

# An Overview of the HFL Model Checking Project

Naoki Kobayashi

The University of Tokyo  
Tokyo, Japan

koba@is.s.u-tokyo.ac.jp

In this article, we give an overview of our project on higher-order program verification based on HFL (higher-order fixpoint logic) model checking. After a brief introduction to HFL, we explain how it can be applied to program verification, and summarize the current status of the project.

## 1 Introduction

In this article, we give a brief overview of our project on automated verification of higher-order programs based on (a variation of) Viswanathan and Viswanathan's higher-order fixpoint logic (HFL) [43]. HFL is a higher-order extension of the modal  $\mu$ -calculus and is strictly more expressive than the modal  $\mu$ -calculus, but the HFL model checking problem for finite state systems remains decidable.

In Section 2, we first review HFL, and HFL(Z), an extension of HFL with integer arithmetic, and show that HFL(Z) may also be viewed as an extension of Constrained Horn Clauses (CHC) [3, 12, 19, 36] with higher-order predicates and fixpoint alternations.

In Section 3, we show how various program verification problems can naturally be reduced to HFL(Z) model/validity checking problems. Our program verification framework based on HFL(Z) can be considered a generalization of CHC-based program verification framework [3, 12, 19, 36]. In Section 4, we summarize our methods for automatically solving the HFL(Z) model/validity checking problems, using higher-order model checkers and CHC solvers as backends.

This article is intended to be a non-exhaustive survey of HFL-based approaches to program verification. The main objective is to provide references to technical papers and clarify how they are connected with each other; the explanation of each topic is admittedly short and cryptic.

## 2 Higher-Order Fixpoint Logic and its Relationship with CHC

### 2.1 Higher-Order Fixpoint Logic

The syntax of HFL(Z) formulas and types is given as follows.

$$\begin{array}{lcl} \varphi \text{ (formulas)} & ::= x^\tau \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 & \\ & \mid \langle a \rangle \varphi \mid [a] \varphi & \text{(modal operators)} \\ & \mid \mu x^\kappa. \varphi \mid \nu x^\kappa. \varphi & \text{(fixpoint operators)} \\ & \mid \varphi_1 \varphi_2 \mid \lambda x^\tau. \varphi & \text{(\lambda-abstractions and applications)} \\ & \mid \varphi e \mid e_1 \leq e_2 & \text{(extension with integers)} \\ e \text{ (integer expressions)} & ::= n \mid x^{\text{int}} \mid e_1 + e_2 & \\ \tau \text{ (types)} & ::= \text{int} \mid \kappa & \\ \kappa \text{ (predicate types)} & ::= \text{o} \mid \tau \rightarrow \kappa & \end{array} \quad \left. \vphantom{\begin{array}{l} \varphi \\ e \\ \tau \\ \kappa \end{array}} \right\} \text{pure HFL}$$

Here, each variable (denoted by the metavariable  $x, y, \dots$ ) has its own type (specified as a superscript), and we consider only well-typed formulas and expressions; for example, in  $\varphi_1 \vee \varphi_2$ , both  $\varphi_1$  and  $\varphi_2$  must have the type  $\circ$  of propositions. We often omit the type annotation of a variable. Each formula must have a predicate type, and integer expression must have type  $\text{int}$ . See [27] for typing rules.

The first three lines of the definition of formulas correspond to the syntax of the modal  $\mu$ -calculus [15, 30] in negation normal form (if the types  $\kappa$  and  $\tau$  are restricted to the type  $\circ$  of propositions), and the first four lines correspond to the syntax of pure HFL [43]. Each formula of type  $\circ$  describes a property of labeled transition systems. The formula  $\langle a \rangle \varphi$  means that there exists a transition labeled  $a$  after which the proposition  $\varphi$  holds, while the formula  $[a] \varphi$  means that, after any transition labeled  $a$ , the proposition  $\varphi$  holds. The formulas  $\mu x^\kappa. \varphi$  and  $\nu x^\kappa. \varphi$  respectively denote the least and greatest predicates  $x$  such that  $x = \varphi$ . For example,  $\mu x^\circ. x^\circ$  and  $\nu x^\circ. x^\circ$  respectively denote the least and greatest propositions such that  $x = x$ , i.e., `false` and `true` respectively; henceforth, we treat `false` and `true` as propositional constants. The fifth line is for the extension with integers. We have only constants, additions, and inequality constraints on integers, but other predicates and operations, as well as quantifiers, are definable, as shown below.

**Example 1.** Let  $\varphi$  be a formula of type  $\text{int} \rightarrow \circ$ , and  $\psi$  be  $\nu x. \lambda n. \varphi(n) \vee x(n+1)$ . Then we have

$$\begin{aligned} \psi(0) &\equiv (\lambda n. \varphi(n) \vee \psi(n+1))0 && \text{(by unfolding } \psi) \\ &\equiv \varphi(0) \vee \psi(1) && \text{(by } \beta\text{-reduction)} \\ &\equiv \varphi(0) \vee (\lambda n. \varphi(n) \vee \psi(n+1))(1) && \text{(by unfolding } \psi) \\ &\equiv \varphi(0) \vee \varphi(1) \vee (\lambda n. \varphi(n) \vee \psi(n+1))(2) && \text{(by } \beta\text{-reduction)} \\ &\equiv \varphi(0) \vee \varphi(1) \vee \varphi(2) \vee \dots \end{aligned}$$

Thus,  $\psi(0)$  denotes  $\exists x \geq 0. \varphi(x)$ . Similarly,  $\forall x \geq 0. \varphi(x)$  can be expressed by  $(\nu x. \lambda n. \varphi(n) \wedge x(n+1))0$ , and  $\forall x \in \mathbf{Z}. \varphi(x)$  (where  $\mathbf{Z}$  is the set of integers) can be expressed by  $(\nu x. \lambda n. \varphi(n) \wedge x(n-1) \wedge x(n+1))0$ . The multiplication can be expressed as a ternary predicate  $\text{mult}(x, y, z)$  (which means  $x \times y = z$ ), e.g., by:

$$\text{mult} := \mu u. \lambda(x, y, z). y = z = 0 \vee (1 \leq y \wedge u(x, y-1, z-x)) \vee (y+1 \leq 0 \wedge u(x, y+1, z+x)).$$

Here we have used tuple notations and subtractions ( $-$ ) for readability; as usual, subtractions can be defined by using additions and existential quantifiers.  $\square$

As shown in the example below, pure HFL is already strictly more expressive than the modal  $\mu$ -calculus.

