The National Institute of Aerospace / Galois Inc. / NASA LaRC

An Introduction to Copilot

Nis N. Wegmann
niswegmann@gmail.com

Lee Pike
leepike@galois.com

Sebastian Niller
sebastian.niller@nianet.org

Hampton, Virginia, United States, January 22, 2012

Abstract

This document contains a tutorial on Copilot and its accompanying tools. We do not attempt to give a complete, formal description of Copilot (references are provided in the bibliography), rather we aim at demonstrating the fundamental concepts of the language by using idiomatic expositions and examples.

Contents

This research is supported by NASA Contract NNL08AD13T from the Aviation Safety Program Office.

1 Preliminaries

Copilot is embedded into the functional programming language Haskell [Jon02]. A working knowledge of Haskell is necessary to use Copilot effectively; a variety of books and free web resources introduce Haskell. Copilot uses Haskell language extensions specific to the Glasgow Haskell Compiler (GHC); hence in order to start using Copilot, you must first install an up-to-date version of GHC. (The minimal required version is 7.0.) The easiest way to do this is to download and install the Haskell Platform, which is freely distributed from here:

`http://hackage.haskell.org/platform`

After having installed the Haskell Platform, Copilot is downloaded and installed by executing the following command:

```
> cabal install copilot
```

This should, if everything goes well, install Copilot on your system.

Copilot is distributed throughout a series of packages at Hackage:

- copilot-language: Contains the language front-end.
- copilot-core: Contains an intermediate representation for Copilot programs (shared by all back-ends).
- copilot-c99: A back-end for Copilot targeting C99 (based on Atom, `http://hackage.haskell.org/package/atom`).
- copilot-sbv: A back-end for Copilot targeting C99 (based on SBV, `http://hackage.haskell.org/package/sbv`).
- copilot-libraries: A set of utility functions for Copilot, including a clock-library, a linear temporal logic framework, a voting library, and a regular expression framework.
- copilot-cbmc: A driver for proving the correspondence between code generated by the copilot-c99 and copilot-sbv back-ends.

Many of the examples in this paper can be found at `https://github.com/leepike/Copilot/tree/copilot2.0/Examples`.

To use the language, your Haskell module should contain the following import:

```
import Language.Copilot
```

To use the back-ends, import, them, respectively:

```
import Copilot.Compile.C99
import Copilot.Compile.SBV
```

If you need to use functions defined in the Prelude that are redefined by Copilot (e.g., arithmetic operators), import the Prelude as qualified:

```
import qualified Prelude as P
```

2 Domain

Copilot is a domain-specific language tailored to programming *runtime monitors* for *hard real-time*, *distributed*, *reactive systems*. Briefly, a runtime monitor is program that runs concurrently with a target program with the sole purpose of assuring that the target program behaves in accordance with a pre-established specification. Copilot is a language for writing such specifications.

A reactive system is a system that responds continuously to its environment. All data to and from a reactive system is communicated progressively during execution. Reactive systems differ from transformational systems which transforms data in a single pass and then terminate, as for example compilers and numerical computation software.

A hard real-time system is a system that has a statically bounded execution time and memmory usage. Typically, hard real-time systems are used in mission-critical software, such as avionics, medical equipment, and nuclear power plants; hence, occasional dropouts in the response time or crashes are not tolerated.

A distributed system is a system which is layered out on multiple pieces of hardware. The distributed systems we consider are all synchronized, i.e., each component agree on a shared global clock.

2.1 Language

Copilot is embedded into the functional programming language Haskell [Jon02], and a working knowledge of Haskell is necessary to use Copilot effectively. Copilot is a pure declarative language; i.e., expressions are free of side-effects and satisfies referential transparency. A program written in Copilot, which from now on will be referred to as a *specification*, has a cyclic behavior, where each cycle consists of a fixed series of steps:

- Sample external variables, arrays, and functions.
- Update internal variables.
- Fire external triggers. (In case the specification is violated.)

We refer to a single cycle as an *iteration*.

