Finding Conflicting Instances of Quantified Formulas in SMT

Andrew Reynolds  
University of Iowa

Cesare Tinelli  
University of Iowa

Leonardo de Moura  
Microsoft Research

Abstract—In the past decade, Satisfiability Modulo Theories (SMT) solvers have been used successfully in a variety of applications including verification, automated theorem proving, and synthesis. While such solvers are highly adept at handling ground constraints in a variety of decidable background theories, they primarily rely on heuristic quantifier instantiation methods such as E-matching to process quantified formulas. The success of these methods is often hindered by an overproduction of instantiations which makes ground level reasoning difficult. We introduce a new technique that alleviates this shortcoming by first discovering instantiations that are in conflict with the current state of the solver. The solver only resorts to traditional heuristic methods when such instantiations cannot be found, thus decreasing its dependence upon E-matching. Our experimental results show that our technique significantly reduces the number of instantiations required by an SMT solver to answering “unsatisfiable” for several benchmark libraries, and consequently leads to improvements over state-of-the-art implementations.

I. INTRODUCTION

Many recent formal methods applications rely heavily on Satisfiability Modulo Theories (SMT) solvers for answering logical queries required to solve complex tasks. These tools typically are composed of multiple cooperating decision procedures, or theory solvers, each specialized on sets of ground constraints over some background theory. Thanks to the widespread success and applicability of SMT solvers, there has been a push to use them to handle queries based on richer encodings that include quantified formulas. Handling such formulas in a general way has been an ongoing challenge in the SMT community over the past several decades.

To date, E-matching, first described in [14], is the most popular and successful method used by SMT solvers for handling quantified formulas. In this method, instances of a quantified formula are generated by matching selected terms in the formula (called matching patterns) with ground terms in the rest of the problem. While solvers based on E-matching have had widespread success over many applications, their power is often difficult to wield. One reason is that E-matching often produces a very large number of instances, which may exhaust a solver’s memory or generally cause its performance to degrade. The problem is often compounded by instances that introduce new ground terms which subsequently trigger even more instantiations. This can lead to non-terminating matching loops in the worst case, in which a repeating pattern of terms causes an infinite chain of instantiation steps.

It is thus important to limit the number of instances produced as a result of E-matching. Past research has addressed this issue in various ways, including the use of user-provided matching patterns (or triggers) [7], and methods for recognizing or avoiding matching loops [9]. We present a new quantifier instantiation procedure that aims at decreasing the number of produced instances by decreasing the dependency of SMT solvers on E-matching. This is done by looking for instantiations that lead directly to ground conflicts or to relevant new constraints. In this scheme, the solver resorts to E-matching only when it cannot perform instantiations of this sort. Our goal is to enable the sub-module that handles quantified formulas in a SMT solver to behave more like an efficient theory solver for ground constraints. In particular, our method enables the quantifier module to influence the search performed by the main engine by reporting conflicts and propagating relevant ground constraints, as typically done by efficient theory solvers based on the DPLL(T) [15] framework.

The instantiation procedure described in this paper applies to arbitrary SMT inputs containing quantified formulas. However, it is not intended to be a comprehensive solution for handling such formulas. Instead, it is meant to supplement existing instantiation techniques in a principled manner, so that those, such as E-matching, which are currently cumbersome and expensive, are invoked as little as possible.

1) Contributions: This paper presents a new technique for quantifier instantiation in DPLL(T)-based SMT solvers that on average significantly reduces the number of instantiations required to prove a formula to be unsatisfiable. We give a formal argument for various properties of the technique and the instantiations it produces. We describe an optimized implementation that is efficient in practice. Finally, we provide detailed evidence that our implementation produces significant improvements over state-of-the-art SMT solvers handling quantified formulas according to various metrics.

2) Related Work: Various works have focused on methods for discovering the unsatisfiability of quantified formulas in SMT. The first implementation of E-matching was given in the solver Simplify [7], which included various techniques such as mod-time and pattern-element optimization. These techniques were used by the SMT solver Z3 [6] and enhanced further, as described in [5]. Quantifier instantiation in DPLL(T) as implemented in the SMT solver CVC3 [3] is described in [9]. Specifying decision procedures with quantified formulas through the use of triggers is described in [8]. Techniques also exist for discovering the satisfiability of quantified formulas in SMT, including reasoning in local theory extensions [11], complete instantiation [10] and finite model finding [16].

II. FORMAL PRELIMINARIES

We assume the usual notions from many-sorted first-order logic with equality (denoted by ≈). We fix a set S of sort
symbols and for every $S \in \mathcal{S}$ an infinite set of $X_S$ of variables of sort $S$. We assume the sets $X_S$ are pairwise disjoint and let $X$ be their union. A signature $\Sigma$ consists of a set $\Sigma^a \subseteq \mathcal{S}$ of sort symbols and a set $\Sigma^f$ of (sorted) function symbols $f_{S_1,\ldots,S_n,S}$, where $n \geq 0$ and $S_1,\ldots,S_n,S \in \mathcal{S}$. We drop the sort superscript from function symbols when it is clear from context or unimportant. We assume that signatures always include a Boolean sort $\mathcal{B}$ and constants $\top$ and $\bot$ of that sort (respectively, for true and false).

