Natural Proofs for Structure, Data, and Separation
Supplemental Material

Xiaokang Qiu Pranav Garg Andrei Ștefănescu P. Madhusudan
University of Illinois at Urbana-Champaign, USA
{qiu2, garg11, stefane1, madhu}@illinois.edu

A. Generating the Verification Condition

Assume there are m procedure calls in P, then P can be divided into m + 1 basic segments (subprograms without procedure calls):

\[ S_0 : g_1 : S : \ldots : g_m : S_m \]

where \( S_d \) is the d + 1-th basic segment and \( g_d \) is the d-th procedure call.

For each \( d \in [m] \), let the \( d \)-th procedure call in \( P \) be the \( t_d \)-th statement (we also extend the index \( d \) to \( -1, 0 \) and \( m + 1 \) such that \( t_{-1} = t_0 = 0 \) and \( t_{m+1} = n + 1 \)). Note that \( \mathcal{E} \) requires that a portion of the state \( C_{t_d-1} \) satisfies the precondition of the call, and a portion of the state \( C_{t_d} \) satisfies the postcondition of the call. We denote the two required portions \( C_{t_d-1} \subseteq \text{Call}_d \) and \( C_{t_d} \subseteq \text{Return}_d \), respectively, where \( \text{Call}_d \subseteq R_{t_d-1} \) and \( \text{Return}_d \subseteq R_{t_d} \) are two sets of records.

Let all the location variables appearing in \( P \) be \( \mathcal{L} \). We call a location variable \( v \) dereferenced if \( v \) appears on the left-hand side of a dereferencing operator \( \bullet \) in \( P \). We call a location variable \( v \) modified if \( v \) appears in a statement of the form \( v.pf := u \) or \( v.df := j \) in \( P \). Then we can extract the set of dereferenced variables \( \text{Deref} \) and the set of modified variables \( \text{Mod} \). Note that a modified variable is always dereferenced, i.e., \( \text{Mod} \subseteq \text{Deref} \). For each basic segment \( S_d \), let the dereferenced and modified variables within the segment be \( \text{Deref}_d \) and \( \text{Mod}_d \), respectively.

For the \( d \)-th procedure call, let the pre- and post-condition associated with the procedure be \( \phi^p_{\text{pre}}(\vec{v}, \vec{z}, c) \) and \( \phi^p_{\text{post}}(\text{ret}, \vec{v}, \vec{z}, c) \), respectively. Since \( \mathcal{E} \) is a normal execution, we have \( C_{t_{d-1}} \models T(\phi^p_{\text{pre}}(\vec{v}, \vec{z}_d, \vec{c}_d), \text{Call}_d) \) and \( C_{t_d} \models T(\phi^p_{\text{post}}(u, \vec{v}, \vec{z}_d, \vec{c}_d), \text{Return}_d) \) (assume the procedure call returns a location to \( u \)), where \( \vec{v}_d \) and \( \vec{c}_d \) are the actual parameters of the procedure call, \( \vec{c}_d \) are the complimentary variables with fresh names.

Now we are ready to define the verification condition corresponding to \( P \). We first derive a formula expressing that \( \mathcal{E} \) does not involve null pointer dereference:

\[ \text{NoNullDereference} \equiv \bigwedge_{v \in \text{Deref}} v \neq \text{nil} \]

For each \( i \in [n] \), Figure 1 shows the effect of each statement on the verification condition generated. Each statement’s strongest post condition is captured in the logic, and for procedure calls, the heaplet manipulated by the procedure is carefully taken into account to update the heap at the caller. The conjunction of these

