A Verified SAT Solver with Watched Literals Using Imperative HOL

Mathias Fleury
Max-Planck-Institut für Informatik
Saarbrücken, Germany
mathias.fleury@mpi-inf.mpg.de

Jasmin Christian Blanchette
Vrije Universiteit Amsterdam
Amsterdam, The Netherlands
j.c.blanchette@vu.nl
Max-Planck-Institut für Informatik
Saarbrücken, Germany
jasmin.blanchette@mpi-inf.mpg.de

Peter Lammich
Technische Universität München
Munich, Germany
lammich@in.tum.de
Virginia Tech
Blacksburg, USA
lpeter1@vt.edu

Abstract
Based on our earlier formalization of conflict-driven clause learning (CDCL) in Isabelle/HOL, we refine the CDCL calculus to add a crucial optimization: two watched literals. We formalize the data structure and the invariants. Then we refine the calculus to obtain an executable SAT solver. Through a chain of refinements carried out using the Isabelle Refinement Framework, we target Imperative HOL and extract imperative Standard ML code. Although our solver is not competitive with the state of the art, it offers acceptable performance for some applications, and heuristics can easily be added to improve it further.

Keywords Isabelle/HOL, SAT solving, conflict-driven clause learning (CDCL), stepwise refinement

1 Introduction
SAT solvers are programs that decide the Boolean satisfiability (SAT) problem. Other NP-complete problems are often reduced to SAT, to exploit efficient SAT solvers. For example, the CeFA (non)termination and (non)confluence checker [34], which is formalized in Isabelle/HOL, includes a naive SAT solver based on a disjunctive normal form transformation. Using a verified SAT solver that is reasonably efficient could greatly improve the checker’s performance.

We recently formalized an abstract calculus for conflict-driven clause learning (CDCL) in Isabelle/HOL [8], following Nieuwenhuis, Oliveras, and Tinelli [27]. CDCL is the core of most modern SAT solvers. It generalizes the Davis–Putnam–Logemann–Loveland (DPLL) procedure [12] with clause learning and nonchronological backjumping. We also formalized a CDCL variant due to Weidenbach, described in a paper [35] and in an unpublished book draft, that explores first unique implication points [6, Chapter 3] to learn clauses.

In this paper, we connect the formalized metatheory of CDCL with the code of an imperative SAT solver that implements several key optimizations found in modern CDCL-based solvers. We start by extending Weidenbach’s backjumping rule to minimize conflict clauses [32] (Section 2).

A crucial optimization in modern SAT solvers is the two-watched-literal [26] data structure. It allows for efficient unit propagation and conflict detection—the core CDCL operations. We introduce an abstract transition system, called TWL, that captures the essence of a SAT solver with this optimization as a nondeterministic transition system (Section 3).

Weidenbach’s book draft only presents the main invariant, without a precise description of the optimization. We enrich the invariant based on MiniSat’s [13] source code and prove that it is maintained by all transitions. To get an executable program that can be incorporated into CeFA, we refine the TWL calculus in several correctness-preserving steps. The stepwise refinement methodology enables us to inherit invariants, correctness, and termination from previous refinement steps. The first refinement step implements the rules of the calculus in a more algorithmic fashion, using the nondeterministic programming language provided by the Isabelle Refinement Framework [17] (Section 4). The next step refines the data structure: Multisets are replaced by lists, and clauses justifying propagations are represented by indices into a list of clauses (Section 5). A key ingredient for an efficient implementation of watched literals is a data structure called watch lists. These index the clauses by their two watched literals—literals that can influence their clauses’ truth value in the solver’s current state. Watch lists are introduced in a separate refinement step (Section 6).

Next, we use the Sepref tool [18] to synthesize imperative code for a functional program, together with a refinement proof. Sepref replaces the abstract functional data structures by concrete imperative implementations, while leaving the algorithmic structure of the program unchanged. Isabelle’s code generator can then be used to extract a self-contained...
SAT solver in imperative Standard ML (Section 7). Finally, to obtain reasonably efficient code, we need to implement further optimizations and heuristics (Section 8). In particular, the literal selection heuristic is crucial. We use variable move to front [5] with phase saving [29].

To ascertain the distance between our solver, IsaSAT, and the state of the art, we compare IsaSAT’s performance with four other solvers: MiniSat [13]; the state-of-art solver Glucose [1]; the OCaml-based DPT solver;¹ and the most efficient verified solver we know of, versat [28] (Section 9). The results are sobering; they confirm the view that the generation of and checking of unsatisfiability certificates is the superior approach to combine efficiency and trustworthiness [10, 11, 20]. Compared with versat, the hallmark of our solver is its modularity. Heuristics can easily be incorporated, and further refinement steps can be performed if desired. Furthermore, our solver is guaranteed to terminate.

Much of the scientific value of formalization work is that it constitutes a case study in the use of a proof assistant. We depend heavily on Isabelle’s Refinement Framework. We especially benefited from its ability to align program steps, allowing us to focus on the changes between the refinement steps. The Sepref tool simplifies the last refinement step by generating imperative code and a corresponding refinement theorem. It makes it easy to change data structures. The refinement approach encourages a clean separation of concerns; for example, termination can be proved at the abstract, calculus level, and optimizations can be considered in isolation. Although IsaSAT is not as efficient as the state of the art, we compare IsaSAT’s performance with front [5] with phase saving [29].

To front [5] with phase saving [29].

We define literals as a datatype \( 'v \text{ lit} \) with two constructors: \( \text{Pos} \) and \( \text{Neg} \). The negation of a literal is defined by \(-\text{Pos} A = \text{Neg} A\) and \(-\text{Neg} A = \text{Pos} A\). As is customary in the literature [2, 35], a clause is a multisit of literals and has type \('v \text{ clause} = 'v \text{ lit} \text{ multisit}\). Isabelle multisets are finite. We use logical symbols for clauses to ease reading when there is no risk of confusion, writing \( \neg L, C \lor D \) for \( \emptyset, \{L\}, \) and \( C \lor D \), respectively. A consistent set of literals \( I \) entails a clause \( C (I \models C) \) if and only if \( I \) and \( C \) share a literal. \( I \) entails a (multi)set of clauses \( N \) if and only if \( I \) entails every clause in \( N \).

In our previous paper [8] and in the corresponding journal submission [7], we presented two families of CDCL calculi and connected them through various refinement steps. Here, we briefly describe the calculus that will serve as the starting point for refinement. This calculus, which we call \( \text{W} \), mostly follows Weidenbach’s CDCL variant [35]. It operates on states \((M, N, U, D)\), where \( M \) is the partial model under construction, or \( \text{trail} \); \( N \) is the multiset of initial clauses; \( U \) is the multiset of learned clauses; and \( D \) is a conflict clause, or the special value \( \top \) if no conflict has been detected. The multiset of initial clauses does not change during the execution of the calculus. In contrast, the multiset of learned clauses grows monotonically starting from \( \emptyset \).

The trail \( M \) consists of a list of annotated literals. Each literal \( L \) in \( M \) can be a decision, written \( L^* \), or the result of a unit propagation, in which case it is annotated with the clause \( C \) that caused the propagation, written \( L^C \). The level of a literal \( L \) in \( M \) is the number of decision literals to the right of the atom of \( L \) in \( M \), or 0 if the atom is undefined. The level of a clause is the highest level of any of its literals, with 0 for \( \bot \). The level of a state corresponds to the number of decision literals in the trail. We overload the infix operator \( \cdot \) to denote both the Cons list constructor and list concatenation. In accordance with Isabelle conventions, the trail is extended on the left. In the following, we abuse notation, implicitly converting \( \models \)'s first operand from a list to a set and ignoring annotations on literals.

