Mechanized Proofs of Adversarial Complexity and Application to Universal Composability
Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, Pierre-yves Strub

To cite this version:

HAL Id: hal-03469015
https://hal.archives-ouvertes.fr/hal-03469015
Submitted on 7 Dec 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Mechanized Proofs of Adversarial Complexity and Application to Universal Composability

(long version)

Manuel Barbosa
University of Porto (FCUP) & INESC TEC
Porto, Portugal
mbb@fc.up.pt

Gilles Barthe
MPI-SP & IMDEA Software Institute
Bochum, Germany
gjbarthe@gmail.com

Benjamin Grégoire
Inria
Sophia Antipolis, France
benjamin.gregoire@inria.fr

Adrien Koutsos
Inria
Paris, France
adrien.koutsos@inria.fr

Pierre-Yves Strub
École Polytechnique
Palaiseau, France
pierre-yves@strub.nu

ABSTRACT

In this paper we enhance the EasyCrypt proof assistant to reason about computational complexity of adversaries. The key technical tool is a Hoare logic for reasoning about computational complexity (execution time and oracle calls) of adversarial computations. Our Hoare logic is built on top of the module system used by EasyCrypt for modeling adversaries. We prove that our logic is sound w.r.t. the semantics of EasyCrypt programs — we also provide full semantics for the EasyCrypt module system, which was previously lacking.

We showcase (for the first time in EasyCrypt and in other computer-aided cryptographic tools) how our approach can express precise relationships between the probability of adversarial success and their execution time. In particular, we can quantify existentially over adversaries in a complexity class, and express general composition statements in simulation-based frameworks. Moreover, such statements can be composed to derive standard concrete security bounds for cryptographic constructions whose security is proved in a modular way. As a main benefit of our approach, we revisit security proofs of some well-known cryptographic constructions and we present a new formalization of Universal Composability (UC).

KEYWORDS

Verification of Cryptographic Primitives, Formal Methods, Interactive Proof System, Complexity Analysis

1 INTRODUCTION

Cryptographic designs are typically supported by mathematical proofs of security. Unfortunately, these proofs are error-prone and subtle flaws can go unnoticed for many years, in spite of careful and extensive scrutiny from experts. Therefore, it is desirable that cryptographic proofs are formally verified using computer-aided tools [23]. Over the last decades, many formalisms and tools have been developed for mechanizing cryptographic proofs [4]. In this paper we focus on the EasyCrypt proof assistant [6, 9], which has been used to prove security of a diverse set of cryptographic constructions in the computational model of cryptography [2, 3]. In this setting, cryptographic designs and their corresponding security notions are modeled as probabilistic programs. Moreover, security proofs provide an upper bound on the probability that an adversary breaks a cryptographic design, often assuming that the attacker has limited resources that are insufficient to solve a mathematical problem. While EasyCrypt excels at quantifying the probability of adversarial success, it lacks support for keeping track of the complexity of adversarial computations. This is a limitation that is common to other tools in computer-aided cryptography, and it means that manual inspection is required to check that the formalized claims refer to probabilistic programs that fall in the correct complexity classes. While this may be acceptable for very simple constructions, for more intricate proofs it may be difficult to interpret what a proved claim means in the cryptographic sense; in particular, existing computer-aided tools cannot fully express the subtleties that arise in compositional approaches such as Universal Composability [16]. This is an important limitation, as compositional approaches are ideally suited for proving security of complex cryptographic designs involving many layers of simpler building blocks. This work overcomes this limitation and showcases the benefits of reasoning about computational complexity in EasyCrypt, through three broad contributions.

Formal verification of complexity statements. We define a formal system for specifying and proving complexity claims. Our formal system is based on an expressive module system, which enriches the existing EasyCrypt module system with declarations of memory footprints (specifying what is read and written) and cost (specifying which oracles can be called and how often). This richer module system is the basis for modeling the cost of a program as a tuple. The first component of the tuple represents the intrinsic cost of the program, i.e. its cost in a model where oracle and adversary calls are free. The remaining components of the tuple represent the number of calls to oracles and adversaries. This style of modeling is compatible with cryptographic practice and supports reasoning compositionally about (open) programs.

Our formal system is built on top of the module system and takes the form of a Hoare logic for proving complexity claims that upper bound the cost of expressions and commands. Furthermore, an embedding of the formal system into a higher-order logic provides support for reductionist statements relating adversarial advantage...
and execution cost, for instance:

$$\forall A, B. \text{adv}_S(A) \leq \text{adv}_B(B) + \epsilon \land \text{cost}(B) \leq \text{cost}(A) + \delta$$

where typically $\epsilon$ and $\delta$ are polynomial expressions in the number of oracle calls. The above statement says that every adversary $A$ can be turned into an adversary $B$, with sensibly equivalent resources, such that the advantage of $A$ against a cryptographic scheme $S$ is upper bounded by the advantage of $B$ against a hardness assumption $H$. Note that the statement is only meaningful because the cost of $B$ is conditioned on the cost of $A$, as the advantage of an unbounded adversary is typically 1. The ability to prove and instantiate such $\forall\exists$-statements is essential for capturing compositional reasoning principles.

We show correctness of our formal system w.r.t. an interpretation of programs. Our interpretation provides the first complete semantics for the EasyCrypt module system, which was previously lacking. This semantics is of independent interest and could be used to prove soundness of the two program logics supported by EasyCrypt: a Relational Hoare Logic [8] and a Union Bound logic [7].

**Implementation in the EasyCrypt proof assistant.** We have implemented our formal system as an extension to the EasyCrypt proof assistant, which provides mechanisms for declaring the cost of operators and for helping users derive the cost of expressions and programs. Our implementation brings several contributions of independent interest, including an improvement of the memory restriction system of EasyCrypt, and a library and automation support to reason about extended integers that are used for reasoning about cost. For the latter we follow [31] and reduce formulae about extended integers to integer formulae that can be sent to SMT solvers. Another key step is to embed our Hoare logic for cost into the ambient higher-order logic—similar to what is done for the other program logics of EasyCrypt. This allows us to combine judgments from different program logics, and it enhances the expressiveness of the approach. Implementation-wise, this extension required to add or rewrite around 8 kLoC of EasyCrypt.

The implementation and examples (including those of the paper as well as classic examples from the EasyCrypt distribution, including Bellare and Rogaway BR93 Encryption, Hashed ElGamal encryption, Cramer-Shoup encryption, and hybrid arguments) are open source [20].

**Case study: Universal Composability.** Universal Composability [15, 17] (UC) is a popular framework for reasoning about cryptographic systems. Its central notion, called UC-emulation, formalizes when a protocol $\pi_1$ can safely replace a protocol $\pi_2$. Informally, UC-emulation imposes that there exists a simulator $S$ capable of fooling any environment $Z$ by presenting to it a view that is fully consistent with an interaction with $\pi_1$, while it is in fact interacting with $S(\pi_2)$. This intuition, however, must be formalized with tight control over the capabilities of the environment and the simulator.

If this were not the case, the definition would make no sense: existential quantification over unrestricted simulators is too weak (it is crucial for the compositional security semantics that simulators use comparable resources to real-world attackers), whereas universal quantification over unrestricted environments results in a definition that is too strong to be satisfied [15, 16]. Moreover, when writing proofs in the UC setting, it is often necessary to consider the joint resources of a sub-part of a complex system that involves a mixture of concrete probabilistic algorithms and abstract adversarial entities, when they are grouped together to build an attacker for a reductionistic proof. In these cases, it is very hard to determine by inspection whether the constructed adversaries are within the complexity classes for which the underlying computational assumptions are assumed to hold. Therefore, tool support for complexity claims is of particular importance with UC — conversely, UC is a particularly challenging example for complexity claims.

Using our enriched implementation of EasyCrypt, we develop a new fully mechanized formalization of UC—in contrast to [19], which chooses to follow closely the classic execution model for UC, our mechanization adopts a more EasyCrypt-friendly approach that is closer to the simplified version of UC proposed by Canetti, Cohen and Lindell in [18]; this is further discussed in Section 5. Our mechanization covers the core notions of UC, the classic composition lemmas, transitivity and composability, which respectively state that UC-emulation (as a binary relation between cryptographic systems) is closed under transitivity and arbitrary adversarial contexts. As an illustrative application of our approach we revisit the example used in [19], where modular proofs for Diffie-Hellman key exchange and encryption over ideal authenticated channels are composed to construct a UC secure channel.

**Discussion.** The possibility to quantify over adversary using complexity claims introduces conceptual simplifications in layered proofs by i. supporting compositional reasoning and ii. avoiding the use of explicit cost accounting modeling. The downside is that it also introduces some additional burden on users, who now must prove complexity claims. However, we note that our extension does not invalidate existing Easycrypt developments: complexity claims are optional, existing proofs have been left unchanged, and their type-checking remains as fast as before. Furthermore, it is possible to layer the complexity claims on top of standard EasyCrypt proofs that do not capture the complexity aspects — in effect, this is what we did in our example. We have also provided rudimentary support to automate proofs of complexity claims, and could enhance this support even further by adopting ideas from cost analysis. We think that the current tool is significantly more usable and scalable than prior versions without support for complexity reasoning.

