Program Verification using Constraint Handling Rules and Array Constraint Generalizations

Emanuele De Angelis  
University of Chieti-Pescara  
Viale Pindaro 42, 65127, Pescara, Italy  
emanuele.deangelis@unich.it

Fabio Fioravanti  
University of Chieti-Pescara  
Viale Pindaro 42, 65127, Pescara, Italy  
fabio.fioravanti@unich.it

Alberto Pettorossi†  
University of Rome Tor Vergata  
Via del Politecnico 1, 00133 Rome, Italy  
pettorossi@info.uniroma2.it  
adp@iasi.cnr.it

Maurizio Proietti  
IASI-CNR  
Via dei Taurini 19, 00185 Rome, Italy  
maurizio.proietti@iasi.cnr.it

Abstract. The transformation of constraint logic programs (CLP programs) has been shown to be an effective methodology for verifying properties of imperative programs. By following this methodology, we encode the negation of a partial correctness property of an imperative program prog as a predicate incorrect defined by a CLP program T, and we show that prog is correct by transforming T into the empty program (and thus incorrect does not hold) through the application of semantics preserving transformation rules. We can also show that prog is incorrect by transforming T into a program with the fact incorrect (and thus incorrect does hold). Some of the transformation rules perform replacements of constraints that are based on properties of the data structures manipulated by the program prog. In this paper we show that Constraint Handling Rules (CHR) are a suitable formalism for representing and applying constraint replacements during the transformation of CLP programs. In particular, we consider programs that...

†Address for correspondence: University of Rome Tor Vergata, Via del Politecnico 1, 00133 Rome, Italy

‡This work has been partially supported by the National Group of Computing Science (GNCS-INDAM). E. De Angelis, F. Fioravanti, and A. Pettorossi are research associates at IASI-CNR, Rome, Italy.
manipulate integer arrays and we present a CHR encoding of a constraint replacement strategy based on the theory of arrays. We also propose a novel generalization strategy for constraints on integer arrays that combines CHR constraint replacements with various generalization operators on integer constraints, such as widening and convex hull. Generalization is controlled by additional constraints that relate the variable identifiers in the imperative program prog and the CLP representation of their values. The method presented in this paper has been implemented and we have demonstrated its effectiveness on a set of benchmark programs taken from the literature.

**Keywords:** Constraint Handling Rules, Constraint logic programming, Program transformation, Program verification

1. **Introduction**

It has long been recognized that Constraint Logic Programming (CLP) is a formalism that provides a powerful inference mechanism for the verification of properties of imperative programs. In the landmark paper by Peralta et al. [1] the authors show that the operational semantics of an imperative programming language can be defined by providing an interpreter \( I \) for that language, written in CLP. By specializing that interpreter with respect to a given imperative program \( \text{prog} \), we get a CLP program, say \( I_{\text{prog}} \), that has no reference to the imperative constructs of the program \( \text{prog} \). Then, by analyzing the specialized CLP program \( I_{\text{prog}} \), we can discover properties of the imperative program \( \text{prog} \).

The approach of Peralta et al. [1] has been extended by De Angelis et al. [2] who show how to encode into a CLP program, say \( T \), any partial correctness property specified by a Hoare triple, that is, a triple consisting of a precondition, an imperative program, and a postcondition. The CLP program \( T \) contains a predicate \( \text{incorrect} \) that is equivalent to the negation of the partial correctness property, defined in terms of the operational semantics of the programming language. Then, by specializing \( T \) with respect a given triple \( \{ \varphi \} \text{prog} \{ \psi \} \) one can generate a new CLP program, say \( VC \), which provides the so-called *verification conditions* for \( \text{prog} \) [3]. Indeed, the Hoare triple is valid if and only if the query \( \text{incorrect} \) does not hold in the program \( VC \). However, to check whether or not \( \text{incorrect} \) holds in \( VC \), is often a hard task for standard (either top-down or bottom-up) CLP query evaluation techniques, as it may require the discovery of properties of the execution of \( \text{prog} \) and, in particular, the loop invariants of \( \text{prog} \).

In order to overcome this difficulty, many verification methods extending the standard CLP evaluation strategies have been proposed. Some methods, directly following the approach presented in [1], are based on abstract interpretation [4] and compute an over-approximation of the least model of the CLP program \( VC \) by a bottom-up evaluation of an abstraction of the program [5, 6, 7]. Other methods use goal directed evaluation of the CLP program \( VC \) combined with other symbolic techniques such as interpolation [8, 9, 10]. Some other methods presented in various papers [11, 12, 13, 14, 15], combine CLP (also called constrained Horn clauses in those papers) with different reasoning techniques developed in the areas of Software Model Checking and Automated Theorem Proving, such as the CounterExample-Guided Abstraction Refinement (CEGAR) and the Satisfiability Modulo Theories (SMT).
In this paper we consider C-like imperative programs on integer and array variables and we follow the approach based on the transformation of CLP programs that was first presented in De Angelis et al. [2] for the case of programs on integer variables. Suppose we want to prove a partial correctness property of an imperative program \( \text{prog} \) and assume that the negation of that property is encoded by the predicate \( \text{incorrect} \) defined by the CLP program \( T \). After the generation of the verification conditions \( VC \) obtained by specializing \( T \) with respect to the given property (see the \( \text{VCGen} \) module in Figure 1), the transformation-based method proceeds by applying to \( VC \) some equivalence preserving unfold/fold transformation rules [16, 17] (see the \( \text{VCTransf} \) module in Figure 1), which propagate the pre- and postconditions with the objective of deriving a CLP program \( VC' \) without facts, hence proving that \( \text{incorrect} \) does not hold and \( \text{prog} \) is correct. In the case where we derive a CLP program \( VC' \) with facts, by unfolding we try to generate the fact \( \text{incorrect} \), hence proving that \( \text{incorrect} \) holds and \( \text{prog} \) is incorrect. Obviously, due to the undecidability of partial correctness, it may be the case that we derive a CLP program \( VC' \) with facts, and yet we are not able to generate the fact \( \text{incorrect} \), and hence we establish neither the correctness nor the incorrectness of \( \text{prog} \). However, since the transformation rules preserve equivalence of CLP programs, in the case where the transformation method is inconclusive, we can still apply any Satisfiability Modulo Theories solver (SMT solver, for short) to \( VC' \) and try to prove the property of interest (see the SMT Solver module in Figure 1). Indeed, as confirmed by the results of our experiments that are reported in Section 7, SMT solvers are likely to be more effective when applied to \( VC' \), instead of \( VC \), because of the propagation of the pre- and postconditions performed by the unfold/fold transformation.

The most critical issue to be addressed to make CLP program transformation effective, is to design some suitable transformation strategies that guide the application of the rules towards the goal of verifying the given partial correctness property. In particular, two transformations need special guidance: (i) the replacement of constraints, and (ii) the introduction of new predicate definitions that facilitate proving (or disproving) the predicate \( \text{incorrect} \). The problem of introducing suitable new predicates, which in the context of logic program transformation were traditionally called the eureka predicates [18], corresponds to the problem of finding suitable inductive invariants in Hoare-style program verification. A very well-established approach for introducing eureka predicates is based on the generalization, which is a technique that derives predicate definitions that generalize (that is, are entailed by) different predicate calls derived by the exploration, via unfolding steps, of the symbolic execution of the given logic program. A general unfold/fold strategy for transforming the CLP verification conditions \( VC \) generated from imperative programs that manipulate integers and integer arrays was proposed by De Angelis et al. [19]. In the CLP verification conditions manipulated by that strategy, array properties are written as constraints using \text{read} and \text{write} predicates that represent operations on arrays. The main limitation of that strategy is that the crucial step for introducing new predicates is a highly nondeterministic step.

In this paper we present a new unfold/fold transformation strategy and we provide a new, much less nondeterministic technique for introducing new predicates, thereby drastically reducing the set of potential new predicates (see the \( \text{VCTransf} \) module in Figure 1). This technique is called array constraint generalization, because it works by finding generalizations of array constraints that are derived by unfolding the given CLP verification conditions \( VC \). The form of the new predicate definitions crucially depends on the form of the constraints, and hence a key point of the transformation
strategy is to make use of suitable constraint replacement strategies. Thus, it is very important to have a formalism for designing and implementing constraint replacements within an unfold/fold transformation framework. Here we show that Constraint Handling Rules (CHR) [20] are very suitable for this purpose.

The novel contributions of the paper are the following.

(1) We present a set of CHR rules that formalize the theory of arrays [21] and we show how they can be combined with unfold/fold transformation rules with the objective of proving properties of imperative programs. We prove soundness, termination, and confluence of the CHR rules. To the best of our knowledge, this is the first unfold/fold transformation strategy for CLP programs that makes use of CHR rules for constraint replacement.

(2) We design a novel array constraint generalization strategy, realized by a function called Gen, that automatically introduces, during CLP transformation, new predicate definitions that are useful for the verification of the properties of interest. The function Gen makes use of suitable additional constraints, called val constraints, that relate the variable identifiers occurring in the given imperative programs and the CLP representations of their values. Specifically, val(v,V) means that the variable identifier v occurring in an imperative program holds the value V at some point of the computation. Array generalizations are computed by matching array constraints which are associated to the same imperative variable identifiers. Thus, val constraints can be viewed as an abstract interpretation [22] that maps imperative variable identifiers to the sets of their possible values. While the mutual benefits of program transformation and abstract interpretation have been exploited by many techniques, the representation and manipulation of abstract values via constraints during program transformation is a new idea.

(3) Finally, we present an implementation of the verification method using the VeriMAP system [23], and we demonstrate its effectiveness on a set of benchmark programs taken from the literature. We also show, on our benchmark, a comparison of VeriMAP with Z3 [12], which is one of the most popular SMT-solver for Horn clauses with constraints. Our experiments show that VeriMAP and Z3 together are more effective than each of these tools separately, and in particular it is the case that the use of Z3 after the unfold/fold transformation performed by VeriMAP, allows the verifications of some programs for which VeriMAP alone was not able to establish neither correctness nor incorrectness.
The paper is structured as follows. In Section 2 we show how a partial correctness property of an imperative program is encoded as a CLP program. We also briefly describe the specialization strategy $VCGen$ used for generating verification conditions from a partial correctness property. In Section 3 we present the transformation strategy $VCTransf$ that we apply to transform the verification conditions obtained by $VCGen$ with the aim of deriving either the empty CLP program (hence proving that the imperative program is partially correct) or a CLP program containing the fact incorrect (hence proving that the imperative program is not partially correct). $VCTransf$ makes use of two auxiliary transformation strategies, one for manipulating array constraints (realized by the function $Repl$) and one for introducing new predicate definitions by generalization (realized by the function $Gen$). The array manipulation strategy, implemented as a set of CHR rules, is presented in Section 4, and the generalization strategy is presented in Section 5. The correctness and termination of $VCTransf$ is proved in Section 6. In Section 7 we present the implementation of our transformation-based verification method and its experimental evaluation. Finally, in Section 8, we compare our paper to related work in the area of program verification.

2. Encoding partial correctness into constraint logic programming

In this section we recall the class of Constraint Logic Programs on integers and integer arrays [19] that we consider in this paper, and we show how partial correctness properties of imperative programs can be encoded as programs of this class.

2.1. Constraint logic programs on integer arrays

First we need the following definitions. An atomic integer constraint is either $p_1 = p_2$, or $p_1 \neq p_2$, or $p_1 \geq p_2$, or $p_1 > p_2$, where $p_1$ and $p_2$ are linear polynomials with integer variables and integer coefficients. As usual, sum and multiplication are denoted by + and $\star$, respectively, and we use the predicates $\leq$ and $<$ instead of the negations of $>$ and $\geq$, respectively. An integer array $a$ (or an array, for short) is a finite sequence of integers whose length, called the dimension of the array, is denoted $\dim(a)$. An atomic array constraint is either $\text{read}(a,i,v)$, denoting that the $i$-th element of the array $a$ is the integer $v$, or $\text{write}(a,i,v,b)$, denoting that for $k = 1, \ldots, \dim(a)$, if $k \neq i$ the $k$-th element of $a$ is equal to the $k$-th element of $b$, and if $k = i$ the $k$-th element of $b$ is the integer $v$.

The $\text{read}$ and $\text{write}$ constraints satisfy the following axioms [21], whose variables are assumed to be universally quantified at the front:

\begin{align*}
(A.1) \quad & I = J, \text{read}(A,I,U), \quad \text{read}(A,J,V) \rightarrow U = V \quad \text{(array congruence)} \\
(A.2) \quad & I = J, \text{write}(A,I,U,B), \text{read}(B,J,V) \rightarrow U = V \quad \text{(read-over-write: equal indexes)} \\
(A.3) \quad & I \neq J, \text{write}(A,I,U,B), \text{read}(B,J,V) \rightarrow \text{read}(A,J,V) \quad \text{(read-over-write: different indexes)}
\end{align*}

A constraint is either true, or false, or an atomic (integer or array) constraint, or a conjunction of constraints. An atom is a formula of the form $p(t_1, \ldots, t_m)$, where $p$ is a predicate symbol not in \{=, \neq, \geq, >, \text{read}, \text{write}\} and $t_1, \ldots, t_m$ are terms constructed out of variables, constants, and function symbols different from + and $\star$. A CLP program is a finite set of clauses of the form $A : - c, B,$
where $A$ is an atom, $c$ is a constraint, and $B$ is a (possibly empty) conjunction of atoms. Given a clause $A :- c, B$, the atom $A$ is called the head, and the conjunction `$c, B$' is called the body. We assume that for every clause head $H$, no variable occurs twice in $H$ and there is no occurrence of either an integer constant, or $+$, or $\ast$ in $H$. This assumption is not restrictive, as terms in the head of a clause containing integer constants, $+$, or $\ast$ can be removed in favor of equalities in the body. This assumption also simplifies the presentation of the unfolding rule, as the unification of an atom in the body of a clause with the head of a (renamed apart) clause need not take into account the theory of integers (see Definition 2.1). A clause $A :- c$ is called a constrained fact. If $c$ is true, then it is omitted and the constrained fact is called a fact. A CLP program is said to be linear recursive if all its clauses are of the form $A :- c, B$, where $B$ consists of at most one atom. In a CLP program $P$, we say that predicate $p$ immediately depends on a predicate $q$ iff in $P$ there is a clause of the form $p(...) :- c, B$ such that $q$ occurs in $B$. The relation ‘depends on’ between predicates is the transitive closure of the relation ‘immediately depends on’.

An $A$-interpretation $I$ is a set $D$, together with a function $f$ in $D^n \rightarrow D$ for each function symbol $f$ of arity $n$, and a relation $p$ on $D^n$ for each predicate symbol $p$ of arity $n$, such that: (i) the set $D$ is the Herbrand universe [24] constructed out of the set $\mathbb{Z}$ of the integers and the function symbols different from $+$ and $\ast$, (ii) $I$ assigns to symbols in the set $\{+, \ast, =, \geq, >\}$ the usual meaning in $\mathbb{Z}$, (iii) for all sequences $a_0 \ldots a_{n-1}$ and $b_0 \ldots b_{n-1}$ of integers, for all integers $i$ and $v$, \texttt{read}(a_0 \ldots a_{n-1}, i, v) is true in $I$ iff $0 \leq i \leq n-1$ and $v = a_i$, and \texttt{write}(a_0 \ldots a_{n-1}, i, v, b_0 \ldots b_{n-1}) is true in $I$ iff $0 \leq i \leq n-1$, $n = m$, $b_i = v$, and for $j = 0, \ldots, n-1$, if $j \neq i$ then $a_j = b_j$, (iv) $I$ is an Herbrand interpretation [24] for function and predicate symbols not in the set $\{+, \ast, =, \geq, >, \texttt{read}, \texttt{write}\}$.

We can identify an $A$-interpretation $I$ with the set of all ground atoms that are true in $I$, and hence $A$-interpretations are partially ordered by set inclusion. For every formula $\varphi$, we say that $I$ is an $A$-model of $\varphi$ if $\varphi$ is true in $I$. We say that $\varphi$ holds in $A$, denoted $A \models \varphi$, if every $A$-interpretation is an $A$-model of $\varphi$. In particular, every $A$-interpretation is an $A$-model of Axioms (A.1), (A.2), and (A.3). A constraint $c$ is said to be satisfiable if $A \models \exists(c)$, where in general, for every formula $\varphi$, $\exists(\varphi)$ denotes the existential closure of $\varphi$. A constraint $c$ entails a constraint $d$, denoted $c \sqsubseteq d$, if $A \models \forall(c \rightarrow d)$, where in general, for every formula $\varphi$, $\forall(\varphi)$ denotes the universal closure of $\varphi$. By $\texttt{vars}(\varphi)$ we denote the set of the free variables of the formula $\varphi$. Likewise, by $\texttt{vars}(\varphi_1, \ldots, \varphi_n)$ we denote the set of the free variables occurring in any of the formulas $\varphi_1, \ldots, \varphi_n$. In general, by $\texttt{vars}(e)$ we denotes the set of variables occurring in the expression (or sequence of expressions) $e$. The semantics of a CLP program $P$ is the least $A$-model of $P$, denoted $M(P)$, constructed as usual for CLP programs [25].

### 2.2. The imperative language

We consider C-like imperative programs manipulating integers and integer arrays. In Figure 2 we describe the programming language $\mathcal{L}$ we use. We can deal with other commands, such as \texttt{while} commands and \texttt{for} commands, by considering their translation in terms of \texttt{if-else} and \texttt{goto} commands (see Figure 2). We assume that every program has a single \texttt{halt} command whose execution causes the program to terminate. For reasons of simplicity, we will consider one-dimensional arrays only.
\[ x, y, \ldots, i, j, \ldots \in \text{IVars} \quad \text{(integer variable identifiers)} \]
\[ a, b, \ldots \in \text{AVars} \quad \text{(integer array identifiers)} \]
\[ k \in \mathbb{Z} \quad \text{(integer constants)} \]
\[ \ell, \ell_0, \ell_1, \ldots \in \text{Labels} \quad \text{(labels)} \]
\[ uop, bop \in \text{Ops} \quad \text{(unary and binary operators: \(-, +, *, =, \geq, \ldots\)} \]

\[
\text{prog ::= } (\ell : \text{cmd } ;)^* \\
\text{cmd ::= } x = \text{expr } | \ a[\text{expr}] = \text{expr } | \ \text{goto } \ell \ | \ \text{if } (\text{expr}) \ \ell_1 \ \text{else } \ell_2 \ | \ \text{halt} \\
\text{expr ::= } k \ | \ x \ | \ uop \ \text{expr} \ | \ \text{expr } bop \ \text{expr} \ | \ a[\text{expr}] \\
\]

Figure 2. Syntax of the imperative language \( \mathcal{L} \).

