Synthesis from Assume-Guarantee Contracts using Skolemized Proofs of Realizability

Andreas Katis[1], Grigory Fedyukovich[2], Andrew Gacek[3], John Backes[3], Arie Gurfinkel[4], Michael W. Whalen[1]

[1] Department of Computer Science and Engineering, University of Minnesota, 200 Union Street, Minneapolis, MN 55455, USA
katis001@umn.edu, whalen@cs.umn.edu
[2] Computer Science and Engineering, University of Washington, Seattle, WA, USA
grigory@cs.washington.edu
[3] Rockwell Collins Advanced Technology Center 400 Collins Rd. NE, Cedar Rapids, IA, 52498, USA
{andrew.gacek,john.backes}@rockwellcollins.com
[4] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
agurfinkel@uwaterloo.ca

Abstract. The realizability problem in requirements engineering is to decide existence of an implementation that meets the given formal requirements. A step forward after the realizability is proven is to construct such an implementation automatically, and thus solve the problem of program synthesis. In this paper, we propose a novel approach to program synthesis guided by the proofs of realizability represented by the set of valid $\forall\exists$-formulas. In particular, we propose to extract Skolem functions witnessing the existential quantification, and to compose the Skolem functions into an implementation that is guaranteed to comply with the user-defined requirements. We implemented our approach in a tool for requirements in the form of Assume-Guarantee contracts, using the Lustre specification language. It naturally extends the realizability check by the JKind model checker. Furthermore, we developed a compiler to translate pure Skolem-containing implementations to the C programming language. For a variety of benchmark models, we test their corresponding implementations against the ones provided by the LustreV6 compiler, yielding competitive performance with hand-written implementations.

1 Introduction

Automated synthesis research is concerned with discovering efficient algorithms to construct candidate programs that are guaranteed to comply with predefined temporal specifications. This problem has been well studied for propositional specifications, especially for (subsets of) LTL [21]. More recently, the problem of synthesizing programs for richer theories has been examined, including work in *template synthesis* [40], which attempts to find programs that match

a certain shape (the template), and *inductive synthesis*, which attempts to use counterexample-based refinement to solve synthesis problems [17]. Such techniques have been widely used for stateless formulas over arithmetic domains [38]. *Functional synthesis* has also been effectively used to synthesize subcomponents of already existing partial implementations [32,33].

In this paper, we propose a new approach that can synthesize programs for arbitrary *assume/guarantee contracts* that do not have to conform to specific template shapes or temporal restrictions. The contracts are described using safety properties involving real arithmetic. Although the technique is not guaranteed to succeed or terminate, we have used it to successfully synthesize a range of programs over non-trivial contracts. It is more general than previous approaches for temporal synthesis involving theories, supporting both arbitrary safety properties rather than "stateless" properties (unlike [38]) and arbitrary shapes for synthesized programs (unlike [40]).

Our approach is built on previous work determining the *realizability* of contracts involving infinite theories such as linear integer/real arithmetic and/or uninterpreted functions [19,27]. The algorithm, explained in Section 2, uses a quantified variant of k-induction that can be checked by any SMT solver that supports quantification. Notionally, it checks whether a sequence of states satisfy the contract of depth k is sufficient to guarantee the existence of a successor state that satisfies the contract for an arbitrary input. An outer loop of the algorithm increases k until either a solution or counterexample is found.

The step from realizability to synthesis involves moving from the existence of a witness (as can be provided by an SMT solver such as Z3 or CVC4) to the witness itself. For this, the most important obstacle is the (in)ability of the SMT solver to handle higher-order quantification. Fortunately, interesting directions to solving this problem have already surfaced, either by extending an SMT solver with native synthesis capabilities [38], or by providing external algorithms that reduce the problem by efficient quantifier elimination methods [15]. Our synthesis relies on our previous implementation for realizability checking and the skolemization procedure implemented in the AE-VAL tool [15].

We combined the above ideas to create a reasonable sequential synthesis approach, which we call JSyn. It applies the realizability checker from [19] and then extracts a Skolem witness formula from the AE-VAL tool that can immediately be turned into a C program. In order to support synthesis, several changes were required to the quantifier-elimination approach to produce Skolem *functions* rather than *relations*. The main contributions of the work are therefore:

- To the best of our knowledge, the first synthesis procedure from Assume-Guarantee contracts, modulo infinite theories, usable in a broader list of applications when compared to already existing approaches.
- A framework of extracting fine-grained Skolem functions for $\forall\exists$-formulas in Linear Real Arithmetic
- A prototype tool implementing the algorithm
- An experiment demonstrating the application of the tool on various benchmark examples

This paper presents the first full exposition of the idea, which was originally proposed in a workshop paper without an implementation or experiment [28].

In Section 2, we provide the necessary background definitions that are used in our synthesis algorithm, as well as an informal proof of the algorithm's correctness. Section 3 contains the core formal notions on which the AE-VAL Skolemizer is based, as well as the adjustments that were done for it to better support the needs of this work. Section 4 provides detailed source information for each one of the important components of this work. Section 5 presents our results on using the algorithm to automatically generate leaf-level component implementations for different case studies. In Section 6 we give a brief historical background on the related research work on synthesis, and we discuss potential future work in Section 7. Finally, we conclude this paper in Section 8.

2 Synthesis from Assume-Guarantee Contracts

In this section we provide a brief background on Assume-Guarantee contracts, proceed with summarizing our earlier results on realizability checking of contracts, and finally present our program synthesis procedure.

2.1 Assume-Guarantee Contracts

One popular way to describe software requirements is through Assume-Guarantee contracts, where requirements are expressed using safety properties that are split into two categories. The *assumptions* of the contract correspond to properties that restrict the set of valid inputs a system can process, while the *guarantees* dictate how the system should behave through constraints on the outputs that are produced by the system.

For example, consider the contract with the assumption $A = \{x \neq y\}$ and the guarantee $G = \{x \leq y \implies z = \mathit{true}, x \geq y \implies z = \mathit{false}\}$, for a component with two inputs x and y and one output z. By assumption, $x \neq y$, so the implemented system should set z to true if $x < y$ and false otherwise. Determining whether an implementation can be constructed to satisfy the contract for all possible input sequences is the *realizability* problem, while automatically constructing a witness of the proof of realizability of the contract is the *program synthesis* problem. The contract (A, G) above is obviously *realizable*, and therefore an implementation can be constructed. However, if the assumption is omitted then the contract is *unrealizable*, since there is no correct value for z when $x = y$.

2.2 Formal Preliminaries

We describe a system using the disjoint sets *state* and *inputs*. Formally, an *implementation* is a *transition system* described by an initial state predicate $I(s)$ of type $\mathit{state} \rightarrow \mathit{bool}$ and by a transition relation $T(s, i, s')$ of type $\mathit{state} \rightarrow \mathit{inputs} \rightarrow \mathit{state} \rightarrow \mathit{bool}$.