To make this claim more concrete, let us consider the implications of refactoring an existing EasyCrypt development and extend it to take advantage of cost analysis for both dealing with query counts and to include complexity claims. Removing the layer of modular wrapping that explicitly keeps track of query counts leads to more readable code, and has essentially no impact on the proofs. However, when it comes to complexity claims, new specifications and proof scripts must be added to the development. The new specifications consist of the description of the cost model and the declarations of the types of the various algorithms, which include explicit cost expressions. The additional proof effort consists of applying our logic to prove complexity claims and discharging the relevant side-conditions. As a coarse metric on the additional proof and specification efforts required, we consider the ratio of the number of lines of codes related to the cost analysis over the total number of lines. For the example presented in the next section, this ratio is $117/495$. For the Universal Composability example, the
given an encryption of (PKE) scheme proposed by [11] (BR93) that uses a one-way trapdoor.

To illustrate our approach we will use a public-key encryption as functor parameters) have a cost of 0. This style of modeling is its intrinsic cost, i.e. its cost assuming that oracle calls (modeled

the second component is an upper bound on the number of times

m

declaration is necessary. The module type for (chosen-plaintext)

Scheme (H: RO) = {

module type Adv (H: RO) = {

module type Inv (H: RO) (A:Adv) = {

module type RO = {

proc o (r:rand) : plaintext comp[|intr : t_o|].

proc kg() : pkey * skkey

proc enc(pk,pkey, m:plaintext) : ciphertext

proc dec(sk:skkey, c:plaintext) : plaintext option.

module type Scheme (H: RO) = {

module type (Inv: INV) (H: RO) (A:Adv) = {

var qs : rand list

module QH = {

proc s(x:rand) = { qs ← x; qs; r ← H.o(x); return r; }

proc invert(pk:pkey,y:rand): rand = |

qs = []; intr,

(m_k,m_l) ← A(QH).choose(pk);

h ← A(QH).guess(y || h);

t ← head qs; if (if pk t + y return r; qs ← tail qs; }

}}.

Figure 1: Inverter for trapdoor permutation.

ratio is 270/2300 for the concrete protocol and 791/1775 for the
general composition theorems. We also note that there is a large
body of work on automated complexity analysis, as mentioned in
the related work section, which might reduce this overhead.

2 WARM UP EXAMPLE: PKE FROM A
ONE-WAY TRAPDOOR PERMUTATION

To illustrate our approach we will use a public-key encryption
(PKE) scheme proposed by [11] (BR93) that uses a one-way trapdoor
permutation and a hash function modeled as a random oracle (RO).
Intuitively, the RO is used to convert the message into a random
input for the trapdoor permutation so as to allow a reduction to
the one-wayness property. This proof strategy is used in BR93
and many other schemes, including OAEP [11]. Figure 1 shows the
code of an inverter for the trapdoor permutation that is constructed
from an attacker against the encryption scheme.1 This inverter simulates
the single random oracle used by the encryption scheme for the
attacker and recovers the pre-image to y with essentially the same
probability as the attacker breaks the encryption scheme.

We first define module types for random oracles RO, schemes
Schemes, and adversaries Adv. The module type for random oracles
declares a single procedure o with cost ≤ t_o. The module type for
schemes declares three procedures for key generation, encryption,
and decryption, and is parameterized by a random oracle R. No cost
declaration is necessary. The module type for (chosen-plaintext)
adversaries declares two procedures: choose for choosing two plain-
texts m_0 and m_1, and guess for guessing the (uniformly sampled) bit
b given an encryption of m. The cost of these procedures is a pair:
the second component is an upper bound on the number of times
it can call the random oracle, and the first is an upper bound on
its intrinsic cost, i.e. its cost assuming that oracle calls (modeled
as functor parameters) have a cost of 0. This style of modeling is

1We use the following notation: $\xrightarrow{\$}$ denotes a random sampling; $|$ is bit-string concate-
nation; [] is the empty list; a + 1 appends a to the list l.

2Notice that the condition of the loop is executed at most $k_c + k_g$ time.

routine, and adversaries

Adv. The module type for random oracles
declares a single procedure o with cost ≤ t_o. The module type for
schemes declares three procedures for key generation, encryption,
and decryption, and is parameterized by a random oracle R. No cost
declaration is necessary. The module type for (chosen-plaintext)
adversaries declares two procedures: choose for choosing two plain-
texts m_0 and m_1, and guess for guessing the (uniformly sampled) bit
b given an encryption of m. The cost of these procedures is a pair:
the second component is an upper bound on the number of times
it can call the random oracle, and the first is an upper bound on
its intrinsic cost, i.e. its cost assuming that oracle calls (modeled
as functor parameters) have a cost of 0. This style of modeling is

routinely used in cryptography and is better suited to reason about
open code. This cost model is also more fine-grained than counting
the total cost of the procedure including the cost of the oracles, as
we have a guarantee on the number of time oracles are called.

Next, we define the inverter Inv for the one-way trapdoor
permutation. It runs the adversary A, keeping track of all the calls that
A makes to $H$ in a list qs (using the sub-module QH), and then searches
in the list qs for a pre-image of $y$ under $f_k$. Search is done through
a while loop, which we write in a slightly beautified syntax. This
inverter can be used to state the following reductionist security
theorem relating the advantage and execution cost of an adversary
against chosen-plaintext security of the PKE with the advantage of
the inverter against one-wayness.

Theorem 2.1 (Security of BR93). Let $t_f$ represent the cost of
applying the one-way function $f$ and $t_o$ denote the cost of $H.o$, i.e. the
implementation of a query to a lazily sampled random oracle. Fix the
type for adversaries $\tau_A$ such that:

$\exists \tau_A \text{ such that:}$

and fix $t_f$ such that:

$\exists \tau_f \text{ such that:}$

Then, $\forall \tau_A \in \tau_R, \exists \tau_f \in \tau_f, \text{adv}^{\text{BR93}}_{\text{IND-CPA}}(\tau_A) \leq \text{adv}^{\text{OW}}_\text{f}(\tau)$. Here, IND-CPA refers to the standard notion of ciphertext indis-
tinguishability under chosen-plaintext attacks for PKE, where the
adversary is given the public key and asked to guess which of two
messages of its choice has been encrypted in a challenge ciphertext;
OW refers to the standard one-wayness definition for trapdoor
permutations, where the attacker is given the public parameters
and the image of a random pre-image, which it must invert. In the
former, advantage is the absolute bias of the adversary’s boolean
output w.r.t. 1/2; in the latter, advantage is the probability of suc-
cessful inversion.

We prove the statement by providing Inv($\tau_A$) as a witness for the
existential quantification, which creates two sub-goals. The first
sub-goal establishes the advantage bound, which we prove using
relational Hoare logic. The second sub-goal establishes that our
inverter satisfies the required cost restrictions, and is proved using
our Hoare logic for complexity. We declare the type of Inv as:

and so we first must establish that Inv belongs to this functor type. It
is easy to show that $A\cdot\text{choose}$ and $A\cdot\text{guess}$ are called exactly once, and
that $H.o$ is called at most $k_c + k_g$ times. So we turn to the intrinsic
complexity of Inv. The key step for this proof is to show that the loop
does at most $k_c + k_g$ iterations. We use the length of qs as a variant:
the length of the list is initially 0, and incremented by 1 by each call
to the random oracle, therefore its length at the start of the loop is at
most $k_c + k_g$. Moreover, the length decreases by 1 at each iteration,
so we are done. The remaining reasoning is standard, using the
cost of each operator—fixed by choice in this particular example to
1, except for the operator $f$. Our modeling of cost enforces useful
invariants that simplify reasoning. For instance, proving upper bounds on the execution cost of \( \text{inv} \) requires proving an upper bound on the number of iterations of the loop, and therefore on the length of \( q_s \) upon entering the loop. We derive the complexity statement in the theorem, which shows only the intrinsic cost of \( \text{inv} \), by instantiating the complexity type of \( \text{inv} \) with the cost of its module parameter \( A \). This illustrates how our finer-grained notion of cost is useful for compositional reasoning.

Comparison with EasyCrypt. Our formalization follows the same pattern as the BR93 formalization from the EasyCrypt library. However, the classic module system of EasyCrypt only tracks read-and-write effects and lacks first-class support for bounding the number of calls and for reasoning about the complexity of programs. To compensate for this first point, classic EasyCrypt proofs use wrappers to explicitly count the number of calls and to return dummy answers when the number of adversarial calls to an oracle exceeds a threshold. The use of wrappers suffices for reasoning about adversarial advantage. However, no similar solution can be used for reasoning about the computational cost of adversaries.

Therefore, the BR93 formalization from the EasyCrypt library makes use of the explicit definition of \( I \), and users must analyze the complexity of \( I \) outside the tool. As a result, machine-checked security statements are partial (complexity analysis is missing), cluttered (existential quantification is replaced by explicit witnesses), and compositional reasoning is hard (existential quantification over module types cannot be used meaningfully).

## 3 Enriched EasyCrypt Module System

We present a formalization of our extended module system for EasyCrypt. It is based on EasyCrypt current imperative probabilistic programming language and module system, which we enrich to track the read-and-write memory footprint and complexity cost of module components through module restrictions. These module restrictions are checked through a type system: memory footprint and compositional reasoning is hard (existential quantification over module types cannot be used meaningfully).

### 3.1 Syntax of Programs and Modules

The syntax of our language and module system is (quite) standard and summarized in Figure 2. We describe it in more detail below. We assume given a set of operators \( \mathcal{F}_E \) and a set of distribution operators \( \mathcal{F}_D \). For any \( g \in \mathcal{F}_E \cup \mathcal{F}_D \), we assume given its type: \( \text{type}(g) = t_1 \times \cdots \times t_n \rightarrow t \) where \( t_1, \ldots, t_n, t \in \mathbb{N} \) with \( \mathbb{N} \) the set of base types. We require that bool is a base type, and otherwise leave \( \mathbb{N} \) unspecified.