**Example 2.** Consider  $\varphi$  be the formula  $\nu x. \lambda y. y \vee \langle a \rangle x(\langle b \rangle y)$ . Then, we have:

$$\begin{aligned} \varphi(\langle c \rangle \text{true}) &\equiv (\lambda y. y \vee \langle a \rangle \varphi(\langle b \rangle y))(\langle c \rangle \text{true}) && \text{(unfolding of } \varphi) \\ &\equiv \langle c \rangle \text{true} \vee \langle a \rangle \varphi(\langle b \rangle \langle c \rangle \text{true}) && \text{(}\beta\text{-reduction)} \\ &\equiv \langle c \rangle \text{true} \vee \langle a \rangle (\langle b \rangle \langle c \rangle \text{true} \vee \langle a \rangle \langle a \rangle \varphi(\langle b \rangle \langle b \rangle \langle c \rangle \text{true})) && \text{(unfolding, followed by } \beta) \\ &\equiv \langle c \rangle \text{true} \vee \langle a \rangle \langle b \rangle \langle c \rangle \text{true} \vee \langle a \rangle^2 \langle b \rangle^2 \langle c \rangle \text{true} \vee \dots \end{aligned}$$

Thus,  $\varphi(\langle c \rangle \text{true})$  means that there exists a transition sequence of the form  $a^n b^n$  after which a  $c$ -transition is enabled.  $\square$

We write  $\mathcal{M} \models \varphi$  when a labeled transition system  $\mathcal{M}$  satisfies  $\varphi$ . We omit the formal semantics of HFL( $\mathbf{Z}$ ) [27]. The *model checking problem* for HFL( $\mathbf{Z}$ ) is the problem of checking whether  $\mathcal{M} \models \varphi$  holds, given a finite labeled transition system  $\mathcal{M}$  and a HFL( $\mathbf{Z}$ ) formula  $\varphi$  of type  $\circ$ . The *validity checking problem* is a special case: it is the problem of checking whether  $\mathcal{M}_0 \models \varphi$  holds, where  $\varphi$  is a HFL( $\mathbf{Z}$ ) formula of type  $\circ$  without modal operators ( $\langle a \rangle$ ,  $[a]$ ), and  $\mathcal{M}_0$  is a trivial model consisting

of a single state without transitions. We often just write  $\models \varphi$  for  $\mathcal{M}_0 \models \varphi$  and say “ $\varphi$  is valid” when  $\models \varphi$  holds. For pure HFL, the model checking problem (hence also the validity checking problem) is decidable [43] and  $k$ -EXPTIME complete for the order- $k$  fragment [1]. Here, the order of the model checking problem is defined as the the largest order of types that occur in the HFL formula, and the order of a type  $\tau$ , written  $\text{ord}(\tau)$ , is defined by:

$$\text{ord}(o) = \text{ord}(\text{int}) = 0 \quad \text{ord}(\tau \rightarrow \kappa) = \max(\text{ord}(\tau) + 1, \text{ord}(\kappa)).$$

For example, the order of the formula in Example 2 is 1. For HFL(Z), both the model and validity checking problems are undecidable due to Gödel’s incompleteness theorem (recall that quantifiers and multiplications can be expressed, as discussed in Example 1).

## 2.2 Relationship with CHC

We now explain the connection between the HFL(Z) validity checking problem and the CHC satisfiability problem, through examples. A little formal discussion on the correspondence between HFL(Z) and CHC is found in [25]. We assume that the reader is familiar with Constrained Horn Clauses (CHCs); those not familiar with CHCs may wish to consult [3], which is a good survey CHCs and their applications to program verification.

Let us consider the following system  $S$  of CHCs.

$$\begin{aligned} \forall x, y, r. y = 0 \wedge r = 0 &\implies \text{mult}(x, y, r) \\ \forall x, y, r, s. y \neq 0 \wedge \text{mult}(x, y - 1, s) \wedge r = s + x &\implies \text{mult}(x, y, r) \\ \forall x, y, r. \text{mult}(x, y, r) \wedge x > 0 &\implies r \geq y. \end{aligned}$$

The satisfiability of CHCs above (i.e., the existence of an assignment of a predicate to the predicate variable `mult`) is equivalent to the safety property of the following OCaml program (that assertion failures never occur):

```
let rec mult(x,y) =
  if y=0 then 0
  else let s = mult(x, y-1) in s+x
let main x y = if x>0 then assert(mult(x,y)>=y)
```

Here, the ternary predicate `mult(x,y,r)` in the CHCs intuitively means that the return value of `mult(x,y)` in the program is  $r$ .