\[
\begin{align*}
\{ u := v \} & \\
\varphi_1 & \equiv u = v \land R_i = R_{t_i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u := \text{nil} \} & \\
\varphi_1 & \equiv u = \text{nil} \land R_i = R_{t_i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u := v.pf \} & \\
\varphi_1 & \equiv u \in R_{t_i-1} \land u = pf_{t_i-1}(v) \land R_i = R_{t_i-1} \\
& \quad \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u.pf := v \} & \\
\varphi_1 & \equiv u \in R_{t_i-1} \land pf_i = pf_{t_i-1}(v \leftarrow u) \land R_i = R_{t_i-1} \\
& \quad \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ j := u.df \} & \\
\varphi_1 & \equiv u \in R_{t_i-1} \land j = df_{t_i-1}(u) \land R_i = R_{t_i-1} \\
& \quad \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u.df := j \} & \\
\varphi_1 & \equiv u \in R_{t_i-1} \land df_i = df_{t_i-1}(j \leftarrow u) \land R_i = R_{t_i-1} \\
& \quad \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ j := \text{aexpr} \} & \\
\varphi_1 & \equiv j = \text{aexpr} \land R_i = R_{t_i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u := \text{new} \} & \\
\varphi_1 & \equiv \text{new}_i \neq \text{nil} \land u = \text{new}_i \land \text{new}_i \notin R_{t_i-1} \land R_i = R_{t_i-1} \lor |\text{new}_i| \\
& \quad \land \bigwedge_{pf} (pf_i = pf_{t_i-1}(\text{new}_i \leftarrow \text{new}_i)) \land \bigwedge_{df} (df_i = df_{t_i-1}(0 \leftarrow \text{new}_i)) \\
\{ \text{free } u \} & \\
\varphi_1 & \equiv u \in R_{t_i-1} \land R_i = R_{t_i-1} \lor [u] \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ \text{assume bexpr} \} & \\
\varphi_1 & \equiv \text{bexpr} \land R_i = R_{t_i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1) \\
\{ u := f(\vec{v}, \vec{z}) \} & \\
\varphi_1 & \equiv T(\phi^p_{\text{pre}}(\vec{v}, \vec{z}, c), \text{Call}_d)[i - 1] \land T(\phi^p_{\text{post}}(u, \vec{v}, \vec{z}, c), \text{Return}_d)[i] \\
& \quad \land (R_{t_i-1} \setminus \text{Call}_d) \cap \text{Return}_d = \emptyset \land R_i = (R_{t_i-1} \setminus \text{Call}_d) \cup \text{Return}_d \\
& \quad \text{where } d \text{ is the index such that } t_d = i \\
\{ j := g(\vec{v}, \vec{z}) \} & \\
\varphi_i & \equiv \text{defined in the same way as the above case, except replacing } u \text{ with } j. \\
\end{align*}
\]

Figure 1. Formulas capture modification by statements

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

PLDI’13, June 16–19, 2013, Seattle, WA, USA.
Copyright © 2013 ACM 978-1-4503-2014-6/13/06 . . . $15.00
formulas captures the modification made in $E$:

$$\text{Modification} \equiv \bigwedge_{i \in [n]} \varphi_i$$

Finally, we can define two formulas to capture the pre- and post-conditions:

$$\text{Pre} \equiv T(\varphi_{pre}, R_0)[0]$$
$$\text{Post} \equiv T(\varphi_{post}, R_0)[n]$$

Now the validity of $(\varphi_{pre}) P (\varphi_{post})$ can be captured by the following formula:

$$\psi_{VC} \equiv (\text{Pre} \land \text{NonNull Dereference} \land \text{Modification}) \rightarrow \text{Post}$$

B. Proof of Theorem 6.1

**Proof.** We prove the soundness by contradiction. Assume the Hoare-triple $(\varphi_{pre}) P (\varphi_{post})$ is not valid. Assume $P$ consists of $n$ statements, then there is an execution $E$, which can be represented as a state sequence $(C_0, \ldots, C_n)$ where each $C_i = (R_i, s_i, h_i)$, such that $(C_0, R_0)$ satisfies $\varphi_{pre}[0]$, $(C_n, R_n)$ satisfies $\varphi_{post}[n]$, and the whole execution is memory error free. Then by the definitions of Pre, Post, and NonNull Dereference, and Theorem 6.1, $E \models (\text{Pre} \land \text{NonNull Dereference} \land \text{Modification}) \land \text{Post}$. Now it suffices to show that $E \not\models \text{Modification}$, in which case $E$ dissatisfies $\psi_{VC}$. The contradiction will prove the result.