The calculus assumes that \( N \) contains no duplicate literals and never produces clauses containing duplicates. We write \( S \models_w T \) if the calculus makes a transition from state \( S \) to state \( T \). The following transitions are possible:

- **Propagate** \( (M, N, U, T) \models_w (L^C \cdot M, N, U, T) \)
  if \( C \lor L \in N \lor U \) and \( M \models \neg C \) and \( L \) is undefined in \( M \) (i.e., neither \( L \in M \) nor \(-L \in M \))

- **Decide** \( (M, N, U, T) \models_w (L^\top \cdot M, N, U, T) \)
  if \( L \) is undefined in \( M \) and occurs in \( N \)

- **Conflict** \( (M, N, U, T) \models_w (M, N, U, D) \)
  if \( D \in N \lor U \) and \( M \models \neg D \)

- **Resolve** \( (L^C \cdot M, N, U, D \lor -L) \models_w (M, N, U, C \lor D) \)
  if \( D \) has the level of the current state

- **Skip** \( (L^C \cdot M, N, U, D) \models_w (M, N, U, D) \)
  if \( L \notin D \) and \( D \notin \{\bot, \top\} \)

¹http://dpt.sourceforge.net/
Jump \((M' \cdot K' \cdot M, N, U, D \lor L) \implies w\)
\((L^{\lor L} \cdot M, N, U \lor (D' \lor L), \tau)\)

if \(L\) has the level of the current state, \(D\) has a lower
level, \(D' \subseteq D\), \(N \lor U \vdash D' \lor L\), and \(D'\) has the same
level as \(K\).

The \(W\) calculus works as follows. We start with an ini-
tial state \((e, N, \emptyset, \tau)\) and repeatedly apply the rules until
we reach a normal form. A state \((M, N, U, D)\) is conclusive
if \(D = \tau\) and \(M \models N\) or if \(D = \bot\) and \(N\) is unsatisfiable.

Given a conclusive state, we can extract a solution to the
SAT problem. The calculus always terminates, but there are
no guarantees that the final state is conclusive. If we want
this property, we need a strategy to restrict rule applica-
tions. Weidenbach’s “reasonable” strategy favors Propagate
and Conflict over all other rules. We call the calculus re-
stricted by this strategy \(W^{\text{stgy}}\).

Compared with Weidenbach’s formulation, which formed
the basis of our earlier formalization, the Jump rule has been
generalized to learn \(D' \lor L\) instead of the potentially larger
clause \(D \lor L\). Like its predecessor, this calculus can be seen as
a special case of the abstract CDCL calculus by Nieuwenhuis
et al. [27] and formally connected to it.

Given a relation \(\implies\), we write \(S \implies^* T\) if state \(T\) is a
normal form (i.e., there exists no transition from \(T\)) reachable
from state \(S\).

Theorem 2.1 (Correctness [14, full.cedl_w_stgy_final_state_
conclusive_from_init_state]). \(If (e, N, \emptyset, \tau) \implies W^{\text{stgy}} S'\) and
\(N\) contains no clauses with duplicate literals, then \(S'\) is a con-
nclusive state.

3 Watched Literals

The two-watched-literal (2WL or TWL) scheme [26] is a
data structure that makes it possible to efficiently identify
candidate clauses for unit propagation and conflict. In each
nonunit clause (i.e., clause with at least two literals), we
distinguish two watched literals; the remaining literals are
unwatched. Initially, any of a nonunit clause’s literals can be
chosen to be watched. The solver maintains the following
2WL invariant for each clause:

Unless a conflict has been found, a watched literal may
be false only if the other watched literal is true and all the
unwatched literals are false.

This is the invariant given by Weidenbach. It is inspired
by MiniSat’s code. A consequence of this invariant is that
setting an unwatched literal will never yield a candidate for
propagation or conflict. This can dramatically reduce the
number of candidate clauses to consider.

For each literal \(L\), the clauses that contain a watched \(L\) are
chained together in a list, called a watch list. When a literal \(L\)
becomes true, the solver needs to iterate only through the
watch list for \(\neg L\) to find candidates for propagation or con-

\[1. \neg B \quad C \quad A\]
\[2. \neg C \quad \neg B \quad \neg A\]
\[3. \neg A \quad \neg B \quad C\]
\[4. \neg A \quad B\]

(a) (b)

Figure 1. Evolution of the 2WL data structure on a simple example

1. If the other watched literal is true, do nothing.
2. If one of the unwatched literals \(L'\) is not false, restore
   the invariant by updating the clause so that it watches
   \(L'\) instead of \(\neg L\).
3. Otherwise, consider the other watched literal \(L'\) in the
   clause:
   1. If it is not set, propagate \(L'\).
   2. Otherwise, \(L'\) is false, and we have found a conflict.

Propagation is performed eagerly. When a conflict is de-
tected, the solver stops updating the data structure and pro-
cesses the conflict.

To illustrate how the solver maintains the 2WL invariant,
we consider the small problem shown in Figure 1. The clauses
are numbered from 1 to 4. Gray cells identify the watched
literals. Thus, clause 1 is \(\neg B \lor C \lor A\), where \(\neg B\) and \(C\) are
watched. The following scenario is possible:

1. We start with an empty trail and the clauses shown in
   Figure 1a. We decide to make \(A\) true. The trail becomes
   \(A\). We need to consider every clause where \(\neg A\) is
   watched, i.e., clauses 3 and 4, in any order.
2. We first consider clause 4 for \(\neg A\). We propagate \(B\) from
   it. The trail becomes \(B \cdot A\). We still need to consider
   clause 3 for \(\neg A\) and the clauses for \(\neg B\).
3. We consider clause 3 for \(\neg A\). Since \(C\) is unwatched and
   not false, we swap \(C\) and \(\neg A\), resulting in the clauses
   shown in Figure 1b. We must still consider clauses 1, 2,
   and 3 for \(\neg B\).
4. We consider clause 3 for \(\neg B\): We propagate \(C\). The
   trail becomes \(C \cdot B \cdot A\). We still need to update the
   clauses 1 and 2 for \(\neg B\) and the clauses for \(\neg C\).
5. We consider clause 2. All its literals are false—a con-
   flict. Thanks to the invariant’s precondition (“unless
   a conflict has been found”), we do not need to update
   clause 1 or the clauses for \(\neg C\).

Compatibility with the Jump rule is important for efficiency:
When removing literals from the trail, the invariant is pre-
served without requiring any update.

To capture the 2WL data structure formally, we need a no-
tion of state that takes into account pending updates. These
can concern a specific clause or all the clauses associated
with a literal. As in the example above, we first process the clause-specific updates; then we move to the next literal and start updating its associated clauses.

States have the form \((M, N, U, D, NP, UP, WS, Q)\), of type \(\nu \text{state}_{TWL}\). The pending updates are stored in the last two components: the work stack \(WS\) is a multiset \(\{(L, C_1), \ldots, (L, C_n)\}\), where \(L\) is a false literal and the clauses \(C_i\) \(\) watch \(L\) and may require an update. The other literals to update are stored in the queue \(Q\). For example, at the end of step 4 above, \(WS\) is \(\{\neg B, \neg B \lor C \lor A\}, \neg B, \neg C \lor \neg B \lor \neg A\}\) and \(Q\) is \(\{\neg C\}\).

Moreover, we store the unit clauses separately from the nonunit clauses, in the \(NP\) and \(UP\) components. Each nonunit clause is represented by a value \(\text{Clause}_{TWL}(W, UW)\), where \(W\) is the multiset of watched literals, of cardinality 2, and \(UW\) the multiset of unwatched literals. Unit clauses are represented as singleton multisets.

