

1 Sound Notional Machines

2 ANONYMOUS AUTHOR(S)

3
4 A notional machine is a pedagogical device that abstracts away details of the semantics of a programming
5 language to focus on some aspects of interest. A notional machine should be *sound*: it should be consistent
6 with the corresponding programming language, and it should be a proper abstraction. This reduces the risk
7 of it introducing misconceptions in education. Despite being widely used in computer science education,
8 notional machines are usually not evaluated with respect to their soundness. To address this problem, we first
9 introduce a formal definition of soundness for notional machines. The definition is based on the construction
10 of a commutative diagram that relates the notional machine with the aspect of the programming language
11 under its focus. Derived from this formalism, we present a methodology for constructing sound notional
12 machines, which we demonstrate by applying it to a series of small case studies. We also show how the
13 same formalism can be used to analyze existing notional machines and find inconsistencies in them as well
14 as propose solutions to these inconsistencies. The work establishes a firmer ground for research in notional
machines by serving as a framework to reason about them.

15
16 CCS Concepts: • Social and professional topics → Computing education; • Software and its engineer-
17 ing → Formal language definitions; Context specific languages.

18 Additional Key Words and Phrases: notional machines, programming education, equational reasoning, bisimu-
19 lation

20 1 INTRODUCTION

21 Learning to program involves learning how to
22 express a program in a programming language,
23 but also learning what the semantics of such
24 a program is. For novices, the semantics of a
25 program is often not obviously apparent from
26 the program itself. Instructors then often use a
27 *notional machine* [Fincher et al. 2020] to help
28 teach some particular aspect of programs and
29 programming languages, and also to assess stu-
30 dents' understanding of said aspect. This aspect
31 is the notional machine's focus. For example,
32 showing expressions as trees (the ExPTREE no-
33 tional machine), as depicted in Figure 1, brings
34 out the internal structure of lambda-calculus ex-
35 pressions [Marceau et al. 2011] and can help to
36 explain the step-by-step evaluation of such ex-
37 pressions. Notional machines are used widely
38 in computer science education; Fincher et al.
39 [2020] interviewed computer science teachers
40 to build up a dataset of 37 notional machines¹.

42 1.1 Unsound Notional Machines

43 Given the extensive use of notional machines, and their intended use as devices to help students
44 when learning, it is important to look at their quality. To begin with, one should make sure that the
45 notional machine is *sound*: it is faithful to the aspect of programs it is meant to focus on. Anecdotal

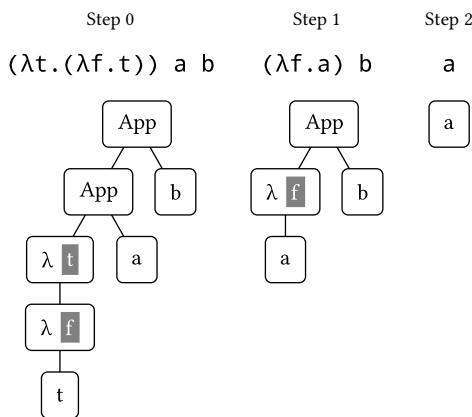


Fig. 1. Evaluation of the term $(\lambda t.(\lambda f.t)) a b$ shown with the notional machine ExPTREE.

46
47 ¹<https://notionalmachines.github.io/notional-machines.html> - The website lists 57 items but some of them are part of what
48 they call a notional machine sequence, which we consider a single notional machine.

50 evidence of using unsound representations in education goes back a long way. In 1960, education
 51 pioneer Jerome Bruner wrote that “the task of teaching a subject to a child at any particular age is
 52 one of representing the structure of that subject in terms of the child’s way of viewing things”, that
 53 this “task can be thought of as one of translation”, but that ideas have to be “represented *honestly*
 54 [...] in the thought forms of children” [Bruner 1960]. Bruner’s use of the term “honestly” can be
 55 seen as a call for soundness of such representations. Decades later, Richard Feynman eloquently
 56 stated [Feynman 1985], after reviewing “seventeen feet” of new mathematics schoolbooks for the
 57 California State Curriculum Commission:

58 [The books] would try to be rigorous, but they would use examples (like automobiles
 59 in the street for “sets”) which were almost OK, but in which there were always some
 60 subtleties. The definitions weren’t accurate. Everything was a little bit ambiguous.

62 Ambiguously specified notional machines and notional machines with imperfect analogies
 63 to programming concepts are a problem. Educators may mischaracterize language features and
 64 students may end up with misconceptions [Chiodini et al. 2021] instead of profoundly understanding
 65 the language.

66 For example, Fincher et al. [2020] describe
 67 the “Array as Row of Spaces in Parking Lot”
 68 notional machine. Figure 2 shows part of their
 69 card summarizing it. Notice the parallels be-
 70 tween the programming language (PL) and the
 71 notional machine (NM). Consider Java, a lan-
 72 guage commonly used in programming courses.
 73 In Java, when an array of objects is allocated,
 74 all its slots contain `null`, which means these
 75 slots don’t contain a reference to any object.
 76 This would be reasonably represented in the
 77 notional machine as an empty parking lot. But if
 78 instead of an array of objects, we have an array
 79 of `ints`, for example, then when we instantiate
 80 an array, all its slots contain `0`, which is not
 81 the absence of a number but a number like any
 82 other. A student could also reasonably question
 83 whether one can park a car in a slot that is al-
 84 ready occupied by another car, or whether one
 85 has to remove a car from a spot to park another
 86 car in the same spot. In fact, the authors point out that, “the effectiveness of the analogy depends
 87 on [...] how well that models the semantics of the programming language.”

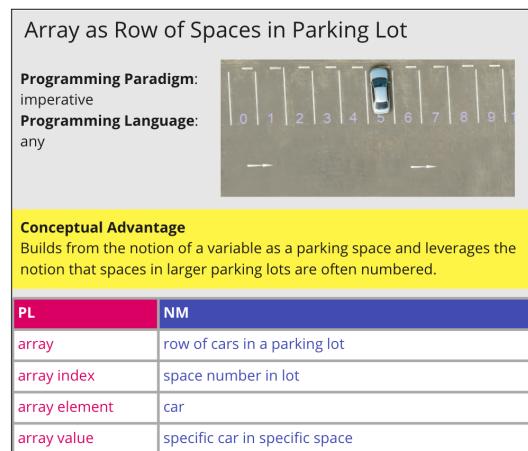


Fig. 2. The “Array as Row of Spaces in Parking Lot” notional machine captured by Fincher et al. [2020].

89 1.2 Soundness of Notional Machines via Simulation

91 To avoid these issues, we need to make sure that a notional machine is indeed an accurate ab-
 92 straction. Although the more general view of notional machines as “pedagogic devices to assist
 93 the understanding of some aspect of programs or programming” [Fincher et al. 2020] makes no
 94 direct reference to programming languages, programs are expressed in programming languages
 95 so we will look at these “aspects of programs” through the lens of how they are realized by some
 96 programming language. If a notional machine represents a part of the operational semantics of a
 97 programming language, for example, then this representation should be sound, in the sense that

99 steps in the notional machine correspond to steps in the operational semantics of the programming
 100 language.

101 Showing the soundness of a notional machine amounts to demonstrating that the notional
 102 machine *simulates* (in the sense described by Milner [1971]) the aspect of programs under the
 103 focus of the notional machine. This property can be given in the form of a commutative diagram.
 104 Milner’s simulation was also used by Hoare [1972] to establish a definition of the correctness
 105 of an ‘abstract’ data type representation with respect to its corresponding ‘concrete’ data type
 106 representation. Cousot and Cousot [1977] use a similar commutative diagram to simulate concrete
 107 computations in their abstract interpretation framework. This interpretation of simulation also
 108 captures the relationship between a notional machine and the underlying programming language
 109 because a notional machine is indeed an *abstraction* of some aspect of interest.

110 1.3 Contributions

111 This paper makes the following contributions:

- 112 • A formal definition of sound notional machine based on simulation (Section 2.1.2).
- 113 • A methodology for designing notional machines that are sound by construction.

114 It consists of deriving part of the notional machine by leveraging the relationship between the
 115 abstract representation of the notional machine and the abstract syntax of the programming
 116 language under its focus.

117 We demonstrate the methodology by applying it to a combination of various small pro-
 118 gramming languages, notional machines, and aspects of programming language semantics
 119 (Section 2).

- 120 • A methodology for analyzing notional machines with respect to their soundness.

121 It consists of modelling the notional machine and the aspect of the programming language
 122 under its focus, relating them via simulation.

123 We demonstrate the methodology by analyzing existing notional machines, sometimes point-
 124 ing out unsoundnesses, and suggesting directions for improvement (Section 3).

125 A brief discussion about the distinction between the abstract and concrete representations of
 126 a notional machine follows in Section 4. We then evaluate, in Section 5, the entire framework by
 127 comparing the notional machines that appeared in Section 2 and Section 3 to an existing dataset
 128 of 37 notional machines. We classify the notional machines in the dataset according to various
 129 dimensions and show that the notional machines we analyzed are representative of the design space
 130 of notional machines used in practice. Section 6 discusses related work and Section 7 concludes.

131 2 DESIGNING SOUND NOTIONAL MACHINES

132 We can only begin to talk about the soundness of a notional machine if we have a formal description
 133 of the programming language the notional machine is focused on. We use a set of small programming
 134 languages with well-known formalizations described in Pierce’s Types and Programming Languages
 135 (TAPL) book [Pierce 2002]. The languages are used to explore different aspects of programming
 136 language semantics. Table 1 shows the notional machines we use in this section as well as the
 137 corresponding programming language and aspect of the semantics of the programming language
 138 that the notional machine focuses on. We use the first example also to introduce the definition of
 139 soundness for notional machines.

140 We model each programming language and notional machine in Haskell. The models are ex-
 141 ecutable, so they include implementations of the programming languages (including parsers,
 142 interpreters, and type-checkers), the notional machines, and the relationship between them². The

143 144 145 146 ²The artifact containing a superset of the examples in this paper is at ANONYMOUS.

Section	Notional Machine	Programming Language	Focus
2.1	EXPTREE	UNTYPEDLAMBDA	Evaluation
2.2	EXPTUTORDIAGRAM	UNTYPEDLAMBDA	Evaluation
2.3	TAPLMEMORYDIAGRAM	TYPEDLAMBDAREF	Evaluation (Refs)
2.4	TYPEDEXPTUTORDIAGRAM	TYPEDARITH	Type-checking

Table 1. Notional machines, programming languages, and aspects of focus used in Section 2.

$$\begin{array}{ccc}
 A_{NM} & \xrightarrow{f_{NM}} & B_{NM} \\
 \alpha_A \uparrow & & \uparrow \alpha_B \\
 A_{PL} & \xrightarrow{f_{PL}} & B_{PL}
 \end{array}$$

$$\alpha_B \circ f_{PL} \equiv f_{NM} \circ \alpha_A \quad (1)$$

Fig. 3. Soundness condition for notional machines shown as a commutative diagram and in algebraic form.

soundness proofs presented in this section are done using equational reasoning [Bird 1989; Gibbons 2002].

2.1 Isomorphic Notional Machines

As a first straightforward example, let's look at a notional machine for teaching how evaluation works in the untyped lambda-calculus (we will refer to this language as UNTYPEDLAMBDA³). While most research papers discuss the lambda-calculus using its textual representation, textbooks sometimes illustrate it using tree diagrams [Pierce 2002, p. 54]. We use this as an opportunity to define a simple notional machine which we call EXPTREE.

2.1.1 *Illustrative Example.* Figure 1 uses EXPTREE to demonstrate the evaluation of a specific lambda expression, which happens in two reduction steps. The top of the figure shows the terms in the traditional textual representation of the programming language, while the bottom shows the terms as a tree.

2.1.2 *Soundness via Commutative Diagrams.* In general, a notional machine is sound if the diagram in Figure 3 commutes. We call the commutativity of this diagram the *soundness condition* for a notional machine. In this diagram, the vertices are types and the edges are functions. We will explain the diagram while instantiating it for this illustrative example (the result of this instantiation is shown in Figure 4).