An Assume-Guarantee (AG) contract can be formally defined by a set of *assumptions* and a set of *guarantees*. The *assumptions*, $A : state \rightarrow inputs \rightarrow bool$, impose constraints over the inputs which may be modal in terms of the previous state. The *guarantees* G consist of two separate subsets $G_I : state \rightarrow bool$ and $G_T : state \rightarrow inputs \rightarrow state \rightarrow bool$, where G_I defines the set of valid initial states, and G_T specifies the properties that need to be met during each new transition between two states. Note that we do not necessarily expect that a contract would be defined over all variables in the transition system, but we do not make any distinction between internal state variables and outputs in the formalism. This way, we can use state variables to (in some cases) simplify specification of guarantees.

2.3 Realizability of Contracts

The synthesis algorithm proposed in this paper is built on top of our realizability algorithm originally presented in [19]. Using the formal foundations described in Sect. 2.2, the problem of realizability is expressed using the notion of a state being *extendable*:

Definition 1 (One-step extension). *A state s is extendable after n steps, denoted $Extend_n(s)$, if any valid path of length $n-1$ starting from s can be extended in response to any valid input.*

$$\begin{aligned} Extend_n(s) \triangleq \forall i_1, s_1, \ldots, i_n, s_n.\\ A(s, i_1) \wedge G_T(s, i_1, s_1) \wedge \cdots \wedge A(s_{n-1}, i_n) \wedge G_T(s_{n-1}, i_n, s_n) \implies\\ \forall i.\ A(s_n, i) \implies \exists s'.\ G_T(s_n, i, s') \end{aligned}$$

The algorithm for realizability uses Def. 1 in two separate checks that correspond to the two traditional cases exercised in k-induction. Initially, we prove that the set of initial states is not empty, which is done by checking for the existence of at least one state that satisfies G_I. For the *BaseCheck*, we ensure that all initial states are extendable for any path of length $k < n$, while the inductive step of *ExtendCheck* tries to prove that all valid states are extendable for any path of length n. Therefore, we attempt to find the smallest n, for which the two following $\forall\exists$-formulas are valid:

$$BaseCheck(n) \triangleq \forall k < n.(\forall s.G_I(s) \implies Extend_k(s)) \tag{1}$$

$$ExtendCheck(n) \triangleq \forall s.Extend_n(s) \tag{2}$$

The realizability checking algorithm has been used to effectively find cases where the traditional consistency check (i.e. the existence of an assignment to the input variables for which the output variables satisfy the contract) failed to detect conflicts between stated requirements in case studies of different complexity and importance. It has also been formally verified using the Coq proof assistant in terms of its soundness, for the cases where it reports that a contract is realizable [27].

Algorithm 1: Synthesis from AG-Contracts

Input: AG-Contract in Lustre, (A, G)
Output: Result $\in \{\text{REALIZABLE}, \text{UNREALIZABLE}\}$, Skolem list *Skolems*

```
1  Skolems ← ∅;
2  for (i ← 0; true; i ← i + 1) do
3  |  BaseResult ← AE-VAL(BaseCheck_k(i));
4  |  ExtendResult ← AE-VAL(ExtendCheck(i));
5  |  if (isInvalid(BaseResult)) then
6  |  |  return unrealizable, ∅;
7  |  Skolems.Add(BaseResult.Skolem);
8  |  if (isValid(ExtendResult)) then
9  |  |  Skolems.Add(ExtendResult.Skolem);
10 |  |  return realizable, Skolems;
```

Template 1: Structure of implementations

```
1  assign_G_I_witness();
2  read_inputs();
3  Skolems[0]();
4  ...
5  read_inputs();
6  Skolems[k-2]();
7  forever do
8  |  read_inputs();
9  |  if k = 0 then
10 |  |  Skolems[1]();
11 |  else
12 |  |  Skolems[k-1]();
13 |  end
14 |  update_history();
```

2.4 Program Synthesis from Proofs of Realizability

An important outcome of our previous work on realizability is that it can be further used for solving the more complex problem of *program synthesis*. That is, we should be able to automatically derive implementations from the proof of a contract's realizability.

The idea behind our approach to solving the synthesis problem is simple and elegant. Consider checks (1) and (2) that are used in the realizability checking algorithm. Both checks require that the reachable states explored are extendable using Def. 1. The key insights are then 1) we can start with a arbitrary state in G_I since it is non-empty, 2) we can use witnesses from the proofs of $Extend_k(s)$ in *BaseCheck* to create a valid path of length $n-1$, and 3) we can extend that path to arbitrary length by repeatedly using the witness of the proof of $Extend_n(s)$ in $ExtendCheck(n)$.

In first order logic, witnesses for valid $\forall\exists$-formulas are represented by Skolem functions. Intuitively, a Skolem function expresses a connection between all universally quantified variables in the left-hand side of the $\forall\exists$-formulas (1) and (2) and the existentially quantified variable s' within *Extend* on the right-hand side. Our algorithm uses the AE-VAL tool, detailed in Sect. 3, to generate such Skolem functions from the validity of (1) and (2).

Alg. 1 provides a summary of the synthesis procedure. The algorithm repeatedly proves $BaseCheck_k(i) \triangleq \forall s.G_I(s) \implies Extend_k(s)$ and accumulates the resulting Skolem functions. If $BaseCheck_k(i)$ ever fails, we know $BaseCheck(i)$ would also fail and so the system is unrealizable. At the same time, the algorithm tries to prove $ExtendCheck(i)$. As soon as the inductive step of $ExtendCheck(i)$ passes, we have a complete k-inductive proof stating that the contract is realizable. We then complete our synthesis procedure by generating a Skolem function that corresponds to the inductive step, and return the list of the Skolem functions.

Given a list of Skolem functions, it remains to plug them into an implementation skeleton as shown in Template 14. Combination of Lustre models and k-inductive proofs allow the properties in the model to manipulate the values of variables up to $k-1$ steps in the past. Thus, the first step of an implementation

(method ASSIGN_G_I_WITNESS()) is creating an array for each state variable up to k, where k is the depth at which a solution to Alg. 1 has been delivered. In each array, the i-th element, with $0 \leq i \leq k-1$, corresponds to the value assigned to the variable after the call to i-th Skolem function. As such, the first $k-1$ elements of each array correspond to the $k-1$ Skolem functions produced by the *BaseCheck* process, while the last element is used by the Skolem function generated from the formula corresponding to the *ExtendCheck* process. For the special case of $k = 0$, we still use both the base and the inductive step Skolem functions. This is to ensure that we capture cases where the initial state guarantees G_I differ from the transitional guarantees G_T.

The template then uses the Skolem functions generated by AE-VAL for each of the *BaseCheck* instances to describe the initial behavior of the implementation up to depth k. This process starts from the memory-free description of the initial state (G_I). There are two "helper" operations: UPDATE_HISTORY() shifts each element in the arrays one position forward (the 0-th value is simply forgotten), and READ_INPUTS() reads the current values of inputs into the i-th element of the input variable arrays, where i represents the i-th step of the process. Once the history is entirely initialized using the *BaseCheck* witness values, we add the Skolem function that represents the witness for the *ExtendCheck* instance to describe the recurrent behavior of the implementation, i.e., the next value of outputs in each iteration in the infinite loop.