Since $\text{Modification} \equiv \bigwedge_{i \in [n]} \varphi_i$, we just need to prove $E \models \varphi_i$ for each $i \in [n]$, by case analysis on the type of the $i$-statement in $P$.

\[u := v\]
$$\varphi_i \equiv u = v \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

The variable assignment makes $u$ points to the same location as $v$ points to. Hence $u = v$. Since the heap is unmodified from $C_{i-1}$ to $C_i$, the heap domain remains the same ($R_i = R_{i-1}$), and all the field functions remain the same ($\text{FieldsUnmod}(PF \cup DF, i, i - 1)$).

\[u := \text{nil}\]
$$\varphi_i \equiv u = \text{n} \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

The variable assignment makes $u$ points to nil, so $u = \text{n}$. Similar to the above case, the heap is also unmodified from $C_{i-1}$ to $C_i$.

\[u := v.pf\]
$$\varphi_i \equiv v \in R_{i-1} \land u = pf_{i-1}(v) \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

The dereferencing on $v$ implies that $v$ points to a valid location at timestamp $i - 1$, i.e., $v \in R_{i-1}$. Moreover, the assignment makes $u$ points to the pf field of $v$ at timestamp $i - 1$, formally $u = pf_{i-1}(v)$. Similar to the above case, the heap is also unmodified from $C_{i-1}$ to $C_i$.

\[u.pf := v\]
$$\varphi_i \equiv u \in R_{i-1} \land pf_i = pf_{i-1}(v \leftarrow u) \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup (DF \setminus \{pf\}), i, i - 1)$$

Similar to the above case, $u$ points to a valid location at timestamp $i - 1$ ($u \in R_{i-1}$), the mutation makes the pf field at timestamp $i$ updated from that at timestamp $i - 1$: $pf_i = pf_{i-1}(v \leftarrow u)$. Moreover, the heap domain is unmodified, so $R_i = R_{i-1}$. The other field functions also remain the same, which is captured by $\text{FieldsUnmod}(PF \cup (DF \setminus \{pf\}), i, i - 1)$.

\[j := u.df\]
$$\varphi_i \equiv u \in R_{i-1} \land j = df_{i-1}(u) \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

Similar to the $u := v.pf$ case.

\[u.df := j\]
$$\varphi_i \equiv u \in R_{i-1} \land df_i = df_{i-1}(j \leftarrow u) \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \setminus \{df\}) \cup DF, i, i - 1)$$

Similar to the $u.pf := v$ case.

\[j := aexpr\]
$$\varphi_i \equiv j = aexpr \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

The statement assigns the value of $aexpr$, which is expressible in our logic, to $j$. Hence $j = aexpr$. The result is similar to other variable assignment cases.

\[u := \text{new}\]
$$\varphi_i \equiv \text{new} \neq newline \land u = \text{new} \land \text{null} \not\in R_i \land R_i = R_{i-1} \cup \{\text{new}\} \land \bigwedge_{pf_i} (\text{pf}_i(\text{null} \leftarrow \text{new})) \land \bigwedge_{df_i}(\text{df}_i(\text{null} \leftarrow \text{new}))$$

This statement makes $u$ points to a freshly allocated location, namely $\text{new}$, in $E$. So it is clear that $\text{new} \neq newline \land u = \text{new}$. Since the heap domain at timestamp $i$ is an extension of that at timestamp $i - 1$ by adding $\text{new}$, we know that $\text{new} \not\in R_i \land R_i = R_{i-1} \cup \{\text{new}\}$. By default, for $\text{new}$, each pointer field initially points to nil, each data field initially stores 0. The remaining portion of the heap is exactly the same as $C_{i-1}$. Hence $\bigwedge_{pf_i} (\text{pf}_i(\text{null} \leftarrow \text{new})) \land \bigwedge_{df_i}(\text{df}_i(\text{null} \leftarrow \text{new}))$.

\[free u\]
$$\varphi_i \equiv u \in R_{i-1} \land R_i = R_{i-1} \setminus \{u\} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

This statement removes the location pointed by $u$ from the heap. So the old heap contains this location, and the new heap can be obtained by subtracting it from the old heap: $u \in R_{i-1} \land R_i = R_{i-1} \setminus \{u\}$. Since the domain is shrunk, the field function can be simply unchanged.

\[assume bexpr\]
$$\varphi_i \equiv \text{bexpr} \land R_i = R_{i-1} \land \text{FieldsUnmod}(PF \cup DF, i, i - 1)$$

The assumed condition $\text{bexpr}$, which can be expressed in our logic, must be true. The heap is simply unmodified.

\[u := f(v, z)\]
$$\varphi_i \equiv T(\psi_{post}(\bar{a}, \bar{d}, \bar{c}, \bar{d}_c), \text{Calla})[i - 1] \land T(\psi_{pre}(\bar{a}, \bar{d}, \bar{c}, \bar{d}_c), \text{Returna})[i - 1] \land (R_{i-1} \setminus \text{Calla}) \cap \text{Returna} = \emptyset \land R_i = (R_{i-1} \setminus \text{Calla}) \cup \text{Returna}$$

where $d$ is the index such that $t_d = i$.