The bottom layer (A_{PL}, f_{PL}, B_{PL}) represents the aspect of a programming language⁴ we want to focus on. A_{PL} is an abstract representation of a program in that language. In our example, that is the

³The syntax and reduction rules for UNTYPEDLAMBDA are reproduced in the appendix provided as supplementary material .

⁴Although we refer to the bottom layer of the diagram as the programming language layer and we restrict ourselves to analyzing aspects of the syntax and semantics of programming languages, for which we have well-established formalizations, that is not an intrinsic restriction of the approach. In principle, the bottom level of the diagram can be whatever aspects of programs or programming the notional machine is focused on.

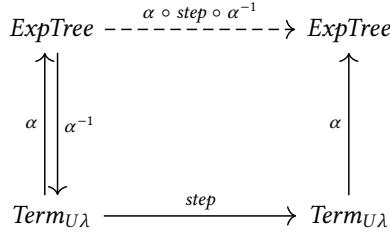


Fig. 4. Instantiation of the commutative diagram in Figure 3 for the notional machine ExpTree and the programming language UNTYPEDLAMBDA .

abstract syntax of UNTYPEDLAMBDA (given by the type $\text{Term}_{U\lambda}$). The function f_{PL} is an operation the notional machine is focusing on. In our example, that would be step , a function that performs a reduction step in the evaluation of a program according to the operational semantics of the language, which in this case also produces a value of type $\text{Term}_{U\lambda}$.

The top layer of the diagram (A_{NM}, f_{NM}, B_{NM}) represents the notional machine. A_{NM} is an abstract representation of the notional machine (its abstract syntax). In our simple example, that is a type ExpTree trivially isomorphic to $\text{Term}_{U\lambda}$ via a simple renaming of constructors. The function f_{NM} is an operation on the notional machine which should correspond to f_{PL} . Connecting the bottom layer to the top layer, there are the functions α_A and α_B from the abstract representation of a program in the programming language to the abstract representation of the notional machine. α is also called an abstraction function.

Definition 2.1. Given the notional machine $(A_{NM}, B_{NM}, f_{NM} : A_{NM} \rightarrow B_{NM})$, focused on the aspect of a programming language given by $(A_{PL}, B_{PL}, f_{PL} : A_{PL} \rightarrow B_{PL})$, the notional machine is *sound* iff there exist two functions $\alpha_A : A_{PL} \rightarrow A_{NM}$ and $\alpha_B : B_{PL} \rightarrow B_{NM}$ such that $\alpha_B \circ f_{PL} \equiv f_{NM} \circ \alpha_A$.

If the abstract representation of the programming language (A_{PL}) is isomorphic to the abstract representation of the notional machine (A_{NM}) , we can construct an inverse mapping α_A^{-1} such that $\alpha_A^{-1} \circ \alpha_A \equiv id \equiv \alpha_A \circ \alpha_A^{-1}$. In that case, we can always define a correct-by-construction operation f_{NM} on A_{NM} in terms of an operation f_{PL} on A_{PL} :

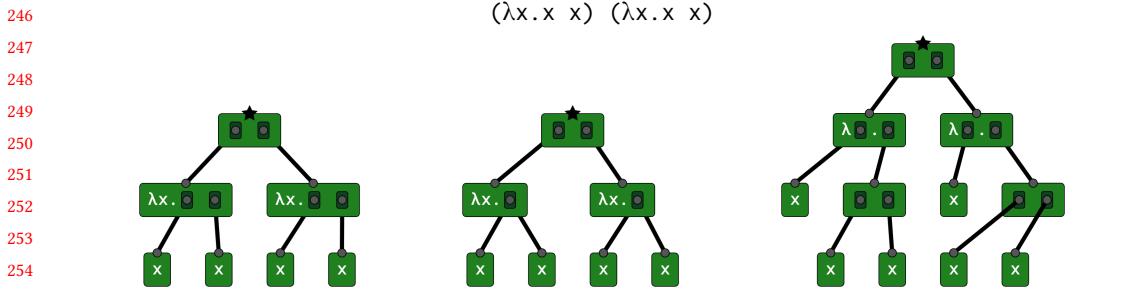
$$\begin{aligned} f_{NM} &:: A_{NM} \rightarrow B_{NM} \\ f_{NM} &= \alpha_B \circ f_{PL} \circ \alpha_A^{-1} \end{aligned}$$

In such cases, the diagram always commutes and therefore the notional machine is sound:

$$f_{NM} \circ \alpha_A \equiv \alpha_B \circ f_{PL} \circ \alpha_A^{-1} \circ \alpha_A \equiv \alpha_B \circ f_{PL} \quad (2)$$

Instantiating the commutative diagram for ExpTree and UNTYPEDLAMBDA yields the diagram in Figure 4. A dashed line indicates a function that is implemented in terms of the other functions in the diagram and/or standard primitives.

We call these isomorphic notional machines because they are isomorphic to the aspect of the programming language they focus on (a condition sometimes called *strong simulation* [Milner 1971]). Of course that's a rather strong condition and not every notional machine is isomorphic so throughout the next sections we will move further away from this simple example, arriving at other instantiations of this commutative diagram.



2.2 Monomorphic Notational Machines

Notational machines can also serve as the basis for so-called “visual program simulation” [Sorva et al. 2013] activities, where students manually construct representations of the program execution. This effort often is supported by tools, such as interactive diagram editors, that scaffold the student’s activity. Obviously, instructors will want to see their students creating correct representations. However, to prevent students from blindly following a path to a solution prescribed by the tool, the visual program simulation environment should also allow *incorrect* representations.

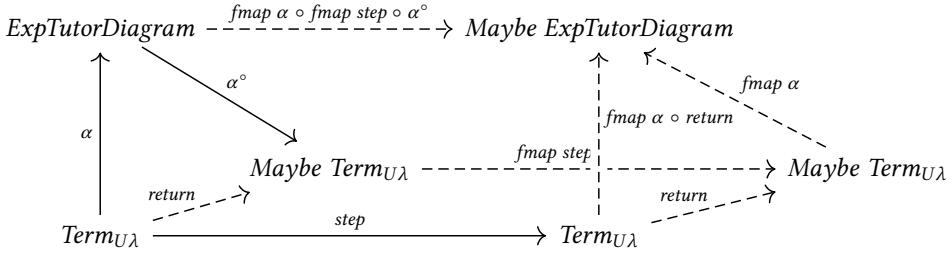
ExpressionTutor⁵ is such an educational tool to teach the structure, typing, and evaluation of expressions in programming courses. In ExpressionTutor, students can interactively construct expression tree diagrams given a source code expression. The tool is language agnostic so each node can be freely constructed (by the instructor or the student) to represent nodes of the abstract syntax tree of any language. Nodes can contain any number of holes that can be used to connect nodes to each other. Each hole corresponds to a place in an abstract syntax tree node where an expression would go. Nodes can be connected in a variety of ways, deliberately admitting incorrect structures that not only may not be valid abstract syntax trees of a given programming language but may not even be trees. Even the root node (labeled with a star) has to be explicitly labeled by the student, so it is not guaranteed to exist in every diagram.

We define the notational machine ExpTUTORDIAGRAM, which models the behavior of ExpressionTutor. The fact that ExpressionTutor allows students to construct incorrect expression tree diagrams means that the abstraction function α is not bijective, as was the case of EXPREE’s α . Such incorrect diagrams do not correspond to programs, thus α is deliberately not surjective.

2.2.1 Illustrative Example. Figure 5 uses ExpTUTORDIAGRAM to represent the omega combinator. The top shows the textual form on the level of the programming language. Below that are three different incorrect representations students could produce. The left tree collapses the applications (the terms $x x$) into the enclosing lambda abstraction. The middle tree similarly does this, but it preserves the structure of the lambda abstraction node, while violating the well-formedness of the tree by plugging two children into the same hole. The right tree shows a different problem, where the definition of the name is pulled out of the lambda abstraction and shown as a name use.

2.2.2 Commutative Diagram. In general, if the mapping α_A , from the abstract representation of the programming language (A_{PL}) to the abstract representation of the notational machine (A_{NM}), is an injective but non-surjective function, we can still define the operations on A_{NM} in terms of the

⁵expressiontutor.org

Fig. 6. Instantiation of the commutative diagram in Figure 3 for the notional machine `ExpTutorDiagram`

operations on A_{PL} . For this we define a function $\alpha_A^\circ : A_{NM} \rightarrow \text{Maybe } A_{PL}$ to be a left inverse of α_A such that $\alpha_A^\circ \circ \alpha_A \equiv \text{return}$ (we use `return` and `fmap` to refer to the *unit* and *map* operations on monads). Here we modeled the left inverse using a *Maybe* but another monad could be used, for example, to capture information about the values of type A_{NM} that do not have a corresponding value in A_{PL} . The top-right vertex of the square (B_{NM}) in this case is the type $\text{Maybe } B'_{NM}$ and the mapping α_B can be implemented in terms of a mapping $\alpha'_B : B_{PL} \rightarrow B'_{NM}$ like so:

$$\begin{aligned} \alpha_B &: B_{PL} \rightarrow B_{NM} \\ \alpha_B &= \text{return} \circ \alpha'_B \end{aligned}$$

Using the left inverse α_A° and α'_B , we define the operation on A_{NM} as follows:

$$\begin{aligned} f_{NM} &: A_{NM} \rightarrow B_{NM} \\ f_{NM} &= \text{fmap } \alpha'_B \circ \text{fmap } f_{PL} \circ \alpha_A^\circ \end{aligned}$$

This square commutes like so:

$$\begin{array}{ll} \begin{array}{l} f_{NM} \circ \alpha_A \\ \equiv \{ \text{definition of } f_{NM} \} \\ \text{fmap } \alpha'_B \circ \text{fmap } f_{PL} \circ \alpha_A^\circ \circ \alpha_A \\ \equiv \{ \alpha_A^\circ \text{ is left inverse of } \alpha_A \} \\ \text{fmap } \alpha'_B \circ \text{fmap } f_{PL} \circ \text{return} \\ \equiv \{ \text{third monad law} \} \\ \text{fmap } \alpha'_B \circ \text{return} \circ f_{PL} \end{array} & \begin{array}{l} \alpha_B \circ f_{PL} \\ \equiv \{ \text{definition of } \alpha_B \} \\ \text{return} \circ \alpha'_B \circ f_{PL} \\ \equiv \{ \text{third monad law} \} \\ \text{fmap } \alpha'_B \circ \text{return} \circ f_{PL} \end{array} \end{array}$$

We can use this result to instantiate the commutative diagram of Figure 3 for `ExpTutorDiagram` and `UNTYPEDLAMBDA`, shown in Figure 6. A_{PL} is defined to be the type `ExpTutorDiagram`, which essentially implements a graph. Each node has a top plug and any number of holes, which contain plugs. Edges connect plugs. That allows for a lot of flexibility in the way nodes can be connected.

The ExpressionTutor tool is language agnostic but we can only talk about soundness of a notional machine with respect to some language and some aspect of that language. In this case, we say the tool implements a family of notional machines, each one for a given aspect of focus and a given programming language. We consider here a notional machine focused on evaluation and the programming language again `UNTYPEDLAMBDA` (denoted again by the type `Term_{U\lambda}`), with f_{PL} equal to `step`.

The construction of a mapping $\alpha : \text{Term}_{U\lambda} \rightarrow \text{ExpTutorDiagram}$ is straightforward because a term $t : \text{Term}_{U\lambda}$ forms a tree and from it we can always construct a corresponding ExpressionTutor diagram $d : \text{ExpTutorDiagram}$ (a graph). For each possible term in `Term_{U\lambda}`, we need to define a pattern

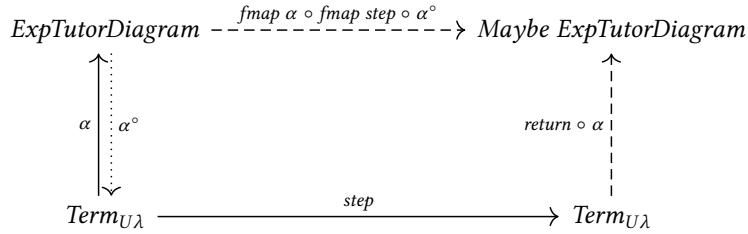


Fig. 7. Simplified version of the commutative diagram for *ExpTutorDiagram* shown in Figure 6.

for the content of the corresponding *ExpTutorDiagram* node which will help the student identify the kind of node. The construction of the left inverse mapping $\alpha^o : ExpTutorDiagram \rightarrow Maybe Term_{U\lambda}$ requires more care. We need to make sure that the diagram forms a proper tree and that the pattern formed by the contents of each *ExpTutorDiagram* node corresponds to a possible $Term_{U\lambda}$ node, besides making sure that they are connected in a way that indeed corresponds to a valid $Term_{U\lambda}$ tree.