All transformation of data in Copilot is propagated through streams. A stream is an infinite, ordered sequence of values which must conform to the same type. E.g., we have the stream of Fibonacci numbers:

$$s_{fib} = \{0, 1, 1, 2, 3, 5, 8, 13, 21, \dots\}$$

We denote the nth value of the stream s as $s(n)$, and the first value in a sequence s as $s(0)$. For example, for s_{fib} we have that $s_{fib}(0) = 0$, $s_{fib}(1) = 1$, $s_{fib}(2) = 1$, and so forth.

Constants as well as arithmetic, boolean, and relational operators are lifted to work pointwise on streams:

```
x :: Stream Int32
x = 5 + 5

y :: Stream Int32
y = x * x

z :: Stream Bool
z = x == 10 && y < 200
```

Here the streams `x`, `y`, and `z` are simply *constant streams*:

$$\texttt{x} \rightsquigarrow \{10, 10, 10, \dots\},\ \texttt{y} \rightsquigarrow \{100, 100, 100, \dots\},\ \texttt{z} \rightsquigarrow \{\mathrm{T},\ \mathrm{T},\ \mathrm{T},\ \dots\}$$

Two types of *temporal* operators are provided, one for delaying streams and one for looking into the future of streams:

```
(++) :: [a] -> Stream a -> Stream a
drop :: Int -> Stream a -> Stream a
```

Here `xs ++ s` prepends the list `xs` at the front of the stream `s`. For example the stream `w` defined as follows, given our previous definition of `x`:

```
w = [5,6,7] ++ x
```

evaluates to the sequence $\texttt{w} \rightsquigarrow \{5, 6, 7, 10, 10, 10, \dots\}$. The expression `drop k s` skips the first `k` values of the stream `s`, returning the remainder of the stream. For example we can skip the first two values of `w`:

```
u = drop 2 w
```

which yields the sequence `u` $\rightsquigarrow \{7, 10, 10, 10, \dots\}$.

2.2 Streams as Lazy-Lists

A key design choice in Copilot is that streams should mimic *lazy lists*. In Haskell, the lazy-list of natural numbers can be programmed like this:

```
nats_ll :: [Int32]
nats_ll = [0] ++ zipWith (+) (repeat 1) nats_ll
```

As both constants and arithmetic operators are lifted to work pointwise on streams in Copilot, there is no need for `zipWith` and `repeat` when specifying the stream of natural numbers:

```
nats :: Stream Int32
nats = [0] ++ (1 + nats)
```

In the same manner, the lazy-list of Fibonacci numbers can be specified as follows:

```
fib_ll :: [Int32]
fib_ll = [1, 1] ++ zipWith (+) fib_ll (drop 1 fib_ll)
```

In Copilot we simply throw away `zipWith`:

```
fib :: Stream Int32
fib = [1, 1] ++ (fib + drop 1 fib)
```

Copilot specifications must be *causal*, informally meaning that stream values cannot depend on future values. For example, the following stream definition is allowed:

```
f :: Stream Word64
f = [0,1,2] ++ f


g :: Stream Word64
g = drop 2 f
```

But if instead `g` is defined as `g = drop 4 f`, then the definition is disallowed. While an analogous stream is definable in a lazy language, we bar it in Copilot, since it requires future values of `f` to be generated before producing values for `g`. This is not possible since Copilot programs may take inputs in real-time from the environment (see Section 2.6).

2.3 Functions on Streams

Given that constants and operators work pointwise on streams, we can use Haskell as a macro-language for defining functions on streams. The idea of using Haskell as a macro language is powerful since Haskell is a general-purpose higher-order functional language.

Example 1:
We define the function, `even`*, which given a stream of integers returns a boolean stream which is true whenever the input stream contains an even number, as follows:*

```
even :: Stream Int32 -> Stream Bool
even x = x `mod` 2 == 0
```

Applying `even` *on* `nats` *(defined above) yields the sequence* $\{T, F, T, F, T, F, \dots\}$.