Finally, to further strengthen our claims regarding the correctness of the algorithm, we wrote machine-checked proofs regarding the validity of $BaseCheck(n)$ and $ExtendCheck(n)$, when Skolem functions are used as witness states towards synthesizing the implementations. The entirety of the models explored in this paper only involved proofs of realizability of length k equal to 0 or 1[5]. As such, we limited our proofs of soundness to these two specific cases. We hope to extend the proofs to capture any arbitrary k as part of our future work. The theorems were written and proved using the Coq proof assistant [41].

Theorem 1 (Bounded Soundness of BaseCheck and ExtendCheck using Skolem Functions). *Let* $BaseCheck_{S(s_n,i,s')}(n)$ *and* $ExtendCheck_{S(s_n,i,s')}(n)$, $n \in 0, 1$ *be the valid variations of the corresponding formulas* $BaseCheck(n)$ *and* $ExtendCheck(n)$*, where the existentially quantified part* $\exists s'.\ G_T(s_n, i, s')$ *has been substituted with a witnessing Skolem function* $S(s_n, i, s')$*. We have that:*

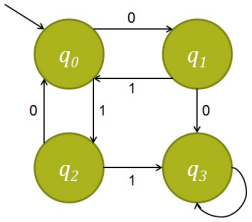
- $\forall(A, G_I, GT).BaseCheck(n) \Rightarrow BaseCheck_{S(s_n,i,s')}(n)$
- $\forall(A, G_I, GT).ExtendCheck(n) \Rightarrow ExtendCheck_{S(s_n,i,s')}(n)$

Proof. The proof uses the definition $Extend_n(s)$ of an extendable state, after replacing the next-step states with corresponding Skolem functions. From there, the proof of the two implications is straightforward. □

2.5 Running Example

Fig. 1 shows an example contract as specified in Lustre. There are two unassigned variables `x` and `state`. The `--%REALIZABLE` statement specifies that `x` is a

[5] The proofs can be found at `https://github.com/andrewkatis/Coq`.




```
node top(x : bool; state: int) returns (  );
var
  bias : int;
  guarantee1, guarantee2, guarantee3,
  guarantee4, guarantee5, guarantee_all : bool;
  bias_max : bool;
let
  bias = 0 -> (if x then 1 else -1) + pre(bias);
  bias_max = false ->
        (bias >= 2 or bias <= -2) or pre(bias_max);
  guarantee1 = (state = 0 => (bias = 0));
  guarantee2 = true ->
          (pre(state = 0) and x) => state = 2;
  guarantee3 = true ->
          (pre(state = 0) and not x) => state = 1;
  guarantee4 = bias_max => state = 3;
  guarantee5 = state = 0 or state = 1 or state = 2 or
                  state = 3;
  guarantee_all = guarantee1 and guarantee2 and
                  guarantee3 and guarantee4 and
                  guarantee5;
  --%PROPERTY guarantee_all;
  --%REALIZABLE x;
tel;
```

Fig. 1: Automaton and Requirements for running example

system input, and by its absence, that `state` is a system output. There are five guarantees: `guarantee2` and `guarantee3` are used to indirectly describe some possible transitions in the automaton; `guarantee5` specifies the range of values of variable `state`; `guarantee1` and `guarantee4` are the requirements with respect to two local variables `bias` and `bias_max` where `bias` calculates the number of successive ones or zeros read by the automaton, and `bias_max` is used as a flag to indicate that at least two zeros or two ones have been read in a row.

The realizability check on this example succeeds with a k-inductive proof of length $k = 1$. The two corresponding $\forall\exists$-formulas ($k = 0$ for the base check and $k = 1$ for the inductive check) are valid, and thus AE-VAL extracts two witnessing Skolem functions that effectively describe assignments to the local variables of the specification, as well as to `state` (see Appendix A for the particular formulas).

The Skolem functions are used to construct the final implementation following the outline provided in Template 14. It is 144 lines of code, and due to the space constraints we do not present it here[6]. The main idea is to redefine each variable in the model as an array of size equal to k and to use the k-th element of each array as the corresponding output of the call to k-th Skolem function. After this initialization process, we use an infinite loop to assign new values to the element corresponding to the last Skolem function, to cover the inductive step of the original proof.

Recall that the user-defined model specifies explicitly two transitions (via `guarantee2` and `guarantee3`) only, while the set of implicitly defined transitions (via `guarantee1` and `guarantee4`) is incomplete. For example, the model does not specify an incoming transition to (`state = 0`). In contrast, the synthesized implementation turns all implicit transitions into explicit ones which makes them able to execute, and furthermore adds the missing ones (e.g., from `state = 1` to `state = 0`).

[6] The implementation for the example is available at `https://arxiv.org/abs/1610.05867`

Algorithm 2: AE-VAL$\Big(S(\vec{x}), \exists \vec{y}\,.\,T(\vec{x},\vec{y})\Big)$, cf. [16]

Input: $S(\vec{x}), \exists \vec{y}\,.\,T(\vec{x},\vec{y})$.
Output: Return value $\in \{\text{VALID}, \text{INVALID}\}$ of $S(\vec{x}) \implies \exists \vec{y}\,.\,T(\vec{x},\vec{y})$, Skolem.
Data: models $\{m_i\}$, MBPs $\{T_i(\vec{x})\}$, local Skolems $\{\phi_i(\vec{x},\vec{y})\}$.

1 SmtAdd($S(\vec{x})$);
2 **for** ($i \leftarrow 0$; **true**; $i \leftarrow i+1$) **do**
3 **if** (isUnsat(SmtSolve())) **then return** VALID, $Sk_{\vec{y}}(\vec{x},\vec{y})$ from (3);
4 SmtPush(); SmtAdd($T(\vec{x},\vec{y})$);
5 **if** (isUnsat(SmtSolve())) **then return** INVALID, $\varnothing$;
6 $m_i \leftarrow$ SmtGetModel();
7 $(T_i, \phi_i(\vec{x},\vec{y})) \leftarrow$ GetMBP$(\vec{y}, m_i, T(\vec{x},\vec{y}))$;
8 SmtPop(); SmtAdd($\neg T_i$);

3 Witnessing existential quantifiers with AE-VAL

In this section, we briefly describe the prior work on AE-VAL to be able (in Sect. 3.2) to present the key contributions on delivering Skolem functions appropriate for the program synthesis from proofs of realizability.

3.1 Validity and Skolem extraction

Skolemization (i.e., introducing Skolem functions) is a well-known technique for removing existential quantifiers in first order formulas. Given a formula $\exists y\,.\,\psi(\vec{x}, y)$, a *Skolem function* for y, $sk_y(\vec{x})$ is a function such that $\exists y\,.\,\psi(\vec{x}, y) \iff \psi(\vec{x}, sk_y(\vec{x}))$. We generalize the definition of a Skolem function for the case of a vector of existentially quantified variables $\vec{y}$, by relaxing the relationships between elements of $\vec{x}$ and $\vec{y}$. Given a formula $\exists \vec{y}\,.\,\Psi(\vec{x},\vec{y})$, a *Skolem relation* for $\vec{y}$ is a relation $Sk_{\vec{y}}(\vec{x},\vec{y})$ such that 1) $Sk_{\vec{y}}(\vec{x},\vec{y}) \implies \Psi(\vec{x},\vec{y})$ and 2) $\exists \vec{y}\,.\,\Psi(\vec{x},\vec{y}) \iff Sk_{\vec{y}}(\vec{x},\vec{y})$.