Let us now convert the satisfiability problem for the CHCs above to the validity checking problem for a HFL(Z) formula. First, note that the first two clauses are equivalent to:

$$\forall x, y, r. (y = 0 \wedge r = 0) \vee \exists s. (y \neq 0 \wedge \text{mult}(x, y - 1, s) \wedge r = s + x) \implies \text{mult}(x, y, r).$$

The least predicate  $\varphi$  that satisfies the condition above is expressed by:

$$\mu u. \lambda(x, y, r). (y = 0 \wedge r = 0) \vee \exists s. (y \neq 0 \wedge u(x, y - 1, s) \wedge r = s + x).$$

Thus, the satisfiability of  $S$  is equivalent to:

$$\forall x, y, r. \varphi(x, y, r) \wedge x > 0 \implies r \geq y,$$

which is also equivalent to:

$$\forall x, y, r. \overline{\varphi}(x, y, r) \vee x \leq 0 \vee r \geq y,$$

where  $\bar{\varphi}$  is the de Morgan dual of  $\varphi$ , given as:

$$\forall u. \lambda(x, y, r). (y \neq 0 \vee r \neq 0) \wedge \forall s. (y = 0 \vee u(x, y - 1, s) \vee r \neq s + x).$$

In this manner, the satisfiability problem for any CHCs on integer arithmetic can be converted to the validity checking problem for a formula of the first-order,  $v$ -only fragment (i.e. the fragment without  $\mu$ ) of HFL(Z); recall that universal quantifiers can be expressed by using  $v$ . Conversely, the validity checking problem for any formula of the first-order,  $v$ -only fragment where the types of fixpoint variables are restricted to those of the form  $\text{int} \rightarrow \dots \rightarrow \text{int} \rightarrow o$  can be reduced to the satisfiability problem for CHCs on integer arithmetic [25]. In this sense, the HFL(Z) validity checking problem can be considered a generalization of the CHC satisfiability problem, where higher-order predicates and fixpoint alternations between  $\mu$  and  $v$  are allowed.

Burn et al. [5, 35] recently studied a higher-order extension of CHCs called HoCHC. The HFL(Z) validity checking problem can also be considered an extension of the satisfiability problem for HoCHC with fixpoint alternations.

### 3 From Program Verification to HFL(Z) Model Checking

This section explains how HFL(Z) model/validity checking can be applied to program verification. As seen at the end of the last section, HFL(Z) validity checking subsumes CHC solving, which already have a plenty of applications to program verification [3], but how can we exploit the additional power of HFL(Z) model/validity checking for program verification?

A standard approach to applying model checking to program verification is to model a program as a transition system, and a property of the program to be checked as a specification; that is indeed the case for applications of finite-state model checking [7], pushdown model checking [2], and HORS model checking (which is another kind of higher-order extension of model checking) [21, 34]. In applying HFL(Z) model checking to higher-order program verification, we actually switch the roles of systems and specifications: a program is mapped to a HFL(Z) formula, and a property is mapped to a finite state system, where the HFL(Z) formula is a kind of “characteristic formula” of the program. This has been partially inspired by the correspondence between HFL model checking and HORS model checking, where we also need to switch the roles of systems and specifications [24].

Let us consider the following file-accessing program, taken from [27].

```
let x = open "foo" in (read(x); read(x); close(x))
```

This program opens the file “foo”, and then reads and closes the file. Suppose we wish to check that the file “foo” is indeed accessed as a read-only file. To this end, we express the valid access protocol for a read-only file pointer as a labeled transition system, as shown in Figure 1. The LTS corresponds to a deterministic automaton that accepts the valid traces  $\text{read}^* \cdot \text{close} \cdot \text{end}$ . Here,  $\text{end}$  denotes the termination of a program. In the state  $q_0$  (which is the initial state immediately after a file is opened), both  $\text{read}$  and  $\text{close}$  operations are allowed, but after the  $\text{close}$  operation, only the  $\text{end}$  operation is allowed. The program can be converted to the HFL(Z) formula:

$$\langle \text{read} \rangle \langle \text{read} \rangle \langle \text{close} \rangle \langle \text{end} \rangle \text{true},$$

which intuitively means that the program follows the access protocol represented by the LTS. It is obtained by just replacing each of the  $\text{read}$ ,  $\text{close}$ , and  $\text{end}$  operations with the corresponding modal operators that say “those actions are allowed in the current state.”<sup>1</sup> It is easy to see that the program accesses

<sup>1</sup>Please ignore the open operation here; it matters when more than one file is used in a program, as in [21].

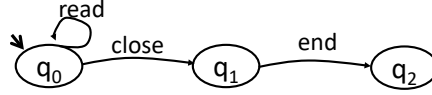


Figure 1: An LTS  $\mathcal{M}_{file}$  expressing the valid file access protocol

the file “foo” just if

$$\mathcal{M}_{file} \models \langle \text{read} \rangle \langle \text{read} \rangle \langle \text{close} \rangle \langle \text{end} \rangle \text{true}.$$

The same idea applies to more complex programs that contain recursion and conditionals. Let us consider the following program:

```

let x = open "foo" in
let rec f n = if n <= 0 then close x else (read x; f (n-1) x) in
f 10

```

To make the reduction clearer, let us write it in the continuation passing style.

```

let x = open "foo" in
let rec f n k = if n <= 0 then close x k else read x (f (n-1) x k) in
f 10 ()

```

Here, `read` and `close` now take an additional continuation parameter, which is invoked after the read/close operations. Then, the property that the program accesses the file “foo” as a read-only file just if:

$$\mathcal{M}_{file} \models (\mu f. \lambda n. \lambda k. (n \leq 0 \Rightarrow \langle \text{close} \rangle k) \wedge (n > 0 \Rightarrow \langle \text{read} \rangle (f (n-1) k))) 10 (\langle \text{end} \rangle \text{true}).$$

Here, the formula contains integers and order-1 fixpoint operators. As before, the formula has been obtained by just replacing each of the read/close operations, and program termination (represented by `()`) with the corresponding modal operator. The conditional “if `n <= 0` then ... else ...” has been replaced by the corresponding logical formula  $(n \leq 0 \Rightarrow \dots) \wedge (n > 0 \Rightarrow \dots)$ , and the recursion has been replaced by the fixpoint operator  $\mu$  (here, by using  $\mu$ , we require that the program terminates).