If a function is required to return multiple results, we simply use plain Haskell tuples:

Example 2:
We define complex multiplication as follows:

```
mul_comp
  :: (Stream Double, Stream Double)
  -> (Stream Double, Stream Double)
  -> (Stream Double, Stream Double)
(a, b) `mul_comp` (c, d) = (a * c - b * d, a * d + b * c)
```

Here `a` *and* `b` *represent the real and imaginary part of the left operand, and* `c` *and* `d` *represent the real and imaginary part of the right operand.*

2.4 Stateful Functions

In addition to pure functions, such as `even` and `mul_comp`, Copilot also facilitates *stateful* functions. A *stateful* function is a function which has an internal state, e.g. as a latch (as in electronic circuits) or a low/high-pass filter (as in a DSP).

Example 3:
We consider a simple latch, as described in [Far04], with a single input and a boolean state. Whenever the input is true the internal state is reversed. The operational behavior and the implementation of the latch is shown in Figure 1.[1]

[1] In order to use conditionals (if-then-else's) in Copilot specifications, as in Figures 1 and 2, the GHC language extension `RebindableSyntax` must be set on.

x_i:	y_{i-1}:	y_i:
F	F	F
F	T	T
T	F	T
T	T	F

```
latch :: Stream Bool -> Stream Bool
latch x = y
  where
  y = if x then not z else z
  z = [False] ++ y
```

Figure 1: A latch. The specification is provided at the left and the implementation is provided at the right.

$\texttt{inc}_i$:	$\texttt{reset}_i$:	$\texttt{cnt}_i$:
F	F	$\texttt{cnt}_{i-1}$
$*$	T	0
T	F	$\texttt{cnt}_{i-1} + 1$

```
counter :: Stream Bool -> Stream Bool
        -> Stream Int32
counter inc reset = cnt
  where
  cnt = if reset then 0
          else if inc then z + 1
                 else z
  z = [0] ++ cnt
```

Figure 2: A resettable counter. The specification is provided at the left and the implementation is provided at the right.

Example 4:
We consider a resettable counter with two inputs, `inc` *and* `reset`*. The input* `inc` *increments the counter and the input* `reset` *resets the counter. The internal state of the counter,* `cnt`*, represents the value of the counter and is initially set to zero. At each cycle, i, the value of $\texttt{cnt}_i$ is determined as shown in the left table in Figure 2.*

2.5 Types

Copilot is a typed language, where types are enforced by the Haskell type system to ensure generated C programs are well-typed. Copilot is *strongly typed* (i.e., type-incorrect function application is not possible) and *statically typed* (i.e., type-checking is done at compile-time). The base types are Booleans, unsigned and signed words of width 8, 16, 32, and 64, floats, and doubles. All elements of a stream must belong to the same base type. These types have instances for the class `Typed a`, used to constrain Copilot programs.

We provide a `cast` operator

```
cast :: (Typed a, Typed b) => Stream a -> Stream b
```

that casts from one type to another. The cast operator is only defined for casts that do not lose information, so an unsigned word type `a` can only be cast to another unsigned type at least as large as `a` or to a signed word type strictly

larger than `a`. Signed types cannot be cast to unsigned types but can be cast to signed types at least as large.

2.6 Interacting With the Target Program

All interaction with the outside world is done by sampling *external symbols* and by evoking *triggers*. External symbols are symbols that are defined outside Copilot and which reflect the visible state of the target program that we are monitoring. They include variables, arrays, and functions (with a non-void return type). Analogously, triggers are functions that are defined outside Copilot and which are evoked when Copilot needs to report that the target program has violated a specification constraint.

Sampling. A Copilot specification is *open* if defined with external symbols in the sense that values must be provided externally at runtime. To simplify writing Copilot specifications that can be interpreted and tested, constructs for external symbols take an optional environment for interpretation.