The state\(_{TWL}\) of function converts a TWL state to a \(W\) state:

\[
\text{definition state}_{TWL} \equiv \lambda \text{state}_{TWL} \Rightarrow \text{state}_{TWL} \text{ where } \\
\text{state}_{TWL} \equiv (M, N, U, D, NP, UP, WS, Q) = \\
(M, \text{image \_of state}_{TWL}(N \equiv NP), \text{image \_of state}_{TWL}(U \equiv UP), D) \\
\text{where \text{clause\_of (Clause}_{TWL}(W, UW)) = W \lor UW \text{ and image } f N \text{ applies the function } f \text{ to each element of multiset } N.}
\]

The first two TWL rules have direct counterparts in \(W\):

Propagate \((M, N, U, \tau, NP, UP, \{(L, C)\} \equiv WS, Q) \Rightarrow_{TWL} (L \cdot C \cdot M, N, U, \tau, NP, UP, WS, \{\neg L\} \equiv Q)\) if watched \(C = \{L, L'\}\), \(L'\) is not set in \(M\), and \(\forall K \in \text{unwatched } C\), \(\neg K \in M\).

Conflict \((M, N, U, \tau, NP, UP, \{(L, C)\} \equiv WS, Q) \Rightarrow_{TWL} (M, N, U, C, NP, UP, \emptyset, Q)\) if watched \(C = \{L, L'\}, \neg L' \in M\), and \(\forall K \in \text{unwatched } C\), \(\neg K \in M\).

For both rules, the condition \(\forall K \in \text{unwatched } C\), \(\neg K \in M\) is necessary because the 2WL invariant trivially holds for \(C\) as long as an update on \(C\) is pending.

The next rules manipulate the state’s 2WL-specific components, without affecting its semantics as seen through the function \(\text{state}_{TWL}\):

Update \((M, N, U, \tau, NP, UP, \{(L, C)\} \equiv WS, Q) \Rightarrow_{TWL} (M, N', U', NP, UP, WS, Q)\) if \(K \in \text{unwatched } C\), \(\neg K \notin M\), and \(N'\) and \(U'\) are obtained from \(N\) and \(U\) by replacing the clause \(C = \text{Clause}_{TWL}(W, UW)\) with \(\text{Clause}_{TWL}(W - \{L\} \equiv \{K\})\) \((UW - \{K\} \equiv \{L\})\).

Ignore \((M, N, U, \tau, NP, UP, \{(L, C)\} \equiv WS, Q) \Rightarrow_{TWL} (M, N, U, \tau, NP, UP, WS, Q)\) if watched \(C = \{L, L'\}\) and \(L' \in M\).

Next_Literal \((M, N, U, \tau, NP, UP, \emptyset, \{L\} \equiv Q) \Rightarrow_{TWL} (M, N, U, \tau, NP, UP, \{(L, C)\}, L \in \text{watched } C \land C \notin N \cup U, Q)\)

As in \(W + \text{stgy}\), we postpone decisions. This is achieved by requiring that \(WS\) and \(Q\) are empty in the Decide rule. Skip and Resolve are as before, except that they also preserve the 2WL-specific components of the state. Due to the distinction between unit and nonunit clauses, we need two rules for nonchronological backjumping:

Decide \((M, N, U, \tau, NP, UP, \emptyset, Q) \Rightarrow_{TWL} (L \cdot M, N, U, \tau, NP, UP, \emptyset, \{L\})\) if \(L\) is not defined in \(M\) and appears in \(N\).

Jump\_Nonunit \((M' \cdot K \cdot M, N, U, D \lor L, NP, UP, \emptyset, Q) \Rightarrow_{TWL} (L \lor L, M, N, U \lor \{\text{Clause}_{TWL}(L, L')\} \cdot (D' - \{L'\}), \tau, NP, UP, \emptyset, L)\) if the conditions on Jump are satisfied by \(D, D', L, L' \in D, L'\) has the highest level among \(D'\)’s literals.

Jump\_Unit \((M' \cdot K \cdot M, N, U, D \lor L, NP, UP, \emptyset, L) \Rightarrow_{TWL} (L \cdot M, N, U, \tau, NP, UP \lor \{L\}, \emptyset, L)\) if the conditions on Jump are satisfied by \(D, D' = \emptyset, and L\).

In Jump\_Nonunit, we need to choose a literal \(L'\) of \(D'\) with the highest level among \(D'\)’s literals, or the next-highest level in \(D' \lor L\) (since \(L\) has a higher level than \(L'\)). Jump\_Nonunit is documented in MiniSat’s code (“find the first literal assigned at the next-highest level”). Remarkably, this important property is mentioned neither in Weidenbach’s book draft nor in the description of MiniSat [13].

**Theorem 3.1** (Invariant [14, cdcl\_twl\_stgy\_twl\_struct\_inv]). If the state \(S\) satisfies the 2WL invariant and \(S \Rightarrow_{TWL} T\), then \(T\) satisfies the 2WL invariant.

**Theorem 3.2** (Refinement [14, full\_cdcl\_twl\_stgy\_cdcl\_stgy]). Let \(S\) be a state that satisfies the 2WL invariant. If \(S \Rightarrow_{TWL} T\), then \(\text{state}_{TWL}\_of (S) \Rightarrow_{W} \text{state}_{TWL}\_of T\).

TWL refines \(W + \text{stgy}\)’s end-to-end behavior and produces final states that are also final states for \(W\). We can apply Theorem 2.1 to establish partial correctness. Termination of TWL is a direct consequence of the termination of \(W\).

### 4 Refining to an Algorithm

Our final goal is to obtain a SAT solver implementation from the TWL calculus. We achieve it by refining the calculus in multiple consecutive steps to an implementation.

The Isabelle Refinement Framework [17, 18, 21] provides a tool chain for program development via stepwise refinement. It is based on the nondeterminism monad over the datatype \(\text{a nres = FAIL | RES (\text{a set})}\). If the program has an execution that diverges or raises an error, its result is FAIL; otherwise, the result is RES \(X\), where \(X\) is the set of possible return values. The function \(\text{RETURN}\_x\), which abbreviates \(\text{RES (\text{x})}, returns the value \(x\); bind \(m f\) nondeterministically chooses a return value from \(m\) and applies \(f\) to it. Based on these constructs and Isabelle’s standard \(\text{if-then-else}\) and \text{case expressions}, the Refinement Framework defines
higher-level constructs such as ‘while’ and ‘for each’ loops.

The Haskell-style ‘do’ monadic notation is also supported:
do \{ a \leftarrow m; f a \} is syntactic sugar for bind \( m . f \).

The first step in the refinement chain is to implement the

\( \mathcal{P} \times \mathcal{U} \) calculus as a program in the nondeterministic monad. The

program operates on states of type \( \mathcal{P} \times \mathcal{U} \) as in the

TWL calculus, but it reduces some of the calculus’s nonde-
terminism. The program consists of a few functions that

implement mutually disjoint sets of rules. We focus on the

function that applies Propagate, Conflict, Update, or Ignore,

assuming that its first argument, the pair \( \mathcal{P} \mathcal{U} = (L, C) \), has

already been removed from the WS component of \( S \):

\[
definition \text{PCUI}_{\text{algo}} ::
\begin{align*}
\{ \mathcal{P} \mathcal{U} \} \times \{ \mathcal{P} \mathcal{U} \} & \Rightarrow \{ \mathcal{P} \mathcal{U} \} \times \{ \mathcal{P} \mathcal{U} \} \\
\text{where} & \\
\text{PCUI}_{\text{algo}}(L, C) = \{ \mathcal{P} \mathcal{U} \} & = \{ \text{do} \} \\
& \begin{cases} 
\text{let} (M, N, U, D, NP, UP, WS, Q) = S; & \\
\text{let} (L, C) = LC; & \\
L' \leftarrow \mathcal{R}(L' | L' \in \text{watched}\ C - \{L\}); & \\
\text{if} L' \in M & \\
\text{return} S \\
\text{else} & \\
\text{if} \: VL \in \text{unwatched}\ C, \: -L \in M & \\
\text{return} M, N, U, C, NP, UP, WS, Q & \\
\text{else} & \\
\text{return} (L', M, N, U, D, NP, UP, WS, Q) & \\
\end{cases} \\
\text{else} & \\
\text{return} (L', M, N, U, D, NP, UP, WS, Q) & \\
\end{cases}
\]

The predicate \( \text{update}_{\text{algo}}(N, U) \) updates the

clause \( C \) by exchanging the watched literal \( L \) and the un-

watched literal \( K \) in \( C \). The update is performed in \( N \) and \( U \),

yielding \( N' \) and \( U' \). Since propagations are performed ea-

gerly, WS never refers to unit clauses.