The algorithm AE-VAL for deciding validity and Skolem extraction assumes that a formula Ψ can be transformed into the form $\exists \vec{y}\,.\,\Psi(\vec{x},\vec{y}) \equiv S(\vec{x}) \implies \exists \vec{y}\,.\,T(\vec{x},\vec{y})$, where $S(\vec{x})$ has only existential quantifiers, and $T(\vec{x},\vec{y})$ is quantifier-free. To decide validity of a $\forall\exists$-formula, AE-VAL partitions the formula, and searches for a witnessing local Skolem relation of each partition. AE-VAL iteratively constructs (line 7) a set of Model-Based Projections (MBPs): $T_i(\vec{x})$, such that (a) for each i, $T_i(\vec{x}) \implies \exists \vec{y}\,.\,T(\vec{x},\vec{y})$, and (b) $S(\vec{x}) \implies \bigvee_i T_i(\vec{x})$. Each MBP $T_i(\vec{x})$ is connected with the local Skolem $\phi_i(\vec{x},\vec{y})$, such that $\phi_i(\vec{x},\vec{y}) \implies (T_{\vec{y}_i}(\vec{x}) \implies T(\vec{x},\vec{y}))$. AE-VAL relies on external procedure [31,12] to obtain MBPs that is based on Loos-Weispfenning quantifier elimination [34]. While the pseudocode of AE-VAL is shown in Alg. 2, we refer the reader to [16] for more detail.

A Skolem relation $Sk_{\vec{y}}(\vec{x},\vec{y})$ by AE-VAL maps each model of $S(\vec{x})$ to a corresponding model of $T(\vec{x},\vec{y})$. Intuitively, ϕ_i maps each model of $S \wedge T_i$ to a model of T. Thus, in order to define the Skolem relation $Sk_{\vec{y}}(\vec{x},\vec{y})$ it is enough

Algorithm 3: ExtractSkolemFunction$(y_j, \phi(\vec{x}, \vec{y}))$

Input: $y_j \in \vec{y}$, local Skolem relation $\phi(\vec{x}, \vec{y}) = \bigwedge_{y_j \in \vec{y}}(\psi_j(\vec{x}, y_j, \ldots, y_n))$, Skolem functions $y_{j+1} = f_{j+1}(\vec{x}), \ldots, y_n = f_n(\vec{x})$.
Data: Factored formula $\pi_j(\vec{x}, y_j) = L_{\pi_j} \wedge U_{\pi_j} \wedge E_{\pi_j} \wedge N_{\pi_j}$.
Output: Local Skolem function $y_j = f_j(\vec{x})$.

1 **for** $(i \leftarrow n; i > j; i \leftarrow i - 1)$ **do**
2 $\quad \psi_j(\vec{x}, y_j, \ldots, y_n) \leftarrow$ Substitute$(\psi_j(\vec{x}, y_j, \ldots, y_n), y_i, f_i(\vec{x}))$;
3 $\pi_j(\vec{x}, y_j) \leftarrow \psi_j(\vec{x}, y_j, \ldots, y_n)$;
4 **if** $(E_{\pi_j} \neq \varnothing)$ **then return** E_{π_j};
5 $\pi_j(\vec{x}, y_j) \leftarrow$ Merge$(L_{\pi_j}, MAX, \pi_j(\vec{x}, y_j))$;
6 $\pi_j(\vec{x}, y_j) \leftarrow$ Merge$(U_{\pi_j}, MIN, \pi_j(\vec{x}, y_j))$;
7 **if** $(N_{\pi_j} = \varnothing)$ **then**
8 $\quad$ **if** $(L_{\pi_j} \neq \varnothing \wedge U_{\pi_j} \neq \varnothing)$ **then return** Rewrite$(L_{\pi_j} \wedge U_{\pi_j}, MID, \pi_j(\vec{x}, y_j))$;
9 $\quad$ **if** $(L_{\pi_j} = \varnothing)$ **then return** Rewrite$(U_{\pi_j}, LT, \pi_j(\vec{x}, y_j))$;
10 $\quad$ **if** $(U_{\pi_j} = \varnothing)$ **then return** Rewrite$(L_{\pi_j}, GT, \pi_j(\vec{x}, y_j))$;
11 **else return** Rewrite$(L_{\pi_j} \wedge U_{\pi_j} \wedge N_{\pi_j}, FMID, \pi_j(\vec{x}, y_j))$;

to match each ϕ_i against the corresponding T_i:

$$Sk_{\vec{y}}(\vec{x}, \vec{y}) \equiv \begin{cases} \phi_1(\vec{x}, \vec{y}) & \text{if } T_1(\vec{x}) \\ \phi_2(\vec{x}, \vec{y}) & \text{else if } T_2(\vec{x}) \\ \cdots & \text{else } \cdots \\ \phi_n(\vec{x}, \vec{y}) & \text{else } T_n(\vec{x}) \end{cases} \tag{3}$$

3.2 Refining Skolem Relations into Skolem Functions

In low-level, AE-VAL constructs each ϕ_i for (3) from the substitutions made in T to produce T_i. Furthermore, each MBP in AE-VAL is constructed iteratively for each variable $y_j \in \vec{y}$. Thus, y_j may depend on the variables of $y_{j+1}, \ldots, y_n$ that are still not eliminated in the current iteration j.

Inequalities in a Skolem relation are the enemies of program synthesis. Indeed, the final implementation should contain assignments to each existentially quantified variable, which for the current algorithm is difficult to get. The Skolem relation provided by AE-VAL should be post-processed to get rid of inequalities. We formalize this procedure as finding a Skolem function $f_j(\vec{x})$ for each $y_j \in \vec{y}$, such that $(y_j = f_j(\vec{x})) \implies \exists y_{j+1}, \ldots, y_n \,.\, \psi_j(\vec{x}, y_j, \ldots, y_n)$.

The key idea is presented in Alg. 3. The algorithm is applied separately for each $y_j \in \vec{y}$, starting from y_n to y_1. That is, for iteration j, the previous runs of the algorithm already delivered Skolem functions $f_{j+1}(\vec{x}), \ldots, f_n(\vec{x})$ for variables $y_{j+1}, \ldots, y_n$. Thus, the first step of the algorithm is to substitute each appearance of variables $y_{j+1}, \ldots, y_n$ in ψ_j by $f_n(\vec{x}), \ldots, f_{j+1}(\vec{x})$.

Once formula $\psi_j(\vec{x}, y_j, \ldots, y_n)$ is rewritten to form $\pi_j(\vec{x}, y_j)$ (line 3), the algorithm starts looking for a function $f_j(\vec{x})$, such that $y_j = f_j(\vec{x})$. In other

words, it aims at constructing a graph of a function that is embedded in a relation.