We have given above just order-1 examples, but it should be clear that the idea of the translation should work for higher-order programs. A general translation for linear-time properties is found in [27], a translation for arbitrary  $\omega$ -regular properties (including both linear-time and branching time properties) is found in [44]. For linear-time properties of first-order recursive programs, a more optimized translation is given in [25]. In those general translations, program verification problems are actually reduced to the *validity* checking problem for HFL(Z) formulas, by using a kind of product construction.

## 4 Solving HFL(Z) Model Checking Problems

In this section, we discuss how to solve instances of the HFL(Z) model checking problem obtained from program verification problems. For the sake of simplicity, we actually focus on the validity checking problem (which is a special case of the model checking problem where the formula contains no modal operators; recall Section 2.1), but most of the techniques apply to the model checking problem as well. Some of our tools and benchmark sets mentioned below are available from <https://github.com/hopv>. For the other tools, please consult each paper cited below.

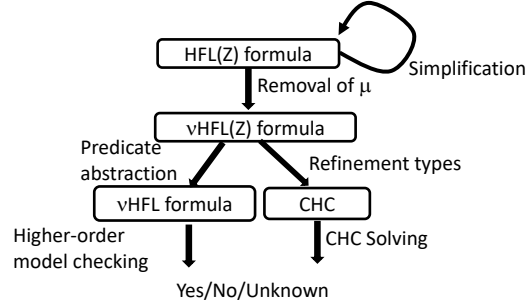


Figure 2: An overview of our method for HFL(Z) validity checking

Our overall method for HFL(Z) validity checking is summarized in Figure 2. In the figure, a “vHFL(Z) formula” refers to a HFL(Z) formula without the least fixpoint operator  $\mu$ . The overall strategy for solving the validity checking problem is analogous to, and has been inspired by automated program verification methods. The first phase of removing the least fixpoint operator  $\mu$  corresponds to reductions from liveness property verification (such as termination verification) to safety property verification [8, 32, 37]. The two methods for checking the validity of vHFL(Z) formula correspond to two major approaches to automated verification of higher-order programs: higher-order model checking [26] and refinement types [38, 41, 42, 45]. We discuss each step of Figure 2 below.

Due to underapproximation in various steps (a formula  $\phi$  is replaced by another formula  $\phi'$  such that  $\phi' \Rightarrow \phi$ , so that the validity of  $\phi'$  implies that of  $\phi$ , but not vice versa), the procedure shown in Figure 2 cannot conclude that the original formula  $\phi$  is invalid even if an approximation of the formula is invalid. Thus, given a HFL(Z) formula  $\phi$ , we also prepare its de Morgan dual  $\bar{\phi}$ , and apply the whole procedure in parallel to  $\phi$  and  $\bar{\phi}$ . If  $\bar{\phi}$  is valid, then we can conclude that  $\phi$  is invalid.

#### 4.1 Removing $\mu$

In the reductions from program verification problems to HFL(Z) validity checking [25, 27, 44], liveness and safety properties are respectively turned into  $\mu$ - and  $\nu$ -formulas. Thus, following the techniques for liveness property verification [8, 14, 32, 33, 37], it is natural to first remove  $\mu$ -formulas by using analogous techniques.

In [25], we have adopted the technique of Fedyukovich et al. [14] for the first-order fragment of HFL(Z) formulas. Suppose that we wish to prove the validity of a  $\mu$ -formula of the form  $\mu x. \phi(x)$ . By the standard fixpoint theorem, we have

$$\phi^n(\text{false}) \Rightarrow \mu x. \phi(x)$$

for any natural number  $n$ . The formula  $\phi^n(\text{false})$  is equivalent to  $(\nu x'. \lambda z. (z > 0 \wedge \phi(x'(z-1))))n$ , which is also equivalent to the following formula  $\psi$ :

$$\psi := \forall u \geq n. (\nu x'. \lambda i. (i > 0 \wedge \phi(x'(i-1))))u.$$

Thus, it suffices to show that  $\psi$  is valid. Here,  $n$  can be considered a bound for the number of unfoldings of the original  $\mu$ -formula; by gradually increasing  $n$ , we can obtain a better approximation of the original formula.

In the case of the first-order HFL(Z) formulas, the above translation yields order-1 vHFL(Z) formulas (where all the types are of the form  $\text{int}^k \rightarrow \circ$ ), whose validity checking problems can be further reduced to the CHC satisfiability problem, as discussed in Section 2.

**Example 3.** Let us consider proving the validity of the formula:

$$\forall i. (\mu x. \lambda y. y \leq 0 \vee x(y-1))i.$$

Based on the above translation, it suffices to show:

$$\forall i. \forall u \geq \max(i+1, 1). (\nu x'. \lambda(z, y). z > 0 \wedge (y \leq 0 \vee x'(z-1, y-1)))(u, i).$$

Here,  $\max(i+1, 1)$  corresponds to the bound  $n$  above; in general, the bound may depend on free variables as in this example. Note that the resulting formula contains only  $\nu$  and  $\forall$ , where the latter can also be expressed by  $\nu$ , as seen in Example 1.

To translate the formula above to CHCs, observe that the formula is equivalent to:

$$\forall i. \forall u \geq \max(i+1, 1). (\mu \bar{x}'. \lambda(z, y). z \leq 0 \vee (y > 0 \wedge \bar{x}'(z-1, y-1)))(u, i) \Rightarrow \text{false}.$$

The  $\mu$ -formula  $\mu \bar{x}'. \lambda(z, y). z \leq 0 \vee (y > 0 \wedge \bar{x}'(z-1, y-1))$  is the least predicate  $X$  that satisfies the following clauses:

$$\begin{aligned} z \leq 0 &\implies X(z, y) \\ y > 0 \wedge X(z-1, y-1) &\implies X(z, y). \end{aligned}$$

Thus, the validity of the formula above is equivalent to the satisfiability of the two clauses above with the goal clause:

$$u \geq i+1 \wedge u \geq 1 \wedge X(u, i) \implies \text{false}.$$

The above system of CHCs is indeed satisfiable, and has the model:  $X(z, y) := z \leq 0 \wedge z \leq y$ . We can thus conclude that the original HFL(Z) formula is valid.  $\square$

We have implemented the above method for the first-order fragment of HFL(Z) and applied it to automated verification of temporal properties [25]. Despite the generality of the approach (which works for arbitrary  $\omega$ -regular properties of while-programs), our implementation generally outperformed Cook and Koskinen's method specialized for CTL verification [9], probably thanks to the recent advance of CHC solvers [6, 16, 28] and the streamlined approach. Work is under way to extend the translation above for HFL(Z) formulas of arbitrary orders.