The operational semantics of programs is defined in terms of a transition relation, denoted \( \rightarrow \), between configurations. A configuration is a pair \( \langle c, \delta \rangle \) of a labeled command (or a command, for short) \( c \) and an environment \( \delta \) that maps: (i) every integer variable identifier \( x \) to its value \( v \), and (ii) every integer array identifier \( a \) to a finite sequence \( a_0 \ldots a_n \) of integers, where \( n \) is the dimension of the array \( a \). The transition relation specifies a ‘small step’ operational semantics in the style of Reynolds [26]. Its definition is shown in Figure 3, where we use the following expressions.

Given any mapping \( g : X \rightarrow A \), by the expression \( \text{update}(g, x, a) \), with \( x \in X \) and \( a \in A \), we denote the mapping \( g' \) that is equal to \( g \), except that \( g'(x) = a \). If \( a \) is a finite function denoting an array, \( i \) is an integer in \( \{0, \ldots, \text{dim}(a)\} \), and \( v \) is an integer in \( \mathbb{Z} \), we write \( \text{write}(a, i, v) \), instead of \( \text{update}(a, i, v) \). For any program \( P \), for any label \( \ell \), (i) \( \text{at}(\ell) \) denotes the command in \( P \) with label \( \ell \), and (ii) \( \text{nextlab}(\ell) \) denotes the label of the command, if any, that is written in \( P \) immediately after the command with label \( \ell \). For any expression \( e \) and environment \( \delta \), \( [e] \delta \) denotes the value of \( e \) in \( \delta \).

We assume that the evaluation of expressions has no side effects.

**Assignment.**
\[
\begin{align*}
\langle \ell : x = e, \delta \rangle & \rightarrow \langle \text{at}(\text{nextlab}(\ell)), \text{update}(\delta, x, [e] \delta) \rangle & \text{if } x \in \text{IVars} \\
\langle \ell : a[i]e = e, \delta \rangle & \rightarrow \langle \text{at}(\text{nextlab}(\ell)), \text{update}(\delta, a, \text{write}(\delta(a), i, [e] \delta)) \rangle & \text{if } a \in \text{AVars}
\end{align*}
\]

**Conditional.**
\[
\begin{align*}
\langle \ell : \text{if } (e) \ell_1 \text{ else } \ell_2, \delta \rangle & \rightarrow \langle \text{at}(\ell_1), \delta \rangle & \text{if } [e] \delta \neq 0 \\
\langle \ell : \text{if } (e) \ell_1 \text{ else } \ell_2, \delta \rangle & \rightarrow \langle \text{at}(\ell_2), \delta \rangle & \text{if } [e] \delta = 0
\end{align*}
\]

**Jump.**
\[
\langle \ell : \text{goto } \ell', \delta \rangle \rightarrow \langle \text{at}(\ell'), \delta \rangle
\]

Figure 3. Operational semantics of the imperative language \( \mathcal{L} \).

Let us now introduce the notion of program correctness. An environment \( \delta \) is said to satisfy a formula \( \varphi(z_1, \ldots, z_r) \) iff \( A \models \varphi(\delta(z_1), \ldots, \delta(z_r)) \) holds. Given two formulas \( \varphi_{\text{init}} \) and \( \varphi_{\text{error}} \) that are constraints with free variables \( z_1, \ldots, z_r \), we say that program \( \text{prog} \) is incorrect with respect to these formulas iff there exist two environments \( \delta_{\text{init}} \) and \( \delta_{\text{halt}} \) such that: (i) \( \delta_{\text{init}} \) satisfies \( \varphi_{\text{init}} \), (ii) \( \langle \ell_0 : c_0, \delta_{\text{init}} \rangle \rightarrow^* \langle \ell_h : \text{halt}, \delta_{\text{halt}} \rangle \), and (iii) \( \delta_{\text{halt}} \) satisfies \( \varphi_{\text{error}} \), where \( \ell_0 : c_0 \) is the first labeled command of \( \text{prog} \) and \( \ell_h : \text{halt} \) is the unique halt command of \( \text{prog} \). (In a paper by De Angelis et al. [27], the reader may find an extension of these definitions where \( \varphi_{\text{init}} \) and \( \varphi_{\text{error}} \) are predicates
defined by any CLP program.) A program is said to be correct (with respect to ϕ_{init} and ϕ_{error}) if it is not incorrect (with respect to ϕ_{init} and ϕ_{error}). Our notion of correctness is equivalent to the notion of partial correctness specified by the Hoare triple \{ϕ_{init}\} prog {¬ϕ_{error}}.

2.3. Encoding partial correctness into CLP

An imperative program is translated into a set of CLP facts of the form at(L,C), meaning that the command C has label L.

Configurations are represented as terms of the form cf(cmd(L,C), D), where: (i) L and C encode a label and a command, respectively, and (ii) D encodes an environment. An environment is represented as a list of pairs of the form [(...,(x,X),...),(a,A),...], where x and a are (integer and array, respectively) variable identifiers, and X and A are their values (that is, an integer and a sequence of integers, respectively). The transition relation ⇒ between configurations is represented by the binary predicate tr, which constitutes the CLP interpreter specifying the operational semantics, shown in Figure 3, of our imperative language, shown in Figure 2. In Figure 4 we have the clauses for tr relative to: (i) assignments (clauses 1i and 1a), (ii) conditionals (clauses 2t and 2f), and (iii) jumps (clause 3).

1i. tr(cf(cmd(L,iasgn(X,E)), D), cf(cmd(L1,C), D1)) :- eval(E,D,V), update(D,X,V,D1), nextlab(L,L1), at(L1,C).
1a. tr(cf(cmd(L,aasgn(A,IE,E)), D), cf(cmd(L1,C), D1)) :- lookup(A,D,S), eval(IE,D,I), eval(E,D,V), write(S,I,V,S1), update(D,A,S1,D1), nextlab(L,L1), at(L1,C).
2t. tr(cf(cmd(L,ite(E,L1,L2)), D), cf(cmd(L1,C), D)) :- beval(E,D), at(L1,C).
2f. tr(cf(cmd(L,ite(E,L1,L2)), D), cf(cmd(L2,C), D)) :- beval(not(E), D), at(L2,C).
3. tr(cf(cmd(L,goto(L1)), D), cf(cmd(L1,C), D)) :- at(L1,C).

Figure 4. The CLP interpreter for the operational semantics.

The term iasgn(X,E) encodes the (integer) assignment command X = E, where X ranges over integer variable identifiers and E ranges over expressions. The predicate eval(E,D,V) holds iff V is the value of the expression E in the environment D. The predicate update(D,X,V,D1) holds iff the new environment D1 is derived from the old environment D, by binding the variable X to the value V, using the function update (see Section 2.2). The predicate nextlab(L,L1) holds iff L1 is the label of the command that is written in the given imperative program immediately after the command with label L. The term aasgn(A,I,E) encodes the (array) assignment command A[I] = E, where A ranges over array variable identifiers, while I and E range over integer expressions. The predicate lookup(A,D,S) holds iff the value of the array variable identifier A stored in the environment D is S. By the definitions given in Sections 2.1 and 2.2, the constraint write(S,I,V,S1) holds iff write(S,I,V) = S1. (To improve the readability of clause 1a, we have not written this write constraint in the leftmost position of the body, but since conjunction is commutative, this does not modify the semantics of that clause.) The term ite(E,L1,L2) encodes the conditional command, and labels L1 and L2 specify where to jump to, depending on the value of the expression E. The predicate beval(E,D) holds iff the value of
the expression $E$ is not 0 (that is, $false$) in the environment $D$. The term $goto(L)$ encodes the jump to the command with label $L$.

As shown above, the CLP interpreter uses a write constraint to represent an array write (see clause 1a). Array reads are represented by read constraints, which are used in the definition of the eval and beval predicates. For instance, the predicate $eval(E,D,V)$, in the case where $E$ is an array expression $arr(A,IE)$, representing $[i]$, is defined by the following clause:

$$eval(arr(A,IE),D,V) :- eval(IE,D,I), lookup(A,D,S), read(S,I,V).$$

Note that the CLP interpreter does not need any explicit representation of the arrays. Array constraints will be dealt with by using the theory of arrays, without the need of such an explicit representation.

Now, we encode the problem of checking whether or not the program $prog$ is incorrect into the problem of checking whether or not the atom $incorrect$ is a consequence of the following CLP program $T$:

$$incorrect :- errorConf(Y), reach(Y).$$

$$reach(Y) :- tr(X,Y), reach(X).$$

$$reach(Y) :- initConf(Y).$$

Program $T$

where: (i) $initConf(Y)$ holds iff $Y$ is an initial configuration, that is, a configuration of the form $⟨⟨\ell_0: c_0, \delta_{init}⟩⟩$ and $\delta_{init}$ satisfies $\varphi_{init}$, and (ii) $errorConf(Y)$ holds iff $Y$ is an error configuration, that is, a configuration of the form $⟨⟨\ell_h: halt, \delta_{halt}⟩⟩$ and $\delta_{halt}$ satisfies $\varphi_{error}$. We also have that $reach(Y)$ holds iff the configuration $Y$ can be reached, in zero or more steps, from an initial configuration. Program $prog$ is correct with respect to $\varphi_{init}$ and $\varphi_{error}$ iff $incorrect \notin M(T)$.

Thus, program $T$ consists of two sets of clauses: the clauses defining the predicates $incorrect$, $reach$, and $tr$, which encode the semantics of a (generic) Hoare triple (through the negation of the postcondition), and the clauses defining the predicates at, $initConf$, and $errorConf$, which encode the specific program and property under consideration.

### 2.4. Generating verification conditions through CLP program specialization

Our verification method applies unfold/fold transformation rules to program $T$ and consists of the following two steps: (i) the application of the $VCGen$ strategy (see Figure 5), which generates the Verification Conditions $VC$ for the given imperative program $prog$, and (ii) the application of the $VCTransf$ strategy (see Figure 8), which checks the Satisfiability of the Verification Conditions via program transformation.

If $VCTransf$ fails to establish the satisfiability or the unsatisfiability of the Verification Conditions (and hence the correctness or the incorrectness of $prog$), then an SMT solver is applied to the new version $VC'$ of the Verification Conditions derived after applying the $VCTransf$ strategy. In Figure 1 we show a picture of the entire verification process.

Similarly to what is done in other papers [2, 19], the $VCGen$ strategy performs the specialization of program $T$ with respect to: (i) the predicate at, encoding the program $prog$, and (ii) the predicates $initConf$ and $errorConf$, encoding the property of interest, specified by the precondition $\varphi$ and the postcondition $\neg \psi$, respectively. The output of $VCGen$ is a CLP program $VC$, where the predicate $tr$
(see Figure 4), which encodes the interpreter for prog, does not occur, and for this reason the VCGen strategy is also called the removal of the interpreter [2].

Now we will present the VCGen strategy, while in the next section we will present the VCTransf strategy. In order to apply the VCGen strategy (see Figure 5) we need the following unfolding rule.

**Definition 2.1. (Unfolding Rule)**

Let \( P \) be a CLP program and \( C \) be a clause of the form \( H :- c, A, R \), where \( H \) and \( A \) are atoms, \( c \) is a constraint, and \( R \) is a (possibly empty) conjunction of atoms. By \( \text{Unf}(C, P) \) we denote the set \( \{ (H :- c, c_i, B_i, R) \mid i = 1, \ldots, m \} \), where \( \{ K_i :- c_i, B_i \mid i = 1, \ldots, m \} \) is the set of the (renamed apart) clauses of \( P \) such that, for \( i = 1, \ldots, m \), \( A \) is unifiable with \( K_i \) via the most general unifier \( \vartheta_i \).

In order to apply the unfolding rule during VCGen, we assume that the atoms occurring in bodies of clauses are annotated as either unfoldable or not unfoldable. This annotation is chosen so that any sequence of clauses that can be constructed from a given clause \( C \) by unfolding with respect to unfoldable atoms, is finite. In particular, we annotate the atoms with predicate \( \text{initConf} \), \( \text{errorConf} \), and all those occurring in the definition of \( \text{tr} \) (see Figure 4) as unfoldable. Every atom of the form \( \text{reach}(\text{cf}) \) is annotated as unfoldable in the case where: (i) the command in the configuration \( \text{cf} \) has label \( \ell \), and (ii) in the given imperative program there is neither a goto \( \ell \) command, nor an if-else command whose left or right arm is \( \ell \). Otherwise \( \text{reach}(\text{cf}) \) is annotated as not unfoldable.

---

**Input:** CLP program \( T \).

**Output:** CLP program \( VC \) such that incorrect \( \in M(T) \) iff incorrect \( \in M(VC) \).

```
INITIALIZATION
InDefs := \{ incorrect :- errorConf(Y), reach(Y) \};
VC := \emptyset; Defs := \emptyset;
while in InDefs there is a clause \( C \) do
  • UNFOLDING
    TransfC := Unf(C, T);
    while in TransfC there is a clause \( D \) whose leftmost atom is annotated as unfoldable do
      TransfC := (TransfC \(- D\)) \cup \text{Unf}(D, T);
    end-while;
  • DEFINITION & FOLDING
    while in TransfC there is a clause \( E \) of the form \( H :- c, \text{reach}(\text{cf}) \), where \( c \) is a constraint, do
      if in Defs there is no clause whose body is \( \text{reach}(\text{cf}) \)
        then add both to Defs and to InDefs the definition clause \( \text{newp}(V) :- \text{reach}(\text{cf}) \),
        where \( \text{newp} \) is a new predicate name and \( V \) is the tuple of variables occurring in \( \text{reach}(\text{cf}) \);
        TransfC := (TransfC \{- E\}) \cup \{ H :- c, \text{newp}(V) \};
      end-if;
    end-while;
    InDefs := InDefs \{- C\};
    VC := VC \cup TransfC;
end-while;
```

Figure 5. The VCGen strategy: Generating the verification conditions \( VC \).
A distinctive feature of the approach presented in this paper is that we add to program VC obtained by applying VCGen some additional constraints that will be used for controlling the generalization strategy, which is part of the VCTransf strategy. These additional constraints are of the form val(v,V), where v is a CLP constant representing a variable identifier occurring in the imperative program prog and V is a logical variable holding the values that can be taken by v during the computation. Obviously, these constraints are true and do not change the least model of VC. Their role is to identify the program variables whose values occur in the read constraints that appear in the clauses of VC. For instance, the constraint ‘val(a,A), val(i,I), read(A,I,U)’ expresses the property that read(A,I,U) gets the element of the array a at index i. The val constraints will be used, during the generalization strategy (see Section 5) to match read constraints that occur in different clauses. Indeed, to do this matching we cannot refer to the names of the logical variables, because their scope is always a single clause. In contrast, we will be able to match the constraint ‘val(a,A), val(i,I), read(A,I,U)’ with the constraint ‘val(a,B), val(i,J), read(B,J,Y)’, even if they occur in different clauses, because A and B refer to the same integer array identifier a, and I and J refer to the same integer variable identifier i. By restricting the matching of read constraints only to the read constraints which are associated with val constraints referring to the same identifiers in prog, we drastically decrease the number of possible matching read pairs, and thus we decrease the nondeterminism of the generalization strategy. This makes the generalization strategy more effective as confirmed by the experimental results (see Section 7).

In order to add val constraints to the clauses of VC we use the algorithm presented in Figure 6.

**Input:** The verification conditions VC.
**Output:** The verification conditions VC with added val constraints.

For every clause C in the verification conditions VC of the form:

C: newp(X) :- ..., read(A,I,U), ..., newq(Y)

where X and Y are two tuples of variables, each tuple being made out of distinct variables (the two tuples not being necessarily disjoint), for every constraint of the form read(A,I,U), for every B ∈ {A, I}, add val(b,B) to the body of C, if

either (i.1) B ∈ X, and (ii.1) the definition of newp introduced by VCGen is (modulo variable renaming) of the form:

\[ D_{newp}: \text{newp}(X) :- \text{reach}(\text{cf}(\text{cmd}(L,C)), [..., (b,B), ...]) \]

or (i.2) B ∈ Y, and (ii.2) the definition of newq introduced by VCGen is (modulo variable renaming) of the form:

\[ D_{newq}: \text{newq}(Y) :- \text{reach}(\text{cf}(\text{cmd}(L,C)), [..., (b,B), ...]) \]

where [..., (b,B), ...] is a list of pairs representing the environment.

---

**Figure 6.** Algorithm for adding val constraints to the verification conditions VC.

Now let us see how the VCGen works and how the val addition is performed on an example.

**Example 2.2.** Let us consider the program bubble-sort-inner shown in Column (a) of Figure 7. Given the array a[0], ..., a[n−1] and any \( i \in \{0, \ldots, n-1\} \), the program bubble-sort-inner stores in \( a[n−i−1] \) the maximum value of the prefix \( a[0], \ldots, a[n−i−1] \) by iteratively swapping adjacent elements. The translation of the program bubble-sort-inner into the language \( \mathcal{L} \) of Figure 2 is shown in Column (b) of Figure 7. The CLP representation of this translation is shown in Column (c).

Let us also consider the two properties \( \varphi_{\text{init}}(i, n, a) \equiv 0 \leq i < n \) and \( \varphi_{\text{error}}(i, j, n, a) \equiv \exists k \exists x \exists y \ 0 \leq i < n \land 0 \leq k < j \land j = n - i - 1 \land \text{read}(a, k, x) \land \text{read}(a, j, y) \land x > y. \)
The error property states that, upon termination of the program, there exists an index $k$ smaller than $n - i - 1$ such that $a[k] > a[n - i - 1]$, that is, the program bubble-sort-inner has failed to store in $a[n - i - 1]$ the maximum value of the prefix $a[0], \ldots, a[n - i - 1]$.