In the next section, we construct another commutative diagram where f_{NM} is defined using f_{PL} and a left inverse mapping α_A^o . To emphasize that point and simplify the diagrams, we will depict the left inverse in the diagram as a dotted line pointing from A_{NM} to A_{PL} (even though α_A^o is of type $A_{NM} \rightarrow Maybe A_{PL}$ and not $A_{NM} \rightarrow A_{PL}$) and omit the path via $Maybe A_{PL}$ as shown in Figure 7.

We call these monomorphic notional machines because there is a monomorphism (injective homomorphism) between the notional machine and the aspect of the programming language it focuses on. This is the case here by design, to allow students to make mistakes by constructing wrong diagrams that don't correspond to programs. In general, this will be the case whenever there are values of A_{NM} (the abstract syntax of the notional machine) that have no correspondence in the abstract representation of the language (A_{PL}). That's often the case in memory diagrams [Dalton and Krehling 2010; Dragon and Dickson 2016; Holliday and Luginbuhl 2004] (notional machines used to show the relationship between programs and memory) because they typically allow for the representation of memory states that cannot be produced by legal programs. We show an example of such a notional machine in the next section.

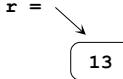
2.3 A Monomorphic Notional Machine to Reason About State

A common use of notional machines is in the context of reasoning about state. In fact, 16 of the 37 notional machines in the dataset by Fincher et al. [2020] focus on either References, Variables, or Arrays (see Section 5). An example of the use of a visual notation to represent state can also be found in TAPL [Pierce 2002, p. 155]. In Chapter 13 (“References”), the book extends the simply typed lambda-calculus with references (a language we will refer to as **TYPEDLAMBDAREF**⁶). It explains references and aliasing by introducing a visual notation to highlight the difference between a *reference* and the *cell* in the store that is pointed to by that reference. We will refer to this notation, which we will develop into a notional machine, as **TAPLMEMORYDIAGRAM**. In this notation, references are represented as arrows and cells are represented as rounded rectangles containing the representation of the value contained in the cell. Before designing the notional machine, we need to see the context in which this notation is used in the book.

The book first uses this notation to explain the effect of creating a reference. It shows that when we reduce the term `ref 13` we obtain a reference (a store location) to a store cell containing 13.

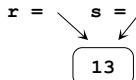
⁶The syntax and reduction rules for **TYPEDLAMBDAREF** are reproduced in the appendix provided as supplementary material.

393 The book then represents the result of binding the name r to such a reference with the following
 394 diagram:



399 In the book, this operation is written as $r = \text{ref } 13$, but as we will see in the next Section, this
 400 form of name binding (name = term) exists only in a REPL-like context which is not part of the
 401 language.

402 The book continues explaining that we can “make a copy of r ” by binding its value to another
 403 variable s (with $s = r$) and shows the resulting diagram:



408 The book then explains that one can verify that both names refer to the same cell by *assigning* a
 409 new value to s and reading this value using r (for example, the term $s := 82$; $\text{!}r$ would evaluate to
 410 82). Right after, the book suggests to the reader an exercise to “draw a similar diagram showing the ef-
 411 fects of evaluating the expressions $a = \{\text{ref } 0, \text{ ref } 0\}$ and $b = (\lambda x:\text{Ref Nat}. \{x, x\}) (\text{ref } 0)$.“
 412 Although we understand informally the use of this diagram in this context, how can we know what
 413 a correct diagram would be in general for any given program? This is what we aim to achieve by
 414 designing a notional machine based on this notation.

415 Let’s see how we would turn that kind of diagram into a sound notional machine. We want
 416 to construct a commutative diagram where A_{PL} is an abstract representation of the state of a
 417 TYPEDLAMBDAREF program execution, A_{NM} is an abstract representation of the diagram presented
 418 in the book, and f_{PL} is an operation that affects the state of the store during program execution.

419 In a first attempt, let’s choose f_{PL} to be an evaluation step and A_{PL} to be modeled as close as
 420 possible to the presentation of a TYPEDLAMBDAREF program as described in the book. In that
 421 case, A_{PL} is the program’s abstract syntax tree together with a *store*, a mapping from a location (a
 422 reference) to a value.

423 **2.3.1 Problem: Beyond the Language.** The first challenge is that the name-binding mechanism
 424 used in the examples above (written as name = term) exists only in a REPL-like context in the
 425 book used for the convenience of referring to terms by name. It is actually not part of the language
 426 (TYPEDLAMBDAREF) so it is not present in this representation of A_{PL} and as a result it cannot be
 427 mapped to A_{NM} (the notional machine). We will avoid this problem by avoiding this name-binding
 428 notation entirely and writing corresponding examples fully in the language. The only mechanism
 429 actually in the language to bind names is by applying a lambda to a term. Let’s see how we can write
 430 a term to express the behavior described in the example the book uses to introduce the diagram
 431 (shown earlier), where we:

- 433 (1) Bind r to the result of evaluating $\text{ref } 13$
- 434 (2) Bind s to the result of evaluating r
- 435 (3) Assign the new value 82 to s
- 436 (4) Read this new value using r

437 Using only the constructs in the language, we express this with the following term:
 438

439 $(\lambda r:\text{Ref Nat}. (\lambda s:\text{Ref Nat}. s := 82; !r) r) (\text{ref } 13)$
 440

```

442 a = {ref 0, ref 0};
443
444 a = {•, •}
445
446
447 b = (\x: Ref Nat. {x, x}) (ref 0);
448
449

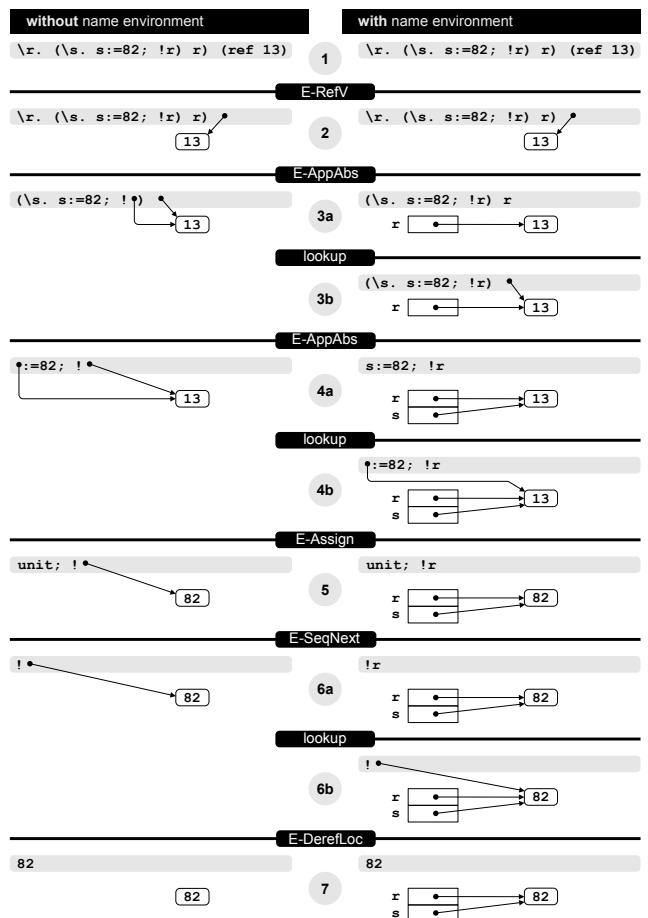
```

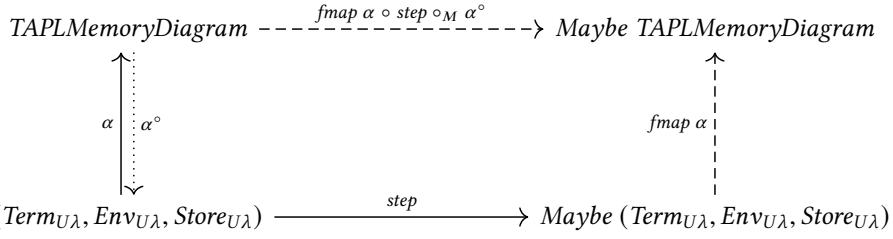
Fig. 9. TAPL MEMORY DIAGRAM for TYPED LAMBDA REF for TAPL Exercise 13.1.1

2.3.2 *Problem: Direct Substitution.* The problem now is that if we model A_{PL} and evaluation as described in the book, the result of reducing a term $(\lambda x.t_1) t_2$ is the term obtained by replacing all free occurrences of x in t_1 by t_2 (modulo alpha-conversion), so we don't actually keep track of name binding information. What we have in A_{PL} at each step is an abstract syntax tree and a store, but we have no information about which names are bound to which values because the names were already substituted in the abstract syntax tree. That would be enough to do Exercise 13.1.1, for example, whose solution is shown in Figure 9. But the absence of explicit information mapping names to values makes it less suitable to talk about aliasing, because even though a term may contain, at any given point during evaluation, multiple occurrences of the same location, it is not possible to know if these locations correspond to different names, and one may need to trace several reduction steps back to find out when a name was substituted by a location.

We need to change A_{PL} and step to capture this information, keeping not only a store but an explicit name environment that maps names to values, and only substituting the corresponding value when we evaluate a variable. Like the definition of application in terms of substitution, we have to be careful to avoid variable capture by generating fresh names when needed.

2.3.3 *Illustrative Example.* Figure 8 shows two variations of the notional machine being used to explain the evaluation of the term we had described before. It shows the state after each reduction step, on the left without an explicit name environment and on the right with an explicit name environment. Between each step, a line with the name of the applied reduction rule is shown. Notice that the representation with

Fig. 8. Using TAPL MEMORY DIAGRAM to trace the evaluation of $(\lambda r:\text{Ref Nat.} (\lambda s:\text{Ref Nat.} s := 82; !r) r) (\text{ref 13})$



The type *DLocation* corresponds to arrow destinations (arrow endpoints). A term is represented as a rose tree of *Strings* augmented with a case for location.

The concrete representation of a *DTerm* can be in linearized text form or as a tree akin to that shown in Section 2.1. The representation of the nodes in a *DTerm* tree that are *TLoc* are shown as arrow starting points. These arrows end in the cell corresponding to the *DLocation* in each *TLoc*. The concrete representation of the store relates the visual position of each cell with the *DLocation* of each cell. That leads to the commutative diagram in Figure 10, where we use the symbol \circ_M to denote monadic function composition (the fish operator $<=<$ in Haskell).

2.4 A Monomorphic Notional Machine to Reason About Types

So far we have seen examples of commutative diagrams where f_{PL} is *step* (a function that performs a reduction step) but in principle, f_{PL} could be any operation on A_{PL} that is the focus of a given notional

540 machine. Let's look at an example of notional machine where we do not focus on evaluating but on
 541 typing an expression. The language this notional machine focuses on is TYPEDARITH⁷, a language
 542 of typed arithmetic expression, which is the simplest typed language introduced in TAPL [Pierce
 543 2002, p. 91]. We describe two designs.

544 In the first design, the data type used for the abstract representation of the notional machine
 545 (A_{NM}) is *ExpTutorDiagram*, used in Section 2.2. We represent a program in TYPEDARITH with the
 546 type $Term_{TyArith}$ and the operation we focus on (f_{PL}) is $typeof :: Term_{TyArith} \rightarrow Maybe\ Type_{TyArith}$,
 547 a function that gives the type of a term (for simplicity we use a *Maybe* here to capture the cases
 548 where a term is not well-typed).