## 4.2 Predicate Abstraction for vHFL(Z) Validity Checking

One approach [18] to proving the validity of a vHFL(Z) formula  $\phi$  is to apply predicate abstraction to obtain a pure vHFL formula  $\phi'$  (i.e., a vHFL(Z) formula without integers) as an underapproximation of  $\phi$ , and then apply an algorithm for pure HFL model checking [17]<sup>2</sup> (recall that pure HFL model checking is decidable; despite its high worst-case complexity, practical algorithms exist, which do not always suffer from the high complexity). This approach may be viewed as a generalization of the HORS model checking approach to (un)reachability verification [26] and non-termination verification [31].

<sup>2</sup>In the actual implementation, we actually use a HORS model checker [4, 22] based on the correspondence between HFL and HORS model checking [24].

Given a set of predicates on integers, a given  $\nu\text{HFL}(\mathbb{Z})$  formula can be underapproximated by a pure HFL formula. For example, suppose that we have decided to abstract every integer with the predicate  $\lambda y. y > 0$ . Then, the formula  $\phi := (\nu x. \lambda y. y \geq 0 \wedge x(y+1))1$  can be underapproximated by  $\phi'$ :

$$(\nu x. \lambda b. b \wedge x(b))\text{true},$$

where  $b$  is a Boolean variable corresponding to the condition  $y > 0$ . Since  $\phi'$  is valid (as can be confirmed by a pure HFL model checker), we can conclude that the original formula  $\phi$  is also valid. As in standard approaches to combining predicate abstraction and model checking, predicates to be used for abstraction can be found in a counterexample-guided manner. More details can be found in [18].

### 4.3 Refinement Types for $\nu\text{HFL}(\mathbb{Z})$ Validity Checking

We have also studied another approach to  $\nu\text{HFL}(\mathbb{Z})$  validity checking, based on a (sound but incomplete) reduction to a refinement type inference problem [20]. The approach has been inspired by the refinement type system of Burn et al. [5] for HoCHC, whose idea can further be traced back to refinement type systems for functional programs [38, 41, 42, 45].

The syntax of refinement types for  $\nu\text{HFL}(\mathbb{Z})$  is given by:

$$\sigma ::= o[\psi] \mid \sigma_1 \rightarrow \sigma_2 \mid x:\text{int} \rightarrow \sigma.$$

Here,  $\psi$  is a quantifier-free formula of integer arithmetic (which may contain integer variables bound by  $x:\text{int} \rightarrow \dots$ ). The type  $o[\psi]$  describes propositions that hold whenever  $\psi$  holds. For example, the  $\nu\text{HFL}$  formula  $x \geq 0$  has type  $o[x > 0]$ , since  $x \geq 0$  holds whenever  $x > 0$  holds. A predicate  $\lambda p. p(0)$  has type  $(x:\text{int} \rightarrow o[x \geq 0]) \rightarrow o[\text{true}]$ , because  $p(0)$  holds whenever  $p$  is a predicate on integers such that  $p(x)$  holds for every  $x \geq 0$ . Based on the intuition, one can construct a refinement type system for  $\nu\text{HFL}(\mathbb{Z})$ , such that a  $\nu\text{HFL}(\mathbb{Z})$  formula  $\phi$  is valid if  $\phi$  has type  $o[\psi]$ , and reduce the type inference problem to a constraint satisfaction problem on predicate variables in a standard manner [5, 6, 41]. Unlike the case of refinement type systems for (un)reachability verification of functional programs [6, 41], the resulting constraint satisfaction problem is no longer a CHC problem in general; constraints on predicates may be of the form:

$$P_1(\tilde{x}, \tilde{y}) \wedge \dots \wedge P_k(\tilde{x}, \tilde{y}) \wedge \psi(\tilde{x}, \tilde{y}) \implies Q_1(\tilde{x}) \vee \dots \vee Q_\ell(\tilde{x}),$$

where disjunction may occur in the head (here,  $P_i, Q_j$  are unknown predicate variables and  $\psi(\tilde{x}, \tilde{y})$  is a formula of integer arithmetic). Solving this generalized form of constrained clauses [39] is the current major bottleneck of this approach; work is under way to extend the ICE-based CHC solving approach [6, 13] to deal with the generalized constrained clauses.

Despite the bottleneck mentioned above, the refinement type-based approach to  $\nu\text{HFL}(\mathbb{Z})$  validity checking is generally faster than the predicate abstraction-based approach, while the latter tends to be more precise. Thus, the two approaches are complementary to each other.

### 4.4 Unfold/fold Transformations for Simplification

Inspired by the unfold/fold transformation techniques for CHC solving [10, 11], we have also studied unfold/fold transformations for the first-order fragment of HFL( $\mathbb{Z}$ ) [23] to enhance the power of an automated HFL( $\mathbb{Z}$ ) validity checker. The transformations are useful for reasoning about relations between fixpoint formulas.