Given a many-sorted signature $\Sigma$, well-sorted terms, atoms, literals, clauses, and formulas with variables in $X$ are defined as usual and referred to respectively as $\Sigma$-terms, $\Sigma$-atoms and so on. A ground term/formula is a $\Sigma$-term/formula with no variables. When $x = (x_1,\ldots,x_n)$ is tuple of variables and $Q$ is either $\forall$ or $\exists$, we write $Q x \varphi$ as an abbreviation of $Q x_1 \ldots Q x_n \varphi$. If $e$ is a $\Sigma$-term or formula and $x$ has no repeated variables, we write $e(x)$ to denote that $e$’s free variables are from $x$; if $s = (s_1,\ldots,s_n)$ and $t = (t_1,\ldots,t_n)$ are term tuples, we write $e(t)$ for the term or formula obtained from $e$ by simultaneously replacing each occurrence of $x_i$ in $e$ by $t_i$; we write $s \approx t$ for the set $\{s_1 \approx t_1,\ldots,s_n \approx t_n\}$.

A $\Sigma$-interpretation $I$ maps: each $S \in \Sigma^a$ to a non-empty set $S^I$, the domain of $S$ in $I$, with $\mathcal{B}^I = \{\top, \bot\}$; each $x \in X$ of sort $S$ to an element $x^I \in S^I$; and each $f_{S_1,\ldots,S_n,S} \in \Sigma^f$ to a total function $f^I : S_1^I \times \ldots \times S_n^I \rightarrow S^I$. A satisfiability relation between $\Sigma$-interpretations and $\Sigma$-formulas is defined inductively as usual.

A theory is a pair $T = (\Sigma, I)$ where $\Sigma$ is a signature and $I$ is a class of $\Sigma$-interpretations, the models of $T$, that is closed under variable reassignment (i.e., every $\Sigma$-interpretation that differs from one in $I$ only for how it interprets the variables is also in $I$) and isomorphism. A $\Sigma$-formula $\varphi[x]$ is $T$-satisfiable (resp., $T$-unsatisfiable) if it is satisfied by some (resp., no) interpretation in $I$. A set $\Gamma$ of formulas $T$-entails a $\Sigma$-formula $\varphi$, written $\Gamma \models_T \varphi$, if every interpretation in $I$ that satisfies all formulas in $\Gamma$ satisfies $\varphi$ as well. The set $\Gamma$ is $T$-satisfiable if $\Gamma \not\models_T \bot$. For a given signature $\Sigma$ the theory of equality (with uninterpreted functions) or $E$, consists of the set of $\Sigma$-interpretations. Informally, we refer to the sort and function symbols in this theory as uninterpreted.

A substitution $\sigma$ is a mapping from variables to terms of the same sort, such that the set $\{x \mid \sigma(x) \neq x\}$, the domain of $\sigma$, is finite. We say that $\sigma$ is a grounding substitution for a tuple $x = (x_1,\ldots,x_n)$ of variables if $\sigma$ maps each element of $x$ to a ground term. If $t = (t_1,\ldots,t_n)$, we write $x \mapsto t$ to denote the substitution $\sigma = \{x_1 \mapsto t_1,\ldots,x_n \mapsto t_n\}$; for a term or formula $e[x]$, we write $e\sigma$ to denote the expression $e[t]$. This notation extends to sets of formulas/terms as expected.

### III. Finding Conflicts for Quantified Formulas

To handle quantified formulas, DPLL($T$) solvers typically divide the input set of formulas into a set $Q$ of quantified formulas and a set $G$ of ground ones. To determine if $Q \cup G$ is unsatisfiable in the background theory $T$, they heuristically add to $G$ selected ground instances of formulas from $Q$, and succeed when they have added enough instances to make $G$ $T$-unsatisfiable. When $G$ is $T$-satisfiable, they build a truth assignment for the atoms in $G$ that satisfies all the formulas in $G$ and is consistent with $T$. The truth assignment is represented as a set $M$ of ground literals, which we will call a context. In this case, a possible quantifier instantiation heuristic is to, when possible, add ground instances $\varphi$ of formulas from $Q$ that are in conflict with the current context $M$, in the sense that $M \cup \{\varphi\}$ is $T$-unsatisfiable. Adding such an instance to $G$ will effectively force the solver to discard $M$ and look for another context (if one exists).

This section presents a new quantifier instantiation procedure that, as described above, searches for instances of universally quantified formulas that are in conflict with the context maintained by the solver. For simplicity, we describe only a basic version of the procedure here. A more practical implementation is discussed in the next section.

For the rest of the section we fix a theory $T$ of signature $\Sigma$, a $\Sigma$-formula $\forall x \psi \in Q$ with $\psi[x]$ quantifier-free, and a context $M$ consisting of a $T$-satisfiable set of ground $\Sigma$-literals. We will use $T_M$ to denote the set of all terms occurring in $M$.

#### A. Conflict Finding Instantiation Procedure

Our instantiation procedure tries to construct grounding substitutions $\sigma$ for $x$ such that $M \models_T \neg \psi[\sigma]$. We refer to $\sigma$ as a conflicting substitution for $(M, \psi)$. Conflicting substitutions are of interest since they suffice to show that there is no model of $T$ that satisfies both $M$ and $\forall x \psi$.

Example 1: If $M = \{f(a) \neq g(b), b = h(a)\}$, then $(x \mapsto a)$ is a conflicting substitution for $(M, f(x) \approx g(h(x)))$. $\square$

To simplify its presentation, we assume our procedure is run on the flat form of quantified formulas $\forall x \psi$, defined as follows.

Definition 1: A flat form of a quantified formula $\forall x \psi$ is an equivalent formula $\forall x, y (\mu \Rightarrow \varphi)$ where

- $\mu$ is a conjunction of equalities $x_0 \approx f(x_1,\ldots,x_n)$, which we will call the matching constraints, where $n \geq 0$ and $x_0,\ldots,x_n$ are variables from $x, y$;
- $\varphi$ is a quantifier-free formula, which we will call the flattened body, whose non-ground atoms are equalities between variables from $x, y$.