The \( \text{PCUI}_{\text{algo}} \) algorithm still contains abstract, nondeter-

ministic parts. For example, in the Update part, we leave the

choice of the new watched literal \( K \) unspecified.

To allow us to specify the connection between two pro-

grams, the Refinement Framework defines a partial order

\( \leq \) on \( \mathcal{P} \mathcal{U} \) revises as \( \text{FAIL} \) as the top element: \( \mathcal{P} \mathcal{U} \leq \mathcal{P} \mathcal{U} \)

if and only if \( X \subseteq \mathcal{Y} \), and \( r \leq \text{FAIL} \) for all \( r \). The bottom

element \( \mathcal{P} \mathcal{U} \) is an unrefinable program. We also use this

partial order to state program correctness: The statement

\( P \mathcal{U} \hookrightarrow f \mathcal{U} \leq \mathcal{P} \mathcal{U} \{ y | Q y \} \) expresses the total correctness

of program \( f \) with precondition \( P \) and postcondition \( Q \). For

\( \text{PCUI}_{\text{algo}} \), we have the following refinement theorem:

\[ \forall L \in M: \exists \mathcal{P} \mathcal{U} \subseteq \mathcal{P} \mathcal{U} \text{sat} \rightarrow \mathcal{P} \mathcal{U} \text{sat}. \]

\[ \text{Lemma 4.1 (Refinement) [14, unit_propagation_inner_loop_body_}

add]). If the 2WL invariant holds for all clauses occurring in

the \( N \) and \( U \) components of \( S \), then

\[ \text{PCUI}_{\text{algo}}(L, C) \mathcal{P} \mathcal{U} \subseteq \mathcal{P} \mathcal{U} \{ T | \text{add}_{\text{to} WS}(L, C) S \Rightarrow \text{PCUI}_{\text{algo}}(L, C) \mathcal{P} \mathcal{U} \} \]

The PCUI subcircuit on the transition arrow refers to the

fragment of TWL consisting of the four rules Propagate,

Conflict, Update, and Ignore, whereas \( \text{add}_{\text{to} WS}(L, C) \mathcal{P} \mathcal{U} \) returns the

state obtained by adding \( (L, C) \) to \( S \)'s WS component.

For the entire SAT solver, we have the following

\[ \text{Theorem 4.2 (Refinement) [14, add_twcl_sty prog spec]}. \text{ If the} \]

2WL invariant holds for all clauses occurring in the \( N \) and \( U \) components of \( S \), then

\[ \text{TWL}_{\text{algo}} \mathcal{P} \mathcal{U} \subseteq \mathcal{P} \mathcal{U} \{ T | S \Rightarrow \text{TWL}_{\text{algo}} \mathcal{P} \mathcal{U} \} \]

The state returned by the program is a final state for TWL.

From Theorem 3.2, we deduce that it is also a final state

for W+stg. Hence, the program TWL_{\text{algo}} is a SAT solver by

Theorem 2.1.

5 Representing Clauses as Lists

The nondeterministic program \( \text{TWL}_{\text{algo}} \) presented in Section

4 relies on the same state type as the TWL calculus. This

changes with the next refinement step: We now store the

initial and learned clauses together in a list, and we use indices

to refer to the clauses. States are now tuples \( \langle M, NU, u, D, NP, UP, WS', Q \rangle \):

\[ \begin{align*} \& \quad \text{NU is the list of all nonunit clauses. It simultaneously} \\
\& \quad \text{refines N and U. The initial clauses occupy indices 1} \\
\& \quad \text{to u - 1, and the learned clauses start at index u. The} \\
\& \quad \text{list’s first element is left unused to keep index 0 as a} \\
\& \quad \text{null clause reference.} \\
\& \quad \text{M is the trail, where the annotations are replaced by} \\
\& \quad \text{numeric indices. For nonunit clauses, } L' \text{ is used instead of} \\
\& \quad \text{L if } NU ! ! i = C, \text{ where the ! operator denotes 0-} \\
\& \quad \text{based list access. When annotating literals with unit} \\
\& \quad \text{clauses (which are not present in } NU \text{), we use the} \\
\& \quad \text{special index 0—i.e., we put } L' \text{ on the trail to mean } L'. \\
\& \quad \text{In WS'}, \text{ we implement a pair } (L, C) \text{ by the index of} \\
\& \quad \text{clause } C. \text{ The literal } L, \text{ which is the same for all pairs} \\
\& \quad \text{in WS, is stored locally in the refined unit propagation} \\
\& \quad \text{algorithm.} \\
\end{align*} \]

Abusing notation, we will use the letter \( C \) to refer to clause

indices and will not insist on the distinction between a clause

and the index that refers to it.

In addition to the modifications to the state, we also trans-

form the representation of clauses, from a pair of multisets

holding the watched and unwatched literals to a list of lit-

erals such that its first two elements are watched. Given a

nonunit clause (index) \( C \), its watched literals are available

as \( (NU ! C)! 0 \) and \( (NU ! C)! 1 \). Furthermore, we set the

stage for future refinements by replacing the test \( L \in M \) by a
call to a function, polarity, that returns Some True if \( L \in M \),
Some False if \(-L \in M \), and None otherwise.

The refined version of the PCUI\(_{algo}\) algorithm follows:

```latex
\begin{align*}
\text{definition PCUI\textsubscript{list} ::} \\
&'\nu \text{ lit} \Rightarrow '\nu \text{ clause_idx list} \Rightarrow '\nu \text{ state list} \\
&\text{where} \\
&\text{PCUI\textsubscript{list} } L C S \text{ do} \\
&\text{let (} M, N U, u, D, N P, U P, W S, Q \text{) } = S; \\
&\text{let } i = \text{ if } (N U \mid C) \cdot 1 = L \text{ then } 0 \text{ else } 1; \\
&\text{let } L' = (N U \mid C) \cdot (1 - i); \\
&\text{let } pol' = \text{ polarity } M L'; \\
&\text{if } pol' = \text{ Some True then} \quad \text{(\textit{\# Ignore \#})} \\
&\text{RETURN (} M, N U, u, D, N P, U P, W S, Q \text{)} \\
&\text{else} \\
&\text{case find_unwatched } M (N U \mid C) \text{ of} \\
&\text{None } \Rightarrow \\
&\text{if } pol' = \text{ Some False then} \quad \text{(\textit{\# Conflict \#})} \\
&\text{RETURN (} M, N U, u, N U \mid C, N P, U P, \emptyset, \emptyset \text{)} \\
&\text{else} \quad \text{(\textit{\# Propagate \#})} \\
&\text{RETURN (} L C \cdot M, N U, u, D, N P, U P, W S, \\
&\{ -L' \} \cup Q \text{)} \\
&| \text{ Some } j \Rightarrow \text{ do} \quad \text{(\textit{\# Update \#})} \\
&\text{let } N U'' = \text{ list_update } N U C \\
&\text{ (list_swap } (N U \mid C) i j \text{)}; \\
&\text{RETURN (} M, N U', u, D, N P, U P, W S, Q \text{)} \\
&\end{align*}
```

Refinement between a concrete program \( g \) and an abstract program \( f \) is expressed by a statement \( \forall x. y. (y, x) \in R \Rightarrow g y \leq \downarrow S f x \), where \( R \) is a relation between concrete and abstract arguments, and \( S \) is a relation between concrete and abstract results. The function \( \downarrow S \) maps an abstract result to the largest concrete result whose values are related, by \( S \), to abstract values. Two edge cases are \( \downarrow S \text{ FAIL} = \text{ FAIL} \) and \( \downarrow S r = r \). The former implies that a failing assertion is refinable by any program, so we can assume in the refinement proof that assertions on the abstract side never fail. The latter makes correctness a special case of refinement, the abstract program being of the form \( \text{RES} \{ x \mid Q x \} \).