We consider well-typed arity-respecting expressions built from \( \mathcal{F}_E \) and variables in \( \mathcal{V} \). Similarly, distribution expressions \( d \) are built upon \( \mathcal{F}_D \) and \( \mathcal{V} \). For any expression \( e \), we let \( \text{vars}(e) \) be the set of variables appearing in \( e \) (idem for distribution expression).

We assume a simple language for program statements. A statement \( s \) can be an abort, a skip, a statement sequence \( s_1; s_2 \), an assignment \( x \leftarrow e \) of an expression to a variable, a random sampling \( x \leftarrow d \) from a distribution expression, a conditional, a while loop, or a procedure call \( x \leftarrow \text{call} \ f(\vec{e}) \).

### Expressions (distribution expressions are similar):

- \( e ::= v \in \mathcal{V} \) (variable)
- \( f(e_1, \ldots, e_n) \) (if \( f \in \mathcal{F}_E \))

### Statements:

- \( s ::= \text{abort} \) (abort)
- \( \text{skip} \) (skip)
- \( s_1; s_2 \) (sequence)
- \( x \leftarrow e \) (assignment)
- \( x \leftarrow d \) (sampling)
- \( x \leftarrow \text{call} \ f(\vec{e}) \) (proc. call)
- \( \text{if} \ e \text{ then} \ s_1 \text{ else} \ s_2 \) (cond.)
- \( \text{while} \ e \text{ do} \ s \) (loop)

### Procedure body:

\( \text{body} ::= \{ \text{ var} (\vec{v} : \vec{T}); s; \text{return} \ e \} \)

### Function paths:

- \( F ::= p.f \) (proc. lookup)

### Module paths:

- \( p ::= x \) (mod. ident.)
- \( p.x \) (mod. comp.)
- \( p(p) \) (func. app.)

### Module expressions:

- \( m ::= p \) (mod. path)
- \( \text{struct} \ s \text{ end} \) (structure)
- \( \text{func}(x : M) \ m \) (functor)

### Module structures:

- \( s ::= d_1; \ldots ; d_n \) (\( n \in \mathbb{N} \))

### Module declarations:

- \( d ::= \text{module} \ x = m \)
- \( \text{proc} \ f(\vec{u} : \vec{T}) \rightarrow \tau_r = \text{body} \)

Figure 2: Program and module syntax

The module system. In a procedure call, \( F \) is a function path of the form \( p.f \) where \( f \) is the procedure name and \( p \) is a module path. Basically, when calling \( p.f \), the module system will resolve \( p \) to a module structure, which must declare the procedure \( f \) (this will be guaranteed by our type system). Formally, a module structure \( s \) is a list of module declarations, and a module declaration \( d \) is either a procedure (with typed arguments, and a body which comprises a list of local variables with their types \( \vec{u} : \vec{T} \), a statement \( s \) and a return expression \( e \)) or a sub-module declaration.

The component \( c \) of a module \( x \) can be accessed through the module path expression \( x.c \). Since a module can contain sub-modules, we can have nested accesses, as in \( x.\ldots .z.c \). Hence, a module path is either a module identifier, a component access of another module path \( p \), or a functor application. Finally, a module expression \( M \) is either a module path, a module structure or a functor.

### 3.2 Module Signatures and Restrictions

The novel part of our system is the use of module restrictions in module signatures. Objects related to module restriction are highlighted in red throughout this paper (this is only here to improve readability, not to convey additional information). The syntax of module signatures and restrictions is given in Figure 3. A module structure signature \( S \) is a list of module signature declarations, which are procedure signatures or sub-module signatures. Then, a module signature \( M \) is either a functor signature, or a structure signature with a module restriction \( \theta \) attached.

Module restrictions. A module restriction restricts the effects of a module’s procedures. We are interested in two types of effects. First, we characterize the memory footprint (i.e. global variables which are read or written to) of a module’s procedures through memory restrictions. Second, we upper bound the execution cost of a procedure, and the number of calls a functor’s procedure can make to the functor’s parameters, through complexity restrictions.
Signature structures (for any \( n \in \mathbb{N} \)):
\[
S ::= D_1 : \cdots : D_n
\]
Module signature declarations:
\[
D ::= proc f (\overline{t} : T) \rightarrow r_p | module x : M
\]
Module signatures:
\[
M ::= sig S restr \theta \ end \ func(x : M) M'$
\]
Module restrictions:
\[
\theta ::= \epsilon | \theta (f : \lambda) \quad \lambda ::= \top | \lambda_m \land \lambda_c
\]
Memory restrictions (for any \( I \in \mathbb{N} \)):
\[
\lambda_m ::= +all mem \setminus \{v_1, \ldots, v_I\} \cup \{v_I, \ldots, v_I\}
\]
Complexity restrictions (for any \( l, k, k_1, \ldots, k_I \in \mathbb{N} \)):
\[
\lambda_c ::= \top | \text{compl} [\text{intr} : k, x_1.f_1 : k_1, \ldots, x_I.f_I : k_I]
\]

Figure 3: Module signatures and restrictions

```
module type HSM = {
  proc enc (x:msg) : cipher .
module Hsm : HSM = {
  proc enc (x:msg) : cipher = {
module type Adv (H : HSM) = {
  proc guess () : skey
  H.enc (x:msg) : cipher = {
}
}
```

Figure 4: Example of adversary with restrictions.

Restrictions are useful for compositional reasoning, as they allow stating and verifying properties of a module’s procedures at declaration time. In the case of an abstract module (i.e. a module whose code is unknown), restrictions allow to constrain, through the type system, its possible instantiations. This is a key idea of our approach, which we exploit to prove complexity properties of cryptographic reductions.

For example, we give in Figure 4 EasyCrypt code corresponding to an adversary against a hardware security module. In this scenario the goal of the adversary is to recover the secret key stored in the module Hsm. The example uses two types of restrictions. The module-level restriction \(+all mem\ -\ Hsm\) states that such an adversary can access all the memory, except for the memory used by the module Hsm. The procedure-level restriction \([\text{intr} : k_0, \text{Henc} : k]\) attached to guess, states that guess execution time is at most \(k_0\) (excluding calls to Henc), and that guess can make at most \(k\) queries to the procedure Henc.

Formally, a module restriction is a list of pairs comprising a procedure identifier \(f\) and a procedure restriction \(\lambda\), and a procedure restriction \(\lambda\) is either \(\top\) (no restriction), or the conjunction of a memory restriction \(\lambda_m\) and a complexity restriction \(\lambda_c\).

Memory. A memory restriction \(\lambda_m\) attached to a procedure \(f\), restricts the variables that \(f\) can access directly. We allow for positive memory restrictions \(\{v_1, \ldots, v_I\}\), which states that \(f\) can only access the variables \(v_1, \ldots, v_I\); and negative memory restrictions \(+all mem\ \setminus \{v_1, \ldots, v_I\}\), which states that \(f\) can access any global variables except the variables \(v_1, \ldots, v_I\).

Note that \(\lambda_m\) only restricts \(f\)’s direct memory accesses: this excludes the memory accessed by the procedure oracles (which are modeled as function’s parameters). This is crucial, as otherwise, an adversary that is not allowed to access some oracle’s memory (a standard assumption in security proofs) would not be allowed to call this oracle. E.g., the adversary of Figure 4 can call the oracle H.enc (which can be instantiated by Hsm), even though it cannot access directly Hsm’s memory.

Complexity. A complexity restriction \(\lambda_c\) attached to a procedure \(f\) restricts its execution time and the number of calls that \(f\) can make to its parameters: it is either \(\top\), i.e. no restriction; or the restriction \(\text{compl} [\text{intr} : k, x_1.f_1 : k_1, \ldots, x_I.f_I : k_I]\), which states that: i) its execution time (excluding calls to the parameters) must be at most \(k\); ii) \(f\) can call, for every \(i\), the parameter’s procedure \(x_i.f_i\) at most \(k_i\) times. We require that all parameters’ procedures appear in the restriction. This can be done w.l.o.g. by assuming that any missing entry is zero (which is exactly what is done in our EasyCrypt implementation).

### 3.3 Typing Enriched Module Restrictions

We check that modules verify their signatures through a type system. The novelty of our approach lies in the enriched restrictions attached to module signatures, and the typing rules that check them. For space reasons, we only present the two main restriction checking rules here (the full type system is in Appendix B).

Environments. Typing is done in an environment \(E\). Essentially, an environment is a list of declarations, which are either variable, module or abstract module declarations.

\[
E ::= \epsilon | E, \text{var } v : \tau | E, \text{module } x : m : M | E, \text{module } x = \text{absopen } : M_1
\]

An abstract module declaration module \(x = \text{absopen} : M_1\) states that \(x\) is a module with signature \(M_1\) whose code is unknown, and allows to model open code. For any \(E\), we let \((E) = \{x_1, \ldots, x_n\}\) be the set of abstract module names declared in \(E\).