A flat form of $\forall x \psi$ can be computed by starting with $\mu = 1$ and $\varphi = \psi$ and repeatedly replacing any non-ground term $t$ in $\mu \Rightarrow \varphi$ by a fresh variable $x_t$ and adding the equation $x_t \approx t$ to $\mu$ until all non-ground terms have the form $f(x_1,\ldots,x_n)$.

Definition 2: Let $z$ be a tuple of variables. An assignment over $z$ is a set of equations of the form $z \approx t$ with $z \in z$ and $t \in T_M$. A constrained assignment over $z$ is a set $E \cup C$ where $E$ is an assignment over $z$ and $C$ is a set of equalities and disequalities over $z$. A constrained assignment $A$ is $M$-feasible if $M \cup A$ is satisfiable in $T$.

Given the context $M$ and a flat form $\forall x, y (\mu \Rightarrow \varphi)$ of $\forall x \psi$, our instantiation procedure will attempt to construct a constrained assignment $A$ over the variables $x, y$ that summarizes the conditions under which one can build a conflicting
proc falsify($\varphi_0, b_0$)
  if $\varphi_0$ is ground
    if $M \models_T \varphi_0 \leftrightarrow b_0$ then $\emptyset$ else $\emptyset$
  else if $\varphi_0$ is $x_1 \approx x_2$
    if $b_0$ is $T$ then $\{\{x_1 \neq x_2\}\} \cup \{\{x_1 \approx x_2\}\}$
  else if $\varphi_0$ is $\neg \varphi_1$
    falsify($\varphi_1, b_0$)
  else if $\varphi_0$ is $\varphi_1 \lor \varphi_2$
    if $b_0$ is $T$ then
      $\{A_1 \cup A_2 : A_1 \in$ falsify($\varphi_1, b_0$), $A_2 \in$ falsify($\varphi_2, b_0$)$\}$
  else
    falsify($\varphi_1, b_0$) $\cup$ falsify($\varphi_2, b_0$)

Fig. 1. The falsify procedure. It returns a set $A$ of constrained assignments such that $M \cup A \models_T (\varphi_0 \leftrightarrow b_0)$ for each $A \in A$, where $b_0$ denotes the complement of $b_0$.

proc match($S_0$)
  if $S_0$ is $\{y \approx f(z)\} \cup S_1$ then
    $\{A \cup \{y \approx f(t)\} : t \approx z, A \in$ match($S_1$), $f(t) \in T_M\}$
  else
    $\emptyset$

Fig. 2. The match procedure. It returns a set $A$ of constrained assignments such that $M \cup A \models_T S_0$ for each $A \in A$.

substitution for $(M, \psi)$. When it succeeds in building $A$, the procedure is also able to return one such substitution.

1) Quantifier Instantiation Procedure: A basic, unoptimized version of the procedure consists of three steps. The first step returns constrained assignments $A$ by which construction falsify the flattened body $\varphi$; that is, constrained assignments $A$ such that $M \cup A \models_T \neg \varphi$. The second step constructs constrained assignments $A’$ which by construction entail the matching constraints $\mu$, that is, $M \cup A' \models_T \mu$. The third step considers unions of the constrained assignments $A \cup A'$ constructed in steps one and two, and tries to extract from $A \cup A'$ a grounding substitution $x \mapsto s \lor y \mapsto t$ such that $M, x \approx s, y \approx t \models_T A \cup A'$. If such a substitution exists, the procedure returns $x \mapsto s$ as a conflicting substitution for $(M, \psi)$; otherwise, it fails. We discuss these three steps in more detail in the following.

a) Step 1: Construct constrained assignments conflicting with the flattened body $\varphi$: This step is executed by the recursive subprocedure falsify shown in Figure 1 (where for brevity we assume that the only Boolean connectives in $\varphi$ are $\neg$ and $\lor$), which takes as input a subformula $\varphi_0$ of the flattened body $\varphi$, and a Boolean constant $b_0 \in \{T, \bot\}$ indicating the polarity of $\varphi_0$ in $\varphi$, and returns a set of constrained assignments computed according to that polarity. ² It initial inputs are $(\varphi, T)$.

b) Step 2: Construct constrained assignments that entail the matching constraints $\mu$: This step constructs a set $A$ of constrained assignments each of which entails $\mu$. It does so by using the subprocedure match shown in Figure 2, which is called on the set of all the constraints $S_\mu$ in $\mu$. For each matching constraint $z \approx f(z_1, \ldots, z_n) \in S_\mu$, the subprocedure considers all terms of the form $f(t_1, \ldots, t_n) \in T_M$, and adds to $A$ the constraints $z \approx f(t_1, \ldots, t_n), z_1 \approx t_1, \ldots, z_n \approx t_n$.

²Formula $\varphi_0$ has positive polarity in $\varphi$ if and only if it occurs beneath an even number of $\neg$ symbols.

c) Step 3: Extract a conflicting substitution from constrained assignment: This step tries to generate a conflicting substitution for $(M, \psi)$, if there exists one. To do so, it considers all $M$-feasible constrained assignments $A' \cup A'_m$, where $A'_f \in$ falsify($\varphi, T$) and $A'_m \in$ match($S_\mu$). It partitions $A'$ into two sets $B'$ and $C'$ such that the equivalence closure of $B'$ contains at most one ground term per equivalence class. Using $B'$, the procedure constructs a grounding substitution $\sigma = (x \mapsto s \lor y \mapsto t)$, which we call a completion of $A'$, by computing the equivalence closure of $B'$, and then mapping every variable in the same equivalence class to the ground term in that class if there is one, or to one from $T_M$ otherwise. If it succeeds in constructing a completion $\sigma$ such that $M \models C' \sigma$, the procedure ends, returning the substitution $x \mapsto s$. Otherwise, it tries to extract a conflicting substitution from a different constrained assignment in $A'$.