Definition 2. *Given a variable y_j, a relation $\pi_j(\vec{x}, y_j)$, and a set $C(\pi_j)$ of linear combinations over $\vec{x}$ appeared in $\pi_j(\vec{x}, y_j)$, let us denote the following groups of conjuncts, π_j is composed from:*

$$L_{\pi_j} \triangleq \bigwedge_{l \in C(\pi_j)} (y_j > l(\vec{x})) \quad U_{\pi_j} \triangleq \bigwedge_{u \in C(\pi_j)} (y_j < u(\vec{x})) \quad M_{\pi_j} \triangleq \bigwedge_{l \in C(\pi_j)} (y_j \geq l(\vec{x}))$$

$$V_{\pi_j} \triangleq \bigwedge_{u \in C(\pi_j)} (y_j \leq u(\vec{x})) \quad E_{\pi_j} \triangleq \bigwedge_{e \in C(\pi_j)} (y_j = e(\vec{x})) \quad N_{\pi_j} \triangleq \bigwedge_{h \in C(\pi_j)} (y_j \neq h(\vec{x}))$$

In the rest of the section, we present several primitives needed to construct $y_j = f_j(\vec{x})$ out of $\pi_j(\vec{x}, y_j)$. For simplicity, we omit some straightforward details on dealing with non-strict inequalities consisting in M_{π_j} and V_{π_j} since they are similar strict inequalities consisting in L_{π_j} and U_{π_j}. Thus, without loss of generality, we assume that M_{π_j} and V_{π_j} are empty.

Lemma 1. *After all substitutions at line 3 of Alg. 3, each $\psi_j(\vec{x}, y_j, \ldots, y_n)$ is a conjunction of the form $L_{\pi_j} \wedge U_{\pi_j} \wedge M_{\pi_j} \wedge V_{\pi_j} \wedge E_{\pi_j} \wedge N_{\pi_j}$.*

Proof. Follows directly from the MBP algorithm at [31]. □

The procedure to extract $y_j = f_j(\vec{x})$ out of $\pi_j(\vec{x}, y_j)$ proceeds by analyzing terms in L_{π_j}, U_{π_j}, M_{π_j}, V_{π_j}, E_{π_j} and N_{π_j}. If there is at least one conjunct $(y_j = e(\vec{x})) \in E_{\pi_j}$ then $(y_j = e(\vec{x}))$ itself is a Skolem function. Otherwise, the algorithm creates it from the following primitives.

Definition 3. *Let $l(\vec{x})$ and $u(\vec{x})$ be two linear terms, then operators MAX, MIN, MID, LT, GT are defined as follows:*

$$MAX(l,u)(\vec{x}) \triangleq ite(l(\vec{x}) < u(\vec{x}), u(\vec{x}), l(\vec{x})) \quad MIN(l,u)(\vec{x}) \triangleq ite(l(\vec{x}) < u(\vec{x}), l(\vec{x}), u(\vec{x}))$$

$$LT(u)(\vec{x}) \triangleq u(\vec{x}) - 1 \qquad GT(l)(\vec{x}) \triangleq l(\vec{x}) + 1$$

$$MID(l,u)(\vec{x}) \triangleq \frac{l(\vec{x}) + u(\vec{x})}{2}$$

Lemma 2. *If L_{π_j} consists of $n > 1$ conjuncts then it is equivalent to $y_j > MAX(l_1, MAX(l_2, \ldots MAX(l_{n-1}, l_n)))(\vec{x})$. If U_{π_j} consists of $n > 1$ conjuncts then it is equivalent to $y_j < MIN(u_1, MIN(u_2, \ldots MIN(u_{n-1}, u_n)))(\vec{x})$.*

This primitive is applied (lines 5-6) in order to reduce the size of L_{π_j} and U_{π_j}. Thus, from this point on, with out loss of generality, we assume that each L_{π_j} and U_{π_j} have at most one conjunct.

Lemma 3. *If each of L_{π_j} and U_{π_j} consist of one conjunct each, and E_{π_j} and N_{π_j} are empty then the Skolem can be rewritten into $y_j = MID(l,u)(\vec{x})$.*

This primitive is applied (line 8) in case if the graph of a Skolem function can be constructed exactly in the middle of the two graphs for the lower- and the upper boundaries for the Skolem relation. Otherwise, if some of the boundaries are missing, but still N_{π_j} is empty (lines 9-10) the following primitive is applied:

Lemma 4. *If L_{π_j} consists of one conjunct and the rest of U_{π_j}, E_{π_j} and N_{π_j} are empty then the Skolem can be rewritten into $y_j = GT(l)(\vec{x})$. If U_{π_j} consists of one conjunct and the rest of L_{π_j}, E_{π_j} and N_{π_j} are empty then the Skolem can be rewritten into $y_j = LT(l)(\vec{x})$.*

Finally, the algorithm handles the cases when N_{π_j} is not empty. For this, we introduce another operator *FMID* that for the given l, u and h and each $\vec{x}$ outputs either $MID(l,u)$ or $MID(l, MID(l,u))$ in case if $MID(l,u)$ is equal to h.

Lemma 5. *If each of L_{π_j},U_{π_j} and N_{π_j} consist of one conjunct and E_{π_j} and N_{π_j} are empty then the Skolem can be rewritten into $y_j = FMID(l,u,h)(\vec{x})$, where*

$$FMID(l,u,h)(\vec{x}) \triangleq ite\Big(MID(l,u)(\vec{x}) = h(\vec{x}),\\ MID\big(l, MID(l,u)\big)(\vec{x}),\ MID(l,u)(\vec{x})\Big)$$

For bigger number of conjuncts of N_{π_j}, the Skolem gets rewritten in a similar way recursively.

Lemma 6. *If each of L_{π_j} and N_{π_j} consist of one conjunct, and E_{π_j} and U_{π_j} are empty then the Skolem can be rewritten into $y_j = FMID(l, GT(l))(\vec{x})$. If each of U_{π_j}, N_{π_j} consist of one conjunct, and the rest of M_{π_j},V_{π_j}, E_{π_j} and L_{π_j} are empty then the Skolem can be rewritten into $y_j = FMID(LT(u), u)(\vec{x})$.*

Theorem 2 (Soundness). *Iterative application of Alg. 3 to all variables $y_n, \ldots, y_1$ returns a local Skolem function to be used in* (3).

Proof. Follows from the case analysis that applies the lemmas above. □

4 Implementation

We develop JSyn, our synthesis algorithm on top of JKind [18], a Java implementation of the KIND model checker [22]. Each model is described using the Lustre Specification language, which is used as an intermediate language to formally verify contracts in the Assume-Guarantee Reasoning (AGREE) framework [9]. Internally, JKind uses two parallel engines (for *BaseCheck* and *ExtendCheck*) in order to construct a k-inductive proof for the property of interest. The first order formulas that are being constructed are then fed to the Z3 SMT solver [11] which provides state of the art support for reasoning over quantifiers and incremental search.