The $\varphi_{\text{init}}$ and $\varphi_{\text{error}}$ properties are used to express the initial and error configurations in CLP as follows:

$$\text{initConf}(\text{cf}(\text{cmd}(0,C),[(i,I),(n,N),(j,J),(a,A),(tmp,Tmp),(k,K)])) :- \text{at}(0,O), 0 \leq I, I < N.$$  
$$\text{errorConf}(\text{cf}(\text{cmd}(8,C),[(i,I),(n,N),(j,J),(a,A),(tmp,Tmp),(k,K)])) :- \text{at}(8,C), 0 \leq I, I < N, 0 \leq K, K < J, J = N - I - 1, X > Y, \text{read}(A,K,X), \text{read}(A,J,Y).$$

Note that index variables occurring in $\varphi_{\text{init}}$ and $\varphi_{\text{error}}$, and not in the program bubble-sort-inner (the so-called ghost variables, like $k$ in this example), are stored in the environment, and hence val constraints can be added also for those variables. At the end of the VCGen strategy and the algorithm for the addition of val constraints, we get the following CLP program $VC$ that expresses the verification conditions for the program bubble-sort-inner:

1. $\text{incorrect} :- 0 \leq I, 0 \leq K, K \leq J, J = N - I - 1, X > Y,$  
   Program $VC$  
   $\text{read}(A,K,X), \text{read}(A,J,Y), \text{val}(a,A), \text{val}(k,K), \text{val}(j,J), \text{loop}(I,J,N,A,Tmp,K).$

2. $\text{loop}(I,J1,N,A2,Tmp1,K) :- J1 = I + J, J < N - I - 1, J \geq 0, J < N - 1, X > Y,$  
   $\text{read}(A,J,X), \text{read}(A,J1,Y), \text{read}(A,J,Tmp1), \text{read}(A,J1,Z), \text{write}(A,J,Z,A1), \text{write}(A1,J1,Tmp1,A2), \text{val}(a,A), \text{val}(j,J), \text{val}(j,J1), \text{loop}(I,J,N,A,Tmp,K).$

3. $\text{loop}(I,J1,N,A,Tmp,K) :- J1 = I + J, J < N - I - 1, J \geq 0, J < N - 1, X \leq Y,$  
   $\text{read}(A,J,X), \text{read}(A,J1,Y), \text{val}(a,A), \text{val}(j,J), \text{val}(j,J1), \text{loop}(I,J,N,A,Tmp,K).$

4. $\text{loop}(I,J,N,A,Tmp,K) :- 0 \leq I, I < N, J = 0.$
of the for statement in the two mutually exclusive cases: (i) \(a[j] > a[j+1]\), and (ii) \(a[j] \leq a[j+1]\), respectively.

The \(\text{val}\) constraints are derived from the environment occurring in the following (renamed apart) definition of the loop predicate, which has been introduced by \textit{VCGen}:

\[
D: \text{loop}(I,J1,N,A,\text{Tmp},K) :- \text{reach}(\text{cf}(\text{cmd}(1,\text{ite}(\text{lt}(j,n-i-1),2,8))),
\[(i,I),(j,J1),(n,N),(a,A),(\text{tmp},\text{Tmp}),(k,K)]).
\]

Indeed, in clause 3 we have added the constraint \(\text{val}(a,A)\), because: (i) the variable \(A\) of the constraint \(\text{read}(A,J1,Y)\) occurs in the head of clause 3, and (ii) in the environment in definition \(D\) there is the pair \((a,A)\). In clause 3 we have added also the constraint \(\text{val}(j,J1)\), because: (i) the variable \(J1\) of the constraint \(\text{read}(A,J1,Y)\) occurs in the head of clause 3, and (ii) in the environment in definition \(D\) there is the pair \((j,J1)\). Finally, in clause 3 we have added the constraint \(\text{val}(j,J)\), because: (i) the variable \(J\) of the constraint \(\text{read}(A,J,X)\) occurs in the body atom \(\text{loop}(I,J,N,A,\text{Tmp},K)\) of clause 3, and (ii) in the environment in definition clause \(D\), once renamed by the substitution \(J1/J\), there is the pair \((j,J)\).

The termination and correctness of \textit{VCGen} are established by using the same techniques used by De Angelis et al. [2]. In particular, termination is derived from the fact that, since for any program the sets of labeled commands and variable identifiers are finite, we get that the set of possible new definitions that can be introduced is finite. The correctness is derived from the fact that the unfold/fold transformations preserve the least model of the given initial CLP program \(T\) [16]. We omit the details for lack of space.

3. A transformation strategy for verification

The \textit{VCTransf} strategy of our verification method transforms the verification conditions derived at the end of the \textit{VCGen} strategy, that is, the CLP program \(VC\), into a program \(VC'\) such that \(\text{incorrect} \in M(VC)\) iff \(\text{incorrect} \in M(VC')\). This transformation makes use of transformation rules that preserve the least \(A\)-model semantics of CLP programs. In particular, we apply the following rules, which are collectively called unfold/fold rules: (i) \textsc{Unfolding}, (ii) \textsc{Constraint Replacement}, (iii) \textsc{Clause Removal}, (iv) \textsc{Definition}, and (v) \textsc{Folding}. These rules are an adaptation to CLP programs on integer arrays of the unfold/fold rules for general CLP programs, and hence inherit the correctness properties of the general rules as described in the paper by Etalle et al. [16].

During the \textit{VCTransf} strategy we apply the unfold/fold rules according to a strategy whose effect is the propagation throughout the program \(VC\) of the constraints constituting the property \(\varphi_{\text{error}}\), which occur in the clauses defining the predicate \text{incorrect}. The objective of \textit{VCTransf} is to derive a program \(VC'\) without any constrained fact, thereby proving that \text{incorrect} does not hold, and hence that \text{prog} is correct with respect to \(\varphi_{\text{init}}\) and \(\varphi_{\text{error}}\). If, otherwise, we derive a CLP program \(VC'\) with some constrained facts, then we try to generate by unfolding the fact \text{incorrect}, hence proving that \text{incorrect} holds and \text{prog} is incorrect. Obviously, due to the undecidability of partial correctness, it may be the case that we derive a CLP program \(VC'\) with constrained facts, and yet we are not able to generate the fact \text{incorrect}, and hence we can establish neither correctness nor incorrectness of \text{prog}. 

**Input:** A linear recursive CLP program $VC$ and a positive integer $MaxUnf$.

**Output:** Program $VC'$ such that $\text{incorrect} \in M(VC)$ iff $\text{incorrect} \in M(VC')$.

**INITIALIZATION**

Let $InDefs$ be the set of all clauses of $VC$ whose head is the atom $\text{incorrect}$.

$VC' := \emptyset$; $Defs := InDefs$;

while in $InDefs$ there is a clause $C$ of the form $H :- c, A$ do

- **UNFOLDING** $TransfC := \text{Unf}(C, VC)$;
- **CONSTRAINT REPLACEMENT** $TransfC := \bigcup_{D \in TransfC} \text{Repl}(D)$;
- **REMOVAL OF SUBSUMED CLAUSES** Remove from $TransfC$ every clause $H :- d, B$ such that there exists a different clause $H :- e$ in $TransfC$ with $d \sqsubseteq e$;
- **DEFINITION & FOLDING**
  
  while in $TransfC$ there is a clause $E$ of the form $H :- e(V, X), p(X)$, where $V$ and $X$ are tuples of variables, $e(V, X)$ is a constraint and $p$ is a predicate defined in $VC$ do
  
  if in $Defs$ there is a clause $D$ of the form $\text{newp}(X) :- c(X), p(X)$, where $c(X)$ is a constraint such that $e(V, X) \sqsubseteq c(X)$
  
  then $TransfC := (TransfC - \{E\}) \cup \{H :- e(V, X), \text{newp}(X)\}$;
  
  else let $Gen(E,Defs)$ be $\text{newq}(X) :- \text{gen}(X), p(X)$.
  
  $Defs := Defs \cup \{Gen(E,Defs)\}$;
  
  $InDefs := InDefs \cup \{Gen(E,Defs)\}$;
  
  $TransfC := (TransfC - \{E\}) \cup \{H :- e(V, X), \text{newq}(X)\}$;
  
end-while;

$VC' := VC' \cup TransfC$; $InDefs := InDefs - \{C\}$;
end-while;

- **REMOVAL OF USELESS CLAUSES** Remove from $VC'$ all clauses with head predicate $p$, if in $VC'$ there is no constrained fact $q(\ldots) :- c$, where $q$ is either $p$ or a predicate on which $p$ depends.

- **POST-UNFOLDING**

  Let $Facts$ be the set of constrained facts in $VC'$ and $Rules$ be the set $VC' - Facts$.

  $DerivedFacts := Facts$;
  
  for $i = 1, \ldots, MaxUnf$ do
  
  $UnfVC := \emptyset$;
  
  for each clause $C$ in $Rules$ do
  
  $UnfVC := UnfVC \cup \text{Unf}(C,Facts)$;
  
  end-for;
  
  $Facts := \{f \mid f$ is a constrained fact in $UnfVC$ with head predicate $p$ and there is no constrained fact in $DerivedFacts$ with head predicate $p\}$;
  
  $DerivedFacts := DerivedFacts \cup \{f \mid f$ is a constrained fact in $UnfVC\}$;
  
  end-for;
  
  $VC' := VC' \cup DerivedFacts$;
end-for;

Figure 8. The $VCTransf$ strategy: Checking the satisfiability of the verification conditions $VC$ and deriving the new verification conditions $VC'$. 

However, since $\text{incorrect} \in M(\text{VC})$ iff $\text{incorrect} \in M(\text{VC}')$, we can still apply an SMT solver to the program $\text{VC}'$ derived by the $\text{VCTransf}$ strategy, and by doing so, we can hope to show correctness or incorrectness of $\text{prog}$. Indeed, this is what we have done in the experiments presented in Section 7. In particular, we have run the SMT solver Z3 [12] on the program $\text{VC}'$ produced by the $\text{VCTransf}$ strategy and we have been able to verify the correctness of some programs which could have not been verified by using the $\text{VCTransf}$ strategy alone (see Processes $\text{GT}$ and $\text{GTZ}$ in Table 1 of Section 7).

The $\text{VCTransf}$ strategy is performed by applying the unfold/fold transformation rules according to the $\text{VCTransf}$ strategy shown in Figure 8. Let us briefly describe how the various transformation rules are used within the $\text{VCTransf}$ strategy.

- The Unfolding rule performs one step of propagation of the constraint $\varphi_{\text{error}}$. We can view this step as a backward propagation, as we start from the final, error configuration and, by unfolding, we generate the predecessor configurations, moving backward towards the initial configuration.

- The Constraint Replacement rule infers new constraints on the variables occurring in the single atom of the body of each clause derived by Unfolding. Constraint Replacement makes use of a function $\text{Repl}$ that, given a clause $C$ of the form $H : \neg c_0, B$, returns a set $\{H : \neg c_1, B, \ldots, H : \neg c_n, B\}$ of clauses (with $n \geq 0$), where $c_1, \ldots, c_n$ are constraints such that $\mathcal{A} \models \forall c_0 \leftrightarrow (c_1 \lor \ldots \lor c_n))$ holds. In particular, if $c_0$ is unsatisfiable, then $n = 0$ and clause $C$ is removed. The function $\text{Repl}$ is implemented by a CHR$^*$ program as described in Section 4.

- The rule Removal of Useless Clauses and the rule Removal of Subsumed Clauses remove clauses that do not contribute to the least $\mathcal{A}$-model of the CLP program at hand.

- The Definition rule introduces new predicate definitions by suitable generalizations of the constraints. All new predicate definitions are collected in the set $\text{Defs}$. Generalization is performed by using a function $\text{Gen}$ such that, for any clause $E$ of the form $H : \neg e(V,X), p(X)$, $\text{Gen}(E, \text{Defs})$ is a clause of the form $\text{newq}(X) : \neg \text{gen}(X), p(X)$, where: (i) $\text{newq}$ is a new predicate symbol, and (ii) $\text{gen}(X)$ is a constraint such that $e(V,X) \sqsubseteq \text{gen}(X)$. The details of the function $\text{Gen}$ will be presented in Section 5. We will see that the function $\text{Gen}$ guarantees the termination of the $\text{VCTransf}$ strategy and allows us to prove the correctness of non-trivial programs.

- The Folding rule replaces a clause of the form $H : e(V,X), p(X)$ by a clause of the form $H : e(V,X), \text{newq}(X)$, where the predicate $\text{newq}(X)$ is defined by a clause that: (i) has been introduced in the set $\text{Defs}$ by the Definition rule, and (ii) is of the form $\text{newq}(X) : \neg \text{gen}(X), p(X)$, with $e(V,X) \sqsubseteq \text{gen}(X)$.

- The Post-Unfolding phase adds to $\text{VC}'$ (zero or more) constrained facts derived by repeatedly unfolding the clauses of $\text{VC}'$ with respect to constrained facts. Termination is guaranteed by the fact that, for each predicate $p$, the unfolding of all clauses with respect to $p$ is performed at most a fixed number of times and this number is provided by the value of the parameter $\text{MaxUnf}$.

If the Removal of Useless Clauses phase removes all clauses for $\text{incorrect}$, then $\text{prog}$ is correct with respect to $\varphi_{\text{init}}$ and $\varphi_{\text{error}}$. If the Post-Unfolding phase derives a constrained fact $\text{incorrect} : \neg c$ and $c$ is satisfiable, then $\text{incorrect}$ holds and $\text{prog}$ is not correct with respect to $\varphi_{\text{init}}$ and $\varphi_{\text{error}}$. 
Note that the input program VC of the VCTransf strategy is a linear recursive CLP program. Indeed, during the VCGen strategy the atoms different from reach are unfolded and hence a linear recursive program is generated.

The new predicates introduced by the Definition rule can be understood as over-approximations of the sets of configurations that are backward-reachable from the error configuration. Note, however, that when a new definition is used by the folding rule, the new predicate is called in a context that guarantees the preservation of the least A-model. In particular, with reference to Figure 8, e(V,X), p(X) is equivalent to e(V,X), newq(X). More in general, Theorem 6.2 shows that VCTransf preserves the least A-model, and hence a program is correct with respect to ϕinit and ϕerror if and only if incorrect ∉ M(VC′). Thus, no false positives are possible, that is, no derivations of the atom incorrect are possible for programs which are correct.

4. Constraint replacement via CHR

In this section we show how programs written in the language of Constraint Handling Rules with disjunction, denoted CHR∨ (or CHR, for short), can be used to perform the constraint replacements which are consequences of the axioms (A.1), (A.2), and (A.3) of the theory of arrays. These replacements are performed during the Constraint Replacement phase of the VCTransf strategy.

Now we formally define the particular class of CHR∨ programs we consider in this paper for the manipulation of integer and array constraints. First we need the following definitions.

A CHR∨ integer constraint (or a integer constraint, for short) either true, or false, or an atomic integer constraint (see Section 2.1), or a conjunction of integer constraints. As usual, conjunction is denoted by comma, while ‘=’ and ‘≠’ denote integer equality and disequality, respectively. A CHR∨ array constraint (or an array constraint, for short) is either true, or false, or an atomic array constraint (that is, a read or a write constraint), or a conjunction of array constraints. A CHR∨ constraint (or a constraint, for short) is either true, or false, or an atomic (integer or array) constraint, or a conjunction of constraints (this notion coincides with the one we have introduced for Constraint Logic Programs in Section 2.1). A CHR∨ goal (or a goal, for short) is either true, or false, or an atomic (integer or array) constraint, or a conjunction of goals, or a disjunction of goals. Disjunction is denoted by ‘∨’.

A CHR∨ rule is an expression of the form: r @ H1 \ H2 ⇔ G | B, where: (i) @ is a symbol separating the optional rule identifier r on the left from the rest of the rule on the right, (ii) H1 and H2, called the kept head and the removed head, respectively, are conjunctions of atomic array constraints, (iii) G, called the guard, is a conjunction of constraints, each of which is either an integer constraint or a syntactic identity, denoted ‘==’, and (iv) B, called the body, is a goal. We assume that H1 and H2 are not both empty conjunctions. If H2 is empty, then the rule is called a propagation rule and is simply written as: r @ H1 ⇒ G | B. The variables occurring in any CHR∨ rule are implicitly universally quantified at the front.

Given any CHR∨ rule of the form: r @ H1 \ H2 ⇔ G | B, its logical meaning is the universally quantified formula: ∀(G → ((H1 ∧ H2) ⇔ (H1 ∧ ∃Y B))), where Y is vars(B) − vars(H1 ∧ H2 ∧ G). A CHR∨ program is a set of CHR∨ rules, each of which rewrites old goals into new goals (and thus old states into new states) as specified by the operational semantics defined below (this semantics is a
variant of the one presented in a paper by Frühwirth [20]). Note that the CHR \(^\lor\) rules do not refer to the \(\text{val}\) constraints, and these \(\text{val}\) constraints are taken into consideration only during the execution of the generalization strategy (see Section 5).

Here is the CHR \(^\lor\) program, call it \(\text{Arr}\), that replaces the array constraints \(\text{read}\) and \(\text{write}\) by new constraints during the \text{CONSTRAINT REPLACEMENT} phase.

\[
\text{Program } \text{Arr} \quad \begin{align*}
\text{ac} @ \text{read}(A1,I,U) \setminus \text{read}(A2,J,V) & \iff A1 == A2, I=J | U=V. \\
\text{nac} @ \text{read}(A1,I,U), \text{read}(A2,J,V) & \Rightarrow A1 == A2, U\neq V | I\neq J. \\
\text{row} @ \text{write}(A1,I,U,A2) \setminus \text{read}(A3,J,V) & \iff A2 == A3 | (I=J, U=V) \lor (I\neq J, \text{read}(A1,J,V)).
\end{align*}
\]

Program \(\text{Arr}\) encodes the axioms (A.1), (A.2), and (A.3) presented in Section 2. We have that: (i) rule \(\text{ac}\) encodes axiom (A.1), (ii) rule \(\text{nac}\) encodes the implication \(U\neq V, \text{read}(A,I,U), \text{read}(A,J,V) \Rightarrow I\neq J\) (even if this implication is logically equivalent to axiom (A.1), the addition of rule \(\text{nac}\) may make the verification process more effective because it allows the deduction of disequalities that cannot be deduced by rule \(\text{ac}\) alone), and (iii) rule \(\text{row}\) encodes the two \text{read-over-write} axioms (A.2) and (A.3) (note that a single \(\text{CHR} \lor\) rule is enough for these two axioms because the goal of rule \(\text{row}\) is a disjunction of the two mutually exclusive constraints \((I=J, U=V)\) and \((I\neq J, \text{read}(A1,J,V))\)).

The operational semantics of a \(\text{CHR} \lor\) program is defined in terms of a transition relation, denoted \(\rightarrow\), between \(\text{CHR} \lor\) states [28]. In order to present this relation, we introduce the following definitions.

A \(\text{CHR} \lor\) state (or a \text{state}, for short) is a triple \(\langle g, u, b \rangle\), where: (i) \(g\) is a goal, (ii) \(u\) is a conjunction of array constraints, and (iii) \(b\) is a conjunction of constraints, each of which is either an integer constraint or a syntactic identity. An initial state is a state of the form \(\langle g, \text{true}, \text{true} \rangle\). Starting from any given state \(\langle g, u, b \rangle\), we derive a new state by one of the following transition (or rewriting) rules T1–T4 defining the transition (or rewriting) relation \(\rightarrow\). In these rules, by \(CT\) we denote the theory of the integer constraints and syntactic identities. Thus, in particular, for all logical variables \(X\), \(CT \models X = X\). We assume that in every \(\mathcal{A}\)-interpretation the predicate \(\equiv\) is interpreted as the identity on the domain, and since every \(\mathcal{A}\)-interpretation is a model of the theory of the integer constraints, we also have that \(\mathcal{A} \models CT\).