The Refinement Framework includes a verification condition generator. Hoare-logic-style rules are used to prove correctness goals. For other refinement goals, a heuristic tries to align the concrete and abstract program structure and generates refinement goals for corresponding statements of the two programs. In the refinement proof of the PCUI algorithm, the goal for the definition of the other watched literal \( L' \) is \((N U \mid C) \cdot (1 - i) \in \text{watched } C \cdot \{ L \} \). Intuitively, this holds because for \( i \in \{0, 1\} \), the expression \( 1 - i \) returns the index of the other watched literal.

The generated goals are often easy to discharge with standard Isabelle tactics, but they may also point to missing lemmas or invariants. The primary technical challenge during proof development is to handle cases where the verification condition generator fails to properly align the programs and generates nonsensical, and usually unprovable, proof obligations. In some cases, the tool generates error messages, but these are often cryptic. Another hurdle is that refinement proof goals can be very large, and the Isabelle/jEdit graphical interface is painfully slow at displaying them. We suspect this is mostly due to type annotations and other metainformation available as tooltips.

## 6 Storing Clauses Watched by a Literal: Watch Lists

In the Next\_Literal rule of the TWL calculus, the set of clauses that watch a given literal is calculated. A refinement step eliminates this gratuitous inefficiency: Instead of iterating over all clauses, we maintain a map from literals to the clauses that contain them as watched literals. States now have the form \((M, N U, u, D, N P, U P, Q, W)\), where \( W :: '\nu \text{ lit} \Rightarrow \text{ clause_idx list} \) maps each literal to its watch list.

The abstract state stores all the clauses that watch the current literal \( L \) and still require processing in its WS component. In the concrete algorithm, we use a local variable \( w \) to traverse the watch list. After processing a clause, there are two cases. If the clause still watches \( L \) (rules Propagate, Conflict, and Ignore), we increment \( w \) to move to the next clause. Otherwise, the clause no longer watches \( L \) (rule Update). We exchange the element at index \( w \) with the watch list’s last element and shorten the list by one (function delete\_idx\_and\_swap). Since the traversal order is irrelevant, this is an efficient way to delete an element in constant time based on arrays. This technique is implemented in many solvers.

The refined PCUI algorithm is presented below, where the syntax \( f(x := y) \) denotes the function that maps \( x \) to \( y \) and otherwise coincides with \( f \):

```latex
\begin{align*}
\text{definition PCUI\textsubscript{list} ::} \\
&'\nu \text{ lit} \Rightarrow \text{nat} \Rightarrow '\nu \text{ state list} \Rightarrow \text{nat} \times '\nu \text{ state list} \\
&\text{where} \\
&\text{PCUI\textsubscript{list} } L w S \text{ do} \\
&\text{let (} M, N U, u, D, N P, U P, Q, W \text{) } = S; \\
&\text{let } C = W \cdot L \cdot w; \\
&\text{let } i = \text{ if } C \cdot 0 = L \text{ then } 0 \text{ else } 1; \\
&\text{let } L' = (N U \mid C) \cdot (1 - i); \\
&\text{let } pol' = \text{ polarity } M L'; \\
&\text{if } pol' = \text{ Some True then} \quad \text{(\textit{\# Ignore \#})} \\
&\text{RETURN (} w + 1, \text{ (} M, N U, u, D, N P, U P, Q, W \text{)} \text{)} \\
&\text{else} \\
&\text{case find_unwatched } M (N U \mid C) \text{ of} \\
&\text{None } \Rightarrow \\
&\text{if } pol' = \text{ Some False then} \quad \text{(\textit{\# Conflict \#})} \\
&\text{RETURN (} w + 1, \text{ (} L C \cdot M, N U, u, D, N P, U P, \\
&\text{\{ -L' \} \cup Q, W) \text{)} \\
&\text{else} \quad \text{(\textit{\# Propagate \#})} \\
&\text{RETURN (} w + 1, \text{ (} L C \cdot M, N U, u, D, N P, U P, \\
&\text{\{ -L' \} \cup Q, W) \text{)} \\
&\end{align*}
```
701 When performing a chain of refinements, we often want to reuse information from earlier refinement steps. Assume that we have previously shown the refinement relation
702 \[ g(y) \leq \bigcup_{(u, t) \in S} \{ j_{\text{new}} \cdot u \cdot t \} \cdot g(y) \tag{1} \]
703 where \( R \) relates concrete and abstract states and \( I_1 \) and \( I_2 \) are invariants. Now suppose we want to refine \( g \) by the function \( h \) with relation \( S \) and invariant \( J \). The invariant \( J \) typically consists of a genuinely new part \( J_{\text{new}} \) and a part inherited from higher abstraction levels. We first prove the new part:
704 \[ h(z) \leq \bigcup_{(u, t) \in S} \{ j_{\text{new}} \cdot u \cdot t \} \cdot g(y) \tag{2} \]
705 Then we can combine it with equation (1), using the invariant \( I_1 \) that does not depend on a state \( s \), yielding
706 \[ h(z) \leq \bigcup_{(u, t) \in S} \{ j_{\text{new}} \cdot u \cdot t \land I_1 \cdot t \} \cdot g(y) \tag{3} \]
707 Finally, we can prove the desired refinement relation \( h(z) \leq \bigcup_{(u, t) \in S} \{ j_{\text{new}} \cdot u \cdot t \land I_1 \cdot t \} \cdot g(y) \), by showing the inclusion
708 \[ \{(u, t) \in R \mid j_{\text{new}} \cdot u \cdot t \land I_1 \cdot t \} \subseteq \{(u, t) \in R \mid J \cdot u \cdot t \} \tag{4} \]
709 Because we frequently needed to combine large invariants to derive refinement lemmas such as (3), we developed a specialized tactic in the Eishbach language [25]. It takes as input the relations (1) and (2). It separates \( I_1 \) and \( I_2 \), based on their syntactic dependencies, and derives the relation (3).
710 Another Eishbach tactic takes (3) and the desired refinement goal as arguments and leaves (4) as the goal. Eishbach is very useful for such tedious but straightforward manipulations, especially for goals containing large formulas.

### 7 Generating Code

In the last refinement steps, we introduce imperative data structures. To represent code with side effects, we use Imperative HOL [9], a library for Isabelle/HOL that is based on the heap monad over the datatype 'a Heap = Heap (heap ⇒ ('a × heap) option). A program of type 'a Heap takes a memory state (of type heap) as input and returns, on success, a value (of type 'a) and a new memory state.

For technical reasons, we need an intermediate refinement step between the introduction of watch lists (Section 6) and the change of data structures. This step amounts to adding assertions in the watch list algorithms stating that all literals belong to a fixed, finite domain. Given the set of all literals \( L_{\text{in}} \) that appear in the clause set \( N \), we need to consider only the literals that appear in \( L_{\text{in}} \) or whose negation appear in \( L_{\text{in}} \). We call this set \( L_{\text{all}} \). The intermediate refinement step involves stating and discharging assertions of the form \( I \in L_{\text{all}} \). This sets the stage for many subsequent optimizations, because it allows to allocate arrays that are large enough to represent mappings from atoms or literals. Arrays are used for watch lists (which map literals to clauses), polarity caching (which map atoms to their polarities, corresponding to the polarity function), and other optimizations.

To generate imperative code, the Sepref tool [18] bridges the gap between the Refinement Framework and Imperative HOL. It can be used to automatically replace the operations of the abstract algorithm in the nondeterminism monad by their concrete deterministic counterparts in the heap monad.

The outcome is a deterministic imperative program and a refinement theorem linking it to the original abstract program.