Restrictions. The \text{RestrMem} rule checks that a procedure body \((\_ ; s; \text{return } e)\) (where \(s\) is the procedure’s instructions, and \(e\) the returned expression) verifies a memory restriction through a fully automatic syntactic check.

\[
\frac{\text{RestrMem}}{E \vdash (\_ ; s; \text{return } e) \triangleright \lambda_m}
\]

This syntactic check uses \(\text{mem}_E (s)\) and \(\text{vars} (e)\), which are sound over-approximations of an instruction and expression memory footprint (the approximation is not complete, e.g. it will include memory accesses done by unreachable code).

The \text{RestrCompl} rule checks that an instruction verifies some complexity restriction. The rule generates proof obligations in a

---

\(^5\)Actually, the type system in Appendix B uses more complex environment, called typing environment, to account for sub-modules.

\(^6\)Abstract module must have low-order signatures, i.e. module structures, or functors whose parameters are module structures (see Appendix B). This choice is motivated by the fact that further generality is not necessary for cryptographic proofs (adversaries and simulations usually return base values, not procedures), and it allows the abstract call rule of our cost Hoare logic \text{Ans} (in Figure 6) to remain tractable.
Hoare logic for cost. These proof obligations are discharged interactively using the proof system we present later, in Section 4.

\begin{align*}
\text{RestrCompl} & \\
\mathcal{E} \vdash \{ \top \} \mathbf{s} \{ \psi \mid t \} \quad \mathbf{r} \leq t_r \quad (t + t_r \cdot \text{conc}) \lessapprox \text{compl} \lambda_c \\
\mathcal{E} \vdash \{ \_ ; \text{return } r \} \triangleright \lambda_c
\end{align*}

Here, the proof obligation \( \mathcal{E} \vdash \{ \top \} \mathbf{s} \{ \psi \mid t \} \) states that the execution of \( s \) in any memory has a complexity upper bounded by \( t \), and that the post-condition \( \psi \) holds after \( s \)'s execution. The proof obligation \( \mathbf{r} \leq t_r \) upper-bounds the cost of evaluating the return expression \( r \). Finally, the rule checks that the sum of \( t \) and \( t_r \) is compatible with the complexity restriction \( \lambda_c \) through the premise \( (t + t_r \cdot \text{conc}) \lessapprox \text{compl} \lambda_c \). We leave the precise definition of \( \lessapprox \) to Section 4 (see Figure 27). Intuitively, \( t \) is a record of entries of the form \( (x, f \mapsto l_r) \), each stating that the abstract module \( x \)'s procedure \( f \) has been called at most \( l_r \) times, plus a special entry \( \text{conc} \mapsto l_c \) stating that \( s \) execution time, excluding abstract calls, is at most \( l_c \). Then, \( t \lessapprox \text{compl} \lambda_c \) checks that \( t \cdot [x \mapsto f] \leq \lambda_c \cdot [x \mapsto f] \) for every functor parameter \( x, f \), and that \( \lambda_c \cdot [\text{intr}] \) upper-bounds everything else in \( t_0 \).

4 Complexity Reasoning in EasyCrypt

We now present our Hoare logic for cost, which allows to formally prove complexity upper-bounds of programs. This logic manipulates judgment of the form \( \mathcal{E} \vdash \{ \phi \} \mathbf{s} \{ \psi \mid t \} \), where \( s \) is a statement, \( \phi, \psi \) are assertions, and \( t \) is a cost. We leave the assertion language unspecified, and only require that the models of an assertion formula \( \phi \) are memories, and write \( \nu \in \phi \) whenever \( \nu \) satisfies \( \phi \).

Essentially, the judgment \( \mathcal{E} \vdash \{ \phi \} \mathbf{s} \{ \psi \mid t \} \) states that \( s \) is a program well-typed in the environment \( \mathcal{E} \) (e.g. this means that \( s \) can only call concrete or abstract procedures declared in \( \mathcal{E} \)), and that: i) the execution of the program \( s \) on any initial memory \( \nu_i \) satisfying the precondition \( \phi \) (i.e. \( \nu_i \in \phi \)) terminates in time at most \( t \); and ii) the final memory \( \nu_f \) obtained by executing \( s \) starting from \( \nu_i \) satisfies the post-condition \( \psi \) (i.e. \( \nu_f \in \psi \)).

4.1 Cost Judgment

A key point of our Hoare logic for cost is that it allows to split the cost of a program \( s \) between its concrete and abstract costs, i.e. between the time spent in concrete code, and the time spent in abstract procedures. To reflect this separation between concrete and abstract cost, a cost \( t \) is a record of entries mapping each abstract procedure \( x, f \) to the number of times this procedure was called, and mapping a special element \( \text{conc} \) to the concrete execution time (i.e. excluding abstract procedure calls). Since the set of available abstract procedures (and consequently the number of entries in the cost \( t \)) depends on the current environment \( \mathcal{E} \), we parameterize the notion of cost by the environment \( \mathcal{E} \) considered:

Definition 4.1. A \( \mathcal{E} \)-cost is an element of the form:

\[ t := [\text{conc} \mapsto k, x_1.f_1 \mapsto k_1, \ldots, x_l.f_l \mapsto k_l] \]

where \( \mathcal{E} \) is an environment, \( k, k_1, \ldots, k_l \) are integers, and the \( x_i.f_i \) are all the abstract procedures declared in \( \mathcal{E} \).

Example 4.1. Consider \( \mathcal{E} \) with two abstract modules \( x \) and \( y \):

\[
\mathcal{E} = (\text{module } x = \text{absopen} \cdot \text{sig} (\text{proc } f \_ \text{ restr } \_ \text{ end}); \text{module } y = \text{absopen} \cdot \text{sig} (\text{proc } h \_ \text{ restr } \_ \text{ end})
\]

Then \([\text{conc} \mapsto 10; x.f \mapsto 0; y.h \mapsto 3]\) represents a concrete cost of 10, at most three calls to \( y.h \), and none to \( x.f \).

Definition 4.2. A cost judgment for a statement is an element of the form \( \mathcal{E} \vdash \{ \phi \} \mathbf{s} \{ \psi \mid t \} \) where \( \mathcal{E} \) must be well-typed, \( s \) must be well-typed in \( \mathcal{E} \) and \( t \) must be an \( \mathcal{E} \)-cost. We define similarly a cost judgment for a procedure \( \mathcal{E} \vdash \{ \phi \} F \{ \psi \mid t \} \).

In Figure 5, we give a graphical representation of a cost judgment for the procedure \( \mathcal{E} \vdash \{ \phi \} F \{ \psi \mid t \} \).

4.2 Hoare Logic for Cost Judgment

We present our Hoare logic for cost, which allows to prove cost judgments of programs. Our logic has one rule for each possible program construct (assignment, loop, ...), plus some structural rules (e.g. weakening). We only describe a simple Hoare rule for conditional construct, and then explain a core rule of our logic, which handles abstract calls. All other rules are given in Appendix F.

Basically, our cost judgment defines a branch program is valid whenever \( t \cdot \text{conc} \) upper-bounds the concrete cost (in hatched gray \( \square \)) which is the sum of: i) the intrinsic cost of \( A.a \), which is the cost of \( A.a \) without counting parameter calls, represented in hatched blue \( \bigcirc \) in the figure, and must be at most \( t_{A.a} \) as stated in \( T_A \)'s restriction; and ii) the sum of the cost of the three calls to \( C.c \).

The cost of the execution of the abstract procedure \( B.b \) (in hatched red \( \triangle \)), which excludes the two calls \( B.b \) makes to \( C.c \), are accounted for by the entry \( (B.b \mapsto 1) \) in the cost judgment. Note that it is crucial that this excludes the cost of the two calls to \( C.c \), which are already counted in the concrete cost \( t_{\text{conc}} \).

Expression cost. We have a second kind of judgment \( \mathcal{E} \vdash \{ \phi \} e \leq t_e \) which states that the cost of evaluating \( e \) in any memory satisfying \( \phi \) is at most \( t_e \), where \( t_e \) is an integer, not a \( \mathcal{E} \)-cost (indeed, an expression cost is always fully concrete, as expressions do not contain procedure calls). We do not provide a complete set of rules for such judgments, as this depends on low-level implementation details and choices, such as data-type representation and libraries implementations. In practice, we give rules for some built-ins, as a way for the user to add new rules, and an automatic rewriting mechanism which automatically prove such judgments from the user rules in most cases.

4.2.1 Cost Judgment

We present our Hoare logic for cost, which allows to prove cost judgments of programs. Our logic has one rule for each possible program construct (assignment, loop, ...), plus some structural rules (e.g. weakening). We only describe a simple Hoare rule for conditional construct, and then explain a core rule of our logic, which handles abstract calls. All other rules are given in Appendix F.

Basically, our cost judgment defines a branch program is valid whenever \( t \cdot \text{conc} \) upper-bounds the concrete cost (in hatched gray \( \square \)) which is the sum of: i) the intrinsic cost of \( A.a \), which is the cost of \( A.a \) without counting parameter calls, represented in hatched blue \( \bigcirc \) in the figure, and must be at most \( t_{A.a} \) as stated in \( T_A \)'s restriction; and ii) the sum of the cost of the three calls to \( C.c \).

The cost of the execution of the abstract procedure \( B.b \) (in hatched red \( \triangle \)), which excludes the two calls \( B.b \) makes to \( C.c \), are accounted for by the entry \( (B.b \mapsto 1) \) in the cost judgment. Note that it is crucial that this excludes the cost of the two calls to \( C.c \), which are already counted in the concrete cost \( t_{\text{conc}} \).