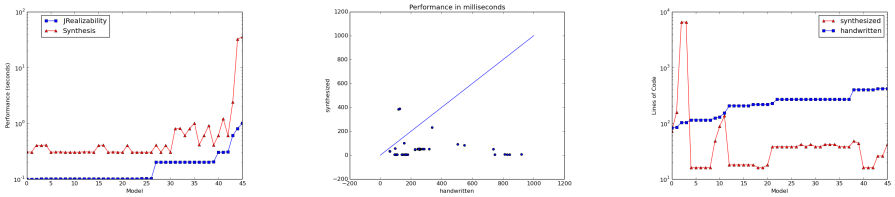
For all valid $\forall\exists$-formulas, JSyn proceeds to construct a list of Skolem functions using the AE-VAL Skolemizer. AE-VAL uses LRA as a background logic,

and thus casts all numeric variables to reals and provides the Skolem relation over reals as well.[7] In future work, we plan to enhance AE-VAL for Linear Integer Arithmetic (LIA) to soundly support Skolem relation over integers.

The final step of our implementation involved the creation of a specific purpose translation tool, which we currently call SMTLib2C[8]. The list of the Skolem functions is given as an input to the compiler, which in turn uses them to generate implementations in the C language. Note that during this translation process, real variables in Skolem functions are being defined as floats in C. This might cause some overflow errors in the final implementation. Improving on this is our primary goal in future work.

5 Experimental Results

We synthesized implementations for 46 Lustre models[9] [23], including the running example from Fig. 1. The original models already contained an implementation, which provided us with a complete test benchmark suite, since we were able to compare the synthesized implementations to handwritten programs. We compared the C implementations by JSyn against the original models, after they had been translated to C using the LustreV6 compiler [26].



(a) (b) (c)

Fig. 2: Experimental results

Fig. 2a shows the overhead of synthesis by JSyn comparing to the realizability checking by JKind. It is at expected levels for the majority of the models. Fig. 2b provides a scatter plot of the results of our experiments in terms of the performance of the synthesized programs against the original, handwritten implementations. Each dot in the scatter plot represents a pair of running times (x - the handwritten program, y - synthesized one) of the 46 models. For the two most complex models in the benchmark suite, the synthesized implementations

[7] For realizability checks over Linear Integer and Real Arithmetic (LIRA), JKind has an option to use Z3 directly.

[8] The source code is available at `https://github.com/andrewkatis/SMTLib2C`

[9] The models are part of a larger collection that can be found at https://tinyurl.com/gt4geqz

underperform when compared to the programs generated by LustreV6. As the level of complexity decreases, we notice that both implementations share similar performance levels, and for the most trivial models in the experiment set, the synthesized programs perform better with a noticeable gap. We attribute these results mainly due to the simplicity of the requirements expressed in the majority of the models, as all of them were proved realizable for $k = 0$ by JKind, except for the running example, which was proved for $k = 1$. It is important at this point to recall the fact that the syntesized implementations are not equivalent to the handwritten versions, in a similar fashion to the example used in Section 2.5

Fig. 2c provides another interesting, as well as important metric in our experiments, which is the lines of code in each pair of implementations. Here, we can see the direct effect of the specification complexity to the size of the Skolem functions generated by AE-VAL. Two of the three synthesized programs are also the ones that underperformed their handwritten counterparts in terms of time. Since the majority of the models contained simple requirements, the overall size of the synthesized implementation remained well below LustreV6-programs.

6 Related Work

Research in the field of program synthesis attributes its origins in the 1970s, when Zohar Manna and Richard Waldinger first introduced a synthesis procedure using theorem proving. [35]. Almost two decades later, Amir Pnueli and Roni Rosner were the first to propose a way to synthesize implementations for temporal specifications [37]. This work also involved the first formal definition of a reactive system's realizability (or implementability) and introduces a *Skolem paradigm* on which we heavily rely in this work.

Since then, a vast variety of techniques have been developed. Efficient algorithms were proposed for subsets of propositional LTL [29,43,14,7] simple LTL formulas [4,24,42], as well as other temporal logics [2,36,25], such as SIS [1]. Component-based approaches have also been explored in [6,10].

Sumit Gulwani in 2010 published a survey on which he discribed the potential future directions of program synthesis research [21]. The approaches that have been proposed are many, and differ on many aspects, either in terms of the specifications that are being exercised, or the reasoning behind the synthesis algorithm itself. Template-based synthesis [40] is focused on the exploration of programs that satisfy a specification that is refined after each iteration, following the basic principles of deductive synthesis. Inductive synthesis is an active area of research where the main goal is the generation of an inductive invariant that can be used to describe the space of programs that are guaranteed to satisfy the given specification [17]. This idea is mainly supported by the use of SMT solvers to guide the invariant refinement through traces that violate the requirements, known as counterexamples. Recently published work on extending SMT solvers with counterexample-guided synthesis shows that they can eventually be used as an alternative to solving the problem under certain domains of arithmetic [38]. Reactive synthesis has also been explored in the context involving propositional

formulas for safety specifications [3]. Finally, functional synthesis is used in applications where only a partial implementation exists, and the user needs an automated way to complete the missing parts of the program [30].

A rather important contribution in the area is the recently published work by Leonid Ryzhyk and Adam Walker [39], where they share their experience in developing and using a reactive synthesis tool for controllers in an industrial environment. While the authors emphasize that the research on program synthesis is still at a very early stage for the technique to be essential to industrial applications, they note its potential advantages in terms of improving the overall development cycle of software.

To the best of our knowledge our work is the first complete attempt on providing a synthesis algorithm for an assume-guarantee framework, using infinite theories. We take advantage of a sophisticated solver that is able to reason about the validity of the intermediate formulas that construct a k-inductive proof, as well as provide witnesses for these formulas through the use of Skolem functions. The ability to express contracts that support ideas from many categories of specifications, such as template-based and temporal properties, increases the potential applicability of this work to multiple subareas on synthesis research.

7 Future Work

The meaningful results of our work so far on the synthesis from Assume-Guarantee contracts have also provided a solid ground towards extending and improving the involved algorithms in the future. A particularly important milestone is to eventually switch to a more efficient algorithm, where we endorse the core idea of Property Directed Reachability [13,5], using efficient ways to further enhance the algorithm's performance through the use of implicit abstractions [8] to further reduce the search space of the algorithm. This will also help our original work on realizability checking, by improving the unsoundness of our unrealizable results. Another promising idea here is the use of Inductive Validity Cores (IVCs) [20], whose main purpose is to effectively pinpoint the absolutely necessary model elements in a generated proof. We can potentially use the information provided by IVCs as a preprocessing tool to reduce the size of the original specification, and hopefully the complexity of the realizability proof. Of course, a few optimizations can be further implemented in terms of AE-VAL's specific support on proofs of realizability and finally, a very important subject is the further improvement of the compiler that we created to translate the Skolem functions into C implementations, by introducing optimizations like common subexpression elimination.

Another important goal is that of supporting additional theories, and primarily LIA, which is currently not fully supported by AE-VAL's model based projection technique. Finally, another potential optimization that could effectively reduce the algorithm's complexity is the further simplification of the transition relation that we are currently using, by reducing its complicated form through the mapping of common subexpressions on different conditional branches. This will also have a direct impact on the skolem relations retrieved by AE-VAL,

reducing their individual size and improving, thus, the final implementation in terms of readability as well as its usability as an intermediate representation to the preferred target language.