Some of the data structures we need are already available in the Imperative Collections Framework [19], while others must be developed specifically for this project. Since the code in Imperative HOL is deterministic, we must commit to a strategy for applying the calculus rules. The precise heuristics and other optimizations are described in Section 8.

The solver state is enriched with some information necessary for optimizations and heuristics (cf. Section 8), and its components are implemented by efficient data structures: For example, literals are refined to 32-bit unsigned integers, representing a positive literal \( \text{Pos} i \) by \( 2 \cdot i \) and a negative literal \( \text{Neg} i \) by \( 2 \cdot i + 1 \). All required operations, such as atom extraction and negation, can be efficiently implemented on this representation. The use of 32-bit numbers restricts our implementation to at most \( 2^{31} \) atoms, which, however, seems to be a common restriction for SAT solvers.

The encoding of literals as unsigned integers can be used to represent a map from literals by an array, indexed by the literal representation. This way, we implement the \( W \) function that maps literals to its watch lists by an array of arrays. The outer array’s size is determined by the actual number of atoms in the problem, while we use a dynamic resizing strategy for the inner arrays that hold the watch lists. Using the same literal encoding, clauses are represented by arrays of 32-bit integers.

Internally, the refinement of the state is done in two steps: The first step handles the addition of the data for optimizations and heuristics, and the second step uses Sepref to refine the functional representations of the state’s components to efficient imperative data structures.

To obtain a complete SAT solver, we must provide code to initialize the data structure with the 2WL invariant using the list of the atoms in the problems. Initialization works as follows: We first go through the clauses and extract all the atoms by taking the literal where it occurs first. Then for each clause, either it contains at least two literals, in which case the first two are watched, or it is a unit clause, in which case the literal is propagated (or a conflict is marked) and
the clause is added to NP. If there is a conflict, there is no need to analyze it—the clauses are unsatisfiable.

Once we have refined TWL to an imperative algorithm and combined it with a function initializing the data structure from a list of clauses, we define the complete imperative SAT solver as a function IsaSAT_code in Imperative HOL. The abstract specification of the solver is given by

$$\text{model_if_satisfiable = RES \{ M | \text{if satisfiable CS then } M \neq \text{None} \land \text{the } M \models CS \text{ else } M = \text{None} \}$$

where the (Some x) = x. This abstract program returns None if the input clauses are unsatisfiable; otherwise, it returns Some M, where M is a model of the clauses. By combining the refinement theorems for all refinement steps, we obtain end-to-end correctness for the entire solver.

**Theorem 7.1 (End-to-End Correctness [14, IsaSAT_code_full_correctness]).** The imperative SAT solver returns a model if its input is satisfiable:

$$(\text{IsaSAT_code, model_if_satisfiable}) \in \text{no_duplicate_no_false} \text{ clauses_assn}^k \rightarrow \text{option_assn (list_assn lit_assn)}$$

The refinement predicate $p', p \in [\text{precond}] \text{ arg } \rightarrow \text{res}$ means that if the precondition precond holds on the arguments and if the arguments are refined by the relation arg, then the two programs $p'$ and $p$ return a result refined by the relation res. The clauses_assn relation refines a multiset of multisets of literals to a list of lists of 32-bit literals, and option_assn (list_assn lit_assn) refines an optional list of literals to an optional list of 32-bit literals.

Finally, we invoke Isabelle’s code generator [15] to extract Standard ML code from the Imperative HOL program. The result is a self-contained program consisting of about 2700 lines of code. It is extended with a simple unverified parser for SAT problems in conjunctive normal form. To give a flavor of the program, we show its main loop below (slightly reformatted for readability):

```ml
fun IsaSAT_code initial_state () =
  let val (_, final_state) =
    heap_WHILELET
      (fn (done, _) => fn () => not done)
      (fn (_, T) =>
        analyze_or_decide_code
        (PCUI_and_Next_Literal T ()))
    (false, initial_state) ()
  in final_state end
```

**8 Optimization and Heuristics**

Our imperative SAT solver relies on a few optimizations that deserve to be explained in more detail: an efficient decision heuristic, a representation of conflicts as a lookup table, and the elimination of redundant components from the state.

### 8.1 Variable Move to Front

The variable-move-to-front (VMTF) heuristic [5], based on the move-to-front algorithm [30], selects which atom to decide next. It offers similar performance to the better-known variable-state-independent-decaying-sum (VSIIDS) scheme [26]. VMTF’s main advantage, from a formalization point of view, is that it does not require floating-point arithmetic.

VMTF works on a list of atoms $A_s$, which must contain all the atoms from $L_0$ in some order. Two operations access or modify this list: When a decision is needed, VMTF traverses $A_s$ to find the first unset atom with respect to the trail. When an atom is heuristically found to be important to the problem, it is moved to the front of $A_s$ so that it is found next—an operation called resoring.

To speed up these operations, we implement some of the optimizations described by Biere and Fröhlich [5]:

- To efficiently remove atoms from $A_s$, we represent it by a doubly linked list. Moreover, we store it in an array $ns$ indexed by the atoms, enabling fast accesses to the associated nodes. Each entry in $ns$ has the form $(st, prev, next)$, where $st$ is the timestamp indicating when the atom was resored, and $prev$ and $next$ are the linked-list “pointers,” or rather indices in $A_s$ (with None representing a null pointer).
- We extend the data structure with a next_search component that stores an atom. If $A_s = A_{S_0} \cdot \cdot \cdot A_{S_{|A_s|-1}}$, with next_search = $A_{S_j}$, all atoms $A_{S_0}, \ldots, A_{S_{j-1}}$ are set in the trail. When searching for an undefined atom, we can start at index $j$.
- Timestamps enable us to efficiently unset a literal (e.g., when jumping): Since atoms are sorted in reverse timestamp order in $A_s$, we need to update next_search only if the unset atom has a higher timestamp than the current next_search atom.
- We batch the rescoring of atoms. Atoms are not removed from $A_s$ until the end of the next jump when rescoring takes place: We sort the atoms to resore by their timestamps and prepend them to $A_s$.

The VMTF data structure is captured as a tuple $\text{vmtf} = ((ns, st, fst, next_search), to_rescore)$. The $ns$ component corresponds to the doubly linked list described above; $st$ is the maximum timestamp; $fst$ gives the first atom in $A_s$; and $to_rescore$ is the batch of atoms that are awaiting resoring.

In Isabelle, we define the inductive predicate $\text{vmtf} As st ns$ that checks whether $ns$ stores a doubly linked list corresponding to $As$ and the timestamps are bounded by $st$. It is defined by the following introduction rules:

**Empty list** $\text{vmtf} \epsilon st ns$, where $\epsilon$ denotes the empty list;

**Singleton list** $\text{vmtf} i st ns$ if $i < |ns|$ and $ns!i = (\text{st, None, None})$;

**List of length 2 or more** $\text{vmtf} (i \cdot j \cdot As) (st + 1) ns$ if $\text{vmtf} (j \cdot As) st ns', i \neq j, i < |ns|$, and $ns$ is $ns'$ where...
\[ns!i = (st + 1, \text{None}, \text{Some } j)\] and the \text{prev} component of \(ns!j\) has been updated to \text{Some } i.

In the function that finds the next unset literal, we iterate over the doubly linked list stored in \(ns\):

\[
\text{find_next_undef }((ns, st, \text{fst, next_search}), _) \ = \ \text{do } \{
\text{WHILE} (\lambda \text{next_search}. \text{next_search} \neq \text{None}) \land \text{defined_atm } M \ (\text{the next_search}) \ \\
(\lambda \text{next_search}. \ \\
\text{RETURN} \ (\text{get_next } (A! \ \text{the next_search})) \ \\
\text{next_search}
\}
\]

The \text{defined_atm} predicate tests whether an atom is set in the trail. The \text{get_next} \(i\) function returns the next component of the node associated with atom \(i\)—i.e., the atom following atom \(i\) in \(As\) (or \text{None} if \(i\) is the last element in \(As\)).