Expression cost. We have a second kind of judgment \( \mathcal{E} \vdash \{ \phi \} e \leq t_e \) which states that the cost of evaluating \( e \) in any memory satisfying \( \phi \) is at most \( t_e \), where \( t_e \) is an integer, not a \( \mathcal{E} \)-cost (indeed, an expression cost is always fully concrete, as expressions do not contain procedure calls). We do not provide a complete set of rules for such judgments, as this depends on low-level implementation details and choices, such as data-type representation and libraries implementations. In practice, we give rules for some built-ins, as a way for the user to add new rules, and an automatic rewriting mechanism which automatically prove such judgments from the user rules in most cases.
Abstract call rule without cost. This is the case of our rule for upper-bounding the cost of a call to an abstract procedure F. To ease the presentation, we first present a version of the rule for usual Hoare judgment without costs, and explain how to add costs after.

**Abs-PARTIAL**

\[ f \text{-res}(F) = (\text{abs}_\text{open} \ x)(\vec{p}); f \]

\[ E(x) = \text{abs}_\text{open} \ x : (\text{func}(\vec{y} : \ldots \text{sig}_{\text{rest}} \theta \text{end})) \]

\[ FV(I) \land \lambda_m = \emptyset \quad \forall p_0 \in \vec{p}, \forall g \in \text{procs}_C(p_0), E \vdash \{I\} p_0.g \{I\} \]

\[ E \vdash \{I\} f \{I\} \]

First, the function path F is resolved to \((\text{abs}_\text{open} \ x)(\vec{p}); f\), i.e. a call to the procedure f of an abstract functor x applied to the modules \(\vec{p}\) (the case where x is not a functor is handled by taking \(\vec{p} = e\)). Then, x’s module type is lookup in E, and we retrieve the module restriction \(\theta_{\text{rest}}\) attached to it. The rule allows to prove that some formula I is an invariant of the abstract call, by showing two things.

First, we show that I is an invariant of \(x.f\), excluding calls to the functor parameters. This is done by checking that x.f cannot access the variables used in I, using its memory restriction \(\lambda_m\) (looked-up by the premise \(0[f] = \lambda_m \land \_\) and requiring that \(FV(I) \land \lambda_m = \emptyset\). Then, we prove that I is an invariant of \(x.f\)’s calls to functor parameters. This is guaranteed by requiring that for every functor parameter \(p_0 \in \vec{p}\), for any of \(p_0\)’s procedure \(g \in \text{procs}_C(p_0)\), the judgment \(E \vdash \{I\} p_0.g \{I\}\) is valid.

Abstract call. We now present our **Abs** rule for cost judgments, which is given in Figure 6. Essentially, the cost of the call to \(x(\vec{p}); f\) is decomposed between:

- the intrinsic cost of \(x.f\) excluding the cost of the calls to x’s functor parameters. This is accounted for by the entry \((x.f \mapsto 1)\) in the final cost \(T_{abs}\).

---

**Figure 5:** Graphical representation of the different cost measurements.

**Figure 6:** Abstract call rule for cost judgment.

- the cost of the calls to \(x.f\) functor parameters, which are enumerated in the restriction:

\[ \lambda_e = \text{comp}[\text{intr} : K, z_{j_1}, f_1 : K_1, \ldots, z_{j_l}, f_l : K_l] \]

We require, for every i, a bound on the cost of the \(k\)-th call to the functor argument \(z_{j_i}\), procedure’s \(f_i\), where \(k\) can range anywhere between 0 and the maximum number of calls \(x.f\) can make to \(z_{j_i}\), which is \(K_i\). The cost of the \(k\)-th call to \(z_{j_i}, f_i\) is bounded by \((t_i k)\) where \(k = \hat{k}[i]\) and:

\[ E \vdash \{I \hat{k}\} \vec{p}[j_i]_I f_i \{I (\hat{k} + 1) \mid t_i k\} \]

To improve precision, we let the invariant \(I\) depend on the number of calls to the functor parameters through the integer vector \(\hat{k}\). After calling \(\vec{p}[j_i]_I f_i\), we update \(\hat{k}\) by adding one to its \(i\)-th entry (\(t_i\) is the vector where the \(i\)-th entry is one and all other entries are zero).

The final cost \(T_{abs}\) (except for \(x.f\)) is obtained by taking the sum, over all functor parameters and number of calls to this functor parameter, of the cost of each call.

### 4.3 Soundness

We define a formal denotational semantics of our language and module system, and use it to prove the soundness of our rules. For space reasons, we omit the details here (they can be found in Appendix E and F), and only state the main soundness theorem.

**Theorem 4.1.** *The proof rules in Figures 6, 26 and 27 are sound.*
5 EXAMPLE: UNIVERSAL COMPOSABILITY

UC security guarantees that a protocol π₁ can safely replace a protocol π₂ while preserving both the functionality and the security of the overall system. The most common application of this framework is to set π₂ to be an idealized protocol that assumes a trusted-third-party (TTP) to which parties delegate the computation; the specification of the TTP is called an ideal functionality \( F \). An ideal functionality \( F \) defines what protocol π₁ should achieve both in terms of correctness and security to securely replace the TTP. Moreover, \( F \) can be used as an ideal sub-component when designing higher-level protocols, which then can be instantiated with protocol π₁ to obtain a fully concrete real-world protocol.

The UC framework defines an execution model where protocol participants, attackers and contexts are modeled as Interactive Turing Machines (ITM). The model was carefully tailored to give a good balance between expressive power—e.g., one can capture complex interactions in distributed protocols involving multiple parties in a variety of communication models, various forms of corruption, etc.—and a tailored (and relatively simple) resource analysis mechanism that permits keeping track of the computing resources available to both honest and malicious parties.

The model is described in detail in [15, 16]. However, most UC proofs found in the literature refer only to a common understanding of the semantics of the execution model and a set of high-level restrictions that are inherent to the model. These include the allowed interactions between different machines, the order in which machines are activated, predefined sequences of events, etc. More fine-grained descriptions of the execution model are sometimes introduced locally in proofs, when they are needed to deal with more subtle points or technicalities that can only be clarified at the cost of extra details. This stands in contrast with typical game-based proofs for simpler cryptographic primitives [8], where security proofs are given in great detail. This is one of the reasons why, while there has been impressive progress in machine-checking game-based proofs [4], we are only now giving the first steps in formalizing proofs in the UC setting [19, 22, 26]. Another reason is that the ITM model for communication is difficult to express in procedure-based semantics offered by tools that target game-based proofs.

To overcome these difficulties, we propose a new approach to machine-checking UC proofs that shares many features of the simplified version of UC proposed by Canetti, Cohen and Lindell in [18]. As in [18], we statically fix the machines/modules in the execution model and we allow an adversarial entity to control which module gets to be executed next, rather than allowing machines to pass control between them more freely as in the original UC execution model. The crucial difference to the ITM execution model is that the above interactions are procedure-based, which means that whenever the environment passes control to the protocol, the internal protocol structure will follow a procedure call tree that guarantees (excluding the possibility of non-terminating code) that control returns to the environment.5 As in [18], we lose some expressiveness, but we do not go as far as hard-wiring a specific communications model for protocols based on authenticated channels; instead, we leave it to the protocol designer to specify the communications model by using an appropriate module structure. We recover the authenticated communications model of [18] by explicitly defining a hybrid real-world, in which concrete modules for ideal authenticated channels are available to the communicating parties. We discuss the trade-offs associated with our approach more in depth at the end of this section, drawing a parallel to the work in [19].

5.1 Mechanized Formalization in EasyCrypt

We propose a natural simplification of the UC execution model that is based on EasyCrypt modules and show that this opens the way for a lightweight formalization of UC proofs. This formalization has been conducted in our extension of EasyCrypt (the proofs of the lemmas and theorems of this section are fully mechanized).

Protocols and Functionalities as EasyCrypt modules. The basic component in our UC execution model is a module of type PROTOCOL given in Figure 7. Inhabitants of this type represent a full real-world configuration—a distributed protocol executed by a fixed number of parties—or an ideal-world configuration—an ideal functionality executing a protocol as a trusted-third party. The type of a protocol has a fixed interface, but it is parametric on the types of values exchanged via this interface. The fixed interface is divided into three parts: i) init allows modeling some global protocol setup; ii) IO captures the interaction of a higher level protocol using this protocol as a sub-component; and iii) BACKDOORS captures the interaction of an adversary with the protocol during its execution.

When we define real-world protocols, a module of type PROTOCOL will be constructed from sub-modules that emulate the various parties and the communications channels between them. In this case, BACKDOORS models adversarial power in this communication model. For ideal-world protocols, a PROTOCOL is typically a flat description of the ideal computation in a single module; here BACKDOORS models unavoidable leakage (e.g., the length of secret inputs or the states of parties in an interactive protocol) and external influence over the operation of the trusted-third party (e.g., blocking the computation to model a possible denial of service attack).6

---

\(^5\) Intuitively, the UC model expresses a single line of execution using a token-passing mechanism that allows one machine to transfer computational resources to another, and even to create new machines. In our setting, resource analysis is much simpler: All modules representing honest and adversarial entities are fixed from the start and the cost model is concrete: all adversarial entities have a resource usage type, which means they are known to execute a maximum number of operations and perform a bounded number of procedure calls. Hence the resources used by any subset of modules in our formalizations can be expressed as an expression on these type parameters.