As assumed, this call is the $d$-th procedure call in $P$, and $C_{i-1}$ satisfies the associated precondition by the heaplet defined by $\text{Calla}$, and $C_i$ satisfies the associated postcondition by the heaplet defined by $\text{Returna}$. Then formally we have $T(\psi_{post}(\bar{a}, \bar{d}, \bar{c}, \bar{d}_c), \text{Calla})[i - 1] \land T(\psi_{pre}(\bar{a}, \bar{d}, \bar{c}, \bar{d}_c), \text{Returna})[i - 1]$ being satisfied by $E$.

Due to the framing property of the separation semantics, the portion of $C_{i-1}$ that is not required by $\psi_{pre}$ remains unchanged, and is disjoint from $\text{Returna}$ (since the returned location is assigned to $u$, the variable $\text{ret}$ can be replaced with $u$). This property can be expressed as $(R_{i-1} \setminus \text{Calla}) \cap \text{Returna} = \emptyset \land R_i = (R_{i-1} \setminus \text{Calla}) \cup \text{Returna}$.

\[j := g(v, z)\]
$$\varphi_i \equiv f(v, z)$$

is defined in the same way as the above case, except replacing $u$ with $j$.

The proof is also similar to the above case. □
C. Formulas Defined in Section 6.2

Let $u$ be a location variable in $\mathcal{L}vars$ and let $i$ be a timestamp such that $1 \leq i \leq n$. For each recursive definition $\Delta$ whose $\Delta$-eliminated version defined as $\text{rec}^\Delta$ whose reach set defined as $\text{reach}^\Delta(x)$, we can derive a formula $\text{Unfold}^\Delta(u, i)$ for unfolding both $\text{rec}^\Delta$ and its corresponding reach set on $u$ at timestamp $i$, provided that $u$ is allocated at the current timestamp ($u \in R_i$). Note that in $\text{def}^\Delta(x, i, \vec{D})$, $x$ will be renamed as $u$, and $\vec{D}$ will not be renamed as they are program variables, but $\vec{D}$ are existentially quantified and should be replaced with fresh variable names. Due to the restrictions on the recursive definitions, every $x$ is unique and can be determined by dereferencing $u$ on the corresponding pointer fields, say $\text{pf}_u$. Hence we can replace each $v$ in $\vec{D}$ distinctly as $u, \text{rec}^u, \text{pf}_u$. Let the renamed formula be $\text{def}^u(u, i, \vec{D}_{\text{fresh}})$, then we can derive

$$\text{Unfold}^\Delta(u, i) \equiv (\text{reach}^\Delta(u) = \text{reach}^\Delta_\text{def}(u)) \land (u \in R_i \rightarrow$$

$$\left(\text{rec}(u) \equiv \text{def}^u(u, i, \vec{D}_{\text{fresh}}) \land \bigwedge_{v \in \vec{D}} (\text{pf}^\Delta(v, u) = u, \text{rec}^u, \text{pf}_u)\right)$$

Now the footprint unfolding is just unfolding $u$ at the beginning and end of each program segment (for the $d$-th segment, the timestamp $t_d$ and $t_{d+1} = 1$, respectively):

$$\text{Unfold}^\Delta_d(u) \equiv \text{Unfold}^\Delta(u, t_d) \land \text{Unfold}^\Delta(u, t_{d+1} - 1, u)$$

The formula $\text{FieldUnchanged}_D(u)$ describes that, in the $d$-th procedure call, if the location $u$ is not nil, then for each field $\text{pf}$ (or $\text{df}$), $\text{pf}_{t_d-1}(u)$ and $\text{pf}_{t_d}(u)$ are the same if $u$ itself is not affected during the call:

$$\text{FieldUnchanged}_D(u) \equiv (u \neq \text{nil} \land u \notin \text{Call} \rightarrow$$

$$\left(\bigwedge_{v \in \vec{D}} (\text{pf}_{t_d-1}(u) = \text{pf}_{t_d}(u)) \land \bigwedge_{v \in \vec{D}} (\text{df}_{t_d-1}(u) = \text{df}_{t_d}(u))\right)$$