1. \text{Introduce:}  \(\langle a \land g, u, b \rangle \rightarrow \langle g, u, a \land b \rangle\) if \(a\) is an atomic integer constraint

\[
\langle a \land g, u, b \rangle \rightarrow \langle g, a \land u, b \rangle\text{ if }a\text{ is an atomic array constraint}
\]

2. \text{Simplify using} \(H1\setminus H2 \Leftrightarrow G | B:\) \(\langle g, H1' \land H2' \land u, b \rangle \rightarrow \langle B \vartheta \land g, H1' \land u, b \rangle\)

\[
\text{if } CT \models b \rightarrow G \vartheta, \text{ where } (H1 \land H2) \vartheta = (H1' \land H2')
\]

3. \text{Propagate using} \(H \Rightarrow G | B:\) \(\langle g, H' \land u, b \rangle \rightarrow \langle B \vartheta \land g, H' \land u, b \rangle\)

\[
\text{if } CT \models b \rightarrow G \vartheta, \text{ where } H \vartheta = H'
\]

4. \text{Split:} \(\langle (g1 \lor g2) \land g, u, b \rangle \rightarrow \langle g1 \land g, u, b \rangle\)

\[
\langle (g1 \lor g2) \land g, u, b \rangle \rightarrow \langle g2 \land g, u, b \rangle
\]
When applying the transition rules $T_2$ and $T_3$, the CHR\(^\vee\) rules $H_1 \land H_2 \Rightarrow G \mid B$ and $H \Rightarrow G \mid B$ are assumed to have no variables in common with the current state. In the Simplify rule $T_2$ the equality $(H_1 \land H_2) \vartheta == (H_1' \land H_2')$ means that: $\vartheta$ is a substitution, with domain $\text{vars}(H_1 \land H_2)$, such that $(H_1 \land H_2) \vartheta$ is syntactically identical to $(H_1' \land H_2')$. Likewise, the equality $H \vartheta == H'$ in the Propagate rule $T_3$ means that: $\vartheta$ is a substitution, with domain $\text{vars}(H)$, such that $H \vartheta$ is syntactically identical to $H'$. Disjunctions in goals are taken into account by the Split rule $T_4$. When applying rules $T_1$–$T_4$ we assume that $\land$ is an associative and commutative operator, and $\text{true}$ is the identity element of $\land$. Thus, for instance, when applying rule $T_1$ the atomic constraint $a$ is considered to be the same as $a \land \text{true}$, and when applying rule $T_4$ the goal $g_1 \lor g_2$ is considered to be the same as $(g_1 \lor g_2) \land \text{true}$. As usual, by $\mapsto^+$ we denote the transitive closure of $\mapsto$, and by $\mapsto^*$ we denote the reflexive, transitive closure of $\mapsto$.

A state is said to be **transient** if at least one of the transition rules $T_1$–$T_4$ is applicable in that state. Thus, for any transient state $s$, there exists at least one state $s'$ such that $s \mapsto s'$. We assume the following: if the Propagate rule $T_3$ is applied using the CHR\(^\vee\) rule $H \Rightarrow G \mid B$ in a state $s = \langle g, H' \land u, b \rangle$ to the conjunction $H'$ of array constraints, thereby deriving the new state $s' = \langle B \vartheta \land g, H' \land u, b \rangle$, where $H \vartheta == H'$, then the Propagate rule $T_3$ is not applicable to the same conjunction $H'$ in any state $\tilde{s}$ such that $s \mapsto^+ \tilde{s}$. This assumption makes it impossible to construct a trivial infinite sequence of states of the form: $s_0 \mapsto s_1 \mapsto s_2 \mapsto \ldots$, by applying rule $T_3$ to an occurrence of the conjunction $H'$ in $s_0$ and also to an occurrence of $H'$ in every state $s_i$, for $i > 0$, of that sequence. (Note that an application of rule $T_3$ adds a goal to the current state.)

A state is said to be **failed** if it is of the form $\langle c \land g, u, b \rangle$, where $c$ is an integer constraint and $CT \models (c \land b) \leftrightarrow \text{false}$. A state is said to be **successful** if it is neither transient nor failed. As a consequence of rules $T_1$ and $T_4$, a successful state is of the form $\langle \text{true}, u, b \rangle$ and, since a successful state is not transient, it cannot be rewritten using rules $T_1$–$T_4$.

A state is said to be **final** if it is either successful or failed. Note that, contrary to a successful state, a failed state may in general be rewritten using rules $T_1$–$T_4$.

The **computation tree** for a CHR\(^\vee\) program $P$ and an initial state $\langle g_0, u_0, b_0 \rangle$ is a maximal tree $T$ of states constructed in a nondeterministic way as follows. (Maximality holds in the sense that, if a node may have a child, then it has that child.) The root of $T$ is $\langle g_0, u_0, b_0 \rangle$. Given a non-failed, transient state $\langle g, u, b \rangle$ in $T$, its children are constructed by choosing either (i) an applicable rule $T_k$ among $T_1, T_2, T_3$, if at least one of these rules is applicable, or (ii) rule $T_4$, if this rule is applicable. In case (i) the state $\langle g, u, b \rangle$ has exactly one child $\langle g', u', b' \rangle$, where $\langle g, u, b \rangle \mapsto \langle g', u', b' \rangle$ by applying $T_k$ using $P$. In case (ii) the state $\langle g, u, b \rangle$ has the two children $\langle g', u', b' \rangle$ and $\langle g'', u'', b'' \rangle$, where $\langle g, u, b \rangle \mapsto \langle g', u', b' \rangle$ and $\langle g, u, b \rangle \mapsto \langle g'', u'', b'' \rangle$ by applying $T_4$. Note that, if during the construction of the computation tree $T$ we get a final state, then that state is a leaf of $T$ (hence the qualification ‘final’ also for failed states which may be rewritten using rules $T_1$–$T_4$).

A CHR\(^\vee\) program $P$ **terminates** starting from an initial state $s$ if all computation trees for $P$ and $s$ are finite.

The construction of a computation tree $T$ reflects the **committed choice** semantics of CHR\(^\vee\). Indeed, the construction of $T$ is nondeterministic, but once a rule that can be applied to a state has been chosen, it is not possible to perform backtracking on that choice. Thus, at every step of the construction of a computation tree, the choice of an applicable rule to any given state is fixed. Any two
computation trees among those that can be nondeterministically constructed, have equivalent sets of leaves in the sense of Proposition 4.1 below.

**Proposition 4.1. (Soundness and Confluence of Program Arr)**

Let us assume that program Arr terminates starting from the initial state \( \langle d, \text{true}, \text{true} \rangle \), for some constraint \( d \). Let \( \langle \text{true}, u_1, b_1 \rangle, \ldots, \langle \text{true}, u_n, b_n \rangle \) be all successful final states of any computation tree for program Arr and \( \langle d, \text{true}, \text{true} \rangle \). For \( i = 1, \ldots, n \), let \( d_i \) be the conjunction \( u_i \land b_i \). Then, 

\[
\begin{align*}
\forall(d \Rightarrow (d_1 \lor \ldots \lor d_n)), \\
\forall(b_1 \leftrightarrow b'_1)
\end{align*}
\]

For any two computation trees whose successful final states are \( \langle \text{true}, u_1, b_1 \rangle, \ldots, \langle \text{true}, u_n, b_n \rangle \) and \( \langle \text{true}, u'_1, b'_1 \rangle, \ldots, \langle \text{true}, u'_m, b'_m \rangle \) (modulo reordering), respectively, we have that \( n = m \) and, for \( i = 1, \ldots, n \), \( (\beta.1) u_i = u'_i \), and \( (\beta.2) CT \models \forall(b_1 \leftrightarrow b'_1) \).

Now we prove the termination of Arr.

First we introduce the following relation \( \ll \). Given a constraint \( c \), we define the relation \( \ll \) on \( \text{vars}(c) \) as follows: \( A \ll B \) iff the constraint \( \text{write}(A, I, U, B) \) occurs in \( c \). A constraint \( c \) is said to be non-circular iff the transitive closure \( \ll^* \) of the relation \( \ll \) is irreflexive. Since \( \text{vars}(c) \) is a finite set, \( \ll^* \) is a well-founded ordering on \( \text{vars}(c) \).

**Proposition 4.2. (Termination of Arr)**

The CHR program Arr terminates for all initial states \( \langle c, \text{true}, \text{true} \rangle \), where \( c \) is a non-circular constraint.

Now we define the function \( \text{Repl} \) that is used in the CONSTRAINT REPLACEMENT phase in the \( \text{VCTransf} \) strategy (see Figure 8). Let us consider a clause \( D \) of the form \( H :- d, B \), and let \( \langle \text{true}, u_1, b_1 \rangle, \ldots, \langle \text{true}, u_n, b_n \rangle \) be all successful final states of any computation tree for the program Arr and the initial state \( \langle d, \text{true}, \text{true} \rangle \). For \( i = 1, \ldots, n \), let \( d_i \) be the conjunction \( u_i \land b_i \) (which, as usual, is written as \( 'u_i, b_i' \), when occurring in bodies of clauses). Then, \( \text{Repl}(D) = \{ H :- d_1, B, \ldots, H :- d_n, B \} \).

As a consequence of Proposition 4.1 (\( \alpha \)), if we view a set of clauses as a conjunction of clauses, we have that \( A \models \forall(D) \leftrightarrow \forall(\text{Repl}(D)) \). This result is used in the proof of Theorem 6.2 below. Moreover, by Proposition 4.1 (\( \beta \)), we also have that the result of the function \( \text{Repl}(D) \) is independent, modulo equivalence up to \( CT \), of the computation tree used for its evaluation.

**Proposition 4.3. (Termination of Constraint Replacement)**

Every application of the function \( \text{Repl} \) during the \( \text{VCTransf} \) strategy terminates.

To see how CONSTRAINT REPLACEMENT works, let us consider the following example which is relative to the application of the \( \text{VCTransf} \) strategy to the program \( VC \), derived from the \text{bubble-sort-inner} program (see Section 2) after the application of the \( \text{VCGen} \) strategy.

**Example 4.4. (Applying the CONSTRAINT REPLACEMENT rule)**

After executing once the body of the outer while-loop of the \( \text{VCTransf} \) strategy (see Figure 8), we start a new execution of that body by considering the following definition clause 5 in \text{Defs}:

5. new2(I, J, N, A, Tmp, K) :- J \leq N - I - 1, J \geq K, I \geq 0, K \geq 0, J \geq N - I - 2, X \geq Y, read(A, J, Y), read(A, K, X), val(a, A), val(j, J), val(k, K), loop(I, J, N, A, Tmp, K).
After unfolding clause 5, we get a set of clauses, among which we have the following one:

6. \texttt{new2(I, J1, N, A2, W, K)} :- \texttt{J1=J+1, J<N-I-1, J\geq K, Z<W, I\geq 0, K\geq 0, J\geq N-I-3, X\succ Y, write(A, J, Z, A1), write(A1, J1, W, A2), read(A, J, W), read(A, J1, Z), read(A2, K, X), read(A2, J1, Y), val(a, A), val(a, A1), val(a, A2), val(j, J), val(j, J1), val(k, K), loop(I, J, N, A, Tmp, K).}

The CHR $^\lor$ program \texttt{Arr} rewrites the constraint occurring in this clause by some applications of the \texttt{row} rule, and thus the CONSTRAINT REPLACEMENT rule derives the following clause for the case $K\neq J$ (together with another clause not listed here, for the case $K=J$):

7. \texttt{new2(I, J1, N, A2, W, K)} :- \texttt{J1=J+1, J<N-I-1, J\geq K, Z<W, I\geq 0, K\geq 0, J\geq N-I-3, X\succ Y, write(A, J, Z, A1), write(A1, J1, W, A2), read(A, J, Y), read(A, J1, W), read(A2, K, X), val(a, A), val(a, A1), val(a, A2), val(j, J), val(j, J1), val(k, K), loop(I, J, N, A, Tmp, K).}

where: (i) by a single application of the rule \texttt{row}, the constraint \texttt{read(A2, J1, Y)} has been replaced by the constraint $Y=W$ (see the constraints with one underline), and (ii) by two applications of the rule \texttt{row} the constraint \texttt{read(A2, K, X)} has been replaced by \texttt{read(A, K, X)} (see the constraints with two underlines), where \texttt{A2} denotes the array $a$ after the two \texttt{write} operations associated with the constraint \texttt{‘write(A, J, Z, A1), write(A1, J1, W, A2)’}, and \texttt{A} denotes the array $a$ before these two operations (this replacement is justified because the additional constraint \texttt{‘J>K, J1>K’} implies \texttt{‘K\neq J, K\neq J1’}). □

5. The generalization strategy

The most critical step of the \texttt{VCTransf} strategy is the introduction of new predicates during the DEFINITION & FOLDING phase. In particular, we should make sure that only a finite number of new predicates are introduced during the execution of the outer while-loop of \texttt{VCTransf}, because otherwise the strategy may not terminate. For this reason, as usual in many program transformation techniques (see, for instance, the paper by Fioravanti et al. [29]), during the execution of the \texttt{VCTransf} strategy we collect in a set, which we call \texttt{Defs}, all predicate definitions that are introduced so far. Then, before introducing a new predicate definition $C$, we compare it with the predicate definitions we have collected in \texttt{Defs}. If $C$ is ‘similar’ to a predicate definition $A$ in \texttt{Defs} (and this similarity relation is formalized via the embedding relation $\prec$ we will define below), then the function \texttt{Gen} introduces, instead of $C$, a new predicate definition which is a generalization of $C$ with respect to $A$ and is computed by using a suitable generalization operator $\texttt{op}$ (see Figure 9).

Following the approach of Fioravanti et al. [29], the termination of the \texttt{VCTransf} strategy is a consequence of the following two facts: (1) the embedding relation is a well-binary relation [30], and hence generalization is eventually applied, and (2) the function \texttt{Gen} uses a constraint generalization operator $\texttt{op}$ by which only a finite number of different generalizations can be computed, and hence only a finite number of new predicates can be introduced during the \texttt{VCTransf} strategy.
Input: (i) A clause $E$ of the form $H :- e(V,X), p(X)$, obtained by unfolding and constraint replacement from a definition clause $C$ while executing the \textit{VCTransf} strategy. Let $e(V,X)$ be the conjunction $i,r,w,v$ of constraints. 
(ii) A tree $\text{Defs}$ of predicate definitions with clause $C$ as a leaf. 

Output: A definition clause $\text{newq}(X) :- \text{gen}(X), p(X)$, where $\text{newq}$ is a new predicate symbol, and $\text{gen}(X)$ is a constraint such that $e(V,X) \subseteq \text{gen}(X)$.

Let $E$ be the clause $H :- i,r,w,v, p(X)$ and let $E_x$, called the \textit{candidate definition clause for $E$}, be the clause $\text{newq}(X) :- i_x, r_x, v_x, p(X)$, where:
- $v_x$ is the conjunction of all constraints $\text{val}(j,J) \in v$ such that, for some $K$, $i \subseteq (J = K)$ and $K$ occurs in $X$,
- $r_x$ is the conjunction of all constraints $\text{read}(A,J,V) \in r$ such that, for some identifiers $a$ and $j$, $\text{val}(a,A) \in v_x$ and $\text{val}(j,J) \in v_x$, and
- $i_x$ is the projection of $i$ onto $\text{vars}(r_x) \cup \text{vars}(X)$.

If in $\text{Defs}$ there is a \textit{variant} $A$ of an ancestor of the definition clause $C$ such that 
(i) $A = H_0 :- i_0, r_0, v_0, p(X) \triangleright E_x = \text{newq}(X) :- i_x, r_x, v_x, p(X)$, and 
(ii) $r_0$ is equal to the subconjunction $r_x \ominus$ of the read constraint $r_x$.

Then let $i_1$ be the projection of $i_x$ onto $\text{vars}(r_0) \cup \text{vars}(X)$; define the constraint $\text{gen}(X)$ to be $i_0 \triangleright i_1, r_0, v_0$; Else define the constraint $\text{gen}(X)$ to be $i_x, r_x, v_x$ (which is the constraint of the candidate definition $E_x$).

Figure 9. The Generalization Function $\text{Gen}(E, \text{Defs})$. It is parameterized by the embedding relation $\triangleright$ and the generalization operator $\triangleright$.

The specific definitions of the embedding relation $\triangleright$ and the generalization operator $\triangleright$ we use, are based on the $\text{val}$ constraints that relate: (i) the logical variables occurring in the $\text{read}$ constraints, and (ii) the associated (integer or array) variable identifiers of the imperative language.

Before introducing the formal definitions of the embedding relation and of the generalization function, let us present a simple example which shows the role of the $\text{val}$ constraints when applying generalization.

Suppose that during the execution of \textit{VCTransf} we are about to introduce a new predicate defined by a clause of the form:

$C$: $\text{newq}(\ldots) :- X \geq 0, Y \leq 0, \text{read}(A,I,U), \text{read}(A,J,V), \text{val}(a,A), \text{val}(i,I), \text{val}(j,J), \ldots$

while in $\text{Defs}$ the following clause is already present:

$A$: $\text{newq}(\ldots) :- X = Y - 1, \text{read}(B,K,X), \text{read}(B,L,Y), \text{val}(a,B), \text{val}(i,K), \text{val}(j,L), \ldots$

Clause $A$ is similar to $C$ in the sense that they have the same conjunction of $\text{read}$ constraints, modulo variable renaming. Now, suppose that we apply a generalization strategy using the widening operator \cite{22} for generalizing integer constraints. If the strategy matches the $\text{read}$ constraints in $A$ against the ones in $C$ by taking into account the $\text{val}$ constraints, then the variables $A,I,J,U,V$ are renamed to $B,K,L,X,Y$, respectively, and hence the integer constraint of $C$ is renamed to $X \geq 0, Y \leq 0$. The widening of $X = Y - 1$ with respect to $X \geq 0, Y \leq 0$ is $X \geq Y - 1$ (indeed, $X = Y - 1$ is split into ‘$X \geq Y - 1, X \leq Y - 1’$ and then $X \leq Y - 1$ is discarded because it is not implied by $X \geq 0, Y \leq 0$), and thus the new generalized definition is of the form:

$G$: $\text{newq}(\ldots) :- X \geq Y - 1, \text{read}(B,K,X), \text{read}(B,L,Y), \text{val}(a,B), \text{val}(i,K), \text{val}(j,L), \ldots$

Now suppose that the generalization strategy does not consider the $\text{val}$ constraints. Besides the one
computed above, another possible matching of the read constraints is the one that renames \( A, I, J, U, V \) to \( B, L, K, Y, X \), respectively, and hence renames the integer constraint of \( C \) to \( Y \geq 0, X \leq 0 \). The widening of \( X=Y-1 \) with respect to \( Y \geq 0, X \leq 0 \) is the constraint true, and we get a different new generalized definition of the form:

\[
G1: \text{newg1}(...) :- \text{read}(B,K,X), \text{read}(B,L,Y), ...
\]

Thus, the use of the val constraints allows us to reduce the number of possible matchings for the read constraints, and hence the number of possible generalizations (from two to one, in our example above). Although in our example the generalization \( G \) seems more informative then \( G1 \), in general, there is no guarantee that our technique always allows to get the best generalization. However, the experimental evaluation of Section 7 shows that our heuristics based on val constraints work well in many examples in practice.

