1 Function Summaries and User-defined Summaries

In HiFrog, *function summaries* are Craig interpolants [3]. The summaries are extracted from an unsatisfiable SMT formula of a successful verification and can be over-approximations of the actual behavior of the functions. The extracted summaries are serialized in a persistent storage so that they are available for other HiFrog runs.

User-defined function summaries are encoded in SMT-Lib2 format and use the *easy-to-read by human* nature of SMT encoding to create high-level summaries to unsupported or complicated to describe functions. User-defined summaries follows the same form of function summaries, and hence HiFrog treats function summaries and user-defined summaries in the same way when loading the serialized files and while using these summaries for the current verification task. We refer both as SMT summaries when modeled with SMT logics.

Several examples of these functions can be $isnan()$, $isinf()$ or even % in C, which have no straight-forward support in SMT. Other examples can contain more complicated functions, as trigonometric functions or `math.h` implementation of other common mathematical functions. The user-defined function summary can be described once and use later many times as needed. The summaries shall be updated only if the definition or the implementation of the function changed or if a summary refinement [1, 2] is required.

For example, Fig. 1 is a user-defined summary of an over-approximation of a Boolean expression of a property of the trigonometric functions sin and cos: $\sin^2 x + \cos^2 x = 1$.

```
(define-fun |c::nonlin#0| (
  (|c::nonlin::x!0| Real)
  (|hifrog::?fun_start| Bool)
  (|hifrog::?fun_end| Bool)
  (|c::nonlin::?retval| Real) )  Bool
  (= 1 |c::nonlin::?retval|)
)
```

Figure 1: *User-Defined function summary for the function:* $\sin^2(x) + \cos^2(x)$ (Over-approximated).

An example of a user-defined summary without approximation is shown in Fig. 2, and is a user-defined summary of a Boolean expression of a property of the trigonometric function cos: $\cos(-x) = \cos x$, where $|_c os\#0|$ is treated as uninterpreted function.

```
(define-fun |cos_neg#0| (
  (|cos_neg::a| Int)
  (|hifrog::fun_start| Bool)
  (|hifrog::fun_end| Bool)
  (|cos_neg::?retval| Int) )  Bool
    (let ((?def274  |cos_neg::?retval|))
    (let ((?def275  (= (|_cos#0| |cos_neg::a|) ?def274)))
    (let ((?def276  (= (|_cos#0| (- |cos_neg::a|)) ?def274)))
    (let ((?def277  (and ?def275 ?def276)))
  ?def277
)))))
```

Figure 2: *User-Defined function summary for the function* $\cos(-x) = \cos x$.

References

[1] Alt, L., Asadi, S., Chockler, H., Even Mendoza, K., Fedyukovich, G., Hyvärinen, A.E.J., Sharygina, N.: HiFrog: SMT-based function summarization for software verification. In: TACAS. LNCS, vol. 10206, pp. 207–213. Springer (2017)

[2] Asadi, S., Blicha, M., Fedyukovich, G., Hyvärinen, A.E.J., Even-Mendoza, K., Sharygina, N., Chockler, H.: Function summarization modulo theories. In: LPAR. EasyChair Publications (2018)

[3] Sery, O., Fedyukovich, G., Sharygina, N.: Interpolation-based Function Summaries in Bounded Model Checking. In: HVC. LNCS, vol. 7261, pp. 160–175. Springer (2012)