Finally, to define $\text{RecUnchanged}_D(u, d)$, we first define a formula expressing that a recursive definition and its corresponding reach set on a location are unchanged between two timestamps:

$$\text{Unchanged}^\Delta(u, i, i') \equiv \text{rec}(u) = \text{rec}(u) \land \text{reach}^\Delta(u) = \text{reach}^\Delta_\text{def}(u)$$

For each non-footprint location variable $u$ and for each recursive predicate $\text{rec}^\Delta$, the formula $\text{RecUnchanged}_D(u, d)$ just captures the fact that $\text{rec}(u)$ and $\text{reach}^\Delta(u)$ are unchanged in two cases: in the $d$-th segment of the program (between timestamp $t_d$ and $t_{d+1} = 1$), they are unchanged if reach set is not modified; or in the $d$-th procedure call (between the timestamp $t_d - 1$ and $t_d$) if the reach set is not affected during the call. Moreover, it also incorporates the fact that the reach set on $u$ contains $u$ itself. Formally,

$$\text{RecUnchanged}_D(u, d) \equiv$$

$$(\text{reach}^\Delta_{t_d}(u) \cap \text{Mod} = \emptyset) \rightarrow \text{Unchanged}^\Delta(u, t_d, t_{d+1} - 1)$$

$$(\text{reach}^\Delta_{t_{d-1}}(u) \cap \text{Call} = \emptyset) \rightarrow \text{Unchanged}^\Delta(u, t_{d-1} - 1, t_d)$$

$$u \neq \text{nil} \rightarrow (\text{reach}^\Delta_{t_d}(u) \cap \text{reach}^\Delta_{t_{d+1} - 1}(u))$$

D. Transforming $\neg \psi_{\text{VC}}^{\text{abs}}$ to $\psi^{\text{APF}}$

Note that $\neg \psi_{\text{VC}}^{\text{abs}}$ is mostly expressible in the quantifier-free theory of arrays, maps, uninterpreted functions, and integers: $\text{Loc}$ can be viewed as an uninterpreted sort; each pointer field $\text{pf}$ can be viewed as an array with both indices and elements of sort $\text{Loc}$; each data field $\text{df}$ can be viewed as an array and indices of sort $\text{Loc}$ and elements of sort $\text{Int}$; each integer set (or multiset) variable $S$ can be viewed as an array with indices of sort $\text{Int}$ and elements of sort $\text{Bool}$ (or $\text{Int}$). Moreover, each array update operation of the form $\text{array}[\text{elem} \leftarrow \text{key}]$ can be viewed as a read-over-write operation in the array property fragment, and each set-operation (union, intersection, etc.) can be viewed as a mapping function applying a Boolean operation ($\land$, $\lor$, etc.) to the range of arrays.

The only construct in $\neg \psi_{\text{VC}}^{\text{abs}}$ that escapes the quantifier-free formulation is the $\leq$ relation between integer sets/multisets; but this can be captured using the array property fragment, which is decidable.

For each atomic formula of the form $S_1 \leq S_2$, if $S_1$ and $S_2$ are sets of integers, we can replace the formula with a universally quantified formula as follows:

$$\forall \text{t}_1, \text{t}_2. (i \leq \text{t}_2 \rightarrow (\neg S_2[i_2] \lor \neg S_1[i_2]) )$$

Similarly, if $S_1$ and $S_2$ are integer multisets, we can replace the formula with

$$\forall \text{t}_1, \text{t}_2. (i \leq \text{t}_2 \rightarrow (S_2[i_2] = 0 \lor S_1[i_2] = 0 )$$

The formula $S_1 \leq S_2$ where $S_1$ and $S_2$ are sets of integers can also be translated to

$$\forall \text{t}_1, \text{t}_2. (S_1[i] \rightarrow i \leq k) \land (S_2[i] \rightarrow k \leq i)$$

where $k$ is an additional existential integer variable, serving as the pivot for splitting $S_1$ and $S_2$. Similarly, when $S_1$ and $S_2$ are integer multisets, the formula is translated to

$$\forall \text{t}_1. (S_1[i] > 0 \rightarrow i \leq k) \land (S_2[i] > 0 \rightarrow k \leq i) .$$

Moreover, the negation of the above relations between sets/multisets can always be expressed using two existential integer variables $k_1$, $k_2$ that witness the violation of the inequality. For instance, $S_1 \not\leq S_2$ can be expressed as $k_1 \in S_1 \land k_2 \in S_2 \land k_2 \leq k_1$.

We thus obtain a formula $\psi^{\text{APF}}$ whose satisfiability is decidable.