549 We then have two abstraction functions:

$$550 \alpha_{Term} :: Term_{TyArith} \rightarrow ExpTutorDiagram$$

$$551 \alpha_{Type} :: Type_{TyArith} \rightarrow Type_{ExpTutor}$$

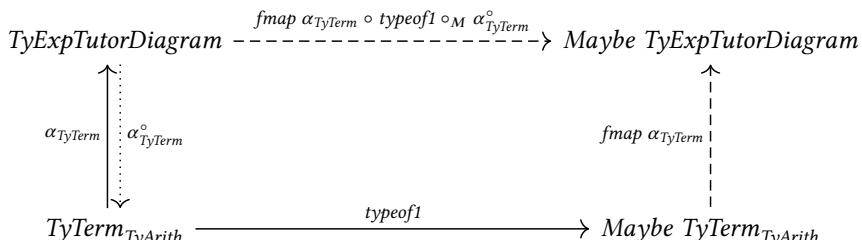
552 The implementation of $f_{TyArith}$, the notional machine operation (f_{NM}) that produces a notional
 553 machine-level representation of maybe the type of a term, is analogous to what is shown in Figure 10
 554 because (1) the abstraction function (α_{Term}) has a left inverse (α_{Term}°) and (2) f_{PL} produces a *Maybe*.
 555

$$556 f_{TyArith} :: ExpTutorDiagram \rightarrow Maybe\ Type_{ExpTutor}$$

$$557 f_{TyArith} = fmap\ \alpha_{Type} \circ typeof \circ_M \alpha_{Term}^\circ$$

558 As is, a student may benefit from the notional machine's representation of the program's abstract
 559 syntax tree and that may be helpful to reason about typing but the notional machine does not
 560 expose to the student the inner workings of the process of typing a term.
 561

562 The second design, represented in the diagram in Figure 11, tackles this issue by enriching the
 563 notional machine in a way that allows it to go step-by-step through the typing algorithm. The
 564 idea is that f_{NM} now does not produce a type but gradually labels each subtree with its type as
 565 part of the process of typing a term. For this, A_{NM} here is *TyExpTreeDiagram*, which differs from
 566 *ExpTreeDiagram* by adding to each node a possible type label. We still want to write f_{NM} in terms
 567 of f_{PL} . The key insight that enables this is to change f_{PL} from *typeof* to *typeof1*. The difference
 568 between *typeof* and *typeof1* is akin to the difference between big-step and small-step semantics:
 569 *typeof1* applies a single typing rule at a time. As a result, we have to augment our representation
 570 of a program by bundling each term with a possible type (captured in type $TyTerm_{TyArith}$). The
 571 abstraction function and its left inverse are updated accordingly. The resulting notional machine is
 572 depicted in Figure 12.
 573



583 Fig. 11. Instantiation of the commutative diagram in Figure 3 for a notional machine focused on type-checking
 584 programs in TYPEDARITH. The notional machine exposes the inner workings of the typing algorithm.
 585

586
 587 ⁷The syntax and typing rules for TYPEDARITH are reproduced in the appendix provided as supplementary material .
 588

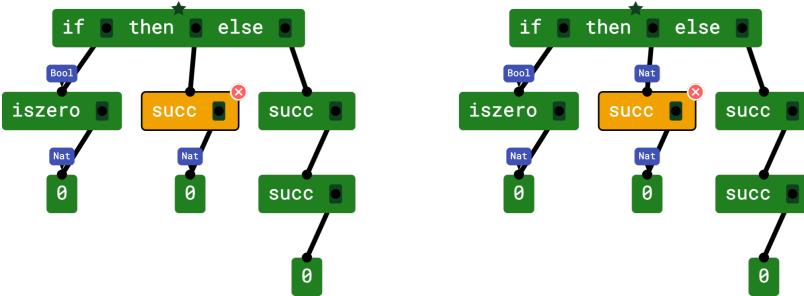


Fig. 12. One step in the notional machine `TYPEDExPTUTORDIAGRAM` as it types the term if `iszzero 0 then succ 0 else succ succ 0` in the language `TYPEDARITH`.

Section	Notional Machine	Programming Language	Focus
3.1	ALLIGATOR	UNTYPEDLAMBDA	Evaluation
3.2	LISTASSTACK	-	Data Structure (List)
3.3	ARRAYASPARKINGSPOTS	JAVA	Evaluation (Arrays)

Table 2. Notional machines, programming languages, and aspects of focus used in Section 3.

Interestingly, given an expression e , once we label all nodes in the ExpressionTutor diagram of e with their types, the depiction of the resulting diagram is similar to the typing derivation tree of e .

Note that types are themselves trees but here we're representing them in a simplified form as textual labels because the primary goal of ExpressionTutor is to represent the structure of terms, not the structure of types.

3 ANALYZING EXISTING NOTIONAL MACHINES

So far we have seen how we can design sound notional machines by constructing f_{NM} using f_{PL} and functions that convert between A_{PL} and A_{NM} . Now we will analyze existing notional machines, using their informal description to construct all components of the commutative diagram. In particular, here, we have a description of f_{NM} entirely in terms of A_{NM} . We then use property-based testing, using the soundness condition as a property, to uncover unsoundnesses and suggest improvements that eliminate them. Table 2 shows the notional machines we use in this section as well as the corresponding programming language and aspect of the semantics of the programming language that the notional machine focuses on.

3.1 Debugging a Notional Machine: The Case of Alligator Eggs

Alligator Eggs⁸ is a game conceived by Bret Victor to introduce the lambda-calculus in a playful way. It is essentially a notional machine for the untyped lambda-calculus. The game has three kinds of pieces and is guided by three rules.

Pieces. The pieces are *hungry alligators*, *old alligators*, and *eggs*. Old alligators are white, while hungry alligators and eggs are colored with colors other than white. The pieces are placed in a plane and their relative position with respect to each other determines their relationship. All pieces placed under an alligator are said to be guarded by that alligator. An alligator together with the

⁸<http://worrydream.com/AlligatorEggs/>

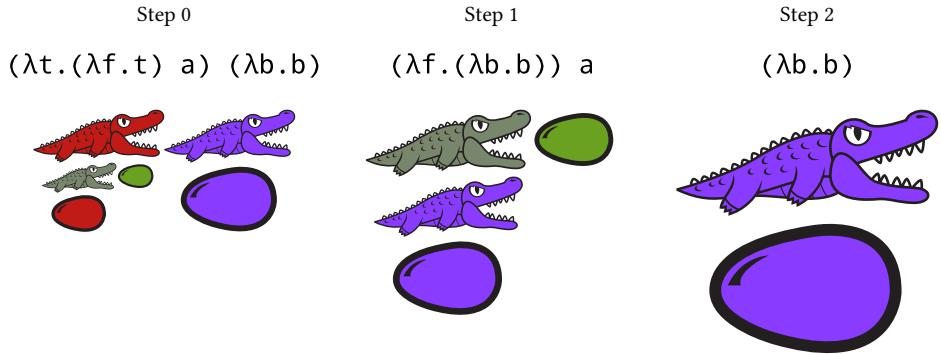


Fig. 13. Evaluation of $(\lambda t.(\lambda f.t) a) (\lambda b.b)$ in the untyped lambda calculus (top) and ALLIGATOR notional machine (bottom).

pieces that may be guarded by it form a family. Families placed to the right of another family may be eaten by the guardian of the family on the left, depending on the applicability of the gameplay rules. Every egg must be guarded by an alligator with the same color (this must be a hungry alligator because eggs cannot be white).

Rules. There are three rules that determine the “evolution of families” over time:

Eating rule If there is a family guarded by a hungry alligator in the plane and there is a family or egg to its right, then the hungry alligator eats the entire family (or egg) to its right and the pieces of the eaten family are removed. The alligator that ate the pieces dies and the eggs that were guarded by this alligator and that have the same color of this alligator are hatched and are replaced by a copy of what was eaten by the alligator.

Color rule Before a hungry alligator A can eat a family B , if a color appears both in A 's proteges and in B , then that color is changed in one of the families to another color different from the colors already present in these families.

Old age rule If an old alligator is guarding only one egg or one family (which itself may be composed of multiple families), then the old alligator dies and is removed.

Relation to the Untyped Lambda-Calculus. According to their description, the way ALLIGATOR relates to the untyped lambda-calculus is as follows: “A hungry alligator is a lambda abstraction, an old alligator is parentheses, and eggs are variables. The eating rule corresponds to beta-reduction. The color rule corresponds to (over-cautious) alpha-conversion. The old age rule says that if a pair of parentheses contains a single term, the parentheses can be removed”. Although very close, this relation is not completely accurate. We will identify the limitations and propose solutions.

3.1.1 Illustrative Example. Figure 13 shows a representation of the evaluation of the lambda-calculus term $(\lambda t.(\lambda f.t) a) (\lambda b.b)$ using the ALLIGATOR notional machine. Step 0 shows the alligator families corresponding to the term. In the first step, the red alligator eats the family made of the purple alligator and the purple egg. As a result, the eaten family disappears, the red egg guarded by the red alligator hatches and is replaced by the family that was eaten, and the red alligator disappears (dies). In the second step, the grey alligator eats the green egg. As a result, the grey alligator dies and no eggs are hatched because it was not guarding any grey eggs. We are left with the purple family.

687 3.1.2 *Commutative Diagram.* To build a commutative diagram for ALLIGATOR, we need to build
 688 the abstract representation of the notional machine A_{NM} , which corresponds to the game pieces
 689 and the game board, the abstraction function $\alpha :: Term_{U\lambda} \rightarrow A_{NM}$, and an f_{NM} function, which
 690 correspond to the rules that guide the evolution of alligator families. First, we look more precisely
 691 at the game pieces and their relationship with $Term_{U\lambda}$ to model A_{NM} .

692 **Eggs** An egg corresponds to a variable use and its color corresponds to the variable name.

693 **Hungry alligators** A hungry alligator somewhat corresponds to a lambda abstraction with its
 694 color corresponding to the name of the variable introduced by the lambda (a variable defini-
 695 tion) and the pieces guarded by the hungry alligator corresponding to the body of the lambda
 696 abstraction. But differently from a lambda abstraction, a hungry alligator does not have to be
 697 guarding any pieces, which has no direct correspondence with the lambda calculus because a
 698 lambda abstraction cannot have an empty body.

699 **Old alligators** An old alligator somewhat corresponds to parentheses but not exactly. The lambda
 700 abstraction in the term $(\lambda t. \lambda f. t) a b$ requires parentheses because conventionally the
 701 body of a lambda abstraction extends as far to the right as possible, so without the parentheses
 702 its body would be $t a b$ instead of t . However the corresponding alligator families shown in
 703 Figure 13 don't require an old alligator. On the other hand, if we want to represent the term
 704 $a (b c)$, then we need an old alligator. Figure 14 shows an example of a term that requires
 705 an old alligator.

706 Now let's look at the terms of the untyped lambda-calculus. If hungry alligators are lambda
 707 abstractions and eggs are variables then what is an application? Applications are formed by the
 708 placement of pieces on the game board. When an alligator family or egg (corresponding to a term
 709 t_1) is placed to the left of another family or egg (corresponding to a term t_2), then this corresponds
 710 to the term t_1 applied to t_2 (in lambda calculus represented as $t_1 t_2$).

711 Notice that because every egg must be guarded by a hungry
 712 alligator with the same color, strictly speaking, an egg cannot
 713 appear all by itself. That corresponds to the fact that in the
 714 untyped lambda-calculus only lambda terms are values, so a
 715 term cannot have unbounds variables. Textbooks, of course,
 716 often use examples with unbound variables but these are ac-
 717 tually metavariables that stand for an arbitrary term. So, for
 718 convenience, we will consider that an egg by itself also forms
 719 a family.

720 We can then model an alligator family as the type
 721 *AlligatorFamily*, and a game board as simply a list of alliga-
 722 tor families. The result is the commutative diagram shown in
 723 Figure 15.