To prove this program correct, we must show the termination of the while loop, which amounts to the well-foundedness of the relation

\[
\{(\text{get_next } (ns! (\text{the next_search})), \text{next_search}) | \ \text{next_search} \neq \text{None}\}
\]

This, in turn, amounts to showing that the chain of get_next calls contains no loops. We achieve this by showing that the chain is a traversal of the list \(As\), which is finite.

When implementing a heuristic such as VMTF, we must prove that it does not fail (e.g., because of an out-of-bound array access) and that it returns a correct result. We do not need to prove that our implementation is actually a “VMTF” as defined by Biere and Fröhlich [5]. For example, there are no formal guarantees that the sorting function we use to rescore the batches by their timestamps is correct; it is sufficient to show that sorting introduces no new atoms.

VMTF gives only the next atom to decide (if there exists one). We also need to choose the literal’s polarity. We use the \text{phase saving} heuristic [29]. It is a mapping \(\varphi\) from an atom to a polarity, implemented as an array of Booleans. Initially, all atoms are mapped to a negative polarity. Then for each conflict, the mapping is updated: Every atom involved in the conflict will be mapped to the polarity it has in the trail.

### 8.2 Conflict Clause as a Lookup Table

In the TWL calculus and the refinements shown so far, the conflict clause is either \(\top\) (\text{None}) or an actual clause (\text{Some } \(C\)).

Four operations access or modify the conflict clause:

- The Conflict rule replaces \(\top\) by a conflict clause.
- The Resolve rule merges the conflict clause with another clause, removing duplicates.
- The choice between rules Resolve and Skip depends on whether the head of the trail appears in the conflict clause.
- The choice between Resolve and Jump requires an iteration through the clause to evaluate the maximum level of the clause minus one literal.

Initially, we tried representing the conflict as an optional resizable array that is converted to a nonresizable array when the clause is learned (rule \text{Jump Nonunit}). However, this now led to many memory allocations and to inefficient code for resolution (rule \text{Resolve}).

Inspired by MiniSat, we moved to an encoding of the conflict clause as a lookup table. We use an array \(ps\) such that the entry at position \(i\) indicates the polarity of atom \(i\) in the conflict clause—i.e., whether the literal \(i\) occurs positively, negatively, or not at all in the clause. More precisely, a conflict clause is represented by a triple \((b, n, ps)\), where \(b\) indicates whether the conflict is \(\top\) and \(n\) stores the size of the conflict clause. The \(n\) component is useful to quickly test whether the conflict clause is empty, or whether it has size one.

There are two main differences between the lookup table and the original version. First, duplicate literals and tautologies cannot be represented. We know from our invariants that this is no problem. Second, the clause can only contain atoms that are smaller than the length of array.

To give a sense of what this involves, we describe the refinement of a small but somewhat tricky program fragment from the abstract level, where a conflict is an optional multiset, to the concrete level, where a conflict is a lookup table. At the end of Jump\_Nonunit, we need to convert the conflict clause \(C\) to a list that we can add to our list of clauses such that two given literals \(L, L' \in C\) are watched (i.e., are at positions 0 and 1). This conversion is specified abstractly as

\[
\text{RES } ((D, \text{None}) \ | \ D! \ = \ L \land \ D!1 = L' \land mset \ D = C \land |D| \geq 2)
\]

The condition \(|D| \geq 2\) ensures that the accesses to positions 0 and 1 are well-defined. In the refined code, we convert the lookup table to an array \((D\text{ in the specification})\) and at the same time empty the lookup table (instead of reallocating a new one later: that is the None of the specification).

The refinement is done in two steps: We first refine the specification to an intermediate function that describes the implementation on the level of the abstract data structures (leftmost column of Figure 2). In a second step, the abstract data structures and operations are refined to concrete data structures and operations (rightmost column of Figure 2). The middle column gives the refinement relation that connects the notions of states used on either side, before and after every statement. Each statement from the intermediate code is mapped to a concrete function, such that the refinement relation of the result is also the refinement relation of the arguments of the next statement. Since intermediate and concrete functions must have the same number of arguments, some arguments are ignored on the concrete side (indicated by _ in the \(\lambda\)-abstraction).

### 8.3 State Representation

The states we are considering before generating code in Imperative HOL are eight-tuples \((M, NU, u, D, NP, UP, Q, \).

---

[931] A Verified SAT Solver with Watched Literals  
Submitted to CPP 2018, January 8–9, Los Angeles, California, USA
**Figure 2.** Conversion from the lookup table to a clause, assuming $C \neq \text{None}$

### Refinement relation

<table>
<thead>
<tr>
<th>Intermediate code</th>
<th>Imperative HOL code</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(b', n', ps'_{C'})$ refines the clause $C$ as a lookup table; $L'$ and $K'$ refine the literals $L$ and $K$</td>
<td>$n' \leftarrow \text{size_conflict_code} (b', n', ps'_{C'})$</td>
</tr>
<tr>
<td>The 32-bit unsigned integer $n'$ is equal to the natural number $n$</td>
<td>$D' \leftarrow \text{Array_new} n' K'$</td>
</tr>
<tr>
<td>The array $D'$ has the same length and same content as the list $D$</td>
<td>$D' \leftarrow \text{Array_upd} 1 D' L'$</td>
</tr>
<tr>
<td>The array $D'$ refines the updated list $D$; both contain $K$ at position 1</td>
<td>$(b', n' - 2, ps'<em>{C'}) \leftarrow \text{remove_from} K' L' (b', n', ps'</em>{C'})$</td>
</tr>
<tr>
<td>$(b', n' - 2, ps'_{C'})$ refines the clause $C'$</td>
<td>$(E', (b', n', ps'<em>{C'})) \leftarrow (\lambda</em>{..}\text{_conflict_with_cls}) K' L' D' (b', n', ps'_{C'})$</td>
</tr>
<tr>
<td>The array $E'$ refines the clause $C$, and $(b', n', ps'_{C'})$ refines $\top$</td>
<td>$\text{the} (\text{get_conflict_wlist} S) = \emptyset$</td>
</tr>
</tbody>
</table>

*W). However, two components are redundant and can be eliminated: Unit clauses are added to $NP$ and $UP$ but never accessed afterwards.

Initially, we wrote code as we have shown in Section 6: All function bodies started with let $(M, NU, u, D, NP, UP, WS, Q) = S$. This made it convenient to refer to the components individually, or to refine them. We could also add information to the components during refinement. For example, since the VMTF heuristic depends on the trail, its vmtf tuple could be added to the refined trail component. However, this approach works only if the additional information depends on a single component. Moreover, it offers no way to eliminate redundant components such as $NP$ and $UP$.

After gathering some experience with the Refinement Framework, we decided to move to a different scheme, following which all state manipulation is mediated by accessor functions. We can then refine each of these functions individually. For example, when refining $(M, NU, u, D, NP, UP, WS, Q)$ to the intermediate representation $(M, NU, u, D, WS, Q, \text{vmtf}, \varphi)$ with heuristics (where $\text{vmtf}$ is the VMTF data structure and $\varphi$ is the mapping used for phase saving), the get_queue function that selects the eighth tuple component is mapped to a function that selects the sixth tuple component.

There is, however, a difficulty with this scheme. In an imperative implementation, a getter that returns a component of a state that is stored on the heap must either copy the component or return a pointer into the state. The first option can be very inefficient, and the alternative is not supported by the Sepref tool, which does not admit pointer aliases. Our solution is to provide ad hoc getters to extract the relevant information from the state, without exposing parts of the state simultaneously to the whole state (which would require aliasing). Similarly, we provide setter functions to update components of the state.