\(^6\) Ideal-world backdoors are used to weaken the security requirements and are usually tailored to bring the security definition down to a level that can be met by real-world protocols. Note that the definition of meaningful ideal functionalities is a crucial aspect of UC security theory; here we just provide a mechanism that permits formalizing such definitions in EasyCrypt.
The central notion to Universal Composability is called UC-emulation, which is a relation between two protocols $\pi_1$ and $\pi_2$: if $\pi_1$ UC-emulates $\pi_2$ with small advantage $\epsilon$ then $\pi_1$ can replace $\pi_2$ in any context (within a complexity class).

**Definition 5.1 (UC emulation).** Protocol $\pi_1$ UC-emulates $\pi_2$ under complexity restrictions $c_{\text{sim}}$ and $c_{\text{env}}$ and advantage bound $\epsilon$ if

$$\exists S \in \pi_{\text{sim}}, \forall \pi_{\text{env}} \in \pi_{\text{env}} \exists S, \Pr\left[Z\left(\langle \pi_2 \parallel S(\pi_2) \rangle : \top \right) \right] - \Pr\left[Z\left(\langle \pi_2 \parallel S(\pi_2) \rangle : \top \right) \right] \leq \epsilon$$

We write this as $\text{Adv}^{\text{UC}}_{\pi_{\text{sim}}, \pi_{\text{env}}} (\pi_1, \pi_2) \leq \epsilon$. The first probability term corresponds to the event that the environment returns true in the real-world execution model described above, i.e., in game $\pi_{\text{sim}}$ parameterized with $\text{ENV} = \mathcal{Z}$ and $\text{P} = \pi_1$. The second probability term corresponds to the equivalent event in the ideal-world (or reference) execution model where, as shown in Figure 9 (right), $\pi_2$ is typically an ideal functionality; this corresponds to game $\pi_{\text{env}}$ parameterized with $\text{ENV} = \mathcal{Z}$ and a protocol $\text{P}$ that results from attaching $S$ to the BACKDOORS interface of $\pi_2$. We denote this ideal-world $\text{P}$ by $\langle \pi_2 \parallel S(\pi_2) \rangle$, corresponding to the EasyCrypt functor $\text{CompS}$ also shown in Figure 8.

UC-emulation imposes that a simulator $S$ is capable to fool any environment by presenting a view that is fully consistent with the real-world, while learning only what the BACKDOORS interface of $\pi_2$ allows. If such a simulator exists, then clearly $\pi_2$ cannot be worse than $\pi_1$ in the information it reveals to the environment via its BACKDOORS interface. Our UC-emulation definition quantifies over simulators and environments using types that give a full characterization of their use of resources, including the ability to access memory, number and types of procedure calls and intrinsic computational costs. The memory access restrictions are depicted in Figure 9, and they can be easily matched to the standard restrictions in the UC framework. Not shown are the cost restrictions,

![Figure 8: Execution model for real/ideal worlds (top) and composition of functionality with a simulator (bottom).](image1)

![Figure 9: Module restrictions. Arrows indicate ability to make procedure calls via the interface specified as a label; all other cross-boundary memory access is disallowed.](image2)
which give explicit bounds for the resources used by various parts of the execution model; these are crucial for obtaining, not only a meaningful definition, but also for obtaining meaningful reductions to computational assumptions, as will be seen below.

Let us examine the types of $\mathcal{Z}$ and $\mathcal{S}$ in more detail. We first note that the definition of emulation is parametric in the resource restrictions $c_{\text{sim}}$ and $c_{\text{env}}$. Clearly the IO interface of $\pi_2$ must match the type of the IO interface of $\pi_1$, which is consistent with the goal that $\pi_1$ can replace $\pi_2$ in any context, and is enforced by our type system. This need not be the case for the BACKDOORS interface and, in fact, if $\pi_2$ is an ideal functionality, the BACKDOORS interface in the ideal world is of a different nature altogether than the one in the real world: it specifies leakage and adversarial control that are unavoidable even when the functionality is executed by a trusted third-party on behalf of the parties. The type of the simulator $\mathcal{S}$ is given by $\tau_{\pi_1, \pi_2, c_{\text{sim}}}$, which defines the type of modules that have access to the BACKDOORS interface of $\pi_2$ and exposes the BACKDOORS interface of $\pi_1$ and is restricted memory-wise to exclude the memory of $\pi_2$ and resource-wise by $c_{\text{sim}}$. Note that, if $\mathcal{S}$ could look inside the ideal functionality, then it would know all the information that is also given to the real-world protocol: a trivial simulator would always exist and the definition would be meaningless because all protocols would be secure. The type of the environment is given by $c_{\text{env}} := \text{comp}[\mathsf{intr} : c_1, \pi.\mathsf{inputs} : c_2, \pi.\mathsf{outputs} : c_3, \pi.\mathsf{backend} : c_4, \pi.\mathsf{step} : c_5]$ where type refinements can set $c_i$ to depend on the types of other modules in the context.

**Warm-up: Transitivity of UC emulation.** It is easy to show that UC-emulation is a transitive relation: if $\pi_1$ UC-emulates $\pi_2$ and this, in turn, UC-emulates $\pi_3$, then $\pi_1$ UC-emulates $\pi_3$. When stating this lemma in EasyCrypt we move the existential quantifications over the simulators in the hypotheses to global universal quantifications; this logically equivalent formulation allows us to refer to the memory of these simulators when quantifying over all adversarial environments in the consequence: we quantify only over those that look inside the simulators that are assumed to exist by hypothesis, which is a natural (and necessary) restriction. In other examples we use the same approach. The lemma is stated in EasyCrypt as follows (we adapt the $\text{Adv}^{\pi_{\mathcal{S}}(\cdot, \cdot)}$ notation by indicating the universally quantified simulator $\mathcal{S}$ in superscript).

**Lemma 5.1 (Transitivity).** For all $\pi_1, \pi_2, \pi_3 \in \mathbb{R}^+$, all protocols $\pi_1$, $\pi_2$ and $\pi_3$ s.t. the IO interfaces of all three protocols are of the same type, all cost restrictions $c_{\pi_1, \pi_2, c_{\text{sim}}(1,2)}, c_{\pi_2, \pi_3, c_{\text{sim}}(2,3)}$ and all simulators $\mathcal{S}_{1,2} \in \tau_{\pi_1, \pi_2, c_{\text{sim}}(1,2)}, \mathcal{S}_{2,3} \in \tau_{\pi_2, \pi_3, c_{\text{sim}}(2,3)}$, we have that:

$$\text{Adv}^{\pi_{\mathcal{S}_{1,2}}, c_{\text{sim}}(1,2)}_{\mathcal{S}_{1,2}}(\pi_1, \pi_2) \leq \epsilon_{1,2} \Rightarrow \text{Adv}^{\pi_{\mathcal{S}_{1,2}}, c_{\text{sim}}(2,3)}_{\mathcal{S}_{1,2}}(\pi_2, \pi_3) \leq \epsilon_{2,3} \Rightarrow \text{Adv}^{\pi_{\mathcal{S}_{1,2}}, c_{\text{sim}}(1,3)}_{\mathcal{S}_{1,2}}(\pi_1, \pi_3) \leq \epsilon_{1,2} + \epsilon_{2,3},$$

where $\epsilon_{1,2}$ corresponds to the cost of sequentially composing $\mathcal{S}_{1,2}$ and $\mathcal{S}_{2,3}$, $c_{\text{sim}}(2,3)$ must allow for an adversarial environment that results from converting a distinguisher between $\pi_1$ and $\pi_3$ in $c_{\text{env}}(1,3)$ and composing it with $\mathcal{S}_{1,2}$, and $\epsilon_{1,2} = c_{\text{env}}(1,3)$.

In the statement of the lemma we use notation $\epsilon$ to denote the fact that these cost restrictions are fixed as a function of the costs of other algorithms: intuitively, the cost of the environment in the consequence is free and it constrains the costs of environments in the hypotheses; then, if for some cost restrictions $c_{\text{sim}}(1,2)$ and $c_{\text{sim}}(2,3)$ the hypotheses hold, these in turn fix the cost of the simulator $\mathcal{S}$ we give as a witness. This pattern is observable in the remaining examples we give in this section.

From the proof, we get a witness simulator $\mathcal{S}_{1,3} = \mathcal{S}_{2,3}(\mathcal{S}_{2,1}, \mathcal{S}_{1,2})$ that results from plugging together the two simulators implied by the assumptions: intuitively, $\mathcal{S}_{1,3}$ is able to interact with $\pi_1$ and emulate the BACKDOORS of $\pi_2$, and this is sufficient to enable $\mathcal{S}_{1,2}$ to emulate the BACKDOORS interface of $\pi_1$, as required. Technically, the proof shows first that one can break down $\mathcal{S}_{1,3}$ and put $\pi_2$ in the place of $\mathcal{Comp}(\pi_3, \mathcal{S}_{2,3})$. To show this, we aggregate $\mathcal{S}_{1,2}$ into the environment to construct a new environment that would break $\pi_2$ if such a modification was noticeable, contradicting the second hypothesis. The proof then follows by applying the first hypothesis. Note that this proof strategy is visible in the resources used by $\mathcal{S}_{1,3}$, since they are those required to run the composed module $\mathcal{S}_{2,3}(\mathcal{S}_{2,1}, \mathcal{S}_{1,2})$. Moreover, the quantification over the resources of the environments in the second hypothesis must accommodate an environment that absorbs simulator $\mathcal{S}_{1,2}$ and runs it internally.

