) & \text{otherwise} \end{cases}$$

a) (Prepare!) Find a suitable loop invariant and prove the following Hoare-triple *on paper*.

$$\{\text{n} \geq 0\}\ \texttt{prog}\ \{\text{result} = \text{fib n}\}$$

b) Translate the proof intro Isabelle/HOL, using the `Hoare.thy` from the website. Apply all Hoare rules manually, like done in the `sqrProp` lemma.

c) Optimize your proof by using the custom `wphoare` method, like done in the `splitcorrect` lemmas.

d) The `splitcorrect` lemma does not prove that split does not change the content of the array.

At the end of the theory file, we have specified a `content` function for arrays in a state. Using this function, we would like to prove the following Hoare-triple:

$$\{\texttt{splitRequires} \wedge \texttt{content myarr} = C\}\ \texttt{splitProg}\ \{\texttt{content myarr} = C\}$$

Find suitable invariants for the loops and prove the triple using `wphoare`.