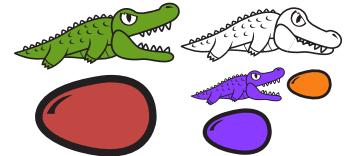


Fig. 14. Old alligator in $(\lambda a. y) ((\lambda b. b) c)$

```
725 data AlligatorFamily = HungryAlligator Color [AlligatorFamily]
 726   | OldAlligator [AlligatorFamily]
 727   | Egg Color
```

728 The abstraction function α relies on some function $nameToColor :: Name \rightarrow Color$.

$\alpha :: Term_{U\lambda}$	$\rightarrow [AlligatorFamily]$
$\alpha (Var\ name)$	$= [Egg\ (nameToColor\ name)]$
$\alpha (Lambda\ name\ e)$	$= [HungryAlligator\ (nameToColor\ name)\ (\alpha\ e)]$
$\alpha (App\ e1\ e2 @ (App\ _\ _))$	$= \alpha\ e1 + [OldAlligator\ (\alpha\ e2)]$
$\alpha (App\ e1\ e2)$	$= \alpha\ e1 + \alpha\ e2$

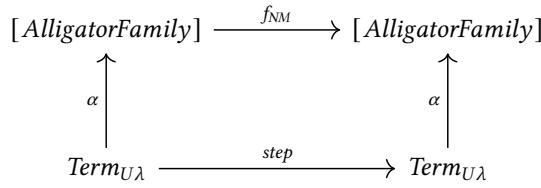


Fig. 15. First attempt at instantiating the commutative diagram in Figure 3 for the notional machine ALLIGATOR.

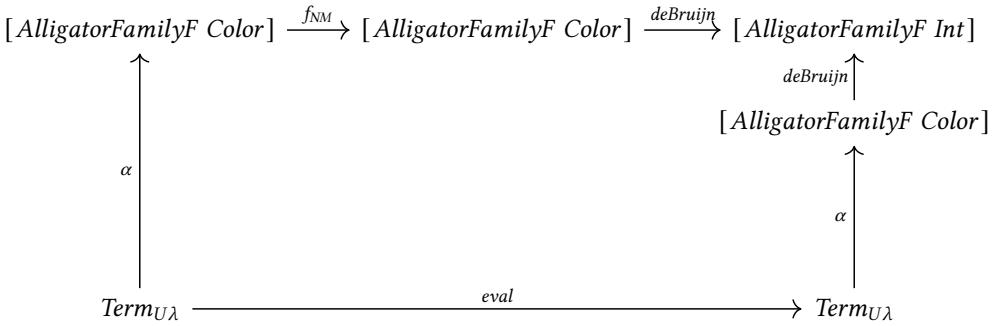
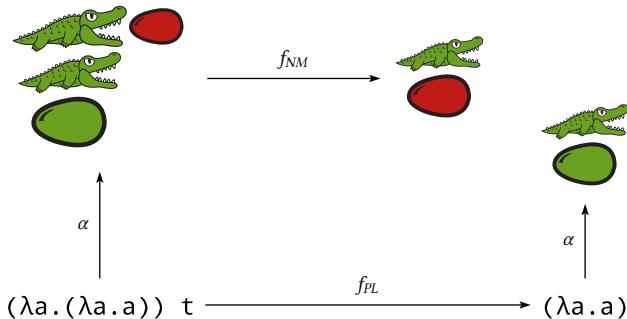


Fig. 16. Second attempt at instantiating the commutative diagram in Figure 3 for the notional machine ALLIGATOR.

From Proof to Property-Based Testing. The commutativity of the diagrams presented in Chapter 2 was demonstrated using equational reasoning. Here instead, we implement the elements that constitute the commutative diagram and use property-based testing to test if the diagram commutes. This approach is less formal and it does not prove the notional machine correct, but it is lightweight and potentially more attractive to users that are not familiar with equational reasoning or mechanised proofs. We will see here that, despite its limitations, this approach can go a long way in revealing issues with a notional machine. The idea is that a generator generates terms $t_i :: Term_{U\lambda}$ and checks that $(f_{NM} \circ \alpha) t_i \equiv (\alpha \circ step) t_i$.

de Bruijn Alligators. The first challenge is that we need to compare values of type $[AlligatorFamily]$ that were produced using f_{NM} with values produced using $step$. As we have seen, the colors in $AlligatorFamily$ correspond to variable names but the way $step$ generates fresh names (which then are turned into colors) may be different from the way f_{NM} will generate fresh colors. In fact, the original description of ALLIGATOR anticipates the challenge of comparing alligator families. In the description of possible gameplays, they clarify that to compare alligator families we need to take into account that families with the same "color pattern" are equivalent. This can be achieved by using a *de Bruijn representation* [Bruijn 1972] of Alligators. We turn $AlligatorFamily$ into $AlligatorFamilyF Color$ and before comparing families we transform them into $AlligatorFamilyF Int$ following the de Bruijn indexing scheme. The commutative diagram we are moving towards is shown in Figure 16.

Evaluation Strategy. With this setup in place, the next step is to implement f_{NM} in terms of the game rules. The eating rule (together with the color rule) somewhat corresponds to beta-reduction but under what evaluation strategy? The choice of evaluation strategy turns out to affect not

Fig. 17. Unsoundness: *bound* occurrences of a variable should not be substituted.

only the eating rule but also the old age rule. According to the original description, any hungry alligator that has something to eat can eat and one of the original examples shows a hungry alligator eating an egg even when they are under another hungry alligator. That would correspond to a *full beta-reduction* evaluation strategy but we will stick to a call-by-value lambda-calculus interpreter so we will adapt the rules accordingly. The old age rule has to be augmented to trigger the evolution of an old alligator family that follows a topmost leftmost hungry alligator and families under a topmost leftmost old alligator. The eating rule should be triggered only for the topmost leftmost hungry alligator, unless it is followed by an old alligator (in which case the augmented old age rule applies). The color rule plays an important role in the correct behavior of the eating rule as a correspondence to beta-reduction. That's because indeed "the color rule corresponds to (over-cautious) alpha-conversion", so it is responsible for avoiding variable capture.

With all the rules implemented, we can define a function *evolve* that applies them in sequence. We will then use *evolve* in the definition of f_{NM} . One application of *evolve* corresponds to one step in the notional machine layer but that step does not correspond to a step in the programming language layer. For example, The main action of the old age rule (to remove old alligators) does not have a correspondence in the reduction of terms in UNTYPEDLAMBDA. In terms of simulation theory, in this case the simulation of the programming language by the notional machine is not lock-step. To adapt our property-based testing approach, instead of making f_{PL} equal to *step*, we will simply reduce the term all the way to a value (leading to the use of *eval* as f_{PL} in Figure 16) and correspondingly define f_{NM} to be the successive applications of *evolve* until we reach a fixpoint.

3.1.3 Problem: Substitution of Bound Variables. Now we have all the building blocks of the commutative diagram. We can put them together by running the property-based tests to try to uncover issues in the diagram and indeed we do. According to the eating rule, after eating, a hungry alligator dies and if it was guarding any eggs of the same color, each of those eggs hatches into what was eaten. So the family corresponding to $(\lambda a. (\lambda a. a)) t$, for example, would evolve to the family corresponding to $\lambda a. t$ instead of $\lambda a. a$, as shown in Figure 17. This issue corresponds to a well-known pitfall in substitution: we cannot substitute *bound* occurrences of a variable, only the ones that are *free*.

The issue can be solved in one of the following ways:

- (1) Refining the description of the eating rule, changing "if she was guarding any eggs of the same color, each of those eggs hatches into what she ate" into "if she was guarding any eggs of the same color **that are not guarded by a closer alligator with the same color**, each of those eggs hatches into what she ate";

- 834 (2) Restricting all colors of hungry alligators in a family to be distinct;
 835 (3) Defining colors to correspond to de Bruijn indices instead of names. This means that not
 836 only colors wouldn't be repeated in the same family but also that every family would use the
 837 same "color scheme" for structurally equivalent terms.
 838

839 3.2 Notional Machines for Data Structures

840 Although most notional machines focus on the semantics of programming language constructs,
 841 some notional machines instead focus on data structures. One such notional machine, which we
 842 model in this section, is the "List as Stack of Boxes" (Figure 18), described by Du Boulay and O'Shea
 843 [1976] and included in the dataset of notional machines analyzed by Fincher et al. [2020].
 844

845 For notional machines focussing on the dy-
 846 namic semantics of a language (EXPTREE, EX-
 847 PTREE, TAPLMEMORYDIAGRAM), the type A_{PL}
 848 represents a program in the language under
 849 focus (and in the case of TAPLMEMORYDIA-
 850 GRAM, additional information needed to eval-
 851 uate the program) and the function f_{PL} performs
 852 an evaluation step. In the case of TYPEDEXPTU-
 853 TORDIAGRAM, which focusses on type-checking
 854 (the static semantics of TYPEDARITH), A_{PL} also
 855 represents a program in that language and f_{PL}
 856 performed type-checking. Now we will model a
 857 notional machine focussing on a data structure,
 858 so A_{PL} represents that data structure and there
 859 are several f_{PL} functions, one for each opera-
 860 tion supported by that data structure. The type
 861 A_{NM} can be seen as an abstraction of A_{PL} and it
 862 should provide corresponding operations. The
 863 commutation of the diagram demonstrates the correctness of this abstraction.

Modelling "List as Stack of Boxes" requires some adaptations to the original description:

- 864 (1) To avoid partiality of the operations typically used to access the head and tail of a list (FIRST
 865 and REST in the original description), we define a list using three operations: *Empty* and *Cons*
 866 to construct a list and *uncons* :: $List\ a \rightarrow Maybe\ (a, List\ a)$ to deconstruct it. That change also
 867 has a convenient representation in the notional machine.
- 868 (2) In the stack of boxes, each value is shown as a *String* in a box, which means we can only
 869 represent lists of values for which we can create a *String* representation.
- 870 (3) The original description wasn't explicit about the representation of an empty list. We need a
 871 corresponding empty stack of boxes that can be treated as a stack and not just the absence of
 872 boxes. For that we will use a pallet (used to hold boxes in storage). The original description
 873 mentions a pallet in two contexts:
 - 874 (a) "boxes are stacked on a pallet so that they can be picked up as one stack". That's an
 875 important part of the notional machine's behavior but we also need to be able to pick up a
 876 box from the top of the stack;
 - 877 (b) "The beginning of a list, the top of the stack, is marked with [and the end of the list, the
 878 pallet is marked with]". Here there's an asymmetry between the end of the list, represented
 879 with a pallet, and the beginning of the list, which has no representation in the notional
 880 machine. Our denotation of pallet is different: it is the representation of an empty list.

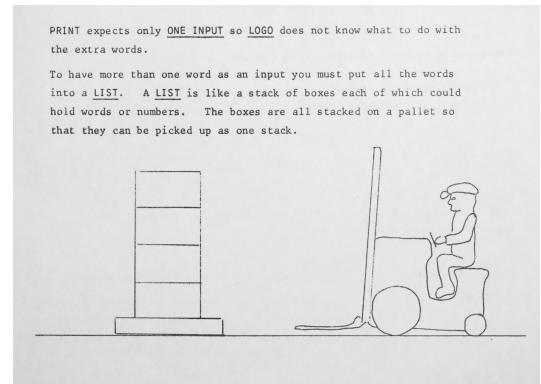


Fig. 18. The "List as Stack of Boxes" notional machine as described by Du Boulay and O'Shea [1976].

The result is that we can construct lists either with a pallet or by stacking a box on top of a stack, which must have eventually a pallet at the end. To deconstruct it, we can pick up a box from the top of the stack ($\text{pickUp} :: \text{Stack} \rightarrow \text{Maybe}(\text{Box}, \text{Stack})$). When trying to pick up a box, either there is only the pallet, in which case we get nothing, or there is a box on top of a stack, in which case we are left with the box and the rest of the stack.

The process of formalizing the notional machine, making it precise, once again helped to identify the issues and improve the notional machine.

3.3 A Notional Machines for Arrays

With the techniques we have developed so far, we can turn again to the notional machine "Array as Row of Parking Spaces is Parking Lot", presented in Section 1.1. There we considered Java as the underlying programming language and already identified the first issue, caused by the difference between the representation of arrays of primitive types and arrays of reference types. Here, we will make the notional machine more precise and in the process resolve two problems.