External variables are defined by using the `extern` construct:

```
extern :: Typed a => String -> Maybe [a] -> Stream a
```

It takes the name of an external variable, a possible Haskell list to serve as the environment for the interpreter, and generates a stream by sampling the variable at each clock cycle. For example,

```
sumExterns :: Stream Word64
sumExterns = let ex1 = extern "e1" (Just [0..])
                 ex2 = extern "e2" Nothing
             in  ex1 + ex2
```

is a stream that takes two external variables `e1` and `e2` and adds them. The first external variable contains the infinite list `[0,1,2,...]` of values for use when interpreting a Copilot specification containing the stream. The other variable contains no environment (`sumExterns` must have an environment for both of its variables to be interpreted).

Sometimes, type inference cannot infer the type of an external variable. For example, in the stream definition

```
extEven :: Stream Bool
extEven = e0 `mod` 2 == 0
  where e0 = externW8 "x" Nothing
```

the type of `extern "x"` is ambiguous, since it cannot be inferred from a Boolean stream and we have not given an explicit type signature. For convenience, typed `extern` functions are provided, e.g., `externW8` or `externI64` denoting an external unsigned 8-bit word or signed 64-bit word, respectively. In general it is best practice to define external symbols with top-level definitions, e.g.,

```
e0 :: Stream Word8
e0 = extern  "e0" (Just [2,4..])
```

so that the symbol name and its environment can be shared between streams.

Besides variables, external arrays and arbitrary functions can be sampled. The external array construct has the type

```
externArray :: (Typed a, Typed b, Integral a)
            => String -> Stream a -> Int
            -> Maybe [[a]] -> Stream b
```

The construct takes (1) the name of an array, (2) a stream that generates indexes for the array (of integral type), (3) the fixed size of the array, and (4) possibly a list of lists that is the environment for the external array, representing the sequence of array values. For example,

```
extArr :: Stream Word32
extArr = externArray "arr1" arrIdx size
           (Just $ repeat (permutations [0,1,2]))
  where
  arrIdx :: Stream Word8
  arrIdx = [0] ++ (arrIdx + 1) `mod` size

  size = 3
```

`extArr` is a stream of values drawn from an external array containing 32-bit unsigned words. The array is indexed by an 8-bit variable. The index is ensured to be less than three by using modulo arithmetic. The environment provided produces an infinite list of all the permutations of the list `[0,1,2]`.[2]

Example 5:
Say we have defined a lookup-table (in C99) of a discretized continuous function that we want to use within Copilot:

```
double someTable[42] = { 3.5, 3.7, 4.5, ... };
```

[2]The function `permutations` comes from the Haskell standard library `Data.list`.

We can use the table in a Copilot specification as follows:

```
lookupSomeTable :: Stream Word16 -> Stream Double
lookupSomeTable idx =
  externArray "someTable" idx 42 Nothing
```

Given the following values for `idx`, $\{1, 0, 2, 2, 1, \dots\}$, *the output of* `lookupSomeTable idx` *would be*

$$\{3.7, 3.5, 4.5, 4.5, 3.7, \dots\}$$

Finally, the constructor `externFun` takes (1) a function name, (2) a list of arguments, and (3) a possible list of values to provide its environment.

```
externFun :: Typed a => String -> [FunArg]
          -> Maybe [a] -> Stream a
```

Each argument to an external function is given by a Copilot stream. For example,

```
func :: Stream Word16
func = externFun "f" [funArg e0, funArg nats] Nothing
  where
  e0 = externW8 "x" Nothing
  nats :: Stream Word8
  nats = [0] ++ nats + 1
```

samples a function in C that has the prototype

```
uint16_t f(uint8_t x, uint8_t nats);
```

Both external arrays and functions must, like external variables, be defined in the target program that is monitored. Additionally, external functions must be without side effects, so that the monitor does not cause undesired side-effects when sampling functions. Finally, to ensure Copilot sampling is not order-dependent, external functions cannot contain streams containing other external functions or external arrays in their arguments, and external arrays cannot contain streams containing external functions or external arrays in their indexes. They can both take external variables, however.