Example 2: To see how substitutions like $\sigma$ above are computed, suppose $T$ is the theory of equality, $M = \{f(a) \neq f(b)\}, B' = \{x \approx y, z \approx a, z \approx w\}$, and $C' = \{x \neq w\}$. Note that $A' = B' \cup C'$ is an $M$-feasible constrained assignment. The set $B'$ induces the equivalence relation $\{\{x, y\}, \{w, z, a\}\}$. Adding $b$ to the equivalence class of $x$ leads to the grounding substitution $\sigma = (x \mapsto b, y \mapsto b, z \mapsto a, w \mapsto a)$ which is such that $M \models E C' \sigma$.

We remark that, in our experience, guessing ground terms to add to the equivalence classes in the equivalence closure of $B'$ in the third step of the procedure is rarely needed. The reason is that $B'$ typically contains a grounding equation $z \approx t$ (with $t \in T_M$) for each variable $z$ in it. When this is not the case, it is because either $z$ does not occur as an argument of a function symbol in the flattened form $\forall x, y (\mu \models \varphi)$, or it is not relevant to the falsification of that formula.

We illustrate our procedure as a whole with a simple example where $T$ is again the theory $E$ of equality.

Example 3: Say $M$ is $\{f(a) \neq g(b), b \approx h(a)\}$ and consider the formula $\forall x \psi$ where $\psi$ is $f(x) \equiv g(h(x))$. A flattened form of $\forall x \psi$ is

$$\forall x, y_1, y_2, y_3 \,(y_1 \approx f(x) \land y_2 \approx h(x) \land y_3 \approx g(y_2)) \rightarrow y_1 \approx y_3 \psi$$

If we run our procedure on this formula, falsify($y_1 \approx y_3, T$) returns the set of constrained assignments $\{\{y_1 \neq y_3\}\}$. The procedure then invokes match($S_\mu$) where $S_\mu$ is $\{y_1 \approx f(x), y_2 \approx h(x), y_3 \approx g(y_2)\}$. The recursive calls of match when processing each equality in $S_\mu$ are as follows:

<table>
<thead>
<tr>
<th>equation</th>
<th>output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y_2 \approx g(y_2)$</td>
<td>${{y_2 \approx g(y_2), y_2 \approx b}}$</td>
</tr>
<tr>
<td>$y_2 \approx h(x)$</td>
<td>${{y_2 \approx g(b), y_2 \approx b, y_2 \approx h(a), x \approx a}}$</td>
</tr>
<tr>
<td>$y_1 \approx f(x)$</td>
<td>${{y_2 \approx g(y_2), y_2 \approx b, y_2 \approx h(a), x \approx a, y_1 \approx f(a)}}$</td>
</tr>
</tbody>
</table>

Let $A'$ be the union of the (single) constrained assignments produced by falsify and match. Notice that $A'$ is $M$-feasible. Splitting $A'$ into $B' = \{x \approx a, y_1 \approx f(a), y_2 \approx h(a), y_3 \approx g(b)\}$ and $C' = \{y_2 \approx b, y_1 \neq y_3\}$, say, the procedure can generate (in this case only) the substitution $\sigma = (x \mapsto a, y_1 \mapsto f(a), y_2 \mapsto h(a), y_3 \mapsto g(b))$. Since $M \models_E C' \sigma$, the procedure returns the substitution $x \mapsto a$. Note that $M \models_E f(a) \neq g(h(a))$, that is, $M \models_E \neg \psi[a]$, which shows that the returned substitution is indeed conflicting. □
One can show by structural induction that the subprocedures falsify and match have the following properties:

Lemma 1: For all $A \in \text{falsify}(\varphi, T)$ and $A' \in \text{match}(S_M)$, $M, A \models T \varphi$, and $M, A' \models T \mu$.

Lemma 2: Let $\forall x, y (\mu \models \varphi)$ be the flat form of $\forall x \psi[x]$. Let $A' \in \text{falsify}(\varphi, T)$, $A'_m \in \text{match}(S_M)$, $A'[x, y] = A'_l \cup A'_r$, and $\sigma = x \mapsto s \cup y \mapsto t$. If $M, x \approx s, y \approx t \models T \mu$, then $M, \psi[s] \models T (A' \setminus C)[s, t]$.

Proof: Let $\sigma, A', A'_m$ and $A'$ be as above. By Lemma 1, $M, A' \models T \varphi$ and $M, A'_m \models T \mu$. Thus, we have that $M, A' \models T \mu \land \varphi$ or, equivalently, $M, A' \models T \neg (\mu \models \varphi)$. By our assumption, we have that $M, x \approx s, y \approx t \models T C$. Hence, $M, x \approx s, y \approx t, (A' \setminus C) \models T \neg (\mu \models \varphi)$ which implies that $M,(\mu \models \varphi)[s, t] \models T (A' \setminus C)[s, t]$. The claim then follows by the equivalence of $(\mu \models \varphi)[s, t]$ and $\psi[s]$.

This justifies the correctness result for our procedure.

Proposition 1: Every substitution returned by the instantiation procedure is conflicting for $(M, \psi)$.

Proof: Let $\sigma, A', A'_m$ and $A'$ be as in Lemma 2. Recall our instantiation procedure in Step 3 partitions $A'$ into $B' \cup C'$. We have that $M \models T B' \sigma$ due to our construction of $\sigma$. Furthermore, by assumption the procedure returns $\sigma$ only such that $M \models T C' \sigma$. Hence, $M, x \approx s, y \approx t \models T A'$, and by Lemma 2 with $C = A'$, we have that $M, \psi[s] \models T \neg (A' \setminus A')[s, t]$, thus, $M, \psi[s] \models T \bot$.