In Appendix A we give a more elaborate example of the properties of UC emulation definition, by showing that our formalization inherits an important property from the general UC framework: that including an explicit adversary in the real world that colludes with an arbitrary environment to break the protocol leads to an equivalent definition to the one we have, which assumes an (implicit) dummy adversary that just follows the instructions of the adversarial environment. Moreover, in our setting with concrete costs, this is equivalent to our execution model where the dummy adversary is implicit.

**Universal Composability.** The fundamental theorem of Universal Composability is stated in our EasyCrypt formalization as follows.

**Theorem 5.2 (Universal Composability).** For all $\pi, \pi' \in \mathbb{R}^+$, all ideal functionalities $f, F$, all protocols $f(\pi)$ and $\pi$, such that the IO interfaces of $\pi$ and $f$ (resp. $\pi'$ and $F$) are of the same type, all cost restrictions $c_{\text{sim}}(\rho), c_{\text{sim}}(\pi)$, and all simulators $\mathcal{S}_{\rho} \in \tau_{\pi, f(\pi), F, c_{\text{sim}}(\rho)}$, $\mathcal{S}_{\pi} \in \tau_{\pi', c_{\text{sim}}(\pi)}$, we have:

$$\text{Adv}^{\pi_{\mathcal{S}_{\rho}}, c_{\text{sim}}(\pi)}_{\mathcal{S}_{\rho}, c_{\text{sim}}(\pi)}(\pi, f) \leq \epsilon_{\pi} \Rightarrow \text{Adv}^{\pi_{\mathcal{S}_{\rho}}, c_{\text{sim}}(\pi)}_{\mathcal{S}_{\rho}, c_{\text{sim}}(\pi)}(f(\pi), F) \leq \epsilon_{f} \Rightarrow \text{Adv}^{\pi_{\mathcal{S}_{\rho}}, c_{\text{sim}}(\pi)}_{\mathcal{S}_{\rho}, c_{\text{sim}}(\pi)}(\rho(\pi), F) \leq \epsilon_{\rho} + \epsilon_{\pi}$$

where $\epsilon_{\text{env}}(\pi)$ accommodates an environment that internally uses $\epsilon_{\text{env}}$ resources and additionally runs $\rho$, $\epsilon_{\text{sim}}$ corresponds to the cost of composing $\mathcal{S}_{\pi}$ and $\mathcal{S}_{\rho}, \epsilon_{\text{env}}(\pi)$, allows for an adversarial environment built by composing $\mathcal{S}_{\pi}$ with an environment in $\epsilon_{\text{env}}$.

This theorem establishes that any protocol $f(\pi)$ that UC-emulates a functionality $F$ when relying on an ideal sub-component $f$ offers the same level of security when it is instantiated with a protocol $\pi$.
that UC-emulates \( f \). The proof first shows that the simulator \( S_{\pi} \) that exists by hypothesis can be converted into a simulator that justifies that \( \rho(\pi) \) UC-emulates \( \rho(f) \); intuitively this new simulator uses \( S_{\pi} \) when interacting with the backdoors of \( f \) and just passes along the environment’s interactions with the backdoors of \( \rho \). This part of the proof combines any successful environment \( Z \) against the composed protocol into a successful environment that absorbs \( \rho \) and breaks \( \pi \). This justifies the cost restriction on \( c_{\text{env}} \). Then, we know by hypothesis that \( \rho(f) \) UC emulates \( F \), and the result follows by applying the transitivity lemma, which also explains the remaining cost restrictions.

**Example: Composing key exchange with encryption.** We conclude this section with an example of the use of our framework and general lemmas stated above for concrete protocols. Consider the code snippets in Figure 10. On the left we show the inner structure of a two-party protocol formalization (Diffie-Hellman) when one assumes an ideal sub-component (in this case a bi-directional ideal authenticated channel \( F_{\text{auth}} \) exposing IO interface \( \Pi_{\text{REAL}()}, I_{\text{IO}} \)). The full real-world configuration is obtained by applying a functor \( \text{CompRF} \) that composes this protocol with \( F_{\text{auth}} \) and exposes the backdoors of both \( \text{DHKE} \) and \( F_{\text{auth}} \) in a combined \( \text{BACKDOORS} \) interface. The IO interface to this real-world protocol is simply the input/output interface for both parties; parties take as input a role (initiator/responder) and the identities of parties involved in the protocol (type unit pkg); they output a session key when the protocol completes.

The Initiator code is shown in Figure 11. On initialization it samples its ephemeral key pair and resets the derived key. When the environment provides input, which includes the identities of the parties that will take part in the key exchange, the ephemeral public key is transmitted via one of the ideal authenticated channels. The party then returns control to the environment (note that delivering a message to the authenticated channel does not pass control to the authenticated channel). When the environment calls step, the initiator checks the incoming ideal channel to see if it received a message. At any point the environment can check the initiator output using output. The backdoor interface provides no information, since all communications go through the authenticated channels. The responder code is symmetric.

In the middle code-snippet of Figure 10 we give an example ideal functionality for a simple one-shot unidirectional authenticated channel; one party provides input with the party identities and the message to transmit (type msg pkg), and the other party can obtain the message if it calls outputs with matching identities (type unit pkg). The attacker can use the backdoor procedure to observe the state of the channel, including the transmitted message and the party identities and it can use the step procedure to control when the message is delivered (the unlock operator changes the state so that, if a message is buffered, then it is made available at the output procedure) to the receiving party (get_message is checking for identity consistency, which models authentication).

The example starts with a proof that the Diffie-Hellman protocol on the left of Figure 10 UC-emulates the ideal functionality for key exchange shown on the right of Figure 10 in a hybrid-real world where the parties have access to authenticated channels. The \( \text{FKE} \) functionality runs internally a state machine that waits for both parties to provide input, and allows an adversary/simulator interacting with its BACKDOORS interface to control when the different parties obtain a fresh shared secret key. This result is stated as follows; note the accounting of resources spent by the combined Diffie-Hellman attacker, making it explicit that the DDH assumption must be valid for such an attacker.

**Lemma 5.3 (Security of \( \text{DHKE} \)).** Fix \( c_{\text{ddh}} \in \mathbb{R}^+ \) and let \( \epsilon_{\text{DDH}} \) be the maximum advantage of any DDH attacker against the group over which we implement \( \text{DHKE} \). Then, we have that
\[
\text{Adv}^{\text{uc}}_{\text{env(UCHKE) + env(DHKE))}}(\text{DHKE}(F_{\text{auth}}), \text{FKE}) \leq \epsilon_{\text{DDH}}
\]
where \( c_{\text{sim}(\text{DHKE})} \) is the cost of a concrete simulator \( S_{\text{DHKE}} \) that just samples random group elements as the protocol messages and mimics the states of the real-world parties and \( F_{\text{auth}}; c_{\text{env(\text{DHKE})}} \) must be such that \( c_{\text{ddh}} \) accommodates the cost of an adversary that runs internally the entire UC emulation experiment (including the environment) and interpolates between the real and ideal worlds, depending on the external DDH challenge.

The second result shows that the ideal functionality for key exchange can be combined with one-time-pad encryption to transform a one-shot authenticated channel into a one-shot secure channel that also guarantees confidentiality. Formally:

**Lemma 5.4 (Security of \( \text{OTP} \)).** Fix any \( c_{\text{env(OPT)}} \). Then we have
\[
\text{Adv}^{\text{uc}}_{c_{\text{env(OPT)}}, c_{\text{env(OTP)}}}(\text{OTP}(\text{FKE}, F_{\text{auth}}), F_{\text{SC}}) = 0
\]
where \( c_{\text{sim}(\text{OPT})} \) is the cost of a concrete simulator \( S_{\text{OPT}} \) that just samples a random string in place of the ciphertext and mimics the states of the real-world parties, \( \text{FKE} \) and \( F_{\text{auth}} \).

Here, \( F_{\text{SC}} \) represents the secure channel ideal functionality, which operates exactly as \( F_{\text{auth}} \), but does not leak the transmitted message; leakage includes only information on the state of the channel. The protocol runs in a hybrid world where it has access to both \( \text{FKE} \) and \( F_{\text{auth}} \), uses the former to obtain a shared key between the two parties, and then transmits the one-time-padded message using \( F_{\text{auth}} \). We apply our Universal Composability theorem to derive that \( \text{FKE} \) can be replaced by the \( \text{DHKE} \) protocol, resulting in a protocol that still UC-emulates the secure channel functionality. The final theorem is stated as follows.

**Theorem 5.5 (Security of \( \text{OTP} \) composed with \( \text{DHKE} \)).** Fix \( c_{\text{ddh}} \in \mathbb{R}^+ \) and let \( \epsilon_{\text{DDH}} \) be the maximum advantage of any DDH attacker against the group over which we implement \( \text{DHKE} \). Then
\[
\text{Adv}^{\text{uc}}_{c_{\text{env(OPT)}, c_{\text{env(DHKE)}}}}(\text{OTP}(\text{DHKE}, \text{Fauth}), \text{FSC}) \leq \epsilon_{\text{DDH}}
\]
where \( c_{\text{env}} \) is constrained so that \( c_{\text{env(DHKE)}} \) accommodates an environment that internally uses \( c_{\text{env}} \) resources and additionally runs \( \text{OTP} \), and \( c_{\text{sim}} \) corresponds to the cost of composing \( S_{\text{OPT}} \) and \( S_{\text{DHKE}} \).