One approach would be to model the subset of Java needed for the notional machine to work, but Java is a fairly complex language. Instead we start by following the approach taken in the last section: we model the PL layer as an idealized array and the operations it supports. An array supports three operations: *allocating* an array of a given type and a given length, *reading* an element at a given index, and *writing* an element to a given index.

3.3.1 Problem: reference types versus primitive types. One of the appeals of the notional machine is that we would represent a newly allocated array of objects as an empty parking lot, because it does not contain "valid" values (their slots contain *null*). The first issue is that arrays of primitive types are really different in that, when newly allocated, their slots already contain valid values. These arrays would be represented as fully booked parking lots with slots that can never be empty! Here, instead of changing the design of the notional machine, we can use this misfit in the metaphor as a learning opportunity and explicitly discuss it with students. There is still a decision to be made about how exactly the values in the array are going to be represented. We could represent a value as a car with the string representation of the value drawn on its roof, but representing both unboxed and boxed versions of an integer with the same string could be confusing. Instead, we could opt for representing values of reference types as cars of a different color, for example. Of course an array can also contain other arrays, which are themselves objects, and that complicates the picture.

3.3.2 Problem: representing multiple arrays. To represent multiple arrays, and the relationship between them, we cannot model the PL layer simply as an idealized array⁹. Instead, we use the programming language LAMBDAREF augmented with arrays. We first used this language in Section 2.3, where the TAPLMEMORYDIAGRAM notional machine represented all constructs of the language as well as the program's state as it ran (its memory): the store and name environment. Here we want to represent only arrays and values so the notional machine layer contains, besides the parking lot, essentially a sequence of statements equivalent to the occurrences of all terms in the program that manipulate arrays (an array allocation, array access, and assignment of a value to an array slot) as they happen when the program runs. This way we can ignore all other terms in the language and aspects of the program's memory as it runs. Besides the information present in the array-manipulating terms themselves, we need one more thing: to be able to uniquely identify each array (e.g. with its location, or address). We annotate each parking lot with the corresponding location (for example using an @ and the location identifier) which we use to identify the parking lot when we write to (or read from) its slots.

⁹ The representation of lists shown in Section 3.2 is not suitable to represent lists that contain lists.

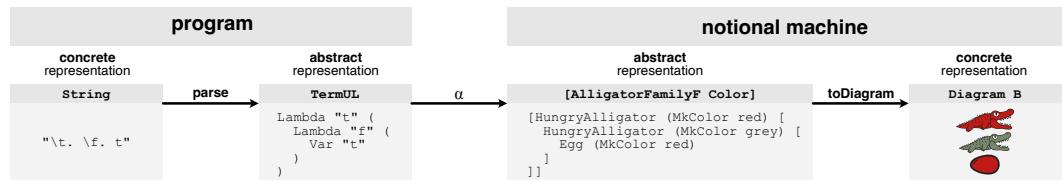


Fig. 20. Both program and notional machine have abstract and concrete representations.

We can then represent values of reference type using their locations. We could instead use arrows, like we have done in TAPLMEMORYDIAGRAM, but that would not work for ref's because here we are only representing arrays.

4 ABSTRACT VS. CONCRETE SYNTAX OF NOTIONAL MACHINES

When reasoning about a notional machine, it's important to distinguish between the data types that represents the notional machine (the information present in A_{NM} and B_{NM}) and how the notional machine is visualized. This difference is akin to the distinction between the concrete syntax and the abstract syntax of a language. Like a programming language, a notional machine has a concrete and an abstract syntax as well. We also refer to those as concrete and abstract representations of a notional machine. Notice that the concrete representation of a notional machine may not only be a diagram or image that can be depicted on paper but it could also be made of physical objects or enacted with students. In fact, many notional machines are ludic in nature or are built around a metaphor, so the concrete representation of a notional machine is very important.

Figure 20 shows the different layers at play here. On the programming language side, the *parse* function converts from the concrete to the abstract syntax of the language. The function α maps from language constructs to notional machine constructs. On the notional machine side, the function *toDiagram* maps from the abstract representation of the notional machine to its concrete representation, e.g., in the form of an actual diagram. In the case of ALLIGATOR, we use the *diagrams* library [Yates and Yorgey 2015; Yorgey 2012] to construct the concrete representation so *toDiagram* produces a value of type *Diagram B*, where the type parameter *B* (for Backend) determines the output format of the diagram (e.g. SVG). In fact, the depictions of Alligator Eggs shown here are generated by calls to our artifact that are embedded directly into the paper.

By decoupling the abstract from the concrete representation, a notional machine can have multiple concrete representations. Alligator Eggs, for example, also describes another concrete syntax that it calls "Schematic Form". This concrete representation is suitable for working with the notional machine using pencil and paper. Figure 19 shows the Church numeral two (the term $\lambda f. \lambda x. f (f x)$), represented using both concrete representations. In the schematic representation, colors are presented with variable names. An alligator is drawn as a line ending with a < for a mouth, and is preceded by a variable name corresponding to its color. An old alligator is drawn with a line without a mouth. An egg is drawn just with the variable name corresponding to its color.

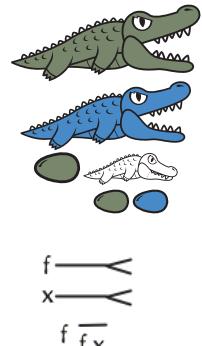


Fig. 19. Multiple concrete representations.

981 5 EVALUATION

982 The notional machines we presented not only exemplify how to use our framework to reason
 983 about notional machines but also were chosen to be representative of the design space of notional
 984 machines used in practice. To characterize this design space we analyzed the notional machines in
 985 the dataset collected by Fincher et al. [2020] and classified them according to three dimensions:
 986 form, focus, and language construct. For each dimension, we present the categories of the dimension
 987 and for each category we show the number of notional machines in that category, the percentage
 988 that number represents of the total, and the sections of the paper containing notional machines
 989 that fall into that category. The notional machines are often not precisely described so we often had
 990 to make assumptions about their characteristics, how they relate to an underlying programming
 991 language, and how they are used to teach programming concepts.

992 The form (Table 3) of a notional machine
 993 can be metaphorical (primarily inspired by
 994 and represented with real world objects) or
 995 diagrammatic (represented with diagrams).
 996 The distinction between the two is not always
 997 clear-cut, given that a notional machine
 998 may mix both forms and some real
 999 world objects can be represented diagrammatically.
 1000 Nevertheless, this distinction is
 1001 useful because metaphorical notional
 1002 machines may be more difficult to be made
 1003 sound, given the existing degrees of freedom and constraints of the real world objects they are
 1004 inspired by. We used our approach to reason about notional machines of the two forms.

Form	Num	Perc.	Covered
Metaphorical	22	56.41%	3.2 3.3 3.1
Diagrammatic	16	41.03%	2.1 2.2 2.3 2.4
Both	1	2.56%	-
Total	37	100.00%	-

Table 3. Notional machines in the dataset published by Fincher et al. [2020] classified according to their form.

1005 Most notional machines in the dataset focus (Table 4) on the runtime semantics (Evaluation)
 1006 of a programming language construct (or set of conceptually related constructs) so we further
 1007 break down these notional machines into the constructs they are primarily focused on (Table 5).
 1008 Some entries in the table refer to sets of related constructs. For example, the category Control Flow
 1009 encompasses constructs like loops and conditional statements, which primarily affect control flow.
 1010 Here the classification is also not clear-cut, not only because a notional machine may focus on
 1011 multiple constructs but also because some constructs are related to others. For example, notional
 1012 machines that focus on functions often (although not always) represent variables as well but
 1013 only the ones that solely (or primarily) focus on variables are classified as such. The category
 1014 Misc includes five notional machines each of which focuses on a different construct: String literal,
 1015 Procedure (side-effecting functions), Objects, Instructions (lower level operations), and one that
 1016 is not clear from the description. The notional machines we reasoned about using our approach
 1017 cover the majority of these dimensions.

1019 5.1 Expressing Complex Language Semantics

1020 Although the notional machines presented here as well as in the dataset by Fincher et al. [2020] focus
 1021 on aspects of program semantics that one may consider simple, the framework we presented can
 1022 be used to reason about more complex aspects of program semantics. An example is the conceptual
 1023 models to reason about Ownership Types in Rust by Crichton et al. [2023]. The authors present
 1024 two models: a dynamic and a static one. In our framework, each model can be seen as a notional
 1025 machine. The authors divide each model into a formal model (about which formal statements can
 1026 be made), which would correspond to the abstract representation of the notional machine, and an
 1027 informal model, which would correspond to the concrete representation of the notional machine.

Focus	Num	Perc.	Covered
Evaluation	32	82.05%	2.1 2.2 2.3 3.3 3.1
Type-checking	2	5.13%	2.4
Parsing	2	5.13%	no
Data Structure	2	5.13%	3.2
Logic Gates	1	2.56%	no
Total	37	100.00%	-

Table 4. Notional machines in the dataset published by Fincher et al. [2020] classified according to their focus.

Construct	Num	Perc.	Covered
References	8	20.51%	2.3
Functions	5	12.82%	2.1 2.2
Variables	4	10.26%	2.1 2.2 2.3
Arrays	4	10.26%	3.3
Methods	3	7.69%	no
Control Flow	2	5.13%	no
Expressions	1	2.56%	2.1 2.2
Misc	5	12.82%	no
Total	32	82.05%	-

Table 5. Notional machines that focus on evaluation broken down by the set of construct they focus on.

In the dynamic model, our PL layer would be the Rust language and our NM layer would be Miri. In the static model, our PL layer would be the polonius model of borrow checking and our NM layer would be the permissions model of borrow checking, introduced by the authors.

6 RELATED WORK

The term notional machine was coined by Du Boulay [1986] to refer to “the idealised model of the computer implied by the constructs of the programming language”. Therefore it restricts the use of notional machines as means to help understand the runtime behavior of a program or the dynamic semantics of a language. Fincher et al. [2020], a working group that included du Boulay, presented a thorough literature review and discussion of the term notional machine and established a broader definition as “pedagogic devices to assist the understanding of some aspect of programs or programming”, which includes uses of notional machines as means to help understand the static semantics of a language. The “Expressions as Trees” notional machine, for example, is used for both. We adopt here this broader view of notional machine.

Another related and important term is conceptual model. Fincher et al. [2020] states that a “notional machine is effectively a special kind of conceptual model.” That’s important because conceptual models, such as the Substitution Model and the Environment Model used in the SICP book (Structure and Interpretation of Computer Programs) [Abelson et al. 1996], and SICPJS [Abelson and Sussman 2022], for example, are well understood to be essential for reasoning about programs. Notional machines that are sound are indeed conceptual models. The concrete representation of the notional machine can be thought of as embodying the visualization of this conceptual model.

The idea of simulating or representing a program by means of another program is an old one, and was first studied in detail in the 1970s by Milner [1971] and Hoare [1972]. Many of our notional machines illustrate a reduction, stepping, or evaluation ‘aspect’ of a programming language. Wadler et al. [2020] has a nice description of how to relate such reduction systems with simulation, lock-step simulation, and bisimulation. The commutative diagram describing the desired property of a notional machine appears in many places in the literature, and is a basic concept in Category Theory. Closer to our application is its use as ‘promotion condition’ [Bird 1984; Wang et al. 2013].

Where computing education researchers capture program behavior through notional machines, programming language researchers instead use semantics [Krishnamurthi and Fisler 2019]. Our work can be seen as a rather standard approach to show the correctness of one kind of semantics of (part of) a programming language, most often the operational semantics, with respect to another

1079 semantics, often a reduction semantics. An example of such an approach has been described
 1080 by Clements et al. [2001], whose Elaboration Theorem describes a property that is very similar to
 1081 our soundness requirement. The lack of a formal approach to showing the soundness of notional
 1082 machines is also noted by Pollock et al. [2019], who develop a formal approach to specifying
 1083 correct program state visualization tools, based on an executable semantics of the programming
 1084 language formulated in the K framework [Roșu and Șerbănuță 2010]. In this paper we study a
 1085 broader collection of notional machines than just program state visualization tools, and we apply
 1086 our approach to study the soundness of notional machines.