2) Constraint-Inducing Substitutions: Even when no conflicting substitutions exist for $(M, \psi)$, it may be useful to find other substitutions that help the solver deduce useful information about the terms in $M$. This can be done by relaxing one of the requirements on the substitutions returned by our instantiation procedure. Let $\sigma = x \mapsto s \cup y \mapsto t$ and $A' = B' \cup C'$ be as in Step 3 of the procedure, except that $M \models T D \sigma$ does not hold for a non-empty subset $D \subseteq C'$. Since the proof of Lemma 2 does not rely on that entailment, we still have $M \cup \psi[s] \models T \neg D[s, t]$, even though $\sigma$ is no longer conflicting for $(M, \psi)$. We refer to $\sigma$ as a constraint-inducing substitution for $(M, \psi)$. If $D$ is a conjunction of disequalities, we refer to $\sigma$ as an equality-inducing substitution for $(M, \psi)$. Observe that since each predicate symbol in $D$ is applied to variables, and $s$ and $t$ are tuples of terms from $T_M$, the entailed formula $\neg D[s, t]$ is a disjunction of constraints over terms in $T_M$. As a consequence, it may be beneficial to generate the instance $\psi[s]$ anyway since it causes the solver to deduce constraints over terms from $T_M$. This contrasts with instantiations produced by E-matching, which often introduce constraints over fresh terms.

Example 4: Consider the quantified formula $\forall x \psi[x]$ from Example 3, and say $M$ is $\{f(a) \approx c, d \approx g(b), b \approx h(a)\}$. Our procedure produces the same constrained assignment $A'$ as in that example. In this case too, $A'$ is $M$-feasible. However, the completion $\sigma = \{x \mapsto a, y_1 \mapsto f(a), y_2 \mapsto h(a), y_1 \mapsto g(b)\}$, corresponding to the partition $B' \cup C'$ of $A'$ with $C' = \{y_2 \approx b, y_1 \approx y_3\}$, is not such that $M \models E (y_1 \not\approx y_3) \sigma$. In fact, it is not difficult to see there are no conflicting substitutions for $\psi$. However, $M$ together with the instance $\psi[a]$, i.e. $f(a) \approx g(h(a))$, allows the solver to deduce that the terms $f(a)$ and $g(b)$ from $T_M$ are equal.

3) An Instantiation Strategy: A strategy can be used that produces both conflicting and constraint-inducing substitutions for a given context $M$ and set of quantified formulas $Q$. First, if a conflicting substitution can be found for one quantified formula in $Q$, add the corresponding instance to the set of ground clauses $G$. This will cause the solver to backtrack some decision in $M$. Otherwise, if no conflicting substitution can be found, add instances corresponding to every constraint-inducing substitution found for each quantified formula in $Q$.

IV. PIVOTAL IMPLEMENTATION

For greater clarity, the description of the instantiation procedure given in Section III favors simplicity over efficiency. Our actual implementation relies on one major restriction and numerous enhancements, briefly discussed in the following.

A. Restriction to the Theory of Equality

In our current implementation, the instantiation procedure does not reason modulo the actual background theory $T$ but only modulo the theory $E$ of equality. Concretely, this means that all function symbols in $M$ and $\forall x \psi$ (including arithmetic symbols) are treated as uninterpreted. This is done both for uniformity and efficiency since checking $T$-entailment/satisfiability is generally expensive for theories other than $E$. Since every theory $T$ is a refinement of $E$ (in the sense that it allows less interpretations), this restriction is sound: any conflicting substitution with respect to $E$ is also conflicting with respect to a stronger theory. The obvious downside of this naive approach is that for stronger theories the procedure returns only a coarse under-approximation of the set of conflicting substitutions for $(M, \psi)$.

Example 5: Let $M = \{f(a) \approx b, (g(a) \approx b+1) \approx \top\}$ and let $\forall x \psi$ be $\forall x f(x) \approx g(x)$ where $f, g, a, b$ are uninterpreted symbols and $\geq, +, 1$ are from the theory $A$ of integer arithmetic. In this case, the background theory $T$ is the union of $E$ and $A$. Consider the following flat form of $\forall x f(x) \approx g(x)$:

$\forall x, y_1, y_2 (y_1 \approx f(x) \land y_2 \approx g(x)) \Rightarrow y_1 \approx y_2$.

By treating the arithmetic symbols as symbols of $E$, our procedure will not discover any conflicting substitutions in this example. To see this, note that equating $y_1$ to $f(a)$ and $y_2$ to $g(a)$ in match (the only possibility) would produce the $M$-feasible constrained assignment $\{y_1 \not\approx y_2, y_1 \approx f(a), y_2 \approx g(a), x \approx a\}$. The corresponding substitution $\sigma = \{y_1 \mapsto f(a), y_2 \mapsto g(a), x \mapsto a\}$ is not conflicting for $(M, \psi)$ in $E$ because $\models E (f(x) \not\approx g(x)) \sigma$, so our current implementation of the procedure will return no substitutions in this case. In contrast, $M \models E_{\bot} (f(x) \not\approx g(x)) \sigma$ when $\geq, +, 1$ are treated as symbols of $A$. Hence, if our procedure did so and we were able to determine the latter entailment it would be able to return the substitution $\{x \mapsto a\}$.