**Notation.** In the following we will denote constraints as conjunctions of the form \( i, r, w, v \), where \( i \) is an integer constraint, and \( r, w, \) and \( v \) are conjunctions of read, write, and val constraints, respectively. Conjunctions of constraints will also be represented as sequences. If a constraint \( c \) occurs in a conjunction \( d \) of constraints, we will write \( c \in d \).

Without loss of generality, we assume that, when the generalization function \( Gen \) is applied during the application of the \( VCTransf \) strategy to a CLP program \( P \), we first modify \( P \) so to satisfy the following conditions: in every clause \( C \) of \( P \), (i) the integer variables occurring in read constraints are all distinct, and (ii) these integer variables do not occur in any non-constraint atom of clause \( C \). Obviously, these conditions can always be fulfilled by adding some new variables and some equalities between these new variables and the old variables.

Note that different integer variable identifiers of the imperative program may get the same value, and thus it may be the case that a clause contains distinct val constraints that refer to the same logical variable. However, two array variable identifiers cannot refer to the same logical variable, because our theory of arrays does not include an extensionality axiom that is needed to prove the equality of two arrays. These facts justify the following definition.

**Definition 5.1. (Decorated read constraints)**

Let us consider a clause \( C \) of the form \( H :- i, r, w, v, B \). For every constraint \( \text{read}(A, K, U) \in r \), we construct a decorated read constraint of the form \( \text{read}(A^a, K^S, U) \), where:

- the decoration \( a \) is an array variable identifier such that \( \text{val}(a, A) \in v \), and
- the decoration \( S \) is the set of all integer variable identifiers \( k \) in \( L \) such that for some \( J, \text{val}(k, J) \in v \) and \( i \sqsubseteq (J=K) \).

**Definition 5.2. (Embedding relation \( \triangleleft \) between read constraints and clauses)**

Given any reflexive, binary relation \( \triangleleft \) between sets of identifiers, called an embedding relation, we extend it to decorated read constraints as follows: \( \text{read}(A^a, K^{S1}, U) \triangleleft \text{read}(B^a, H^{S2}, V) \) iff \( S1 \triangleleft S2 \). We further extend the relation \( \triangleleft \) to clauses as follows. Given two clauses \( C1 \) and \( C2 \), we stipulate
In what follows, we will consider various generalization operators on clauses based on the following two relations on sets of identifiers: (i) a given embedding relation $\bowtie$ between two clauses, and (ii) a given generalization operator $op$ on integer constraints. Given two integer constraints $i_0$ and $i_1$, the constraint $i_0 op i_1$, called the generalization of $i_1$ with respect to $i_0$, is such that $i_1 \subseteq (i_0 op i_1)$. In what follows, we will consider various generalization operators $op$ based on widening and convex hull [22, 29, 31].

The function $Gen$ takes as input, together with a clause, say $E$, to be generalized, also the set $Defs$ of the predicate definitions introduced so far during the execution of the $VCTransf$ strategy (see Figure 8). In the definition of the function $Gen$, we need the following notion of an ancestor clause of a given clause in $Defs$. A clause $A$ is said to be an ancestor of a clause $B$ if $A$ is $B$ itself or $A$ is the parent of an ancestor clause of $B$, where the parent relation between two clauses in $Defs$ is defined as follows. A clause $C$ is the parent of every clause $Gen(E, Defs)$, where: (i) $C$ is any clause considered in the outer while-loop of the $VCTransf$ strategy (the one with double vertical lines in Figure 8), and (ii) $E$ is any clause considered in the inner DEFINITION & FOLDING while-loop (the one with a single vertical line in Figure 8) executed for that clause $C$. The parent relation allows us to view the set $Defs$ of definitions as a tree in a natural way: (i) the set of nodes of that tree is $Defs$ itself, and (ii) the set of arcs of that tree is $\{(A, B) | A$ is the parent of $B\} \subseteq Defs \times Defs$.

Actually, since upon initialization of the $VCTransf$ strategy, the set $Defs$ may have, in general, more than one clause (this happens when incorrect is defined by multiple clauses), the parent relation allows us to view $Defs$ as a forest, rather than a tree. However, that forest can trivially be transformed into a tree by considering an extra node which is the parent of all those clauses that are initially in $Defs$, so that the roots of the trees of the forest are all sons of that extra node. By abuse of language, in what follows we will feel free to refer to $Defs$ as a tree of clauses, rather than a forest of clauses.

The function $Gen$ uses a projection operator (see Figure 9) that, for any integer constraint $i$ and set $X$ of variables, computes an integer constraint $i_p$, called the projection of $i$ onto $X$, such that we have: $Q \models \forall X(i_p \leftrightarrow \exists Y i)$, where $Q$ denotes the usual model of the rational numbers and $Y = \text{vars}(i) - X$. Thus, considering the integer numbers, instead of the rationals, we also have that $A \models \forall(i \rightarrow i_p)$.
Lemma 5.3. (Correctness of the $Gen$ function)

Let $E$ be a clause of the form $H :- e(V,X), p(X)$ and $Defs$ be a tree of definition clauses which are the inputs of the function $Gen$, and let $Gen(E,Defs)$ be the clause $newq(X) :- gen(X), p(X)$. Then $e(V,X) \subseteq gen(X)$.

Now, to fix our ideas, let us see an example of application of the generalization strategy.

Example 5.4. Consider clause 7, which was derived in Example 4.4 starting from the definition clause 5 by applying the $UNFOLDING$, $CONSTRAINT\ REPLACEMENT$, and $REMOVAL\ OF\ SUBSUMED\ CLAUSES$ phases of the $VCTransf$ strategy. The candidate definition for clause 7 is the following clause 8:

8. $new3(I,J,N,A,Tmp,K) :- J<N-I-1, I \geq 0, K \geq 0, J \geq N-I-3, J>K, X>Y,$

$read(A,J,Y), read(A,K,X), val(a,A), val(j,J), val(k,K), loop(I,J,N,A,Tmp,K).$

Here and below, for reasons of brevity, we allow ourselves to write $read$ constraints with integer variables that are in common with the non-constraint atoms. In particular, in clause 8 we have written $read(A,J,Y)$, with the variable $J$ in common with the non-constraint atom $loop(I,J,N,A,Tmp,K)$, instead of ‘$J=H, read(A,H,Y)$’, where $H$ is a new variable.

At this point of execution of the $VCTransf$ strategy we have that the set $Defs$ of definitions contains an ancestor of the definition clause 5 (see Example 4.4) (again, for reasons of brevity, we do not show all the execution steps of that strategy) and that ancestor $A$ (modulo variable renaming) is:

A. $new2(I,J,N,A,Tmp,K) :- J<N-I-1, I \geq 0, K \geq 0, J \geq N-I-2, J>K, X>Y,$

$read(A,J,Y), read(A,K,X), val(a,A), val(j,J), val(k,K), loop(I,J,N,A,Tmp,K).$

That ancestor definition has been inserted into $Defs$ as the result of a previous execution of the $DEFINITION\ \&\ FOLDING$ phases of the $VCTransf$ strategy.

Now, definition $A$ and clause 8 have the same conjunction $read(A^a,J^{[j]},Y), read(A^a,K^{[k]},X)$ of decorated $read$ constraints, and thus definition $A$ is embedded into the candidate definition clause 8 via the relation $\equiv$ (actually $A$ is embedded into clause 8 also via the relation $\sqcap$). We have that:

(i) in clause 8: $\underbrace{r^q_X = read(A,J,Y), read(A,K,X)}$, 
(ii) in clause $A$: $i_0 = J<N-I-1, I \geq 0, K \geq 0, J \geq N-I-2, J>K, X>Y$, and  
(iii) in clause 8: $i_X = i_1 = J<N-I-1, I \geq 0, K \geq 0, J \geq N-I-3, J>K, X>Y$.

The function $Gen(clause\ 7,Defs)$ returns the integer constraint $g$ which is $J<N-I-1, I \geq 0, K \geq 0, J>K, X>Y$. The constraint $g$ is a generalization of the integer constraint $i_1$ of the candidate definition clause 8 with respect to the constraint $i_0$ of $A$, and in our case we compute $g$ by the $widening$ operator, that is, by taking the conjunction of all atomic constraints $c$ of $i_0$ such that $i_1 \sqsubseteq c$. The resulting definition clause computed by the generalization function $Gen$ is the following one:

9. $new3(I,J,N,A,Tmp,K) :- J<N-I-1, I \geq 0, K \geq 0, J>K, X>Y,$

$read(A,J,Y), read(A,K,X), val(a,A), val(j,J), val(k,K), loop(I,J,N,A,Tmp,K).$

Note that the underlined constraint $J \geq N-I-2$ occurring in definition $A$ has been deleted because it is not entailed by the integer constraints of clause 8. Then, clause 9 is added to the set $Defs$ of definitions, and is used for folding clause 7 (see Example 4.4). Then, we begin a new execution of the body of the outer while-loop of the $VCTransf$ strategy. □
6. Termination and correctness of \textit{VCTransf}

In this section we prove that the \textit{VCTransf} strategy always terminates and preserves the least $A$-model semantics.

The following notion is needed to prove the termination of \textit{VCTransf}.

\textbf{Definition 6.1. (Well-binary relation $\preceq$)}

Given any set $C$, a reflexive, binary relation $\preceq \subseteq C \times C$ is said to be a well-binary relation (wbr) on $C$ if for every infinite sequence $C_1, C_2, \ldots$ of elements in $C$, there exist two integers $i$ and $j$, such that $i < j$ and $C_i \preceq C_j$. A wbr $\preceq$ is downward-finite if for every $C \in C$, the set \{$C' | C' \preceq C$\} is finite, where $\preceq^+$ denotes the transitive closure of $\preceq$.

It is easy to see that any embedding relation $\prec$ on clauses is a wbr.

In order to get the termination of \textit{VCTransf} we assume that there exists a downward-finite wbr $\preceq^+$ on the set of integer constraints, modulo variable renaming, such that the following property holds:

\[(W) \quad (i_0 \ op \ i_1) \preceq^+ i_0, \text{ for all integer constraints } i_0, i_1\]

where $op$ is the generalization operator which is a parameter of the function $Gen$. For the generalization operators we have used in our experiments, such wbr $\preceq^+$ exists [29].

The preservation of the least $A$-model after the \textit{VCTransf} transformation is guaranteed by general correctness results for the unfold/fold transformation rules [16, 17].

\textbf{Theorem 6.2.} (i) The \textit{VCTransf} strategy terminates. (ii) Let program $VC'$ be the output of \textit{VCTransf} applied to the input program $VC$. Then, $\text{incorrect} \in M(VC)$ iff $\text{incorrect} \in M(VC')$.

Now let us conclude our bubble-sort-inner example of Section 2. After a few iterations of the body of the outer while-loop, the \textit{VCTransf} strategy terminates and produces the following set $VC'$ of clauses (that we list here as they were generated by our automatic VeriMAP verification system [23]):

\begin{verbatim}
Program VC'
incorrect :- A = -1+B-C, D = -1+ B-C, E-F \leq -1, G \geq 0, C \geq 0, B-G-C \geq 2,
read(H, D, E), read(H, G, F), val(a, H), val(j, A), val(k, G), new1(C, A, B, H, I, G).
new1(A, B, C, D, E, F) :- G \geq F+1, H \geq F+1, A = -2+C-G, B = 1+G, I = 1+G, H = 1+G,
                    J = 1+G, K = 1+G, F-G \leq 0, L-E \leq -1, F \geq 0, C-G \geq 2, M-E \geq 1,
                    read(N, F, M), read(N, K, L), read(N, G, E), write(O, H, E, D), write(N, G, L, O),
                    val(a, N), val(j, G), val(k, F), val(j, B), new2(A, G, C, N, P, F).
new1(A, B, C, D, E, F) :- G \geq F+1, A = -2+C-G, B = 1+G, I = 1+G, F-G \leq 0,
                    F \geq 0, C-G \geq 2, J-K \geq 1, K-L \geq 0, read(D, G, L), read(D, F, J), read(D, H, K),
                    val(a, D), val(j, G), val(k, F), val(j, B), new2(A, G, C, D, E, F).
new2(A, B, C, D, E, F) :- G \geq F+1, H \geq F+1, B = 1+G, I = 1+G, H = 1+G, J = 1+G,
                    K = 1+G, A-C+G \leq -2, F-G \leq 0, L-E \leq -1, A \geq 0, F \geq 0, A-C+G \geq -3, M-E \geq 1,
                    read(N, F, M), read(N, K, L), read(N, G, E), write(O, H, E, D), write(N, G, L, O),
                    val(a, N), val(j, G), val(k, F), val(j, B), new3(A, G, C, N, P, F).
\end{verbatim}
new2(A, B, C, D, E, F) :- G ≥ F + 1, B = 1 + G, H = 1 + G, I = 1 + G, A - C + G ≤ -2, F - G ≤ 0,
    A ≥ 0, F ≥ 0, A - C + G ≥ -3, J - K ≥ 1, K - L ≥ 0, read(D, G, L), read(D, F, J),
    read(D, H, K), val(a, D), val(j, G), val(k, F), val(j, B), new3(A, G, C, D, E, F).
new3(A, B, C, D, E, F) :- G ≥ F + 1, H ≥ F + 1, B = 1 + G, I = 1 + G, H = 1 + G, J = 1 + G,
    K = 1 + G, A - C + G ≤ -2, F - G ≤ 0, L - E ≤ -1, A ≥ 0, F ≥ 0, M - E ≥ 1, read(N, F, M),
    read(N, K, L), read(N, G, E), write(O, H, E, D), write(N, G, L, O),
    val(a, N), val(j, G), val(k, F), val(j, B), new3(A, G, C, N, P, F).
new3(A, B, C, D, E, F) :- G ≥ F + 1, B = 1 + G, H = 1 + G, I = 1 + G, A - C + G ≤ -2, F - G ≤ 0,
    A ≥ 0, F ≥ 0, J - K ≥ 1, K - L ≥ 0, read(D, G, L), read(D, F, J), read(D, H, K),
    val(a, D), val(j, G), val(k, F), val(j, B), new3(A, G, C, D, E, F).

Since this set contains no constrained facts, by performing the REMOVAL OF USELESS CLAUSES
we remove all clauses from VC’ and the VCTransf strategy outputs the empty program. Thus,
incorrect /∈ M(VC’), and we conclude that the program bubble-sort-inner is correct with respect to
the given φInit and φError formulas.

7. Experimental evaluation

Now we present the results of the experimental evaluation we have performed for assessing the verification
techniques presented in this paper. We also compare our results with those obtained by the Z3
system1, which is one of the most popular SMT solvers for Horn clauses with constraints [12].

Implementation. We have implemented our techniques using the VeriMAP verification system [23],
a software model checker based on CLP program transformation and written in SICStus Prolog2. Our
prototype implementation consists of three modules. (1) A front-end module, based on the C Interme-
diate Language (CIL) [32], that compiles a verification problem into a set of Horn clauses (including
the clauses for the predicates at initConf, and errorConf) using a custom implementation of the
CIL visitor pattern. (2) A back-end module, based on VeriMAP, realizing the transformation strategy
VCTransf (see Section 3). (3) A module that translates a CLP program on integers and integer arrays
into the input format for the SMT solver Z3.

In the back-end module the Repl function of the VCTransf strategy has been implemented by
using the chr module3 of SICStus Prolog. Using that module we have computed from an input
constraint d, the set \{d1, ..., dn\} of output constraints, which are the constraints occurring in all
successful final states derived from the initial state (d, true, true) by the CHR rules of program Arr.

Verification problems. We have considered a benchmark set of 88 verification problems written in
the programming language C (63 of which are safe and the remaining 25 are unsafe). They have been
taken from the TACAS Software Verification Competition (65 problems) and from the literature [33, 34, 35, 36, 37] (the source code of those problems is available at http://map.uniroma2.it/smc/array-chr).
The benchmark set consists of programs that make use of: (i) if-then-else commands,
(ii) sequential composition of loops (for instance, the array initialization program and the array copy program), and (iii) nested loops (for instance, the bubble sort program and the selection sort program). In our verification tasks we were able to prove correctness of the selection sort program and to prove incorrectness of faulty versions of the selection sort and bubble sort programs.

Technical resources. The experiments have been performed on an Intel Xeon CPU E5-2640 2.00GHz processor with 64GB of memory under the GNU Linux operating system CentOS 7 (64 bit).

Experimental setup. Our experimental evaluation consists of the following four processes: (i) \(G\), (ii) \(GZ\), (iii) \(GT\), and (iv) \(GTZ\), that are defined as follows.

(i) \(G = VCGen\). In this process we have applied the \(VCGen\) strategy (see Figure 5) to the benchmark set, thereby generating the verification conditions \(VC\) for the problems in that benchmark. \(VCGen\) terminated for every problem in that benchmark within 0.3 s, taking an average time of 0.1 s.

(ii) \(GZ = VCGen ; Z3\). In this process, after the execution of the \(VCGen\) strategy, we have run Z3 using the Duality engine\(^4\) on the verification conditions \(VC\) generated by \(VCGen\).

(iii) \(GT = VCGen ; VCTransf\). In this process, after the execution of the \(VCGen\) strategy, we have executed the \(VCTransf\) strategy (see Figure 8) using as input the verification conditions \(VC\) generated by \(VCGen\).

(iv) \(GTZ = VCGen ; VCTransf ; Z3\). In this process, after the execution of the \(VCGen\) and \(VCTransf\) strategies, as in Process \(GT\), we have run the SMT solver Z3 on the verification conditions \(VC\)' for which satisfiability or unsatisfiability was not proved at the end of the \(VCTransf\) strategy.

We have used a time limit of 5 minutes for the execution of the individual phases of the processes, that is, the \(VCGen\) strategy, the \(VCTransf\) strategy, and the Z3 solver.