Triggers. Triggers, the only mechanism for Copilot streams to effect the outside world, are defined by using the `trigger construct`:

```
trigger :: String -> Stream Bool -> [TriggerArg] -> Spec
```

The first parameter is the name of the external function, the second parameter is the guard which determines when the trigger should be evoked, and the third parameter is a list of arguments which is passed to the trigger when evoked. Triggers can be combined into a specification by using the *do*-notation:

```
spec :: Spec
spec = do
  trigger "f" (even nats) [arg fib, arg (nats * nats)]
  trigger "g" (fib > 10) []
  let x = externW32 "x" Nothing
  trigger "h" (x < 10) [arg x]
```

The order in which the triggers are defined is irrelevant.

Example 6:
We consider an engine controller with the following property: If the temperature rises more than 2.3 degrees within 0.2 seconds, then the fuel injector should not be running. Assuming that the global sample rate is 0.1 seconds, we can define a monitor that surveys the above property:

```
propTempRiseShutOff :: Spec
propTempRiseShutOff =
  trigger "over_temp_rise"
    (overTempRise && running) []

  where
  max = 500 -- maximum engine temperature

  temps :: Stream Float
  temps = [max, max, max] ++ temp

  temp = extern "temp" Nothing

  overTempRise :: Stream Bool
  overTempRise = drop 2 temps > (2.3 + temps)

  running :: Stream Bool
  running = extern "running" Nothing
```

Here, we assume that the external variable `temp` *denotes the temperature of the engine and the external variable* `running` *indicates whether the fuel injector is running. The external function* `over_temp_rise` *is called without any arguments if the temperature rises more than 2.3 degrees within 0.2 seconds and the engine is not shut off. Notice there is a latency of one tick between when the property is violated and when the guard becomes true.*

2.7 Explicit Sharing

```
s1 = let x = nats + nats                s2 = local (nats + nats) $
     in x * x                                \ x -> x * x
```

Figure 3: Implicit sharing (s1) versus explicit sharing (s2).

Copilot facilitates sharing in expressions by the *local*-construct:

```
local
  :: (Typed a, Typed b)
  => Stream a
  -> (Stream a -> Stream b)
  -> Stream b
```

The local construct works similar to *let*-bindings in ordinary Haskell. From a semantic point of view, the streams `s1` and `s2` from Figure 3 are identical. As we will see in Section 4, however, certain advanced Copilot programs may force the compiler to build syntax trees that blow up exponentially. In such cases, using explicit sharing helps to avoid this problem.

3 Tools

Copilot comes with a variety of tools, including a pretty-printer, an interpreter, two compilers targeting C, and a verifier front-end. In the following section, we will demonstrate some of these tools and their usage.

3.1 Pretty-Printing

Pretty-printing is straightforward. For some specification `spec`,

```
prettyPrint spec
```

returns the specification after static macro expansion. Pretty-printing can provide some indication about the complexity of the specification to be evaluated. Specifications that are built by recursive Haskell programs (e.g., the majority voting example in Section 4) can generate expressions that are large. Large expressions can take significant time to interpret or compile.

3.2 Interpreting Copilot

The copilot interpreter is invoked as follows (e.g. within GHCI, the GHC compiler's interpreter for Haskell):

```
GHCI> interpret 10 propTempRiseShutOff
```

The first argument to the function *interpret* is the number of iterations that we want to evaluate. The third argument is the specification (of type `Spec`) that we wish to interpret.

The interpreter outputs the values of the arguments passed to the trigger, if its guard is true, and `--` otherwise. For example, consider the following Copilot program:

```
spec = do
  trigger "trigger1" (even nats) [arg nats, arg $ odd nats]
  trigger "trigger2" (odd nats) [arg nats]
```

where `nats` is the stream of natural numbers, and `even` and `odd` are functions that take a stream and return whether the point-wise values are even or odd, respectively. The output of

```
interpret 10 spec
```

is as follows:

```
trigger:   trigger2:
(0,false)  --
--         (1)
(2,false)  --
--         (3)
(4,false)  --
--         (5)
(6,false)  --
--         (7)
(8,false)  --
--         (9)
```