For example, after reducing a conflict (rules Resolve and Skip), we must distinguish between either jumping (rules Jump_Unit and Jump_Nonunit) or stopping the solver by testing whether the conflict was reduced to $\bot$:

\[
\text{the} (\text{get\_conflict\_wlist} S) = \emptyset
\]

(The result is unspecified if the conflict is $\top$, i.e., None.) Since all we need is the emptiness check and not the conflict clause itself, we can define a specialized getter:

\[
\text{conflict\_is\_empty\_wlist} S \leftarrow \text{the} (\text{get\_conflict\_wlist} S) = \emptyset
\]

Then we refine it to the intermediate state with heuristics:

\[
\text{conflict\_is\_empty\_heuristic} (M, NU, u, D, WS, Q, \text{vmtf}, \varphi) \leftrightarrow \text{conflict\_is\_empty} D
\]

with the following auxiliary function that operates only on the $D$ component:

\[
\text{conflict\_is\_empty} D \leftrightarrow D = \emptyset
\]

Next, we refine the auxiliary function to use the lookup-table representation:

\[
\text{conflict\_is\_empty\_lookup} (b, n, ps) \leftrightarrow n = 0
\]

Finally, this function is given to Sepref, which generates Imperative HOL code.

The representation of states changes between refinement layers. It can also change within a layer, to store temporary information. Consider the number of literals of maximum level in the conflict clause. When it reaches 1, the Resolve rule does not apply anymore. Keeping this number around, in a
9 Evaluation

We compare the performance of our solver, IsaSAT, with MiniSat 2.2 [13], Glucose 4.1 [1], DPT 2.0, and versat [28]. versat, by Oe et al. [28], is specified and verified using the Guru proof assistant [33], which can generate C code. versat consists of 15,000 lines of C code. Optimized data structures are used, including for watched literals and conflict analysis (but not for conflict minimization), and the VSIDS heuristic is in charge of decisions. However, termination is not guaranteed, and model soundness is proved trivially by means of a run-time check of the models; if this check fails, the solver’s outcome is “unknown.”

We ran all solvers on the 150 problems classified easy or medium from the SAT Competition 2009, with a time limit of 900 s. Glucose solves 147 problems in 51 s on average. MiniSat solves 143 problems, spending 98 s on average per problem it solves; DPT solves 70 problems in 206 s on average. versat solves 55 problems in 191 s on average. IsaSAT without the lookup table solves 43 problems in 126 s on average, while the version with lookup table solves only 36 in 127 s on average (including four problems that the version without lookup table could not solve). A more optimized version with the lookup table and the caching of the number of literals of maximum level in the conflict solves 55 problems in 144 s on average. As an indication of how far we have come, the functional solver implementing W [8] and our first imperative unoptimized version with watched literals do not solve any of the problems. The tests were carried out on a Xeon E5-2680 with 256 GB of memory, with Intel Turbo Boost deactivated. Globally, the tests show that Glucose and MiniSat are much faster than the other solvers and that DPT solves substantially more instances than IsaSAT and versat, which are roughly comparable.

A more precise comparison of performance of our solver with and without the lookup table is shown in Figure 3a. A point at coordinates \((x, y)\) indicates that the version with the lookup table took \(x\) seconds, whereas the version without the table took \(y\) seconds. Points located above the main diagonal correspond to problems for which the table pays off. Figure 3b compares versat and the optimized IsaSAT. It shows that either solver solves some problems on which the other solver times out. This is likely due mostly to the different decision heuristic.

There are several reasons explaining why our solver is much slower than the state of the art. First, it lacks restarts, forgetting, and nontrivial conflict minimization. Restarts enable the solver to explore another part of the search space, forgetting removes some learned clauses, and conflict minimization produces smaller learned clauses. Glucose and MiniSat also use preprocessing techniques to simplify the initial set of clauses. Other SAT solvers, such as Lingeling [4], also use inprocessing techniques to simplify initial and learned clauses after restarts.

Another issue is that Isabelle/HOL can only generate code in impure functional languages, whereas most unverified SAT solvers are developed in C or C++. Although we proved that all array accesses are within bounds, functional languages nonetheless check array bounds at run-time. Moreover, other features, such as the arbitrary precision arithmetic used for Isabelle/HOL programs, tend to be less efficient than their C++ counterparts.

To reduce these effects, we implemented literals by 32-bit unsigned integers (which required some extra work to prove absence of overflows). This increased the speed of our solver by a factor between two and four. In a slight extension of the trusted base of the code generation, we convert literals directly to machine-size integers (32- or 64-bit), instead of taking the detour through unbounded integers. This simple change improved performance by another factor of two.

10 Discussion and Related Work

We found formalizing the two watched literals challenging. In the literature, only variants of the invariant from Section 3 are presented. However, there are several other key properties that are necessary to prove that no work is needed when backjumping. For example, the invariant states that “a watched literal may be false only if the other watched literal is true,” but this is not the full story. It would be more precise to state that “a watched literal may be false only if the other watched literal is true and this false literal’s level is greater than or equal to the true literal’s level.” The new version explains why no update is required after Jump: Either both watched literals are now unset in the trail, or only the true literal remains.

One difficulty we often faced when adding optimizations is that the “edit, compile, run” cycle is much longer when code is developed through the Isabelle Refinement Framework instead of directly in a programming language such as C++. For example, the change to the conflict-clause representation took two weeks to prove and implement, before finding out that the overall solver gets slower. We have yet to find a good methodology for carrying out quick experiments.

The closest formalizations to ours are versat by Oe et al. [28] and Marić’s [23, 24]. Marić verified a CDCL-based SAT solver in Isabelle/HOL, including two watched literals, as a purely functional program. His methodology is quite different from ours, as it does not include refinement. While he was able to generate code with an earlier version of Isabelle,
the code export does not work anymore. We expect the performance to be substantially worse than ours, since he uses lists instead of arrays. Beyond Oe et al. and Maric, there are several formalizations of CDCL that do not include watched literals, including Lescuyer’s in Coq [22] and Shankar and Vaucher’s in PVS [31], and also some formalizations of DPLL, including Berger et al. [3], whose Haskell solver outperforms versat on large pigeon-hole problems. (CDCL is not faster than DPLL on such problems, because the learned clauses are useless at pruning the search space.)

Instead of verifying a SAT solver, another way to obtain trustworthy results is to have the solver produce a certificate, which can be processed by a checker. While certificates for satisfiable formulas are simply a valuation of the variables and can be easily generated and checked, certificates for unsatisfiable formulas are more complicated. The de facto standard format is DRAT (deletion resolution asymmetric tautology) [16], which can be easily generated by solvers. The standard DRAT certificate checker [36] is, however, an unverified C program. Recent research [10, 11, 20], including by Lammich, shows that it is now possible to have efficient verified checkers.

The distinguishing feature of our work is the systematic application of refinement to connect abstract calculi with generated code. The Refinement Framework allows us to generate imperative code while keeping programs under-specified for as long as possible. It makes it straightforward to change the implementation or to derive multiple implementations from the same abstract specification. Its support for assertions makes it possible to reuse properties proved on an abstract level to reason about more concrete levels.

11 Conclusion

We have extended our Isabelle/HOL framework for CDCL with a verified imperative SAT solver. Refinement-based development is flexible and makes later changes in the development easier. We expect that many heuristics and optimizations can be added with only comparatively small modular changes to the existing proofs. For example, an initial version of our SAT solver did not include the lookup-table conflicts presented in Section 7; adding it required changes only to the last refinement step.

The refinement steps are an interesting case study of the Refinement Framework, Imperative HOL, and the code generator. In future work, we plan to add (fast) restarts and forget and to extend the CeTA checker to use our verified SAT solver. We would also like to formalize CDCL(T), the theory behind satisfiability-modal-theories (SMT) solvers, and other extensions such as MaxSAT.

Acknowledgments

Max Haslbeck, Anders Schlichtkrull, and Mark Summerfield suggested textual improvements. Blanchette has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program (grant agreement No. 713999, Matryoshka).

References

A Verified SAT Solver with Watched Literals

Submitted to CPP 2018, January 8–9, Los Angeles, California, USA