During the application of the \(VCTransf\) in Processes \(GT\) and \(GTZ\) we have also considered, besides the decorated \texttt{read} constraints (see Definition 5.1), also fully decorated \texttt{read} constraints, in the sense that, for every \texttt{read}(\(A, I, V\)) constraint, (i) we have added \texttt{val} constraints, not only for the array variable \(A\) and the index variable \(I\), but also for the value variable \(V\) (using the algorithm of Figure 6 for \(B \in \{A, I, V\}\), rather than \(B \in \{A, I\}\)), and (ii) we have considered a \texttt{read} atom of the form \texttt{read}(\(A^a, I^S, V^T\)), where, besides the decorations for \(a\) and \(S\), we have the decoration \(T\) that is defined by considering the \texttt{val} constraints for the value variable \(V\), in the same way that the decoration \(S\) has been defined (see Definition 5.1) by considering the \texttt{val} constraints for the index variable \(I\).

We have also used the generalization function \(Gen\) with different generalization operators that combine the \texttt{widen}ing and \texttt{convex hull} operators together with various embedding relations. By abuse of language, we will refer to these different versions of \(Gen\) as different generalization functions.

Different embedding relations are obtained: (1) by selecting different sets of variable identifiers for the introduction of the \texttt{val} constraints, and (2) by using different ways of comparing sets of identifiers. In particular, we have considered the following eight generalization functions: (i) \(Gen_{W,I,\oplus}\), (ii) \(Gen_{W,I,\equiv}\), (iii) \(Gen_{W,A,\oplus}\), (iv) \(Gen_{W,A,\equiv}\), (v) \(Gen_{H,I,\oplus}\), (vi) \(Gen_{H,I,\equiv}\), (vii) \(Gen_{H,A,\oplus}\), and (viii) \(Gen_{H,A,\equiv}\), where the subscripts should be understood as follows.

The first subscript denotes the generalization operator used: \(W\) stands for the \texttt{widen}ing operator, and \(H\) stands for the \texttt{widen}ing-and-\texttt{convex hull} operator [22, 29, 31]. The second subscript denotes

the selected sets of identifiers for defining the embedding relation $\prec$ between decorated (or fully decorated) read constraints (see Definition 5.2). In particular, $I$ refers to the array indexes, so that $\text{read}(A^a, S^1, V^1) \prec \text{read}(B^a, S^2, V^2)$ iff $S^1 \prec S^2$, and $A$ refers to the array indexes and array values, so that $\text{read}(A^a, S^1, V^1) \prec \text{read}(B^a, S^2, V^2)$ iff $(S^1 \prec S^2) \land (T^1 \prec T^2)$. The third subscript denotes the embedding relation $\prec$ that we have used: it is either $\cap$ or $\equiv$ (see Section 5).

**Results.** The results of our experiments are summarized in Tables 1 and 2 below. In Table 1 we report the results we have obtained by executing of Processes $G$, $GZ$, $GT$, and $GTZ$ on the whole benchmark set. In particular, we report: (i) the verification precision, that is, the number of problems which were solved within the time limit, and (ii) the average time taken for solving any of them. For the Processes $GT$ and $GTZ$, we report in different columns the results obtained when applying the $VCTransf$ strategy using the generalization function $Gen$, with the different parameters specified in the table.

For Process $GT$, the precision obtained when VeriMAP uses the widening-and-convex-hull operator $H$ is considerably higher than the precision obtained for Process $GZ$ (up to 74 vs. 49). The situation is reversed when VeriMAP uses the widening operator $W$ (down to 31 vs. 49).

For Process $GTZ$, we obtain a precision which is always higher than the precision obtained for Process $GZ$ (both for safe and unsafe programs), whatever generalization operator is used by the $VCTransf$ strategy (up to 80 vs. 49). This increase of precision is an experimental evidence that the propagation of constraints from the error property throughout the verification conditions performed by $VCTransf$, often improves the effectiveness of the SMT solver.

In terms of precision, for Process $GTZ$ the generalization functions based on the widening operator are competitive with those based on the widening-and-convex-hull operator. Actually, the most precise generalization function is $Gen_{W, A, \cap}$ (80 problems solved out of 88), immediately followed by $Gen_{H, A, \cap}$ (78 problems solved), and $Gen_{W, I, \cap}$ (76 problems solved).

Table 1. Verification results using VeriMAP and Z3 on a set of 88 verification problems: the verification precision (that is, the number of solved problems) and the average time. Times are in seconds.

| (1) $G = VCGen$ |  
|----------------|---|
| average time | 0.1 |
| (2) $GZ = VCGen ; Z3$ |  
| verification precision | 49 |
| average time | 3.5 |
| (3) $GT = VCGen ; VCTransf$ |  
| $Gen$ function parameters | $H, I, \cap$ | $H, I, \equiv$ | $H, A, \cap$ | $H, A, \equiv$ | $W, I, \cap$ | $W, I, \equiv$ | $W, A, \cap$ | $W, A, \equiv$ |
| verification precision | 60 | 70 | 74 | 71 | 34 | 35 | 34 | 31 |
| average time | 7.8 | 18.3 | 5.3 | 23.6 | 3.8 | 10.4 | 21.1 | 24.0 |
| (4) $GTZ = VCGen ; VCTransf ; Z3$ |  
| $Gen$ function parameters | $H, I, \cap$ | $H, I, \equiv$ | $H, A, \cap$ | $H, A, \equiv$ | $W, I, \cap$ | $W, I, \equiv$ | $W, A, \cap$ | $W, A, \equiv$ |
| verification precision | 67 | 75 | 78 | 75 | 76 | 72 | 80 | 67 |
| average time | 16.8 | 22.0 | 8.3 | 26.3 | 3.8 | 7.7 | 20.2 | 16.1 |
Table 2. Results using VeriMAP and Z3 on sets of problems solved by both systems. We used Processes GZ, GT, and GTZ, and different parameters for the generalization function Gen. Times are in seconds.

<table>
<thead>
<tr>
<th>Gen function parameters</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
<th>Column 5</th>
<th>Column 6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GZ</td>
<td>GT</td>
<td>GZ</td>
<td>GT</td>
<td>GZ</td>
<td>GTZ</td>
</tr>
<tr>
<td>(A) problems solved by both systems</td>
<td>42</td>
<td>26</td>
<td>26</td>
<td>44</td>
<td>45</td>
<td>46</td>
</tr>
<tr>
<td>(B) average time</td>
<td>3.4</td>
<td>3.9</td>
<td>3.5</td>
<td>27.2</td>
<td>3.1</td>
<td>4.6</td>
</tr>
</tbody>
</table>

When we use the ≡ operator for comparing sets of identifiers, the verification time is almost always higher than the verification time required when we use the ⊓ operator instead (the other parameters being left unchanged). Thus, while the ≡ operator can in principle be more precise than the ⊓ operator because ≡ triggers generalizations less often than ⊓, it may be the case in practice that ≡ introduces too many definitions and this may prevent the verification process from completing within the time limit.

A similar argument holds when comparing generalization functions based on the set A of identifiers with those based on the set I of identifiers. However, in this case, the increase of verification time generally does not deteriorate the precision of A which is higher than that of I (except for the cases when we use the generalization functions Gen_{W, A, ≡} and Gen_{W, I, ≡}).

In order to assess the relative performance of VeriMAP and Z3, we have compared the time they take on those problems of the benchmark set which can be solved by both systems. In Table 2 we report the results of this comparison.

Row (A) of Table 2 reports: (i) the number of problems which were solved by both Process GZ and Process GT, with three distinct sets of parameters for the generalization function Gen (see Columns 1–3), and (ii) the number of problems which were solved by both Process GZ and Process GTZ, with the same three sets of parameters (see Columns 4–6, respectively).

The three generalization functions used by the VCTransf strategy during Processes GT and GTZ, are: (i) the most precise generalization function for Process GT which is Gen_{H, A, ⊓} (see entry 74 in Table 1), (ii) the most precise generalization function for Process GTZ which is Gen_{W, A, ⊓} (see entry 80 in Table 1), and (iii) the generalization function with the lowest average time which is Gen_{W, I, ⊓}, both for GT and GTZ (see the two entries 3.8 in Table 1).

Row (B) of Table 2 reports the average verification time required by Processes GZ, GT, and GTZ when solving the problems of Row (A).

We observe that when the VCTransf strategy is applied by using Gen_{W, A, ⊓}, which is the most precise generalization function for Process GTZ, the average time is higher than that of Process GZ (see the two entries of Row (B) and Column 5).

A good trade-off between the number of solved problems and average verification time is provided by the use of Gen_{H, A, ⊓} (see the two entries of Row (B) and Column 1). In this case Process GT has an average time that is very close to that of Process GZ. When considering Process GTZ, the use
of \( \text{Gen}_{W,1,n} \) determines an average time that is even lower than that of Process \( GZ \) (see the two entries of Row (B) and Column 6). Finally, note that there are some problems that are verified by Z3 using Process \( GZ \), but cannot be verified, within the time limit, by Z3 after applying the \( \text{VCTransf} \) strategy, that is, using Process \( GTZ \) (see entry 49 for the verification precision of Process \( GZ \) in Table 1 and entry 46 in Column 6 of Table 2). In general, due to well known decidability limitations, it is impossible to provide a formal characterization of when the \( \text{VCTransf} \) strategy is guaranteed to improve the effectiveness of a given solver. In practice, it may be hard to predict the cases where there is a negative impact of \( \text{VCTransf} \) on the Z3 solver, due to the intricacies of the interaction of the transformation with the interpolation-based abstraction refinement heuristic implemented by Z3.

In summary, from our experimental evaluation we may conclude that the program transformation technique implemented in the VeriMAP system is complementary to the fixpoint-based Horn clause solving techniques of Z3 and, when VeriMAP is combined with Z3, there is a substantial synergic effect that results in an increase of the verification precision at the expenses of an acceptable increase of verification time.

8. Related work and conclusions

Already in the Introduction we mentioned some CLP-based program verification methods. Here we briefly recall other methods, not based on CLP, for the verification of array programs.

Some of these methods use abstract interpretation. In one such method [36], which is based on a previous work [38], Halbwachs et al. show how invariants can be discovered by: (i) partitioning the arrays into symbolic slices, and then (ii) associating an abstract variable with each slice. A similar approach is followed by Cousot et al. who present a scalable framework for the automatic analysis of array programs [34]. Flanagan et al. [39] and Lahiri et al. [40] present a predicate abstraction technique for inferring universally quantified properties of array elements. Gulavani et al. present a similar technique which uses template-based quantified abstract domains [41]. Seghir et al. use a backward reachability analysis, based on predicate abstraction and abstraction refinement, for the verification of assertions which are universally quantified over array indexes [42].

The methods based on abstract interpretation construct over-approximations, that is, invariants implied by the program executions. These methods have the advantage of being quite efficient, because they fix in advance a finite set of basic assertions from which the invariants can be constructed. However, for this same reason, these methods may lack flexibility as the abstraction should be re-designed when verification fails.

Also theorem provers have been applied to the derivation of invariants and the proof of the verification conditions once they have been derived. In particular, Bradley et al. [21] present a satisfiability decision procedure for a decidable fragment of the theory of arrays. That fragment is expressive enough to prove arrays properties such as sortedness. Other authors [43, 44, 45] present various techniques that use theorem proving for generating array invariants. Theorem proving techniques for program verification based on Satisfiability Modulo Theories (SMT) have also been studied [46, 47, 37]. The approaches based on theorem proving and SMT are more flexible with respect to those based on abstract interpretation, because no finite set of assertions is fixed in advance and, instead, the suitable assertions needed for the proofs can be generated on demand.
Although the approach based on CLP program transformation shares many ideas and techniques with abstract interpretation and automated theorem proving, we believe that it offers a higher degree of flexibility and parametricity. Indeed, the transformation-based method for the generation of the verification conditions and their proof, is very much independent of: (i) the imperative program, (ii) the operational semantics of the language in which the program is written, and (iii) the property to be verified. Thus, one can easily extend our technique to programs written in an imperative language with additional features (for instance, exception handling) as long as a CLP interpreter the operational semantics is provided for that language. Some experiments on the generation of verification conditions by specialization of CLP interpreters handling various language features have been presented in De Angelis et al. [48].

The use of CHR^∨ rules further enhances the flexibility of our transformation-based approach because CHR^∨ rules transform the constraints that represent operations on the data structures (such as the read and write operations in the case of arrays), while the unfold/fold rules transform the non-constraint atoms of the CLP programs. The experimental results we have reported in this paper, demonstrate that the combination of the two kinds of transformation rules, those for constraints and those for non-constraint atoms, is a promising, powerful technique for proving program properties.

As future work we plan to extend our transformation-based method to the verification of programs which manipulate dynamic data structures such as lists, trees, and heaps. To this aim, for instance, we may combine the CHR^∨ axiomatization of heaps proposed by Duck et al. [8] with the generalization functions based on widening and convex hull considered in this paper.

Acknowledgements

We would like to thank the anonymous referees of CILC 2014 and of the Special Issue of Fundamenta Informaticae for their helpful comments and constructive criticism. This work has been partially supported by the National Group of Computing Science (GNCS-INDAM).

References


Appendix: Proofs

Proof of proposition 4.1

Proof:

Proof of Point (α).

Let $L(\text{Arr})$ be the set of logical meanings of the rules \texttt{ac}, \texttt{nac}, and \texttt{row} of program \texttt{Arr}. Let $CT$ be the theory of the integer constraints and syntactic equalities. Let $T$ be any computation tree for \texttt{Arr} and the initial state $\langle \text{d, true, true} \rangle$, and let $\{\langle \text{true, u}_1, \text{b}_1 \rangle, \ldots, \langle \text{true, u}_n, \text{b}_n \rangle\}$ be the set of all successful final states of any computation tree that can be constructed for program \texttt{Arr} and $\langle \text{d, true, true} \rangle$.

Now for each state $\langle g, u, b \rangle$ in $T$ we have the following two facts.

(i) If $\langle g', u', b' \rangle$ is obtained from $\langle g, u, b \rangle$ by an application of any of the rules $T_1$, or $T_2$, or $T_3$, then $L(\text{Arr}) \cup CT \models \forall((g \land u \land b) \leftrightarrow (g' \land u' \land b'))$.

(ii) If $\langle g', u', b' \rangle$ and $\langle g'', u'', b'' \rangle$ are obtained from $\langle g, u, b \rangle$ by an application of the rule $T_4$, then $L(\text{Arr}) \cup CT \models \forall((g \land u \land b) \leftrightarrow ((g' \land u' \land b') \lor (g'' \land u'' \land b'')))$.  

Thus, by transitivity of equivalence, $L(\text{Arr}) \cup CT \models \forall(d \leftrightarrow (d_1 \lor \ldots \lor d_n))$. Since $\mathcal{A} \models L(\text{Arr}) \cup CT$, we get Point (α).

Proof of Point (β). In this proof we view the construction of a computation tree by using rules $T_1$–$T_4$ as a process of rewriting multisets of states, rather than states. In particular, the initial state is rewritten, possibly in several steps, into the multiset of the leaf states of the computation tree. Note that we consider multisets, rather than sets, of states because we want to prove a one-to-one correspondence between the successful final states of any two computation trees.

Let us first introduce the following definition.

Definition 8.1. (Equivalence of Multisets of States up to $CT$)

We say that two multisets $S$ and $S'$ of states are equivalent up to $CT$ if the following conditions hold (curly brackets denote multisets):

- $S$ is of the form $\{\langle g_1, u_1, b_1 \rangle, \ldots, \langle g_n, u_n, b_n \rangle\} \cup F$, where $F$ is a multiset of failed states,
- $S'$ is of the form (modulo reordering of states) $\{\langle g'_1, u'_1, b'_1 \rangle, \ldots, \langle g'_n, u'_n, b'_n \rangle\} \cup F'$, where $F'$ is a multiset of failed states, and
- for $i = 1, \ldots, n$, (1) $g_i = g'_i$, (2) $u_i = u'_i$, and (3) $CT \models b_i \leftrightarrow b'_i$.

In order to prove Point (β), we have to show that, for any two computation trees with the same initial state, the multisets of their leaf states are equivalent up to $CT$.

The proof of Point (β) is based on the fact that rules $T_1, T_2, T_3$, and $T_4$ are confluent modulo equivalence up to $CT$ in the following sense:

if a multiset of states $S$ can be rewritten into a multiset of states $S_1$ by a (possibly empty) sequence of applications of the rules, and a multiset $S'$ equivalent to $S$ up to $CT$, can be rewritten into a multiset of states $S_2$ by a (possibly empty) sequence of applications of the rules, then there exist multisets of states $S_3$ and $S_4$ and (possibly empty) sequences $\sigma_1$ and $\sigma_2$ of applications of the rules such that: (i) $S_1$ can be rewritten via $\sigma_1$ into $S_3$, (ii) $S_2$ can be rewritten via $\sigma_2$ into $S_4$, and (iii) $S_3$ is equivalent to $S_4$ up to $CT$. 

Since by Proposition 4.2 $\text{Arr}$ terminates (that is, the rewriting relation $\rightarrow$ defined by the rules $T1$–$T4$ using program $\text{Arr}$, is a noetherian relation), in order to prove the property of confluence modulo equivalence up to $CT$ for the rules $T1$–$T4$ using program $\text{Arr}$, it is enough to show the property of local confluence modulo equivalence up to $CT$ (this is a consequence of Lemma 2.7 of a paper by Huet [49]). In our case this local confluence property reduces to the following Properties (A) and (B):

(A) if a multiset $S$ of states is rewritten into a multiset $S_1$ of states by a single application of a rule, and $S$ is rewritten into a multiset $S_2$ of states by a single application of a rule,

then there exist multisets of states $S_3$ and $S_4$ and (possibly empty) sequences $\sigma_1$ and $\sigma_2$ of applications of the rules such that: (i) $S_1$ can be rewritten via $\sigma_1$ into $S_3$, (ii) $S_2$ can be rewritten via $\sigma_2$ into $S_4$, and (iii) $S_3$ is equivalent to $S_4$ up to $CT$, and

(B) if a multiset $S$ of states is rewritten into a multiset $S_1$ of states by a single application of a rule, and $S$ is equivalent up to $CT$ to a multiset $S_2$,

then there exist multisets of states $S_3$ and $S_4$ and (possibly empty) sequences $\sigma_1$ and $\sigma_2$ of applications of the rules such that: (i) $S_1$ can be rewritten via $\sigma_1$ into $S_3$, (ii) $S_2$ can be rewritten via $\sigma_2$ into $S_4$, and (iii) $S_3$ is equivalent to $S_4$ up to $CT$.