1087 Computing educators practitioners use a diverse set of notional machines [Fincher et al. 2020].
 1088 Some notional machines form the basis of automated tools. The BlueJ IDE, which features promi-
 1089 nently in an introductory programming textbook [Kölling and Barnes 2017], includes a graphical
 1090 user interface to visualize objects, invoke methods, and inspect object state. PythonTutor [Guo
 1091 2013], an embeddable web-based program visualization system, is used by hundreds of thousands of
 1092 users to visualize the execution of code written in Python, Java, JavaScript, and other programming
 1093 languages. UUHistle [Sorva and Sirkia 2010], a “visual program simulation” system, takes a different
 1094 approach: instead of visualizing program executions, it requires students to perform the execution
 1095 steps in a constrained interactive environment. When developing such widely used tools, starting
 1096 from a sound notional machine is essential.

1097 Dickson et al. [2022] discuss the issues around developing and using a notional machine in class.
 1098 They note, amongst others, “that a notional machine must by definition be correct, but a student’s
 1099 mental model of the notional machine often is not”, and that “specifying a notional machine was
 1100 more difficult than we thought it would be”. Our work can help in developing a notional machine,
 1101 and pointing out flaws in it.

1102 7 CONCLUSIONS

1103 Notional machines are popular in computer science education, commonly used both by instructors
 1104 in their teaching practice as well as by researchers. Despite their popularity, there has been no
 1105 precise formal characterization of what should be the relationship between a notional machine and
 1106 the aspect of the programming language under its focus that would allow one to evaluate whether
 1107 or not they are consistent with each other. We, therefore, introduced a definition of soundness for
 1108 notional machines. The definition is based on simulation, a well-established notion widely used in
 1109 many areas of computer science. Demonstrating soundness essentially amounts to constructing a
 1110 commutative diagram relating the notional machine with the object of its focus.

1111 Using this definition, we showed how we can (1) systematically design notional machines that
 1112 are sound by construction, and (2) analyze existing notional machines to uncover inconsistencies
 1113 and suggest improvements.

1114 An important insight in the process is to distinguish between the concrete representation of
 1115 the notional machine (typically visual) and its abstract representation, about which we can make
 1116 formal statements. This distinction is akin to the distinction between the concrete and the abstract
 1117 syntaxes of a programming language.

1118 We then evaluated how applicable our approach is to notional machines actually used in practice.
 1119 Using a set of previously published notional machines used in practice, we characterize their design
 1120 space and show that the notional machines we analyzed using our approach are representative of
 1121 that design space.

1122 This work intends more generally to establish a framework to reason about notional machines,
 1123 placing the research on notional machines on firmer ground. As such, it can be used to address
 1124 challenges such as the design, analysis, and evaluation of notional machines, and the construction
 1125 of automated tools based on notional machines.

1128 DATA-AVAILABILITY STATEMENT

1129 The artifact implementing the programming languages, notional machines, and the relationship
 1130 between them as described in the paper is available at ANONYMOUS. The implementation of some
 1131 of the notional machines also includes a concrete representation.
 1132

1133 REFERENCES

- 1134 Harold Abelson and Gerald Jay Sussman. 2022. *Structure and Interpretation of Computer Programs: JavaScript Edition*. MIT
 1135 Press.
 1136 Harold Abelson, Gerald Jay Sussman, and Julie Sussman. 1996. *Structure and Interpretation of Computer Programs, (Second
 1137 Edition)* (second edition ed.). Vol. 33.
 1138 R. S. Bird. 1984. The Promotion and Accumulation Strategies in Transformational Programming. *ACM Transactions on
 Programming Languages and Systems* 6, 4 (Oct. 1984), 487–504. <https://doi.org/10.1145/1780.1781>
 1139 R. S. Bird. 1989. Algebraic Identities for Program Calculation. *Comput. J.* 32, 2 (April 1989), 122–126. <https://doi.org/10.1093/comjnl/32.2.122>
 1140 N.G. de Bruijn. 1972. Lambda Calculus Notation with Nameless Dummies, a Tool for Automatic Formula Manipulation,
 1141 with Application to the Church-Rosser Theorem. *Indagationes Mathematicae (Proceedings)* 75, 5 (Jan. 1972), 381–392.
[https://doi.org/10.1016/1385-7258\(72\)90034-0](https://doi.org/10.1016/1385-7258(72)90034-0)
 1142 Jerome Bruner. 1960. *The Process of Education*. Harvard University Press.
 1143 Luca Chiodini, Igor Moreno Santos, Andrea Gallidabino, Anya Tafliovich, André L. Santos, and Matthias Hauswirth. 2021. A
 1144 Curated Inventory of Programming Language Misconceptions. In *Proceedings of the 26th ACM Conference on Innovation
 1145 and Technology in Computer Science Education V. 1 (ITiCSE '21)*. Association for Computing Machinery, New York, NY,
 1146 USA, 380–386. <https://doi.org/10.1145/3430665.3456343>
 1147 Alonzo Church. 1936. An Unsolvable Problem of Elementary Number Theory. *American Journal of Mathematics* 58, 2 (1936),
 1148 345–363. <https://doi.org/10.2307/2371045> jstor:2371045
 1149 Alonzo Church. 1941. *The Calculi of Lambda-Conversion*. Number 6. Princeton University Press.
 1150 John Clements, Matthew Flatt, and Matthias Felleisen. 2001. Modeling an Algebraic Stepper. In *Proceedings of the 10th
 1151 European Symposium on Programming Languages and Systems (ESOP '01)*. Springer-Verlag, Berlin, Heidelberg, 320–334.
 1152 Patrick Cousot and Radhia Cousot. 1977. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs
 1153 by Construction or Approximation of Fixpoints. In *Proceedings of the 4th ACM SIGACT-SIGPLAN Symposium on Principles
 1154 of Programming Languages (POPL '77)*. Association for Computing Machinery, New York, NY, USA, 238–252. <https://doi.org/10.1145/512950.512973>
 1155 Will Crichton, Gavin Gray, and Shriram Krishnamurthi. 2023. A Grounded Conceptual Model for Ownership Types
 1156 in Rust. *Proceedings of the ACM on Programming Languages* 7, OOPSLA2 (Oct. 2023), 265:1224–265:1252. <https://doi.org/10.1145/3622841>
 1157 Andrew R. Dalton and William Krehling. 2010. Automated Construction of Memory Diagrams for Program Comprehension.
 1158 In *Proceedings of the 48th Annual Southeast Regional Conference (ACM SE '10)*. Association for Computing Machinery,
 1159 New York, NY, USA, 1–6. <https://doi.org/10.1145/1900008.1900040>
 1160 Paul E. Dickson, Tim Richards, and Brett A. Becker. 2022. Experiences Implementing and Utilizing a Notional Machine in
 1161 the Classroom. In *Proceedings of the 53rd ACM Technical Symposium V.1 on Computer Science Education (SIGCSE 2022)*.
 1162 Association for Computing Machinery, New York, NY, USA, 850–856. <https://doi.org/10.1145/3478431.3499320>
 1163 Toby Dragon and Paul E. Dickson. 2016. Memory Diagrams: A Consistant Approach Across Concepts and Languages.
 1164 In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*. Association for
 1165 Computing Machinery, New York, NY, USA, 546–551. <https://doi.org/10.1145/2839509.2844607>
 1166 Benedict Du Boulay. 1986. Some Difficulties of Learning to Program. *Journal of Educational Computing Research* 2, 1 (Feb.
 1167 1986), 57–73. <https://doi.org/10.2190/3LFX-9RFF-67T8-UVK9> arXiv:<https://doi.org/10.2190/3LFX-9RFF-67T8-UVK9>
 1168 Benedict Du Boulay and Tim O'Shea. 1976. *How to Work the LOGO Machine*. Technical Report 4. Department of Artificial
 Intelligence, University of Edinburgh.
 1169 Richard Feynman. 1985. *Surely You're Joking, Mr. Feynman!* W. W. Norton.
 1170 Sally Fincher, Johan Jeuring, Craig S. Miller, Peter Donaldson, Benedict du Boulay, Matthias Hauswirth, Arto Hellas,
 1171 Felienne Hermans, Colleen Lewis, Andreas Mühlung, Janice L. Pearce, and Andrew Petersen. 2020. Notional Machines
 1172 in Computing Education: The Education of Attention. In *Proceedings of the Working Group Reports on Innovation and
 Technology in Computer Science Education (ITiCSE-WGR '20)*. Association for Computing Machinery, New York, NY, USA,
 21–50. <https://doi.org/10.1145/3437800.3439202>
 1173 Jeremy Gibbons. 2002. Calculating Functional Programs. In *Algebraic and Coalgebraic Methods in the Mathematics of Program
 1174 Construction: International Summer School and Workshop Oxford, UK, April 10–14, 2000 Revised Lectures*, Roland Backhouse,
 1175 Roy Crole, and Jeremy Gibbons (Eds.). Springer, Berlin, Heidelberg, 151–203. https://doi.org/10.1007/3-540-47797-7_5

Sound Notional Machines

- 1177 Philip J. Guo. 2013. Online Python Tutor: Embeddable Web-Based Program Visualization for Cs Education. In *Proceeding of
1178 the 44th ACM Technical Symposium on Computer Science Education - SIGCSE '13*. ACM Press, Denver, Colorado, USA, 579.
1179 <https://doi.org/10.1145/2445196.2445368>
- 1180 C. A. Hoare. 1972. Proof of Correctness of Data Representations. *Acta Informatica* 1, 4 (Dec. 1972), 271–281. <https://doi.org/10.1007/BF00289507>
- 1181 Mark A. Holliday and David Luginbuhl. 2004. CS1 Assessment Using Memory Diagrams. In *Proceedings of the 35th SIGCSE
1182 Technical Symposium on Computer Science Education (SIGCSE '04)*. Association for Computing Machinery, New York, NY,
1183 USA, 200–204. <https://doi.org/10.1145/971300.971373>
- 1184 Michael Kölling and David Barnes. 2017. *Objects First With Java: A Practical Introduction Using BlueJ* (6th ed.). Pearson.
- 1185 Shriram Krishnamurthi and Kathi Fisler. 2019. Programming Paradigms and Beyond. In *The Cambridge Handbook of
1186 Computing Education Research*, Anthony V. Robins and Sally A. Fincher (Eds.). Cambridge University Press, Cambridge,
1187 377–413. <https://doi.org/10.1017/9781108654555.014>
- 1188 Guillaume Marceau, Kathi Fisler, and Shriram Krishnamurthi. 2011. Do Values Grow on Trees?: Expression Integrity in
1189 Functional Programming. In *Proceedings of the Seventh International Workshop on Computing Education Research - ICER
'11*. ACM Press, Providence, Rhode Island, USA, 39. <https://doi.org/10.1145/2016911.2016921>
- 1190 Robin Milner. 1971. An Algebraic Definition of Simulation between Programs. In *Proceedings of the 2nd International Joint
Conference on Artificial Intelligence (IJCAI'71)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 481–489.
- 1191 Benjamin C. Pierce. 2002. *Types and Programming Languages*. MIT Press, Cambridge, Mass.
- 1192 Josh Pollock, Jared Roesch, Doug Woos, and Zachary Tatlock. 2019. Theia: Automatically Generating Correct Program
1193 State Visualizations. In *Proceedings of the 2019 ACM SIGPLAN Symposium on SPLASH-E (SPLASH-E 2019)*. Association for
1194 Computing Machinery, New York, NY, USA, 46–56. <https://doi.org/10.1145/3358711.3361625>
- 1195 Grigore Roşu and Traian Florin Ţerbănuţă. 2010. An Overview of the K Semantic Framework. *The Journal of Logic and
Algebraic Programming* 79, 6 (Aug. 2010), 397–434. <https://doi.org/10.1016/j.jlap.2010.03.012>
- 1196 Juha Sorva, Jan Lönnberg, and Lauri Malmi. 2013. Students' Ways of Experiencing Visual Program Simulation. *Computer
1197 Science Education* 23, 3 (Sept. 2013), 207–238. <https://doi.org/10.1080/08993408.2013.807962>
- 1198 Juha Sorva and Teemu Sirkiä. 2010. UUhistle: A Software Tool for Visual Program Simulation. In *Proceedings of the 10th Koli
1199 Calling International Conference on Computing Education Research - Koli Calling '10*. ACM Press, Berlin, Germany, 49–54.
<https://doi.org/10.1145/1930464.1930471>
- 1200 Philip Wadler, Wen Kokke, and Jeremy G. Siek. 2020. *Programming Language Foundations in Agda*.
- 1201 Meng Wang, Jeremy Gibbons, Kazutaka Matsuda, and Zhenjiang Hu. 2013. Refactoring Pattern Matching. *Science of
1202 Computer Programming* 78, 11 (Nov. 2013), 2216–2242. <https://doi.org/10.1016/j.scico.2012.07.014>
- 1203 Ryan Yates and Brent A. Yorgey. 2015. Diagrams: A Functional EDSL for Vector Graphics. In *Proceedings of the 3rd ACM
1204 SIGPLAN International Workshop on Functional Art, Music, Modelling and Design (FARM 2015)*. Association for Computing
1205 Machinery, New York, NY, USA, 4–5. <https://doi.org/10.1145/2808083.2808085>
- 1206 Brent A. Yorgey. 2012. Monoids: Theme and Variations (Functional Pearl). *ACM SIGPLAN Notices* 47, 12 (Sept. 2012), 105–116.
<https://doi.org/10.1145/2430532.2364520>
- 1207
- 1208
- 1209
- 1210
- 1211
- 1212
- 1213
- 1214
- 1215
- 1216
- 1217
- 1218
- 1219
- 1220
- 1221
- 1222
- 1223
- 1224
- 1225