Sometimes it is convenient to observe the behavior of a stream without defining a trigger. We can do so declaring an *observer*. For example:

```
spec :: Spec
spec = observer ‘‘obs’’ nats
```

can be interpreted using

```
interpret 5 spec
```

as usual. Observers can be combined in larger Copilot programs. For example, consider the following:

```
spec :: Spec
spec = do
  let x = externW8 "x" (Just [0..])
  trigger "trigger" true [arg $ x < 3]
  observer "debug_x" x
```

Interpreting `spec` as follows

```
interpret 10 spec
```

yields

```
trigger:  debug_x:
(true)    0
(true)    1
(true)    2
(false)   3
(false)   4
(false)   5
(false)   6
(false)   7
(false)   8
(false)   9
```

3.3 Compiling Copilot

Compiling the engine controller from Example 6 is straightforward. First, we pick a back-end to compile to. Currently, two back-ends are implemented, both of which generate constant-time and constant-space C code. One back-end is called *copilot-c99* and targets the Atom language,[3] originally developed by Tom Hawkins at Eaton Corp. for developing control systems. The second back-end is called *copilot-sbv* and targets the SBV language[4], originally developed by Levent Erkök. SBV is primarily used as an interface to SMT solvers [BSST09] and also contains a C-code generator. Both languages are open-source.

The two back-ends are installed with Copilot, and they can be imported, respectively, as

```
import Copilot.Compile.C99
```

and

```
import Copilot.Compile.SBV
```

[3] `http://hackage.haskell.org/package/atom`
[4] `http://hackage.haskell.org/package/sbv`

After importing a back-end, the interface for compiling is as follows:[5]

```
reify spec >>= compile defaultParams
```

(The compile function takes a parameter to rename the generated C files; `defaultParams` is the default, in which there is no renaming.)

The compiler now generates two files:

- "copilot.c" —
- "copilot.h" —

The file named "copilot.h" contains prototypes for all external variables, functions, and arrays, and contains a prototype for the "step"-functions which evaluates a single iteration.

```
/* Generated by Copilot Core v. 0.1 */

#include <stdint.h>
#include <stdbool.h>

/* Triggers (must be defined by user): */

void over_temp_rise();

/* External variables (must be defined by user): */

extern float temp;
extern bool running;

/* Step function: */

void step();
```

Using the prototypes in "copilot.h" we can build a driver as follows:

```
/* driver.c */
#include <stdio.h>
#include "copilot.h"

bool running = true;
float temp = 1.1;
```

[5]Two explanations are in order: (1) `reify` allows sharing in the expressions to be compiled [Gil09], and `>>=` is a higher-order operator that takes the result of reification and "feeds" it to the compile function.

```
void over_temp_rise()
{
  printf("The trigger has been evoked!\n");
}

int main (int argc, char const *argv[])
{
  int i;

  for (i = 0; i < 10; i++)
  {
    printf("iteration: %d\n", i);
    temp = temp * 1.3;
    step();
  }

  return 0;
}
```

Running "gcc copilot.c driver.c -o prop" gives a program "prop", which when executed yields the following output:

```
iteration: 0
iteration: 1
iteration: 2
iteration: 3
iteration: 4
iteration: 5
iteration: 6
iteration: 7
The trigger has been evoked!
iteration: 8
The trigger has been evoked!
iteration: 9
The trigger has been evoked!
```

3.4 QuickCheck

QuickCheck [CH00] is a library originally developed for Haskell such that given a property, it generates random inputs to test the property. We provide a similar tool for checking Copilot specifications. Currently, the tool is implemented to check the copilot-c99 back-end against the interpreter. The tool generates a random Copilot specification, and for some user-defined number of iterations, the output of the interpreter is compared against the output of the compiled

C program. The user can specify weights to influence the probability at which expressions are generated.

The copilot QuickCheck tool is installed with Copilot and assuming the binary is in the path, it is executed as

```
copilot-c99-qc
```

3.5 Verification

"Who watches the watchmen?" Nobody. For this reason, monitors in ultra-critical systems are the last line of defense and cannot fail. Here, we outline our approach to generate high-assurance monitors. First, as mentioned, the compiler is statically and strongly typed, and by implementing an eDSL, much of the infrastructure of a well-tested Haskell implementation is reused. We have described our custom QuickCheck engine. We have tested millions of randomly-generated programs between the compiler and interpreter with this approach.