We point out that reasoning modulo the actual background theory instead of $E$ is not enough in general to return all possible conflicting substitutions, since the match sub-procedure is in fact incomplete for general theories $T$. To see this, observe that in $A$, an assignment containing $y \approx x + y_1, y_1 \approx 2$ will match with the term $3 + 2$, but fail to match with the equivalent term $2 + 3$. That said, for our purposes, using incomplete yet efficient theory matching and entailment tests may lead to the
proc falsify,(φ₀, b₀, A, S) if φ₀ is ground if \( M \models T \phi₀ \leftrightarrow \neg b₀ \) then \((A, S)\) else \(\emptyset\) else if φ₀ is \( x₁ \approx x₂ \) if \( b₀ \) is \( T \) then match₁(S \mid x₁, x₂), A \cup \{x₁ \neq x₂\}, S \setminus S \mid x₁, x₂\) else match₁(S \mid x₁, x₂), A \cup \{x₁ \approx x₂\}, S \setminus S \mid x₁, x₂\) endif else if \( \neg \phi₀ \) then falsify,(φ₁, b₀, A, S) else if φ₀ is \( \phi₁ \lor \phi₂ \) if \( b₀ \) is \( T \) then \( \bigcup(A', S')\in\text{falsify},(\phi₁, b₀, A, S)\) falsify,(φ₂, b₀, A', S') endif else falsify,(φ₁, b₀, A, S) \cup falsify,(φ₂, b₀, A, S) endelse proc match₁(S₀, A, S) if \( S₀ \) is \( \{y \equiv f(z)\} \cup S₁ \) then \( S₀' := S₀ \cup S \mid z, S' := S \setminus S \mid z, \) \( \bigcup_{f(t)\in\text{T}_M} \text{match₁}(S₀', A \cup \{y \equiv f(t)\} \cup z) \approx t, S' \) else \((A, S)\) endelse

Fig. 3. The falsify, and match, procedures. We have that \( M, A \models T \neg((S₀ \setminus S) \Rightarrow \phi₀) \) for each \((A, S) \in \text{falsify},(\phi₀, T \land \emptyset, S₀), S \mid v \) denotes the set of matching constraints from \( S \) whose left hand side is in \( V \).

best performance, where conflicting substitutions are found only when it is reasonably easy for the procedure to do so.

B. Enhancement to the Basic Procedure

The most important enhancement with respect to the basic procedure described in Section III is that its three main steps are interleaved, as demonstrated in Figure 3. With respect to the basic procedure, falsify, and match, take two additional arguments: a constrained assignment \( A \) and a set of matching constraints \( S \). Intuitively, \( A \) is the current constrained assignment we are building, and \( S \) is the matching constraints that are left to process. When considering a quantified formula with flat form \( \forall x. \mu \mapsto \varphi \), we initially call falsify, with arguments \((\varphi, T, \emptyset, S₀), S \mid v \) denotes the set of matching constraints from \( \mu \). This builds a set of pairs \( A, S \), such that for each \((A, S) \in A \), we have \( M, A \models T \neg((S₀ \setminus S) \Rightarrow \varphi) \). It can be shown that when \( S \neq \emptyset \), the matching constraints in \( S \) do not need to be entailed when constructing a completion for \( A \).

This procedure has several important advantages over the basic one. First, constrained assignments are built incrementally, which (although not shown here) allows us to discard a constrained assignment \( A \) as soon as it becomes \( M \)-infeasible. Second, matching constraints are processed for a variable \( x \) as soon as any constraint involving \( x \) is added to \( A \), as in the second branch of falsify, and in match, allowing us to eagerly determine cases where the current constrained assignment will not lead to a conflicting substitution. Third, we compute the set \( A = \text{falsify,}(\varphi, T, \emptyset, S₀) \) lazily, which allows us to check whether there exists a conflicting substitution for a returned constrained assignment before producing the entire set \( A \).

C. Implementation Details

The ground theory solver maintains an equivalence relation \( \equiv_M \) over the terms in \( \text{T}_M \) induced by the constraints in \( M \) (whereby \( s \equiv_M t \) only if \( M \models E s \approx t \)). For each \( t \in \text{T}_M \), let \([t]_M \) denote the equivalence class of \( t \) in \( \equiv_M \) and let \([t]_M \) denote \((\{t\}, \ldots, [t]_M)\) if \( t = (t₁, \ldots, t_n) \).

For every function symbol \( f \) of arity \( n \) in the input formula, we build an index \( I_f \) containing entries of the form \([t]_M \mapsto f(t)\), mapping an \( n \)-tuple \([t]_M \) of equivalence classes to some \( f(t) \in \text{T}_M \). The index is functional, that is, if \( f(s), f(t) \in \text{T}_M \) with \( s \equiv_M t \) at most one of \( f(s) \) and \( f(t) \) is in \( I_f \). This data structure is used by the falsify procedure when checking entailment of ground equalities thanks to the following invariant maintained within the solver:

\[
M \models E f(t) \approx g(s) \quad \text{iff} \quad \{[t]_M \mapsto f(u) \in I_f, \} \quad \{[s]_M \mapsto g(v) \in I_g, \} \quad \{f[u]_M = g[v]_M, \}
\]

To process matching constraints we build an extended index \( J_f \) with entries of the form \((\{f(t)\}_M, \{t\}_M) \mapsto f(t)\) for terms \( f(t) \in \text{T}_M \). When considering a matching constraint \( x \approx f(x₁, \ldots, x_n) \), the match procedure enumerates, modulo \( \equiv_M \), the terms in \( \text{T}_M \) with top symbol \( f \) by traversing the index \( J_f \) — and backtracking whenever it determines that the constrained assignment it is constructing is not \( M \)-feasible.