Before proving Properties (A) and (B), we state the following failure preservation property, called FP, which we will need below (the easy proof of this property is left to the reader):

(FP) any of the rules $T1$–$T4$ using program $\text{Arr}$, rewrites a failed state into one failed state or two failed states.

Now let us prove Property (A).

If the redexes of the two applications of the rules which produce the multisets $S_1$ and $S_2$ occur in two distinct states of $S$, then Property (A) trivially holds. Thus, we may restrict ourselves to the case where the two applications of the rules have redexes occurring in the same state of $S$. In this case, in order to show Property (A), since each rule in $\{T1, T2, T3, T4\}$ rewrites a single state, it is enough to show the following instance (A1) of Property (A):

(A1) if a state $s$ is rewritten into a multiset $S_1$ of states by a single application of a rule, and $s$ is rewritten into a multiset $S_2$ of states by a single application of a rule,

then there exist (possibly empty) sequences of applications of the rules such that $S_1$ and $S_2$ are rewritten into multisets $S_3$ and $S_4$ of states, respectively, and $S_3$ is equivalent to $S_4$ up to $CT$.

Note that any multiset obtained from a state $s$ by a single application of a rule in $\{T1, T2, T3, T4\}$, has at most two states.

We will only consider the following two cases of overlapping redexes in the same state. The other cases have proofs that are all much simpler than the one of Case 2 and are left to the reader.

(Case 1: redex of rule $T4$ and redex of rule $T3\text{-nac}$)

Suppose that $s$ is rewritten into two new states $s_1$ and $s_2$ by using $T4$, and $s$ is rewritten into $s_3$ by using $T3$. Suppose also that $s$ is a state of the form $\langle (g_1 \lor g_2) \land g_3, u, b \rangle$, and by rule $T4$ we get the two states $s_1$: $\langle g_1 \land g_3, u, b \rangle$ and $s_2$: $\langle g_2 \land g_3, u, b \rangle$. Furthermore, suppose that by applying rule $T3$ to $u$ in $s$ we get a state of the form $s_3$: $\langle (B \theta \land (g_1 \lor g_2) \land g_3), H' \land u, b \rangle$. Now, on one hand, by applying rule $T3$ to the two occurrences of $u$ in $s_1$ and $s_2$ we get $s_4$: $\langle (B \theta \land g_1 \land g_3), H' \land u, b \rangle$ and $s_5$: $\langle B \theta \lor g_2 \land g_3, H' \land u, b \rangle$. On the other hand, by applying $T4$ to $s_3$ we get again $s_4$ and $s_5$. Obviously, $\{s_4, s_5\}$ is equivalent to itself up to $CT$. Thus, Property (A1) holds.
Similar to this Case 1, are the other cases relative to an application of a rule in \{T_1, T_4\} and an application of a rule in \{T_2, T_3\}. Indeed, (i) any application of rule T_1 or T_4 cannot eliminate redexes for the application of rule T_2 or T_3, because: (i.1) the redexes for rules T_2 and T_3 depend only on the second component of the states, and (i.2) every application of T_1 or T_4 does not delete constraints from the second component, and symmetrically, (ii) any application of rule T_2 or T_3 cannot eliminate redexes for the application of rule T_1 or T_4 because: (ii.1) the redexes for rules T_1 and T_4 depend only on the first component of the states, and (ii.2) every application of T_2 or T_3 adds a constraint to the first component.

Similar to Case 1, are also the cases relative to the application of two (not necessarily distinct) rules in \{T_1, T_4\}. In all these cases the redexes of the second rule to be applied is preserved after the application of the first rule.

(Case 2: redex of rule T_2-row and redex of rule T_3-nac)

Let us consider a state s of the form \langle g, u, b \rangle, where the constraint u has the subconjuncton \(u' = \text{write}(A, I, U, B), \text{read}(B, J, V), \text{read}(B, K, W)\), and \(CT \models b \rightarrow V \neq W\). By keeping only the relevant information and forgetting about goal g, because it is irrelevant in our proof, we will write a state of that form as: \(\text{true} \quad || \quad u' \quad || \quad V \neq W\). We will also feel free to write ‘c’, instead of the conjunction ‘true, c’. In u’ the redex ‘\text{write}(A, I, U, B), \text{read}(B, J, V)’ for rule T_2-row overlaps (as shown by the above underlinings) with the redex ‘\text{read}(B, J, V), \text{read}(B, K, W)’ for rule T_3-nac.

From state s by applying once T_2-row, we get the following state:

\[(r) \quad (I=J, U=V) \lor (I \neq J, \text{read}(A, J, V)) \quad || \quad \text{write}(A, I, U, B), \text{read}(B, K, W) \quad || \quad V \neq W\]

From state s by applying once T_3-nac, we get the state:

\[(n) \quad J \neq K \quad || \quad \text{write}(A, I, U, B), \text{read}(B, J, V), \text{read}(B, K, W) \quad || \quad V \neq W\]

Now we have to show that by applying a sequence of rules in T_1–T_4 starting from state (r), we get a multiset of states that are equivalent up to \(CT\) to a multiset of states that can be obtained by applying a sequence of rules in T_1–T_4 starting from state (n). From (r) by applying T_4, we get the states:

\[(r1) \quad \text{true} \quad || \quad \text{write}(A, I, U, B), \text{read}(B, K, W) \quad || \quad I=J, U=V, V \neq W\]

\[(r2) \quad \text{true} \quad || \quad \text{write}(A, I, U, B), \text{read}(B, K, W), \text{read}(A, J, V) \quad || \quad I \neq J, V \neq W\]

From (r1) by applying T_2-row, we get the state:

\[(r1^\lor) \quad (I=K, U=W) \lor (I \neq K, \text{read}(A, K, W)) \quad || \quad \text{write}(A, I, U, B) \quad || \quad I=J, U=V, V \neq W\]

from which, by applying T_4 and a sequence of T_1 (so to move all the integer constraints to the third components of the states), we get the following two states (note that state (r11) is a failed state due to the underlined constraints):

\[(r11) \quad \text{true} \quad || \quad \text{write}(A, I, U, B) \quad || \quad I=K, U=W, I=J, U=V, V \neq W\] (failed state)

\[(r12) \quad \text{true} \quad || \quad \text{write}(A, I, U, B), \text{read}(A, K, W) \quad || \quad I \neq K, I=J, U=V, V \neq W\] (1)

From (r2) by applying T_2-row to the underlined constraints, we get the state:

\[(r2^\lor) \quad (I=K, U=W) \lor (I \neq K, \text{read}(A, K, W)) \quad || \quad \text{write}(A, I, U, B), \text{read}(A, J, V) \quad || \quad I \neq J, V \neq W\]

from which, by applying T_4 and a sequence of T_1 (so to move all the integer constraints to the third components of the states), we get the following two states:
(r21) true || write(A,I,U,B), read(A,J,V) || I=K, U=W, I≠J, V≠W (2)

From (r22) by applying $T3$-nac to the underlined constraints, we get the state:


Now we start the application of the rules from state (n). If we apply $T2$-row from (n), we get the state:


From (n1) by applying $T2$-row, we get the state:

(n1') (I=K, U=W) || write(A,I,U,B) || J≠K, I=J, U=V, V≠W

from which, by applying $T4$ and a sequence of $T1$ (so to move all the integer constraints to the third components of the states), we get the following two states:

(n11) true || write(A,I,U,B) || I=K, U=W, J≠K, I=J, U=V, V≠W (failed state)

From (n12) by applying $T2$-row, we get the state:


from which, by applying $T4$ and a sequence of $T1$ (so to move all the integer constraints to the third components of the states), we get the following two states:


At this point, from state (r) we have derived the non-failed states (1), (2), and (3), while from state (n) we have derived the non-failed states (1'), (2'), and (3').

Now, for $k=1,2,3$, the first two components of the states $(k)$ and $(k')$ are equal, and for the third components, we have that: $CT \models (k)_3 \iff (k')_3$, where $CT$ is the theory of the integer constraints and syntactic identities, and by $(k)_3$ and $(k')_3$ we indeed denote the integer constraint which is the third component of the states $(k)$ and $(k')$, respectively. In particular, we have that: $CT \models (1)_3 \iff (1')_3$, because the underlined constraint ‘$J\neq K$’ in (1') follows from the constraint ‘I=K, I≠J’ in (1'). Similarly, we have that: $CT \models (2)_3 \iff (2')_3$, because the underlined constraint ‘$J\neq K$’ in (2') follows from the constraint ‘I=K, I≠J’ in (2').

Thus, the multisets of states $\{(1),(2),(3)\}$ and $\{(1'),(2'),(3')\}$ are equivalent up to $CT$. This completes the proof of Case 2.

The other cases relative to the application of two (not necessarily distinct) rules in $\{T2,T3\}$, that is: (i) $\langle T2$-ac, $T2$-ac $\rangle$, (ii) $\langle T2$-ac, $T3$-nac $\rangle$, (iii) $\langle T2$-ac, $T2$-row $\rangle$, (iv) $\langle T3$-nac, $T3$-nac $\rangle$, and (v) $\langle T2$-row, $T2$-row $\rangle$, are all similar (and simpler) to Case 2 and, as already said, their proofs are left
to the reader. Note that symmetry holds, that is, a proof for the pair \( \langle r, r' \rangle \) of rules is also a proof for the pair \( \langle r', r \rangle \).

This concludes the proof of Property (A1), and also the proof of Property (A).

Now let us prove Property (B).

Since each rule in \( \{T1, T2, T3, T4\} \) rewrites a single state, it is enough to prove the following instance (B1) of Property (B):

**(B1)** if a state \( s \) is rewritten into a multiset \( S_1 \) of states by a single application of a rule, and \( s \) is equivalent up to \( CT \) to a state \( s_2 \),

*then* there exist multisets of states \( S_3 \) and \( S_4 \) and (possibly empty) sequences \( \sigma_1 \) and \( \sigma_2 \) of applications of the rules such that: (i) \( S_1 \) can be rewritten via \( \sigma_1 \) into \( S_3 \), (ii) \( s_2 \) can be rewritten via \( \sigma_2 \) into \( S_4 \), and (iii) \( S_3 \) is equivalent to \( S_4 \) up to \( CT \).

Let \( s \) be of the form \( \langle g, u, b \rangle \) and \( s_2 \) be of the form \( \langle g, u, b_2 \rangle \), where \( CT \models b \leftrightarrow b_2 \).

(Case 1). By applying to \( s \) any rule in \( \{T1, T2, T3\} \), we get the multiset \( S_1 \) is of the form \( \{\langle g_1, u_1, b_1 \land c \rangle\} \), for some goals \( g_1 \), \( u_1 \), and some (possibly \( \text{true} \)) integer constraint \( c \). Now, we can apply the same rule to the state \( s_2 \) and we get the multiset \( S_4 \) of the form \( \{\langle g_1, u_1, b_2 \land c \rangle\} \). If we take \( \sigma_1 \) to be the empty sequence, we have that \( S_3 = S_1 \). Since \( CT \models (b \land c) \leftrightarrow (b_2 \land c) \), we get that \( S_3 \) and \( S_4 \) are equivalent up to \( CT \).

(Case 2). By applying to \( s \) rule \( T4 \) we have that \( S_1 \) is of the form \( \{\langle g_1, u, b \rangle, \langle g_1', u, b \rangle \} \). Now by applying rule \( T4 \) to the state \( s_2 \), we get \( S_4 \) of the form \( \{\langle g_1, u, b_2 \rangle, \langle g_1', u, b_2 \rangle \} \). If we take \( \sigma_1 \) to be the empty sequence, we have that \( S_3 = S_1 \). Since \( CT \models b \leftrightarrow b_2 \), we have that: (i) \( \langle g_1, u, b \rangle \) is failed iff \( \langle g_1, u, b_2 \rangle \) is failed and (ii) \( \langle g_1', u, b \rangle \) is failed iff \( \langle g_1', u, b_2 \rangle \). Thus, we get that \( S_3 \) and \( S_4 \) are equivalent up to \( CT \).

This concludes the proof of Property (B1), and also the proof of Property (B).

Having proved Properties (A) and (B), from the termination of program \texttt{Arr} (see Proposition 4.2 whose proof is given below) we get confluence modulo equivalence up to \( CT \) of the rules \( T1 \)–\( T4 \), using program \texttt{Arr}. Thus, for any two computation trees with initial state \( \langle d, \text{true}, \text{true} \rangle \), the multisets, say \( L_1 \) and \( L_2 \), of their leaf states are such that: (i) there exist two multisets \( L_3 \) and \( L_4 \), with \( L_1 \rightarrow^* L_3 \) and \( L_2 \rightarrow^* L_4 \), and (ii) \( L_3 \) and \( L_4 \) are equivalent up to \( CT \).

When rewriting \( L_1 \) into \( L_3 \), only failed states can be rewritten. Thus, by Property (FP) above, \( L_1 \) and \( L_3 \) have the same multiset of successful states. For the same reason, also the multisets \( L_2 \) and \( L_4 \) have the same multiset of successful states. Since \( L_3 \) and \( L_4 \) are equivalent up to \( CT \), we get that \( L_1 \) and \( L_2 \) are equivalent up to \( CT \), and Point (\( \beta \)) is proved.

\[\square\]

**Proof of proposition 4.2**

**Proof:**

We have to show that the rewriting relation defined by the rules \( T1 \)–\( T4 \) using program \texttt{Arr} is a noetherian relation. We will reason by reductio ad absurdum.

Let us consider an infinite sequence of states generated by applying a sequence \( \sigma \) of transition rules in \( \{T1, T2, T3, T4\} \) using the \( \text{CHR}^\vee \) rules in \texttt{Arr}. The sequence \( \sigma \) should be of the form \( (T1^+ \ (T2+T3) \ (T1+T4)^*)^\omega \) (here we have used the notation of infinite regular expressions), that is, \( \sigma \) should have an infinite subsequence of not necessarily contiguous applications of rules in \( \{T2, T3\} \),
because for each application of either $T1$ or $T4$, the size of the first component of a state, strictly decreases. (A suitable notion of a size for proving this decrease is the number of $\wedge$’s plus the number of $\lor$’s occurring in the first component of a state.) Now we show that such an infinite subsequence of applications of rules in $\{T2, T3\}$ cannot exist, because, for any $n \geq 0$, the state generated immediately after an application of a rule in $\{T2, T3\}$ is greater, in a well-founded measure, than the state generated immediately after the next application of a rule in $\{T2, T3\}$.

First, we observe that for any sequence of states starting from a state $\langle g_0, u_0, b_0 \rangle$, generated by applying any sequence of transition rules in $\{T1, T2, T3, T4\}$ using a CHR$^\lor$ rule in Arr, the set of variables in every state of that sequence is $\text{vars}(\langle g_0, u_0, b_0 \rangle)$. Call this set $\text{Var}$. Let $\ll$ be the relation defined on $\text{Var} \times \text{Var}$ as we have indicated immediately before Proposition 4.2.

Let us introduce the following measures for a state $s = \langle g, u, b \rangle$ such that $\text{vars}(s)$ is $\text{Var}$:
1. $\mu_n(s)$, which is the number of $\text{read}$ constraints in $g \land u$,
2. $\mu_r(s)$, which is the sum, for all constraints of the form $\text{read}(B, \_ , \_)$ in $g \land u$, of the number of variables $A$ in $\text{Var}$ such that $A \ll^* B$, where $\ll^*$ denotes the reflexive, transitive closure of $\ll$, and
3. $\mu_p(s)$, which is the number of pairs of distinct $\text{read}$ constraints which are available for applying the rule $T2$ using the CHR$^\lor$ rule nac.

Let us assume that we apply one of the rules in $\{T1, T2\}$ to a state $s_i = \langle g_i, u_i, b_i \rangle$, thereby deriving a new state $s_{i+1}$. (Note that any initial state of the form $\langle c, \text{true}, \text{true} \rangle$ is a particular instance of the state $s_i$.) Now, there are three cases.

Case (i): we apply rule $T2$ using ac. In this case the measure $\mu_n(s_i)$ decreases and no other application of a rule in $\{T1, T2, T3, T4\}$ using a CHR$^\lor$ rule in Arr increases this measure.

Case (ii): we apply rule $T2$ using row. In this case the measure $\mu_r(s_i)$ decreases and no other application of a rule in $\{T1, T2, T3, T4\}$ using a CHR$^\lor$ rule in Arr increases this measure. Indeed, in this case, if $\text{write}(A_1, I, X, A_2)$ occurs in $u_i$, then a constraint $\text{read}(A_2, J, Y)$ is replaced by a constraint $\text{read}(A_1, J, Y)$ with $A_1 \ll^+ A_2$. Note also that no other rule application modifies any $\text{write}$ constraint.

Case (iii): we apply rule $T3$ using nac. In this case the measure $\mu_p(s_i)$ decreases and no other application of a rule in $\{T1, T2, T3, T4\}$ using a CHR$^\lor$ rule in Arr increases this measure. Indeed, (1) the number of new distinct $\text{read}$ constraints that can be generated by subsequent applications of the rule $T2$ using row, is not greater than $\mu_r(s_i)$, (2) the Propagation rule cannot be applied to the same pair of $\text{read}$ constraints, and (3) the number of pairs of distinct $\text{read}$ constraints is not greater than $\mu_r(s_i) (\mu_r(s_i) - 1)/2$.

Since $\mu_n(s_i) + \mu_p(s_i) + \mu_r(s_i) > \mu_n(s_{i+1}) + \mu_p(s_{i+1}) + \mu_r(s_{i+1})$, we get the thesis.

**Proof of proposition 4.3**

**Proof:**

By Proposition 4.2 it is enough to show that every constraint occurring in a clause derived during the $VCTransf$ strategy is non-circular.