For example, consider proving  $\forall n. \text{Even}(n) \Rightarrow \text{Odd}(n+1)$ , where *Even* and *Odd* are defined by:

$$\begin{aligned} \text{Even} &:= \mu x. \lambda y. (y = 0 \vee x(y-2)) \\ \text{Odd} &:= \mu x. \lambda y. (y = 1 \vee x(y-2)). \end{aligned}$$

It can be expressed as the HFL(Z) formula  $\forall n. \overline{\text{Even}}(n) \vee \text{Odd}(n+1)$ , where

$$\overline{\text{Even}} := \nu x. \lambda y. (y \neq 0 \wedge x(y-2)).$$

Let  $\overline{\text{Even}}(y) \vee \text{Odd}(y+1)$  be  $\varphi(y)$ . It can be transformed as follows:

$$\begin{aligned} \varphi(y) &\equiv \overline{\text{Even}}(y) \vee \text{Odd}(y+1) \\ &\equiv (y \neq 0 \wedge \overline{\text{Even}}(y-2)) \vee (y+1 = 1 \vee \text{Odd}(y-1)) && \text{(unfold } \overline{\text{Even}} \text{ and } \text{Odd}) \\ &\equiv y+1 = 1 \vee \overline{\text{Even}}(y-2) \vee \text{Odd}(y-1) && \text{(shuffle the formula)} \\ &\equiv y = 0 \vee \varphi(y-2) && \text{(by the definition of } \varphi). \end{aligned}$$

Based on the transformations above, we can replace  $\overline{\text{Even}}(n) \vee \text{Odd}(n+1)$  with  $(\nu x. \lambda y. y = 0 \vee x(y-2))n$ , which is obviously valid (since  $\nu x. \lambda y. y = 0 \vee x(y-2) \equiv \lambda y. \text{true}$ ). The above sequence of transformations are analogous to unfold/fold transformations for CHCs [10], but the soundness of the overall transformations is more subtle, due to the mixture of the least and greatest fixpoint operators: see [23] for the conditions of soundness of unfold/fold transformations for the first-order fragment of HFL(Z).

## 4.5 Semi-Automated Methods

We have so far discussed automated methods for HFL(Z) validity checking. As the HFL(Z) formula obtained from a program verification problem can be considered a kind of “verification condition,”<sup>3</sup> it is also natural to prove the validity of the formula semi-automatically, possibly using a proof assistant such as Coq, as exploited in our recent work [29, 44]. Integration with the automated methods is left for future work.

## 5 Conclusion

We have given an overview of our project on automated program verification based on HFL(Z) model and validity checking. Our framework can be considered a generalization of the CHC-based program verification framework and provides a uniform approach to higher-order program verification. One may wonder whether HFL(Z) is too expressive as the target of reductions from program verification problems. To answer the question, Tsukada [40] has recently shown that, in a certain sense, HFL(Z) is just as expressive as needed for encoding higher-order program verification problems. A lot of work is still left to be done, including a full implementation of the HFL(Z) validity checker and further improvement of backend solvers for CHCs and generalized constrained clauses.

## Acknowledgment

We would like to thank anonymous referees for useful comments. This work was supported by JSPS KAKENHI Grant Number JP20H00577 and JP20H05703.

<sup>3</sup>Thanks to fixpoint operators, no annotations of loop invariants and pre/post-conditions of recursive functions are required.

## References

- [1] Roland Axelsson, Martin Lange & Rafal Somla (2007): *The Complexity of Model Checking Higher-Order Fixpoint Logic*. *Logical Methods in Computer Science* 3(2), doi:10.2168/LMCS-3(2:7)2007.
- [2] Thomas Ball, Byron Cook, Vladimir Levin & Sriram K. Rajamani (2004): *SLAM and Static Driver Verifier: Technology Transfer of Formal Methods inside Microsoft*. In: *Integrated Formal Methods 2004*, LNCS 2999, Springer, pp. 1–20, doi:10.1007/978-3-540-24756-2\_1.
- [3] Nikolaj Bjørner, Arie Gurfinkel, Kenneth L. McMillan & Andrey Rybalchenko (2015): *Horn Clause Solvers for Program Verification*. In: *Fields of Logic and Computation II - Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday*, LNCS 9300, Springer, pp. 24–51, doi:10.1007/978-3-319-23534-9\_2.
- [4] Christopher H. Broadbent & Naoki Kobayashi (2013): *Saturation-Based Model Checking of Higher-Order Recursion Schemes*. In: *CSL 2013, LIPIcs* 23, pp. 129–148, doi:10.4230/LIPIcs.CSL.2013.129.
- [5] Toby Cathcart Burn, C.-H. Luke Ong & Steven J. Ramsay (2018): *Higher-order constrained horn clauses for verification*. *Proc. ACM Program. Lang.* 2(POPL), pp. 11:1–11:28, doi:10.1145/3158099.
- [6] Adrien Champion, Tomoya Chiba, Naoki Kobayashi & Ryosuke Sato (2020): *ICE-Based Refinement Type Discovery for Higher-Order Functional Programs*. *J. Autom. Reason.* 64(7), pp. 1393–1418, doi:10.1007/s10817-020-09571-y.
- [7] Edmund M. Clarke, Orna Grumberg & Doron A. Peled (1999): *Model Checking*. The MIT Press.
- [8] Byron Cook, Alexey Gotsman, Andreas Podelski, Andrey Rybalchenko & Moshe Y. Vardi (2007): *Proving That Programs Eventually Do Something Good*. In: *Proceedings of POPL*, ACM Press, pp. 265–276, doi:10.1145/1190216.1190257.
- [9] Byron Cook & Eric Koskinen (2013): *Reasoning About Nondeterminism in Programs*. In: *Proceedings of PLDI 2013*, ACM Press, pp. 219–230, doi:10.1145/2491956.2491969.
- [10] Emanuele De Angelis, Fabio Fioravanti, Alberto Pettorossi & Maurizio Proietti (2018): *Solving Horn Clauses on Inductive Data Types Without Induction*. *TPLP* 18(3-4), pp. 452–469, doi:10.1017/S1471068418000157.
- [11] Emanuele De Angelis, Fabio Fioravanti, Alberto Pettorossi & Maurizio Proietti (2020): *Removing Algebraic Data Types from Constrained Horn Clauses Using Difference Predicates*. In Nicolas Peltier & Viorica Sofronie-Stokkermans, editors: *Automated Reasoning - 10th International Joint Conference, IJCAR 2020, Paris, France, July 1-4, 2020, Proceedings, Part I, Lecture Notes in Computer Science* 12166, Springer, pp. 83–102, doi:10.1007/978-3-030-51074-9\_6.
- [12] Giorgio Delzanno & Andreas Podelski (2001): *Constraint-based deductive model checking*. *Int. J. Softw. Tools Technol. Transf.* 3(3), pp. 250–270, doi:10.1007/s100090100049.
- [13] P. Ezudheen, Daniel Neider, Deepak D’Souza, Pranav Garg & P. Madhusudan (2018): *Horn-ICE learning for synthesizing invariants and contracts*. *Proc. ACM Program. Lang.* 2(OOPSLA), pp. 131:1–131:25, doi:10.1145/3276501.
- [14] Grigory Fedyukovich, Yueling Zhang & Aarti Gupta (2018): *Syntax-Guided Termination Analysis*. In: *Computer Aided Verification - 30th International Conference, CAV 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings, Part I*, LNCS 10981, Springer, pp. 124–143, doi:10.1007/978-3-319-96145-3\_7.
- [15] Erich Grädel, Wolfgang Thomas & Thomas Wilke, editors (2002): *Automata, Logics, and Infinite Games: A Guide to Current Research*. LNCS 2500, Springer, doi:10.1007/3-540-36387-4.
- [16] H. Hojjat & P. Rümmer (2018): *The ELDARICA Horn Solver*. In: *2018 Formal Methods in Computer Aided Design (FMCAD)*, pp. 1–7, doi:10.23919/FMCAD.2018.8603013.
- [17] Youkichi Hosoi, Naoki Kobayashi & Takeshi Tsukada (2019): *A Type-Based HFL Model Checking Algorithm*. In Anthony Widjaja Lin, editor: *Programming Languages and Systems - 17th Asian Symposium, APLAS 2019, Nusa Dua, Bali, Indonesia, December 1-4, 2019, Proceedings, Lecture Notes in Computer Science* 11893, Springer, pp. 136–155, doi:10.1007/978-3-030-34175-6\_8.