Additionally, Copilot includes a tool to generate a driver to prove the equivalence between the copilot-c99 and copilot-sbv back-ends that each generate C code (similar drivers are planned for future back-ends). To use the driver, first import the following module:

```
import qualified Copilot.Tools.CBMC as C
```

(We import it using the `qualified` keyword to ensure no name space collisions.) Then in GHCI, just like with compilation, we execute

```
reify spec >>= C.genCBMC C.defaultParams
```

This generates two sets of C sources, one compiled through the copilot-c99 back-end and one through the copilot-sbv back-end. In addition, a driver (that is, a `main` function) is generated that executes the code from each back-end. The driver has the following form:

```
int main (int argc, char const *argv[])
{
  int i;

  for (i = 0; i < 10; i++)
  {
    sampleExterns();
    atm_step();
    sbv_step();
    assert(atm_i == sbv_i);
```

```
  }

  return 0;
}
```

This driver executes the two generated programs for ten iterations, which is the default value. That default can be changed; for example:

```
reify spec >>=
  C.genCBMC C.defaultParams {C.numIterations = 20}
```

The above executes the generated programs for 20 executions.

The verification depends on an open-source model-checker for C source-code originally developed at Carnegie Mellon University [CKL04]. A license for the tool is available. [6] CBMC must be downloaded and installed separately; CBMC is actively maintained at the time of writing, and is available for Windows, Linux, and Mac OS.

CBMC symbolically executes a program. With different options, CBMC can be used to check for arithmetic overflow, buffer overflow/underflow, floating-point NaN results, and division by zero. Additionally, CBMC can attempt to verify arbitrary `assert()` statements placed in the code. In our case, we wish to verify that on each iteration, for the same input variables, the two back-ends have the same state.

CBMC proves that for all possible inputs, the two programs have the same outputs for the number of iterations specified. The time-complexity of CBMC is exponential with respect to the number of iterations. Furthermore, CBMC cannot guarantee equivalence beyond the fixed number of iterations.

After generating the two sets of C source files, CBMC can be executed on the file containing the driver; for example,

```
cbmc cbmc_driver.c
```

4 Extended Example: The Boyer-Moore Majority-Vote Algorithm

In this section we demonstrate how to use Haskell as an advanced macro language on top of Copilot by implementing an algorithm for solving the voting problem in Copilot.

Reliability in mission critical software is often improved by replicating the same computations on separate hardware and by doing a vote in the end based

[6] `http://www.cprover.org/cbmc/LICENSE`. It is the user's responsibility to ensure their use conforms to the license.

```
majorityPure :: Eq a => [a] -> a
majorityPure []     = error "majorityPure: empty list!"
majorityPure (x:xs) = majorityPure' xs x 1

majorityPure' []     can _   = can
majorityPure' (x:xs) can cnt =
  let
    can' = if cnt == 0 then x else can
    cnt' = if cnt == 0 || x == can then succ cnt else pred cnt
  in
    majorityPure' xs can' cnt'
```

Figure 4: The first pass of the majority vote algorithm in Haskell.

```
aMajorityPure :: Eq a => [a] -> a -> Bool
aMajorityPure xs can = aMajorityPure' 0 xs can > length xs `div` 2

aMajorityPure' cnt []     _   = cnt
aMajorityPure' cnt (x:xs) can =
  let
    cnt' = if x == can then cnt+1 else cnt
  in
    aMajorityPure' cnt' xs can
```

Figure 5: The second pass of the majority vote algorithm in Haskell.

on the output of each system. The majority vote problem consists of determining if in a given list of votes there is a candidate that has more than half of the votes, and if so, of finding this candidate.

The Boyer-Moore Majority Vote Algorithm [MB81, Hes05] solves the problem in linear time and constant memory. It does so in two passes: The first pass chooses a candidate; and the second pass asserts that the found candidate indeed holds a majority.