8 Conclusion

In this paper, we contributed the approach to program synthesis guided by the proofs of realizability of Assume-Guarantee contracts. Our approach is based on the notion of realizability, the proving of which requires k-induction-based reasoning to decide validity of a set of $\forall\exists$-formulas. Whenever a contract is proven realizable, our approach employs the Skolemization procedure and extracts a fine-grained witness to the realizability. The Skolem functions are finally encoded into a desirable implementation. We implemented the technique in JKind and evaluated for the set of Lustre models of different complexity. The experimental results provided fruitful conclusions on the overall efficacy of the the approach.

Acknowledgments

This work was funded by DARPA and AFRL under contract 4504789784 (Secure Mathematically-Assured Composition of Control Models), and by NASA under contract NNA13AA21C (Compositional Verification of Flight Critical Systems), and by NSF under grant CNS-1035715 (Assuring the safety, security, and reliability of medical device cyber physical systems).

References

1. Aziz, A., Balarin, F., Braton, R., Sangiovanni-Vincentelli, A.: Sequential Synthesis using SIS. Proceedings of the 1995 IEEE/ACM International Conference on Computer-Aided Design (ICCAD'95) pp. 612–617 (1995)
2. Beneš, N., Černá, I., Štefaňák, F.: Factorization for component-interaction automata. In: SOFSEM 2012: Theory and Practice of Computer Science, pp. 554–565. Springer (2012)
3. Bloem, R., Egly, U., Klampfl, P., Könighofer, R., Lonsing, F., Seidl, M.: Satisfiability-based methods for reactive synthesis from safety specifications. arXiv preprint arXiv:1604.06204 (2016)
4. Bohy, A., BruyÃĺre, V., Filiot, E., Jin, N., Raskin, J.F.: Acacia+, a tool for LTL Synthesis. Proceedings of the 24th International Conference on Computer Aided Verification (CAV'12) pp. 652–657 (2012)
5. Bradley, A.: SAT-based model checking without unrolling. VMCAI (2011)
6. Chatterjee, K., Henzinger, T.A.: Assume-Guarantee Synthesis. Proceedings of the 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'07) pp. 261–275 (2007)
7. Cheng, C.H., Hamza, Y., Ruess, H.: Structural synthesis for gxw specifications. arXiv preprint arXiv:1605.01153 (2016)

8. Cimatti, A., Griggio, A., Mover, S., Tonetta, S.: Ic3 modulo theories via implicit predicate abstraction. In: Tools and Algorithms for the Construction and Analysis of Systems, pp. 46–61. Springer (2014)
9. Cofer, D.D., Gacek, A., Miller, S.P., Whalen, M.W., LaValley, B., Sha, L.: Compositional verification of architectural models. In: Goodloe, A.E., Person, S. (eds.) Proceedings of the 4th NASA Formal Methods Symposium (NFM 2012). vol. 7226, pp. 126–140. Springer-Verlag, Berlin, Heidelberg (April 2012)
10. Damm, W., Finkbeiner, B., Rakow, A.: What you really need to know about your neighbor
11. De Moura, L., Bjørner, N.: Z3: An efficient SMT solver. In: Tools and Algorithms for the Construction and Analysis of Systems, pp. 337–340. Springer (2008)
12. Dutertre, B.: Solving Exists/Forall Problems With Yices. In: SMT Workshop (2015), extended abstract
13. Een, N., Mishchenko, A., Brayton, R.: Efficient implementation of property directed reachability. In: Formal Methods in Computer-Aided Design (FMCAD), 2011. pp. 125–134. IEEE (2011)
14. Ehlers, R.: Symbolic bounded synthesis. In: International Conference on Computer Aided Verification. pp. 365–379. Springer (2010)
15. Fedyukovich, G., Gurfinkel, A., Sharygina, N.: Ae-val: Horn clause-based skolemizer for $\forall\exists$-formulas. Presentation-only at HCVS 2015, available at `http://www.inf.usi.ch/phd/fedyukovich/aeval_abstract.pdf`
16. Fedyukovich, G., Gurfinkel, A., Sharygina, N.: Automated discovery of simulation between programs. In: Logic for Programming, Artificial Intelligence, and Reasoning. pp. 606–621. Springer (2015)
17. Flener, P., Partridge, D.: Inductive programming. Automated Software Engineering 8(2), 131–137 (2001)
18. Gacek, A.: JKind – an infinite-state model checker for safety properties in Lustre. `http://loonwerks.com/tools/jkind.html` (2016)
19. Gacek, A., Katis, A., Whalen, M.W., Backes, J., Cofer, D.: Towards realizability checking of contracts using theories. In: NASA Formal Methods, pp. 173–187. Springer (2015)
20. Ghassabani, E., Gacek, A., Whalen, M.W.: Efficient generation of inductive validity cores for safety properties. In: FSE2016: ACM Sigsoft International Symposium on the Foundations of Software Engineering (2016)
21. Gulwani, S.: Dimensions in program synthesis. In: Proceedings of the 12th international ACM SIGPLAN symposium on Principles and practice of declarative programming. pp. 13–24. ACM (2010)
22. Hagen, G.: Verifying safety properties of Lustre programs: an SMT-based approach. Ph.D. thesis, University of Iowa (December 2008)
23. Hagen, G., Tinelli, C.: Scaling up the formal verification of lustre programs with smt-based techniques. In: Formal Methods in Computer-Aided Design, 2008. FMCAD '08. pp. 1–9 (Nov 2008)
24. Hagihara, S., Ueno, A., Tomita, T., Shimakawa, M., Yonezaki, N.: Simple synthesis of reactive systems with tolerance for unexpected environmental behavior. In: Proceedings of the 4th FME Workshop on Formal Methods in Software Engineering. pp. 15–21. ACM (2016)
25. Hamza, J., Jobstmann, B., Kuncak, V.: Synthesis for Regular Specifications over Unbounded Domains. Proceedings of the 2010 Conference on Formal Methods in Computer-Aided Design pp. 101–109 (2010)
26. Jahier, E., Raymond, P., Halbwachs, N.: The Lustre V6 Reference Manual, `http://www-verimag.imag.fr/Lustre-V6.html`