- [18] Naoki Iwayama, Naoki Kobayashi, Ryota Suzuki & Takeshi Tsukada (2020): *Predicate Abstraction and CEGAR for vHFL<sub>Z</sub> Validity Checking*. In David Pichardie & Mihaela Sighireanu, editors: *Static Analysis - 27th International Symposium, SAS 2020, Virtual Event, November 18-20, 2020, Proceedings, Lecture Notes in Computer Science* 12389, Springer, pp. 134–155, doi:10.1007/978-3-030-65474-0\_7.
- [19] Joxan Jaffar, Andrew E. Santosa & Razvan Voicu (2006): *A CLP Method for Compositional and Intermittent Predicate Abstraction*. In: *Proceedings of VMCAI 2006, Lecture Notes in Computer Science* 3855, Springer, pp. 17–32, doi:10.1007/11609773\_2.
- [20] Hiroyuki Katsura, Naoki Iwayama, Naoki Kobayashi & Takeshi Tsukada (2020): *A New Refinement Type System for Automated vHFL<sub>Z</sub> Validity Checking*. In Bruno C. d. S. Oliveira, editor: *Programming Languages and Systems - 18th Asian Symposium, APLAS 2020, Fukuoka, Japan, November 30 - December 2, 2020, Proceedings, Lecture Notes in Computer Science* 12470, Springer, pp. 86–104, doi:10.1007/978-3-030-64437-6\_5.
- [21] Naoki Kobayashi (2013): *Model Checking Higher-Order Programs*. *J. ACM* 60(3), doi:10.1145/2487241.2487246.
- [22] Naoki Kobayashi (2016): *HorSat 2: A Saturation-Based Model Checker for Higher-Order Recursion Schemes*. Available at <https://github.com/hopv/horsat2>.
- [23] Naoki Kobayashi, Grigory Fedyukovich & Aarti Gupta (2020): *Fold/Unfold Transformations for Fixpoint Logic*. In Armin Biere & David Parker, editors: *Tools and Algorithms for the Construction and Analysis of Systems - 26th International Conference, TACAS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings, Part II, Lecture Notes in Computer Science* 12079, Springer, pp. 195–214, doi:10.1007/978-3-030-45237-7\_12.
- [24] Naoki Kobayashi, Étienne Lozes & Florian Bruse (2017): *On the relationship between higher-order recursion schemes and higher-order fixpoint logic*. In: *POPL 2017*, pp. 246–259, doi:10.1145/3009837.3009854.
- [25] Naoki Kobayashi, Takeshi Nishikawa, Atsushi Igarashi & Hiroshi Unno (2019): *Temporal Verification of Programs via First-Order Fixpoint Logic*. In Bor-Yuh Evan Chang, editor: *Static Analysis - 26th International Symposium, SAS 2019, Porto, Portugal, October 8-11, 2019, Proceedings, Lecture Notes in Computer Science* 11822, Springer, pp. 413–436, doi:10.1007/978-3-030-32304-2\_20.
- [26] Naoki Kobayashi, Ryosuke Sato & Hiroshi Unno (2011): *Predicate Abstraction and CEGAR for Higher-Order Model Checking*. In: *PLDI 2011*, ACM Press, pp. 222–233, doi:10.1145/1993498.1993525.
- [27] Naoki Kobayashi, Takeshi Tsukada & Keiichi Watanabe (2018): *Higher-Order Program Verification via HFL Model Checking*. In Amal Ahmed, editor: *Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Lecture Notes in Computer Science* 10801, Springer, pp. 711–738, doi:10.1007/978-3-319-89884-1\_25.
- [28] Anvesh Komuravelli, Arie Gurfinkel & Sagar Chaki (2016): *SMT-based model checking for recursive programs*. *Formal Methods Syst. Des.* 48(3), pp. 175–205, doi:10.1007/s10703-016-0249-4.
- [29] Mayuko Kori, Takeshi Tsukada & Naoki Kobayashi (2021): *A Cyclic Proof System for HFL<sub>N</sub>*. In Christel Baier & Jean Goubault-Larrecq, editors: *29th EACSL Annual Conference on Computer Science Logic, CSL 2021, January 25-28, 2021, Ljubljana, Slovenia (Virtual Conference), LIPIcs* 183, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 29:1–29:22, doi:10.4230/LIPIcs.CSL.2021.29.
- [30] Dexter Kozen (1983): *Results on the Propositional  $\mu$ -calculus*. *Theoretical Computer Science* 27, pp. 333–354, doi:10.1016/0304-3975(82)90125-6.
- [31] Takuya Kuwahara, Ryosuke Sato, Hiroshi Unno & Naoki Kobayashi (2015): *Predicate Abstraction and CEGAR for Disproving Termination of Higher-Order Functional Programs*. In: *Proceedings of CAV 2015, LNCS* 9207, Springer, pp. 287–303, doi:10.1007/978-3-319-21668-3\_17.
- [32] Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno & Naoki Kobayashi (2014): *Automatic Termination Verification for Higher-Order Functional Programs*. In: *Proceedings of ESOP 2014, LNCS* 8410, Springer, pp. 392–411, doi:10.1007/978-3-642-54833-8\_21.