1226 **A PROGRAMMING LANGUAGE DEFINITIONS**

1227 The programming languages used throughout the paper mostly follows the presentation in the
 1228 book Types and Programming Languages by Pierce [2002] with minor changes. In particular, italics
 1229 are used for metavariables and the axioms in the reduction (evaluation) rules and typing rules are
 1230 shown with explicitly empty premises.
 1231

1232 **A.1 UntypedLambda**

1233 Figure 21 shows the syntax and evaluation rules for the untyped lambda calculus by Church [1936,
 1234 1941], that we have referred to as UNTYPEDLAMBDA. This language is used in Sections 2.1, 2.2,
 1235 and 3.1 .
 1236

1237 **Syntax**

1238

$t ::=$ x $\lambda x.t$ $ t t$	terms: variable abstraction application
--	--

1239

1240

1241

1242

1243

1244

1245

Evaluation

$$\begin{array}{c}
 \frac{}{(\lambda x.t_{12}) v_2 \longrightarrow [x \mapsto v_2]t_{12}} \text{E-APPABS} \\
 \frac{t_1 \longrightarrow t'_1}{t_1 t_2 \longrightarrow t'_1 t_2} \text{E-APP1} \\
 \frac{t_2 \longrightarrow t'_2}{v_1 t_2 \longrightarrow v_1 t'_2} \text{E-APP2}
 \end{array}$$

1246 Fig. 21. The untyped lambda calculus (UNTYPEDLAMBDA).

1247 **A.2 TypedArith**

1248 We define here the language TYPEDARITH, used in Section 2.4. Figure 22 shows its syntax and
 1249 evaluation (reduction) rules and Figure 23 shows its typing rules. The appeal of using this language
 1250 to present a notional machine focused on the types is its simplicity. Terms don't require type
 1251 annotations and the typing rules don't require a type environment. In fact, Pierce uses it as the
 1252 simplest example of a typed language when introducing type safety.
 1253

1254 **A.3 TypedLambdaRef**

1255 In Section 2.3, we showed the language TYPEDLAMBDAREF, used to design a notional machine
 1256 that focuses on references. This language is composed of the simply-typed lambda calculus, the
 1257 TYPEDARITH language, tuples, the *Unit* type, sequencing, and references. Our goal is again simplicity
 1258 and this is the simplest language we need for the examples in the book that use the diagram. Figure 24
 1259 shows its syntax and evaluation (reduction) rules. We show only the reduction rules for sequencing,
 1260 references, and tuples because the rules for the rest of the language are similar to what we showed
 1261 before, except for the store then needs to be threaded through all the rules. Although that is a typed
 1262 language, we don't present its typing rules because the notional machine in Section 2.3 is focused
 1263 only on its runtime behavior and not its types.
 1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

Sound Notional Machines

Syntax	Evaluation
1275 $t ::=$	$\frac{}{\text{if true then } t_2 \text{ else } t_3 \longrightarrow t_2} \text{E-IFTRUE}$
1276	$\frac{}{\text{if false then } t_2 \text{ else } t_3 \longrightarrow t_3} \text{E-IFFALSE}$
1277	$\frac{t_1 \longrightarrow t'_1}{\text{if } t_1 \text{ then } t_2 \text{ else } t_3 \longrightarrow \text{if } t'_1 \text{ then } t_2 \text{ else } t_3} \text{E-IF}$
1278	$\frac{t_1 \longrightarrow t'_1}{\text{succ } t_1 \longrightarrow \text{succ } t'_1} \text{E-SUCC}$
1279	$\frac{}{\text{pred } 0 \longrightarrow 0} \text{E-PREDZERO}$
1280	$\frac{\text{pred } (\text{succ } nv_1) \longrightarrow nv_1}{\text{pred } t_1 \longrightarrow \text{pred } t'_1} \text{E-PREDSUCC}$
1281	$\frac{t_1 \longrightarrow t'_1}{\text{pred } t_1 \longrightarrow \text{pred } t'_1} \text{E-PRED}$
1282	$\frac{}{\text{iszero } 0 \longrightarrow \text{true}} \text{E-ISZEROZERO}$
1283	$\frac{\text{iszero } (\text{succ } nv_1) \longrightarrow \text{false}}{\text{iszero } t_1 \longrightarrow \text{iszero } t'_1} \text{E-ISZEROSUCC}$
1284	
1285	
1286	
1287	
1288	
1289	
1290	
1291	
1292	
1293	
1294	
1295	
1296	
1297	
1298	
1299	
1300	
1301	
1302	
1303	
1304	
1305	
1306	
1307	
1308	
1309	
1310	
1311	
1312	
1313	
1314	
1315	
1316	
1317	
1318	
1319	
1320	
1321	
1322	
1323	

Fig. 22. Syntax and reduction rules of the TYPEDARITH language.

1324	Syntax	Typing rules
1325		
1326		$\frac{}{\text{true} : \text{Bool}}$ T-TRUE
1327		$\frac{}{\text{false} : \text{Bool}}$ T-FALSE
1328		$\frac{t_1 : \text{Bool} \quad t_2 : T \quad t_3 : T}{\text{if } t_1 \text{ then } t_2 \text{ else } t_3 : T}$ T-IF
1329		
1330		
1331		
1332	$T ::=$ types: Bool type of booleans Nat type of natural numbers	$\frac{}{0 : \text{Nat}}$ T-ZERO
1333		$\frac{t_1 : \text{Nat}}{\text{succ } t_1 : \text{Nat}}$ T-SUCC
1334		$\frac{t_1 : \text{Nat}}{\text{pred } t_1 : \text{Nat}}$ T-PRED
1335		
1336		
1337		
1338		
1339		$\frac{t_1 : \text{Nat}}{\text{iszero } t_1 : \text{Bool}}$ T-ISZERO
1340		
1341		
1342	Fig. 23. Syntax of types and typing rules of the TYPEDARITH language.	
1343		
1344		
1345		
1346		
1347		
1348		
1349		
1350		
1351		
1352		
1353		
1354		
1355		
1356		
1357		
1358		
1359		
1360		
1361		
1362		
1363		
1364		
1365		
1366		
1367		
1368		
1369		
1370		
1371		
1372		

Sound Notional Machines

1373	Syntax	Evaluation
1374	$t ::=$ terms:	
1375	x variable	
1376	$\lambda x : T. t$ abstraction	
1377	$t t$ application	
1378	$\mid \text{true}$ boolean true	
1379	$\mid \text{false}$ boolean false	
1380	$\mid 0$ zero	
1381	$\mid \text{succ } t$ successor	
1382	$\mid \text{pred } t$ predecessor	
1383	$\mid \text{iszero } t$ zero test	
1384	$\mid \text{unit}$ unit constant	
1385	$\mid t; t$ sequence	
1386	$\mid \text{ref } t$ reference creation	
1387	$\mid !t$ dereference	
1388	$\mid t := t$ assignment	
1389	$\mid l$ location	
1390	$\mid \{t_i\}_{i \in 1..n}$ tuple	
1391	$\mid t.i$ projection	
1392	$v ::=$ values:	
1393	$\lambda x : T. t$	
1394	$\mid \text{true}$	
1395	$\mid \text{false}$	
1396	$\mid 0$	
1397	$\mid \text{succ } v$	
1398	$\mid \text{unit}$	
1399	$\mid l$	
1400	$\mid \{v_i\}_{i \in 1..n}$	
1401	$T ::=$ types:	
1402	$T \rightarrow T$ function type	
1403	$\mid \text{Bool}$ boolean type	
1404	$\mid \text{Nat}$ natural number type	
1405	$\mid \text{Unit}$ unit type	
1406	$\mid \text{Ref } T$ reference type	
1407	$\mid \{T_i\}_{i \in 1..n}$ tuple type	
1408	$\mu ::=$ store:	
1409	\emptyset empty store	
1410	$\mid \mu, l \mapsto v$ location binding	
1411		
1412		Fig. 24. TYPEDLAMBDAREF : Syntax and Evaluation
1413		
1414		
1415		
1416		
1417		
1418		
1419		
1420		
1421		
		$\frac{t_1 \mu \longrightarrow t'_1 \mu'}{t_1; t_2 \mu \longrightarrow t'_1; t_2 \mu'} \text{E-SEQ}$
		$\frac{}{\text{unit}; t_2 \mu \longrightarrow t_2 \mu} \text{E-SEQNEXT}$
		$\frac{l \notin \text{dom}(\mu)}{\text{ref } v_1 \mu \longrightarrow l (\mu, l \mapsto v_1)} \text{E-REFV}$
		$\frac{t_1 \mu \longrightarrow t'_1 \mu'}{\text{ref } t_1 \mu \longrightarrow \text{ref } t'_1 \mu'} \text{E-REF}$
		$\frac{\mu(l) = v}{!l \mu \longrightarrow v \mu} \text{E-DEREFLOC}$
		$\frac{t_1 \mu \longrightarrow t'_1 \mu'}{!t_1 \mu \longrightarrow !t'_1 \mu'} \text{E-DEREF}$
		$\frac{l := v_2 \mu \longrightarrow \text{unit} [l \mapsto v_2] \mu}{l := v_2 \mu \longrightarrow \text{unit} [l \mapsto v_2] \mu} \text{E-ASSIGN}$
		$\frac{t_1 \mu \longrightarrow t'_1 \mu'}{t_1 := t_2 \mu \longrightarrow t'_1 := t_2 \mu'} \text{E-ASSIGN1}$
		$\frac{t_2 \mu \longrightarrow t'_2 \mu'}{v_1 := t_2 \mu \longrightarrow v_1 := t'_2 \mu'} \text{E-ASSIGN2}$
		$\frac{\{v_i\}_{i \in 1..n}.j \mu \longrightarrow v_j \mu}{\{v_i\}_{i \in 1..n}.j \mu \longrightarrow v_j \mu} \text{E-PROJTUPLE}$
		$\frac{t_1 \mu \longrightarrow t'_1 \mu'}{t_1.i \mu \longrightarrow t'_1.i \mu'} \text{E-PROJ}$
		$\frac{t_j \mu \longrightarrow t'_j \mu'}{\{v_i\}_{i \in 1..j-1}, t_j, t_k^{k \in j+1..n} \mu \longrightarrow \{v_i\}_{i \in 1..j-1}, t'_j, t_k^{k \in j+1..n} \mu'} \text{E-TUPLE}$