27. Katis, A., Gacek, A., Whalen, M.W.: Machine-checked proofs for realizability checking algorithms. In: Working Conference on Verified Software: Theories, Tools, and Experiments. pp. 110–123. Springer (2015)
28. Katis, A., Whalen, M.W., Gacek, A.: Towards synthesis from assume-guarantee contracts involving infinite theories: A preliminary report. arXiv preprint arXiv:1602.00148 (2016)
29. Klein, U., Pnueli, A.: Revisiting Synthesis of GR(1) Specifications. Proceedings of the 6th International Conference on Hardware and Software: Verification and Testing (HVC'10) pp. 161–181 (2010)
30. Kneuss, E., Kuncak, V., Kuraj, I., Suter, P.: On integrating deductive synthesis and verification systems. arXiv preprint arXiv:1304.5661 (2013)
31. Komuravelli, A., Gurfinkel, A., Chaki, S.: Smt-based model checking for recursive programs. In: Computer Aided Verification. vol. 8559, pp. 17–34. Springer (2014)
32. Kuncak, V., Mayer, M., Piskac, R., Suter, P.: Complete functional synthesis. ACM Sigplan Notices 45(6), 316–329 (2010)
33. Kuncak, V., Mayer, M., Piskac, R., Suter, P.: Functional synthesis for linear arithmetic and sets. International Journal on Software Tools for Technology Transfer 15(5-6), 455–474 (2013)
34. Loos, R., Weispfenning, V.: Applying linear quantifier elimination. The Computer Journal 36(5), 450–462 (1993)
35. Manna, Z., Waldinger, R.J.: Toward automatic program synthesis. Communications of the ACM 14(3), 151–165 (1971)
36. Monmege, B., Brihaye, T., Estiévenart, M., Ho, H.M., ULB, G.G., Sznajder, N.: Real-time synthesis is hard! In: Formal Modeling and Analysis of Timed Systems: 14th International Conference, FORMATS 2016, Quebec, QC, Canada, August 24-26, 2016, Proceedings. vol. 9884, p. 105. Springer (2016)
37. Pnueli, A., Rosner, R.: On the synthesis of a reactive module. In: POPL. pp. 179–190. ACM Press (1989)
38. Reynolds, A., Deters, M., Kuncak, V., Tinelli, C., Barrett, C.: Counterexample-guided quantifier instantiation for synthesis in smt. In: CAV. vol. 9207, pp. 198–216. Springer (2015)
39. Ryzhyk, L., Walker, A.: Developing a practical reactive synthesis tool: Experience and lessons learned., to appear at SYNT 2016
40. Srivastava, S., Gulwani, S., Foster, J.S.: Template-based program verification and program synthesis. International Journal on Software Tools for Technology Transfer 15(5-6), 497–518 (2013)
41. The Coq Development Team: The Coq Proof Assistant Reference Manual. INRIA, 8.4 edn. (2012-2014)
42. Tini, S., Maggiolo-Schettini, A.: Compositional Synthesis of Generalized Mealy Machines. Fundamenta Informaticae 60(1-4), 367–382 (2003)
43. Tomita, T., Ueno, A., Shimakawa, M., Hagihara, S., Yonezaki, N.: Safraless ltl synthesis considering maximal realizability. Acta Informatica pp. 1–38 (2016)

A Example in more detail

Here we consider our example from Fig. 1 and demonstrate one iteration of the synthesis procedure. In particular the $\forall\exists$-formula of *ExtendCheck* is as follows:

$$
\begin{aligned}
bias_0 &= ite(init, 0, ite(x_0, 1, -1) + bias_{-1}) \wedge \\
bias\_max_0 &= ite(init, false, ((bias_0 \geq 2) \vee (bias_0 \leq -2)) \vee bias\_max_{-1}) \wedge \\
guarantee_{10} &= ((state_0 = 0) \implies (bias_0 = 0)) \wedge \\
guarantee_{20} &= ite(init, true, ((state_{-1} = 0) \wedge x_0) \implies (state_0 = 2)) \wedge \\
guarantee_{30} &= ite(init, true, ((state_{-1} = 0) \wedge (\neg x_0)) \implies (state_0 = 1)) \wedge \\
guarantee_{40} &= (bias\_max_0 \implies (state_0 = 3)) \wedge \\
guarantee_{50} &= ((state_0 = 0) \vee (state_0 = 1) \vee (state_0 = 2) \vee (state_0 = 3)) \wedge \\
guarantee\_all_0 &= (guarantee_{10} \wedge guarantee_{20} \wedge guarantee_{30} \wedge guarantee_{40} \wedge \\
&\quad guarantee_{50}) \wedge guarantee\_all_0 \qquad \wedge \\
bias_1 &= ite(false, 0, ite(x_0, 1, -1) + bias_0) \wedge \\
bias\_max_1 &= ite(false, false, ((bias_1 \geq 2) \vee (bias_1 \leq -2)) \vee bias\_max_0) \wedge \\
guarantee_{11} &= ((state_1 = 0) \implies (bias_1 = 0)) \wedge \\
guarantee_{21} &= ite(false, true, ((state_0 = 0) \wedge x_0) \implies (state_1 = 2)) \wedge \\
guarantee_{31} &= ite(false, true, ((state_0 = 0) \wedge (\neg x_0)) \implies (state_1 = 1)) \wedge \\
guarantee_{41} &= (bias\_max_1 \implies (state_1 = 3)) \wedge \\
guarantee_{51} &= ((state_1 = 0) \vee (state_1 = 1) \vee (state_1 = 2) \vee (state_1 = 3)) \wedge \\
guarantee\_all_1 &= (guarantee_{11} \wedge guarantee_{21} \wedge guarantee_{31} \wedge guarantee_{41} \wedge guarantee_{51}) \implies \\
&\quad \exists bias_2, bias\_max_2, guarantee_{12}, state_2, guarantee_{22}, guarantee_{32}, \\
&\quad guarantee_{42}, guarantee_{52}, guarantee\_all_2 \,. \\
bias_2 &= ite(false, 0, ite(x_1, 1, -1) + bias_0) \wedge \\
bias\_max_2 &= ite(false, false, ((bias_2 \geq 2) \vee (bias_2 \leq -2)) \vee bias\_max_0) \wedge \\
guarantee_{12} &= ((state_2 = 0) \implies (bias_2 = 0)) \wedge \\
guarantee_{22} &= ite(false, true, ((state_0 = 0) \wedge x_1) \implies (state_2 = 2)) \wedge \\
guarantee_{32} &= ite(false, true, ((state_0 = 0) \wedge (\neg x_1)) \implies (state_2 = 1)) \wedge \\
guarantee_{42} &= (bias\_max_2 \implies (state_2 = 2)) \wedge \\
guarantee_{52} &= ((state_2 = 0) \vee (state_2 = 1) \vee (state_2 = 2) \vee (state_2 = 3)) \wedge \\
guarantee\_all_2 &= (guarantee_{12} \wedge guarantee_{22} \wedge guarantee_{32} \wedge guarantee_{42} \wedge guarantee_{52}) \wedge \\
&\quad guarantee\_all_2
\end{aligned}
$$

AE-VAL proceeds by constructing MBPs and creating local Skolem functions. In one of the iterations, it obtains the following MBP:

$$
\begin{gathered}
(x_1 \wedge (-1 = bias_0)) \vee ((\neg x_1) \wedge (1 = bias_0)) \wedge \\
\neg bias\_max_0 \wedge \\
(\neg(state_0 = 0)) \vee (\neg x_1) \wedge (\neg(state_0 = 0)) \vee x_1
\end{gathered}
$$

and the following local Skolem function:

$$state_2 = 0 \qquad\qquad bias_2 = 0$$

In other words, the pair of the MBP and the local Skolem function is the synthesized implementation for some transitions of the automaton: the MBP specifies the source state, and the Skolem function specifies the destination state. From this example, it is clear that the synthesized transitions are from state 1 to state 0, and from state 2 to state 0.