Constrained assignments are represented as a pair \((U, C)\), where \( U \) is a partial map from variables \( x, y \) to a term they are equated to (either a representative term from \( \text{T}_M \) or another variable), and \( C \) is a set of flat constraints over \( x \cup y \). Finally, formulas \( \forall x \psi \) are not actually flattened. Instead of replacing a term \( t \) in \( \psi \) with a fresh variable \( y \), we treat \( t \) itself as \( y \) when needed.

V. Results

We implemented our instantiation procedure with the restrictions and enhancements mentioned in Section IV within the SMT solver cvc4+ci [1] (version 1.3). In this section, we compare the performance of our implementation against various state-of-the-art SMT solvers.

In our experiments, we considered three different configurations of cvc4+ci that vary on the instantiation strategy they use. All three configurations apply quantifier instantiation lazily, that is, after the solver produces a \( T \)-satisfiable context \( M \) that propositionally satisfies the set \( G \) of current ground formulas. Given a set of \( \text{active} \) quantified formulas \( Q \), each configuration of cvc4 runs (a subset of) the following steps in succession until a ground instance is added to \( G \).

1) Add the instance \( \psi[t] \) if there exists a conflicting substitution \( x \mapsto t \) for \( (M, \psi) \) for some \( \forall x \psi \in Q \).
2) Add the instances \( \psi[t] \) for a subset of the equality-inducing substitutions \( x \mapsto t \) for \( (M, \psi) \), for each \( \forall x \psi \in Q \).
3) Add all instances based on \( E \)-matching for \( (M, Q) \).

The first configuration, which we will refer to as cvc4, performs Step 3 only. The second configuration, cvc4+c, performs Step 1 and Step 3. The third, cvc4+ci, performs all three steps. In Step 2, configuration cvc4+ci considers at most one equality-inducing substitution for each constrained assignment.

In [3] the implementation \([t]_M \) is represented by a distinguished term in \([t]_M \).

Details can be found at http://cvc4.cs.nyu.edu/papers/FMCAD2014-qcf/

5
produced by the first two steps of our instantiation procedure; that is, it does not add instances for multiple completions of the same constrained assignment. Configurations cvc4+c and cvc4+ci use the naïve approach for handling interpreted theory symbols described in Section IV-A. A single run of these steps we will refer to as an instantiation round.

A. Comparison with SMT solvers

We compared these three configurations of CVC4 with the SMT solvers Z3 (version 4.3.2) [6] and cvc3 [3], both of which rely on quantifier instantiation to reason about quantified formulas. We report results on unsatisfiable benchmarks from various collections from the verification and automated theorem proving communities: the TPTP library (version 6.0.0) [18], a set of benchmarks produced as proof obligations from Isabelle in [4], as well as SMT-LIB [2]. We considered 12,406 unsatisfiable benchmarks from TPTP. These benchmarks contain primarily quantified formulas and are all over the theory of equality.\(^5\) We considered 13,041 Isabelle benchmarks (many of whose status is unknown or satisfiable), which also primarily contain quantified formulas, but also include both integer and real arithmetic constraints. Many of the SMT-LIB benchmarks represent software verification conditions, and make heavy use of symbols over several theories. We considered all 26,320 benchmarks from SMT-LIB that contained quantified formulas but no non-linear arithmetic constraints, which CVC4 does not yet support. Of all of these SMT-LIB benchmarks, we report results only for the 4,633 that do not have a parser for this format, and no translator from this format was available.

Overall over the three benchmark sets, cvc4+ci solves more problems than any other configuration. In particular, it consistently outperforms cvc4+c (14,445 vs. 14,117), solving 404 problems that cvc4+c cannot, while cvc4+ci only solves 76 that cvc4+ci cannot. This shows that computing constraint-inducing substitutions in addition to conflicting substitutions is beneficial. The scatter plot in Figure 4(a) shows that the new instantiation techniques (cvc4+ci) typically improve the runtime performance of CVC4, although there are several cases where it does not. Over the benchmarks they both solve, cvc4+ci solves 4,419 benchmarks at least 20% faster than cvc4, whereas cvc4 solves 1,845 benchmarks at least 20% faster than cvc4+ci. We believe the improvement in performance is due to the reduction in the number of instantiations produced by cvc4+ci, as discussed later. Over

\(^5\)We did not consider TPTP benchmarks having TFF syntax (which includes theory constraints), since Z3 and cvc3 do not have a parser for this format, and no translator from this format was available.

\(^6\)In particular, cvc4 does not use eager quantifier instantiation, clause deletion, or relevancy (see Section 7 of [5]) for SMT-LIB benchmarks.
all benchmark sets, \texttt{cvc4} solves 235 that \texttt{cvc4+ci} cannot solve, while \texttt{cvc4+ci} solves 1,042 benchmarks that \texttt{cvc4} cannot. At least one configuration of either \texttt{cvc4+ci} or \texttt{cvc4+c} solves 359 benchmarks that no implementation of E-matching (either \texttt{Z3}, \texttt{CVC3}, \texttt{CVC4}) can solve, indicating that our techniques can be used to improve the precision of SMT solvers for unsatisfiable problems containing quantified formulas.

2) Instances Generated: Table II gives the cumulative number of instantiations reported by each solver for the three benchmarks sets. For both the TPTP and the Isabelle set, in addition to solving the most benchmarks, configuration \texttt{cvc4+ci} requires by far the least number of instantiations to do so. For TPTP, \texttt{cvc4+ci} produces about 151 million instances to solve 6,616 problems, which is 5.8 times fewer than what \texttt{cvc4} requires for solving 6,100 problems. Similarly for Isabelle, \texttt{cvc4+ci} requires 28M instantiations to solve 4,082 problems, which is 4.2 times fewer than what \texttt{cvc4} requires for solving 3,858 problems. For SMT-LIB, \texttt{Z3} is by far the most efficient solver, solving 3,983 problems while requiring only 6.4M instantiations. The new techniques in \texttt{CVC4} reduce the instantiations by approximately half, which is less dramatic than the improvements seen on TPTP and Isabelle. This is again likely due to the prevalence of theory symbols in the encodings used by SMT-LIB benchmarks.