First, we have to show that all constraints in the set $VC$ of clauses derived by the $VCGen$ strategy are non-circular. In the CLP program $T$ which is the input for $VCGen$, a $\text{write}$ constraint occurs in clause $1a$ only (see Figure 4), and it is non-circular. Conjunctions of two or more $\text{write}$ constraints
may be derived by the UNFOLDING phase starting from a definition of the form $H :- \text{reach}(cf)$, only if during this phase we unfold twice or more times a $\text{tr}$ atom using clause 1a. The sequence of clauses generated by the UNFOLDING phase will be of the form:

\begin{align*}
C1. & \ H :- \text{reach}(cf) \\
C2. & \ H :- \ldots, \text{reach}(cf1) \\
C3. & \ H :- \ldots, \text{tr}(cf2,cf1), \text{reach}(cf2) \\
C4. & \ H :- \ldots, \text{write}(S2,\ldots,S1), \ldots, \text{reach}(cf2)
\end{align*}

Looking at the clauses for $\text{reach}$ and $\text{tr}$ (clause 1a), the variable $S1$ does not occur in $cf2$. Similarly, when a subsequent unfolding derives a second $\text{write}$ constraint, we will have a sequence of clauses of the form:

\begin{align*}
C5. & \ H :- \ldots, \text{write}(S2,\ldots,S1),\ldots, \text{reach}(cf3) \\
C6. & \ H :- \ldots, \text{write}(S2,\ldots,S1),\ldots, \text{tr}(cf4,cf3), \text{reach}(cf4) \\
C7. & \ H :- \ldots, \text{write}(S2,\ldots,S1),\ldots, \text{write}(S4,\ldots,S3),\ldots, \text{reach}(cf4)
\end{align*}

where $S1$ does not occur in $cf3$ (by induction), and hence $S1$ does not occur in $\text{write}(S4,\ldots,S3)$. (Note that $S2$ could be equal to $S3$, and this case occurs when the unfolding of the predicate $\text{reach}$ corresponds to the execution of two consecutive write operations on the same array, but this is irrelevant for our argument here.) Thus, the constraint in clause $C7$ is non-circular. The variable $S3$ does not occur in $cf4$, and the above argument can be generalized to show (by induction) that all constraints derived during the UNFOLDING phase are non-circular.

During the DEFINITION & FOLDING phase the $\text{write}$ constraints are not modified, and thus at the end of the $VCGen$ strategy, we get a set $VC$ of clauses whose constraints are non-circular.

The same argument goes through for $VCTransf$ by using the additional observations that the $\text{write}$ constraints are not modified during the CONSTRAINT REPLACEMENT phase, and during the DEFINITION & FOLDING phase the generalization function $Gen$ can only introduce new definitions without $\text{write}$ constraints (see Section 5). \hfill $\square$

**Proof of lemma 5.3**

**Proof:**

$e(V,X)$ is the conjunction $i,r,w,v$. We have that $i,r,w,v \sqsubseteq i_X, r_X, v_X$, because $i_X$ is obtained by projection from $i$ and $r_X, v_X$ is a subconjunction of $r, w, v$. In the case where $\text{gen}(X)$ is computed in the Then branch, $\text{gen}(X)$ is $g, r_0, v_0$ and $i_X, r_X, v_X \sqsubseteq g, r_0, v_0$, because $i_X \sqsubseteq i_1$ ($i_1$ is obtained by projection from $i_X$) and $i_1 \sqsubseteq g$ ($g$ is obtained by applying $op$), and hence we get the thesis. In the case where $\text{gen}(X)$ is computed in the Else branch, we get immediately the thesis, as $\text{gen}(X)$ is $i_X, r_X, v_X$. \hfill $\square$

**Proof of theorem 6.2**

First we need some preliminary notions and lemmata.

**Lemma 8.2.** Any embedding relation $\ll$ on clauses is a wbr.
Proof:
(i) By Definition 5.2 it is enough to show that $\prec$ is a wbr on sets of variable identifiers. The variable identifiers used in any given program are taken from a finite set $Id \subseteq IVars \cup AVars$. Thus, for any infinite sequence $S_1, S_2, \ldots$ of finite sets of identifiers in $Id$, there exist two indexes $i, j$, with $i < j$, such that $S_i = S_j$, and hence $S_i \prec S_j$.

Given two clauses $C_1$ and $C_2$, we write $C_1 \preceq_{int} C_2$ if $i_1 \preceq_{int} i_2$, where $i_1$ and $i_2$ are the integer constraints occurring in $C_1$ and $C_2$, respectively.

Let $\prec$ be an embedding relation. We write $x \succ y$ if $y \prec x$, and we write $x \triangleright y$ if $x \prec y$ and $x \neq y$. Given two clauses $C_1$ and $C_2$, we write $C_1 \preceq_{int} C_2$ if $C_1 \prec C_2$ and $C_1 \not\preceq C_2$ or (ii) $C_1 \not\preceq_{int} C_2$.

Lemma 8.3. Let $Defs$ be a set of clauses of the form: $\text{newp}(V) : - i, r, v, p(X)$, where (i) $V$ is a tuple of variables occurring in $i, r, v, p(X)$, (ii) $p \in \Pi$, where $\Pi$ is a finite set of predicate names, and (iii) no two clause bodies are variants of each other. Then, $(\alpha) \preceq_{cl}$ is a wbr on $Defs$. Moreover, $(\beta) \preceq_{int}$ is a downward-finite wbr on $Defs$.

Proof:
(α) $\preceq_{cl}$ is a wbr on $Defs$. Let us consider an infinite sequence $\sigma = C_1, C_2, \ldots$ of clauses in $Defs$. We construct a new sequence $\sigma' = C_1', C_2', \ldots$ by deleting from $C_1, C_2, \ldots$ every $C_k$ for which there exists $h$, with $h < k$, such that $C_h \prec C_k$ and the set $\{C \mid C \in \sigma \text{ and } C_h \prec C\}$ is finite. $\sigma'$ is an infinite sequence, and since, by Lemma 8.2, $\prec$ is a wbr, there exist $i$ and $j$ such that $i < j$ and $C_i' \preceq C_j'$. Now, we consider two cases:

Case $C_i' \not\preceq C_j'$. By the definition of $\preceq_{cl}$, we get that $C_i' \preceq_{cl} C_j'$.

Case $C_i' \succ C_j'$. By construction of $\sigma'$, the set $\Sigma_j = \{C' \mid C' \in \sigma' \text{ and } C_j' \prec C'\}$ is infinite. Let us consider an infinite subsequence $\sigma''$ of $\sigma'$ made out of all the elements of $\Sigma_j$. From $\sigma''$ we can extract an infinite subsequence $\sigma''' = C_{i''}^1, C_{i''}^2, \ldots$ such that for every pair $C_{i''}^u, C_{i''}^v$ of clauses in $\sigma'''$, we have that $C_{i''}^u \triangleright C_{i''}^v$. This fact is proved by the following Points (i)–(iii).

(i) By the definition of $\triangleright$, all clauses in $\Sigma_j$ have the same number $t$ of atomic read constraints.
(ii) We define the equivalence relation $\simeq$ as follows.

Given two decorated atomic read constraints,

$$\text{read}(A^a, K^a_1, U) \simeq \text{read}(B^a, H^a_2, V) \text{ iff } S_1 = S_2$$

Given two clauses $C_1$ and $C_2$ in $\sigma''$ (hence with the same number $t$ of atomic read constraints),

$$C_1 = H_1 : - i_1, r_1, v_1, B_1 \simeq C_2 = H_2 : - i_2, r_2, v_2, B_2 \text{ iff}$$

let $\overline{r_1}, \ldots, \overline{r_t}$ be the decorated read constraints of $r_1$, and let $\overline{r_2}, \ldots, \overline{r_t}$ be the decorated read constraints of $r_2$.

there exists a permutation $i_1, \ldots, i_t$ of $\{1, \ldots, t\}$ such that, for $j = 1, \ldots, t$, $\overline{r_{i_j}} \simeq \overline{r_{i_j}}$.

Clearly, $C_1 \simeq C_2$ implies $C_1 \triangleright C_2$.

(iii) From (i) and the finiteness of the set of variable identifiers in the given imperative program, it follows that $\simeq$ has a finite set of equivalence classes. Thus, it is possible to construct an infinite subsequence $\sigma'''$ of $\sigma''$ whose elements all belong to the same equivalence class of $\simeq$, and hence all elements of $\sigma'''$ are in the relation $\triangleright$. 

\[\square\]
Now, since $\preceq_{\text{int}}$ is a wbr, there exist $C''_m$ and $C''_n$ in $\sigma''$, with $m < n$, such that $i_m \preceq_{\text{int}} i_n$, where $i_m$ and $i_n$ are the integer constraints in $C''_m$ and $C''_n$, respectively. Since, by construction of $\sigma''$, we also have $C''_m \not\succ C''_n$, by definition of $\preceq_{\text{cl}}$, we get $C''_m \preceq_{\text{int}} C''_n$, and thus $C''_m \preceq_{\text{cl}} C''_n$.

$(\beta) \preceq_{\text{int}}$ is a downward-finite wbr on $\text{Defs}$. This fact follows immediately from: (\(\beta.1\)) the hypotheses (i)–(iii) of this lemma, (\(\beta.2\)) the fact that $C_1 \not\succ C_2$ implies that the constraints $r_1$ in $C_1$ and $r_2$ in $C_2$ may only differ for the names of the logical variables (in particular the two constraints have the same cardinality), (\(\beta.3\)) the finiteness of the set of constants in $\text{Defs}$ denoting (integer or array) variable identifiers of the given imperative program, and (\(\beta.4\)) the assumption that $\preceq_{\text{int}}$ is a downward-finite wbr on $\text{Defs}$.

\[\square\]

Now we are ready to prove Theorem 6.2.

**Proof:**

(i) **Termination.** Each of the Unfolding, Constraint Replacement, Removal of Subsumed Clauses, Definition & Folding; Removal of Useless Clauses, and Post-Unfolding phases terminates. In particular, the termination of Constraint Replacement has been proved in Proposition 4.3. The termination of Post-Unfolding follows from the fact that the maximal number of unfolding steps is determined by $\text{MaxUnf}$. The termination of the other phases is straightforward.

Now we note that the while-loop of the $\text{VCTransf}$ strategy terminates if and only if the set of new predicate definitions that is introduced by executions of the Definition & Folding phase is finite. Indeed, each new predicate definition is added to $\text{InDefs}$ and processed in one execution of the body of the while-loop, and the while-loop terminates when $\text{InDefs}$ is the empty set.

In order to prove that the set of new predicate definitions is finite, let us consider a path $D_1, D_2, \ldots$ in the tree $\text{Defs}$ of definitions. The proof proceeds by contradiction: we assume that $D_1, D_2, \ldots$ is an infinite sequence and we derive a contradiction.

By the definition of the $\text{Gen}$ function we have that the clauses in $\text{Defs}$ satisfy the hypothesis of Lemma 8.3, and hence $\preceq_{\text{cl}}$ is a wbr on $\text{Defs}$ and $\preceq_{\text{int}}$ is a downward-finite wbr on $\text{Defs}$. Now we show that, from the infinite sequence $D_1, D_2, \ldots$, of clauses we can construct an infinite subsequence $E_1, E_2, \ldots$, such that, for all $i, j$, if $i < j$, then $E_i \preceq_{\text{cl}} E_j$, and by doing so we derive a contradiction.

Let $E_1$ be $D_1$. Suppose that we have constructed the sequence $E_1, E_2, \ldots, E_k$ such that, for $1 \leq i, j \leq k$, $E_i \not\preceq_{\text{cl}} E_j$. Let $E_k$ be $D_m$ and let $D_n$, with $m < n$, be the first clause in the infinite sequence $D_1, D_2, \ldots$ such that, for every $\tilde{D} \in \{D_1, D_2, \ldots, D_m\}$, $D_n \not\preceq_{\text{int}} \tilde{D}$ does not hold. Such $D_n$ exists because $\preceq_{\text{int}}$ is a downward-finite wbr. We take $E_{k+1}$ to be $D_n$, and hence, for all $i \in \{1, \ldots, n-1\}$, $E_{k+1} \preceq_{\text{int}} D_i$ does not hold.

Now we show that for all $i \in \{1, \ldots, k\}$, we have that $E_i \not\preceq_{\text{cl}} E_{k+1}$. We proceed by contradiction. Suppose that, for some $i \in \{1, \ldots, k\}$, $E_i \preceq_{\text{cl}} E_{k+1}$. Clause $E_{k+1}$, that is, clause $D_n$ in the sequence $D_1, D_2, \ldots$, has been computed by applying the $\text{Gen}$ function as follows, for some clause $E_X$ of the form $\text{new}(X) :: -i_X, r_X, v_X, p(X)$ (see the candidate definition clause in the definition of the function $\text{Gen}$ in Figure 9):

\[\begin{align*}
\text{If} & \quad \text{there exists a clause } \overline{D} \in D_1, \ldots, D_{n-1} \text{ of the form } \text{new}(X) :: -i_0, r_0, v_0, p(X) \text{ such that } \overline{D} \not\preceq E_X \\
\text{Then} & \quad D_n \text{ is the clause } \text{new}(X) :: -(i_0 \circ op_i_1), r_0, v_0, p(X), \text{ for some integer constraint } i_1 \\
\text{Else} & \quad D_n \text{ is } E_X
\end{align*}\]
Now clause \( D_n \) cannot be computed by the \( \text{Else} \) branch, because if \( D_n = E_X \), then there exists a clause \( \overline{D} \) in \( D_1, \ldots, D_{n-1} \), such that \( \overline{D} \not\sqsubset E_X \) (indeed, take \( \overline{D} = E_i \) and recall that \( E_X = D_n = E_{k+1} \) and \( E_i \not\leq_{cl} E_{k+1} \) and \( \leq_{cl} \) implies \( \not\sqsubset \)), and the condition of the \( \text{If-Then-Else} \) holds. Thus, \( D_n \) must have been computed by the \( \text{Then} \) branch and, by the Property (W) we have assumed on the operator \( op \), we have that \( D_n \not\leq_{\text{int}} \overline{D} \), where \( \overline{D} \in \{D_1, \ldots, D_{n-1}\} \), thereby reaching a contradiction. Thus, we have shown that, for all \( i \in \{1, \ldots, k\} \), \( E_i \not\leq_{cl} E_{k+1} \).

By iterating the previous construction we can construct an infinite sequence \( E_1, E_2, \ldots \) such that, for all \( i, j \), if \( i < j \), then \( E_i \not\leq_{cl} E_j \). This infinite sequence contradicts the hypothesis that \( \leq_{cl} \) is a wbr. Thus, every path of the tree \( \text{Defs} \) is finite, and since \( \text{Defs} \) is finitely branching, it is a finite tree. We conclude that the \( \text{VCTransf} \) strategy terminates.

(ii) Correctness. First we recap and adapt to our context known results on the correctness of unfold/fold transformation rules that can be found in [16, 17], where the rules refer to a generic theory of constraints. Moreover, here we consider linear recursive CLP programs only.

A transformation sequence is a sequence of CLP programs \( P_0, P_1, \ldots, P_n \), where, for \( i = 0, \ldots, n-1 \), \( P_{i+1} \) is derived from \( P_i \) by an application of one of the following rules. Let \( \text{p} \) be a predicate in \( P_0 \).

(R1) Definition Introduction. We derive \( P_{i+1} \) by adding to \( P_i \) a clause of the form \( \text{newp}(X) :: c, \text{A} \), where \( \text{newp} \) is a new predicate symbol, \( X \) is the tuple of variables occurring in the atom \( \text{A} \), and \( c \) is a constraint.

(R2) Definition Elimination. We derive \( P_{i+1} \) by removing from \( P_i \) all clauses whose head predicate is \( h \) and \( p \) does not depend on \( h \).

(R3) Unfolding. We derive \( P_{i+1} \) by replacing a clause \( C \) in \( P_i \) by the set \( \text{Unf}(C, P_i) \) as in Definition 2.1.

(R4) Constraint Replacement. Let us consider a clause \( C \) in \( P_i \) of the form: \( H :: c_0, \text{B} \), and some constraints \( c_1, \ldots, c_n \) such that \( A \models (c_0 \leftrightarrow (c_1 \lor \ldots \lor c_n)) \). Then, we derive \( P_{i+1} \) by replacing \( C \) by \( \{H :: c_1, \text{B}, \ldots, H :: c_n, \text{B}\} \).

(R5) Folding. Given a clause \( E: H :: e, \text{B} \) in \( P_i \) and a clause \( D: K :: c, \text{A} \) introduced by the definition rule in a previous transformation step. Suppose that, for some substitution \( \vartheta \), (i) \( B = A \vartheta \), and (ii) \( e \subseteq c \vartheta \). Then we derive \( P_{i+1} \) by replacing \( E \) by \( H :: e, K \vartheta \).

(R6) Clause Removal. We derive \( P_{i+1} \) from \( P_i \) by removing a clause \( C: H :: c, \text{B} \) such that one of the following holds:

1. Subsumed Clause) there exists a different clause \( H :: d \) in \( P_i \) with \( c \subseteq d \);
2. Useless Clause) the head predicate of \( H \) is \( h \) and there is no constrained fact \( q(\ldots) :: c \), where \( q \) is either \( h \) or a predicate on which \( h \) depends.

We have the following property [16, 17].

Theorem: Correctness of a Transformation Sequence. Let \( P_0, P_1, \ldots, P_n \) be any transformation sequence such that every clause introduced by the definition rule is unfolded in this sequence. Then, for every ground atom \( A \) with predicate \( p \), \( A \in M(P_0) \) iff \( A \in M(P_n) \).

The execution of the \( \text{VCTransf} \) strategy can easily be viewed as the construction of a transformation sequence using rules R1–R6, where, for \( i = 0, \ldots, N \), program \( P_i \) in the sequence is the program derived after the \( i \)-th execution of the body of the outer while-loop, and \( N \) is the number of iterations of the body of that while-loop during the execution of \( \text{VCTransf} \) strategy.
We have that program $P_i = \text{InDefs}_i \cup \overline{\text{VC}} \cup \text{VC}'_i$, where: (i) $\text{InDefs}_i$ is the value of the set $\text{InDefs}$ after the $i$-th iteration, (ii) $\overline{\text{VC}}$ is the set of clauses of $\text{VC}$ whose head predicate is not $\text{incorrect}$ (this set is not modified during the execution of the while-loop), and (iii) $\text{VC}'_i$ is the value of the set $\text{VC}'$ after the $i$-th iteration. In particular, we have that $\text{InDefs}_0$ is the set of clauses of $\text{VC}$ whose head predicate is the atom $\text{incorrect}$, $\text{InDefs}_N = \emptyset$, and $\text{VC}'_0 = \emptyset$.

Note that, at the end of the execution of the outer while-loop of the $\text{VCTransf}$ strategy, all clauses in $\overline{\text{VC}}$ are removed by a final application of rule R2, as $\text{incorrect}$ does not depend on the head predicates of those clauses. Note also that in order to show that $\text{VCTransf}$ constructs a transformation sequence, we also use Proposition 4.1, which guarantees that the CONSTRAINT REPLACEMENT phase is indeed an application of rule R4.

The transformation sequence constructed by $\text{VCTransf}$ satisfies the hypothesis of the above theorem stating the correctness of a transformation sequence, because every new predicate definition is added to the current value of $\text{InDefs}$ and it is unfolded during one of the subsequent UNFOLDING phases. Thus, by the correctness of the transformation sequence, we have that:

$\text{incorrect} \in M(\text{VC})$ iff $\text{incorrect} \in M(\text{VC}')$. \[\square\]