- [33] Akihiro Murase, Tachio Terauchi, Naoki Kobayashi, Ryosuke Sato & Hiroshi Unno (2016): *Temporal verification of higher-order functional programs*. In Rastislav Bodík & Rupak Majumdar, editors: *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, St. Petersburg, FL, USA, January 20 - 22, 2016*, ACM, pp. 57–68, doi:10.1145/2837614.2837667.
- [34] C.-H. Luke Ong (2006): *On Model-Checking Trees Generated by Higher-Order Recursion Schemes*. In: *LICS 2006*, IEEE Computer Society Press, pp. 81–90, doi:10.1109/LICS.2006.38.
- [35] C.-H. Luke Ong & Dominik Wagner (2019): *HoCHC: A Refutationally Complete and Semantically Invariant System of Higher-order Logic Modulo Theories*. In: *34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, June 24-27, 2019*, IEEE, pp. 1–14, doi:10.1109/LICS.2019.8785784.
- [36] Julio C. Peralta, John P. Gallagher & Hüseyin Saglam (1998): *Analysis of Imperative Programs through Analysis of Constraint Logic Programs*. In: *Proceedings of SAS '98, Lecture Notes in Computer Science 1503*, Springer, pp. 246–261, doi:10.1007/3-540-49727-7\_15.
- [37] Andreas Podelski & Andrey Rybalchenko (2004): *Transition Invariants*. In: *19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings*, pp. 32–41, doi:10.1109/LICS.2004.1319598.
- [38] Patrick M. Rondon, Ming Kawaguchi & Ranjit Jhala (2008): *Liquid types*. In: *PLDI 2008*, pp. 159–169, doi:10.1145/1375581.1375602.
- [39] Yuki Satake, Hiroshi Unno & Hinata Yanagi (2020): *Probabilistic Inference for Predicate Constraint Satisfaction*. In: *The Thirty-Fourth AAAI Conference on Artificial Intelligence, AAAI 2020, The Thirty-Second Innovative Applications of Artificial Intelligence Conference, IAAI 2020, The Tenth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2020, New York, NY, USA, February 7-12, 2020*, AAAI Press, pp. 1644–1651, doi:10.1609/aaai.v34i02.5526.
- [40] Takeshi Tsukada (2020): *On Computability of Logical Approaches to Branching-Time Property Verification of Programs*. In Holger Hermanns, Lijun Zhang, Naoki Kobayashi & Dale Miller, editors: *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, ACM, pp. 886–899, doi:10.1145/3373718.3394766.
- [41] Hiroshi Unno & Naoki Kobayashi (2009): *Dependent type inference with interpolants*. In: *Proceedings of the 11th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, September 7-9, 2009, Coimbra, Portugal*, ACM, pp. 277–288, doi:10.1145/1599410.1599445.
- [42] Hiroshi Unno, Tachio Terauchi & Naoki Kobayashi (2013): *Automating relatively complete verification of higher-order functional programs*. In Roberto Giacobazzi & Radhia Cousot, editors: *The 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '13, Rome, Italy - January 23 - 25, 2013*, ACM, pp. 75–86, doi:10.1145/2429069.2429081.
- [43] M. Viswanathan & R. Viswanathan (2004): *A Higher Order Modal Fixed Point Logic*. In: *CONCUR, LNCS 3170*, Springer, pp. 512–528, doi:10.1007/978-3-540-28644-8\_33.
- [44] Keiichi Watanabe, Takeshi Tsukada, Hiroki Oshikawa & Naoki Kobayashi (2019): *Reduction from branching-time property verification of higher-order programs to HFL validity checking*. In Manuel V. Hermenegildo & Atsushi Igarashi, editors: *Proceedings of the 2019 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation, PEPM@POPL 2019, Cascais, Portugal, January 14-15, 2019*, ACM, pp. 22–34, doi:10.1145/3294032.3294077.
- [45] Hongwei Xi & Frank Pfenning (1999): *Dependent Types in Practical Programming*. In: *Proceedings of POPL*, pp. 214–227, doi:10.1145/292540.292560.