The scatter plot in Figure 4(b) compares the reported number of instances produced by configurations \texttt{cvc4} and \texttt{cvc4+ci} on the benchmarks they both solve. The plot clearly shows that \texttt{cvc4+ci} consistently requires many fewer instantiations, confirming that the instances it produces are generally effective at contributing towards finding refutations.

Figure 5 shows the cumulative number of instantiations reported by each of the solvers on the benchmarks they solve. For benchmarks with low theory content (from the TPTP and Isabelle libraries), the configuration \texttt{cvc4+ci} consistently produces fewer instances while solving more benchmarks than the other solvers and configurations. For SMT-LIB benchmarks, the plot shows that the configuration \texttt{cvc4+ci} uses noticeably fewer instances than \texttt{Z3} to solve its first 1750 benchmarks. However, \texttt{cvc4+ci} requires more instantiations overall to solve fewer benchmarks than \texttt{Z3}. This suggests that our techniques are highly effective at handling a subset of the SMT-LIB benchmarks, but require further enhancements to account for the encodings used by these benchmarks.

Table III shows a detailed view of the instances produced by the three configurations of \texttt{CVC4}. The first column (IR) gives the cumulative number of instantiation rounds each configuration requires for the benchmarks it solves. The remaining six columns give the percentage of instantiation rounds where they produce instances based respectively on E-matching, conflicting substitutions, and constraint-inducing substitutions; and the total number of instances produced for each of these types. We can see that while configurations \texttt{cvc4+c} and \texttt{cvc4+ci} require significantly more instantiation rounds on average to answer unsatisfiable on each benchmark class, they require much fewer instantiations overall. Overall, a conflicting substitution was found on 77.3% of the instantiations rounds performed by \texttt{cvc4+ci} and on 74.5% of the instantiation rounds performed by \texttt{cvc4+ci}. These percentages are fairly consistent across the three benchmark classes, indicating that a majority of satisfying assignments found at the ground level can be ruled out by a single instance from a conflicting substitution. For \texttt{cvc4+ci}, a conflicting substitution was found on 78.5% of the instantiation rounds where a constraint-inducing substitution was not produced, which is slightly higher than the percentage found by \texttt{cvc4+ci} alone (77.3%). This suggests that constraint-inducing substitutions help the solver find conflicting substitutions. In total, E-matching was called 1.57 fewer times by \texttt{cvc4+ci} than by \texttt{cvc4}, which led to a factor of 5 fewer instantiations produced as a result of such calls.
Overall, 12,165 of the 14,445 benchmarks that cvc4+ci solved required at least one instantiation round by all configurations of cvc4, and 2,520 of these 12,216 benchmarks (20.7%) could be solved by cvc4+ci using only instances resulting from conflicting and constraint-inducing substitutions. In other words, for 20.7% of the benchmarks it solves, cvc4+ci did not rely on E-matching at all to answer unsatisfiable. Moreover, 94 of these 2,251 benchmarks could not be solved by cvc4 within the timeout, showing that difficult benchmarks can be solved solely by the techniques mentioned in this paper.

B. Comparison with Automated Theorem Provers

We do not give a detailed comparison with automated theorem provers, which are capable of handling benchmarks from the TPTP library, but do so using entirely different methods than SMT solvers. For a brief and informal overview, a recent (multi-strategy) run script for iProver [12] solves 6,508 unsatisfiable benchmarks from the TPTP library, while a recent run script for E [17] solves 9,751. A version of both of these scripts as well as the systems themselves were used in CASC 24, the latest competition for automated theorem provers. Using a run script devised for a similar purpose, which incorporates several configurations of E-matching as well as the techniques described here, cvc4 solves 7,227 unsatisfiable TPTP benchmarks, making cvc4 highly competitive with a state-of-the-art instantiation-based provers like iProver.

VI. CONCLUSION

We have presented a technique for quantifier instantiation in SMT that increases the ability of an SMT solver to detect unsatisfiable problems containing quantified formulas. The method relies on a more principled heuristic for choosing instances, focusing on those that communicate conflicts or relevant constraints to the ground-level sub-solver. It handles any set of quantified formulas by treating theory symbols (at worst) as uninterpreted. Our experiments show that the number of instantiations necessary to solve unsatisfiable benchmarks is on average decreased by almost an order of magnitude when compared to implementations using E-matching only. As a result, our implementation shows a noticeable improvement in performance in terms of average runtime and in overall number of unsatisfiable benchmarks solved.

In future work, we plan to implement a more incremental version of our instantiation procedure to recognize conflicts while the SMT is reasoning at the ground level, which has been shown to lead to performance improvements in other implementations of quantifier instantiation in SMT [5], [9]. We also plan to extend the procedure beyond its naïve treatment of interpreted symbols to increase the number of conflicting substitution found for formulas containing such symbols. As discussed in Section IV-A, doing so requires devising fast, if incomplete, $T$-satisfiability tests for theories other than equality. Finally, we would like to identify language fragments and investigate extensions of our techniques that are complete, that is, guaranteeing the existence of a model for the input set when they fail to produce additional instances. A main challenge for this will be to ensure that the extension is also as efficient (or better) than competitive implementations of E-matching when the input problem is unsatisfiable.

ACKNOWLEDGEMENTS

We would like to thank Tim King for implementing preliminary infrastructure in cvc4 for extending these techniques to quantified formulas containing linear arithmetic.

REFERENCES