Without going into details of the algorithm, the first pass can be implemented in Haskell as shown in Figure 4. The second pass, which simply checks that a candidate has more than half of the votes, is straightforward to implement and is shown in Figure 5. E.g. applying `majorityPure` on the string `AAACCBBCCCBCC` yields `C`, which `aMajorityPure` can confirm is in fact a majority.

When implementing the majority vote algorithm for Copilot, we can use reuse almost all of the code from the Haskell implementation. However, as functions in Copilot are macros that are expanded at compile time, care must be taken in order to avoid an explosion in the code size. Hence, instead of using Haskell's built-in *let*-blocks, we use explicit sharing, as described in Section 2.7.

```
majority :: (Eq a, Typed a) => [Stream a] -> Stream a
majority []     = error "majority: empty list!"
majority (x:xs) = majority' xs x 1

majority' []     can _   = can
majority' (x:xs) can cnt =
  local
    (if cnt == 0 then x else can) $
      \ can' ->
        local (if cnt == 0 || x == can then cnt+1 else cnt-1) $
          \ cnt' ->
            majority' xs can' cnt'
```

Figure 6: The first pass of the majority vote algorithm in Copilot.

```
aMajority :: (Eq a, Typed a) => [Stream a] -> Stream a -> Stream Bool
aMajority xs can = aMajority' 0 xs can > (fromIntegral (length xs) `div` 2)

aMajority' cnt []     _   = cnt
aMajority' cnt (x:xs) can =
  local
    (if x == can then cnt+1 else cnt) $
      \ cnt' ->
        aMajority' cnt' xs can
```

Figure 7: The second pass of the majority vote algorithm in Copilot.

The Copilot implementations of the first and the second pass are given in Figure 6 and Figure 7 respectively. Comparing the Haskell implementation with the Copilot implementation, we see that the code is almost identical, except for the type signatures and the explicit sharing annotations.

Further Reading

For detailed background information on Copilot we refer to [PNGW10] and [PNW11].

Acknowledgement

The authors are grateful for NASA Contract NNL08AD13T to Galois Inc. and the National Institute of Aerospace, which partially supported this work. Thanks to Lars Kuhtz, Benedetto Di Vito,

References

[BSST09] Clark Barrett, Roberto Sebastiani, Sanjit Seshia, and Cesare Tinelli. *Satisfiability Modulo Theories*, chapter 26, pages 825–885. Frontiers in Artificial Intelligence and Applications. IOS Press, 2009.

[CH00] Koen Claessen and John Hughes. QuickCheck: a lightweight tool for random testing of haskell programs. In *International Conference of Functional Programming*, pages 268–279, 2000.

[CKL04] Edmund Clarke, Daniel Kroening, and Flavio Lerda. A tool for checking ANSI-C programs. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, LNCS, pages 168–176. Springer, 2004.

[Far04] H.A. Farhat. *Digital design and computer organization*. Number v. 1 in Digital Design and Computer Organization. CRC Press, 2004.

[Gil09] Andy Gill. Type-safe observable sharing in Haskell. In *Proceedings of the 2009 ACM SIGPLAN Haskell Symposium*, Sep 2009.

[Hes05] Wim H. Hesselink. The boyer-moore majority vote algorithm, 2005.

[Jon02] Simon Peyton Jones, editor. *Haskell 98 Language and Libraries: The Revised Report*. http://haskell.org/, 2002.

[MB81] Strother J. Moore and Robert S. Boyer. MJRTY - A Fast Majority Vote Algorithm. Technical Report 1981-32, Institute for Computing Science, University of Texas, February 1981.

[PNGW10] Lee Pike, Sebastian Niller, Alwyn Goodloe, and Nis Wegmann. Copilot: A hard real-time runtime monitor. In *Proceedings of the 1st Intl. Conference on Runtime Verification*, 2010.

[PNW11] Lee Pike, Sebastian Niller, and Nis Wegmann. Runtime verification for ultra-reliable systems. In *Proceedings of the 2nd Intl. Conference on Runtime Verification*, 2011.