The crucial application of the complexity restrictions is visible in the attacker against the DDH assumption, which now has a more complex structure that results from the application of the composition theorem: for this application of composition to be meaningful, it is crucial that the global environment is computationally bounded (even though the OTP protocol is information-theoretically secure) as a function of \( c_{\text{ddh}} \), as otherwise the reduction to DDH would be meaningless. Indeed, the class of DDH attackers must allow for
ticated channel.

FAuth

chinery to reduce proof effort and development size: our devel-

translation of protocols and ideal functionalities.

execution model as closely as possible; this allows a more direct

each other. An important design goal of EasyUC is to follow the UC

strate our formalization. This example is also convenient to show

in [19], it is a good toy example with which to validate and demon-

and Varia [19] for the EasyUC framework. We borrow it because, as

to instantiate only one of them.

functionalities and we apply the Universal Composability theorem

ization of the Universal Composability theorem for the case where

S is given by

module (DHKE : RHO) (F2Auth : Pl.REALIO) = {
module Initiator = {
module Responder = {

proc init() : unit = { Initiator.init(); Responder.init(); }
proc inputs(r : role, p : unit pkg) : unit = {
  if (r = I) { Initiator.inputs(p); }
  else { Responder.inputs(p); }
}
proc outputs(r : role) : group option = { ··· ··· }
proc backdoor(r : role) : unit option = {
  var rr;
  if (r = I) { rr ← Initiator.backdoor(); }
  else { rr ← Responder.backdoor(); }
  return rr; }
}
module FAuth : PROTOCOL = {
var st : state
proc init() : unit = { st ← init_st; }
proc inputs(r : role, p : unit pkg) : unit = {
  st ← set_msg st r p;
}
proc outputs(r : role, p : unit pkg) : msg option = {
  return get_msg st r p;
}
proc step() : unit = {
  st ← unblock st;
}
proc backdoor() : leakage option = {
  return leak st;
}
}
module FKE : PROTOCOL = {
var st : state
proc init() : unit = { k ← gen; st ← init_k; }
proc inputs(r : role, p : unit pkg) : unit = {
  st ← party_start st r p;
}
proc outputs(r : role) : key option = {
  return party_output st r;
}
proc step() : unit = { st ← unblock st;
}
proc backdoor() : leakage option = { return leak st; }
}
Figure 10: Examples of real-world (left) and ideal-world protocols (middle and right). Left: structure of a Diffie-Hellman pro-
tocol relying on FAuth for authenticated communication (one shot each way). Middle: ideal functionality for one-shot authen-
ticated channel FAuth. Right: ideal functionality for key exchange.

module Initiator = {
proc init() : unit = { st ← Init.; x ← $\frac{1}{4}$ FDist.r dt. X ← g^x. K ← None; }
proc inputs(p : unit pkg) : unit = {
  if (st = Init) { p ← _p; Auth.inputs(Left (l, (snd p, rcv p, _X))); st ← ISent; }
}
proc outputs() : group option = { return K; }
proc step() : unit = {
  if (st = ISend)
  if (Y ≠ None)
    return Some (get (getY (getY _Y)) ^ X); st ← IDone;
}
proc backdoor() : unit option = { return None; }
}

Figure 11: Diffie-Hellman Initiator.

extra resources required to run a simulation of OTP protocol in the
reduction. Note also that the execution time of the global simulator
is given by $\mathcal{S}_{OTP}$ and $\mathcal{S}_{DHKE}$, which are very efficient; hence the
UC emulation result has a small simulation overhead [16, 17].

For the proof we used an auxiliary lemma, which is a special-
ization of the Universal Composability theorem for the case where
the hybrid functionality is the parallel composition of two ideal
 functionalities and we apply the Universal Composability theorem
to instantiate only one of them.

Our formalization vs EasyUC. Our Diffie-Hellman example is an
alternative formalization of the example given by Canetti, Stoughton
and Varia [19] for the EasyUC framework. We borrow it because, as
in [19], it is a good toy example with which to validate and demon-
strate our formalization. This example is also convenient to show
that the approach in this paper and EasyUC in effect complement
each other. An important design goal of EasyUC is to follow the UC
execution model as closely as possible; this allows a more direct
translation of protocols and ideal functionalities.

In contrast, our goal is to take advantage of the EasyCrypt ma-
chinery to reduce proof effort and development size: our develop-
ment (including complexity) takes 2300 lines of code and it
includes general UC theorems that can be reused in future work;
this compares to 18K lines of code for EasyUC. The downside of
our approach is the impact in the way one specifies protocols and
ideal functionalities: message passing corresponds to procedure
calls, and these must adhere to the EasyCrypt tree-based procedure
call semantics. For example, we do not allow an execution envi-
ronment where a party communicates with an ideal functionality
arbitrarily without relying on the environment for scheduling; one
could of course formalize a message passing mechanism on top of
EasyCrypt as in [19] to allow for this, but this would then fall out of
the scope of our general composition theorems. Moreover, it
would lead to larger developments and increased proof effort,
which would defeat our original purpose.

In short, one can think of the EasyUC approach as a front-end
for cryptographers, and our approach as a convenient back-end
for conducting the machine-checked proofs. We leave it as an inter-
esting direction for future work to develop a sound translation
between these two approaches to modeling UC for a representative
class of protocols such as those considered in [18]. Another interest-
ing direction for future work is to identify UC security proofs
that cannot be naturally expressed using our approach to formalizing
UC and to investigate how it can be extended to deal with these
examples.

6 RELATED WORK

Cost analysis. There is a very large body of work that uses pro-
gram logics for cost analysis of imperative programs. [28] uses
Hoare logic for proving upper bounds on execution time of de-
terministic programs. In the probabilistic setting, [24] uses a pre-
expectation calculus inspired from Kozen [25] and Morgan, McIver
and Seidel [27] to compute upper bounds on the expected cost of
probabilistic programs. In contrast, cryptography primarily consid-
ers worst-case execution times. In addition, there is a long line of
work on automating cost analysis, both for deterministic and for
probabilistic programs, see e.g. [1, 13, 21]. These techniques could
be helpful to alleviate users efforts, and connecting with tools that
support them is an important direction for future work.

The count excludes general purpose libraries, but we should note that the exact
numbers are not important, as the size of a development varies significantly with style
of coding and the use of automation.
We have developed an extension of the CryptoVerif module system and program logic for complexity would represent a significant endeavor.

Our module system is inspired from EasyCrypt [6, 9]. However, the EasyCrypt module system lacks complexity restrictions, which hampers the use of compositional approaches. Beyond EasyCrypt, several other tools and approaches use structures similar to modules for formalizing cryptographic schemes and their security. Computational Indistinguishability Logic (CIL) [5] rely on oracle systems, which are very closely related to our modules. Interestingly, the main judgment of CIL establishes the approximate equivalence of two oracle systems, and is explicitly quantified by the resources of an adversary. State-separating proofs [14] pursue similar goals, using a notion of package. Packages have the expressivity of modules, but additionally support private functions. Our modules can emulate private functions using restrictions. At present, there is no tool support for state-separating proofs. [30] introduces the notion of interface, which is similar to module, for formalizing cryptography.

7 CONCLUSION

We have developed an extension of the EasyCrypt proof assistant to support reasoning complexity claims. The extension captures reduction statements that faithfully match the cryptographic literature and supports compositional reasoning. As a main example, we have shown how to formalize key results from Universal Composability, a long-standing goal of computer-aided cryptography.

REFERENCES


Consider the functor in Figure 12, which extends any real-world protocol with abstract adversary $\mathcal{A}$ (in EasyCrypt notation) at its BACKDOORS interface. The type of $\mathcal{A}$ is parametric in the BACKDOORS offered by the protocol in our basic execution model, and it fixes the type of the BACKDOORS interface in the extended execution model NONDUMMY.PROTOCOL. This means that when we quantify over such adversaries, we quantify also over the potential forms of environment-to-adversary information exchange. The following theorem shows that we do not lose generality by working with an (implicit) dummy adversary in our execution model.

**Theorem A.1 (Dummy Adversary).** UC emulation is equivalent to UC emulation with an explicit real-world adversary. More precisely:

- Emulation with an implicit dummy adversary implies emulation with an explicit arbitrary adversary: For all $\epsilon \in \mathbb{R}^+$, all protocols $\pi_1$ and $\pi_2$ with I/O interfaces of the same type, all complexity restrictions $\epsilon_{\text{sim}}$, $\epsilon_{\text{env}}$, and all simulators $S \in \pi_1 \parallel \mathcal{A} \quad \epsilon_{\text{sim}}$,
  - we have $\text{Adv}^{\parallel \mathcal{A}}_{\epsilon_{\text{sim}}, \epsilon_{\text{env}}} (\pi_1, \pi_2) \leq \epsilon$ $\Rightarrow$ $\forall A \in \tau_{\text{adv}}, \text{Adv}^{\parallel \mathcal{A}}_{\epsilon_{\text{sim}}, \epsilon_{\text{env}}} (\langle \pi_1 \parallel \mathcal{A} (\pi_1) \rangle, \pi_2) \leq \epsilon$

- Emulation with an implicit dummy adversary is implied by emulation with an explicit arbitrary adversary: For all $\epsilon \in \mathbb{R}^+$, all protocols $\pi_1$ and $\pi_2$ with I/O interfaces of the same type, all complexity restrictions $\epsilon_{\text{sim}}$, $\epsilon_{\text{env}}$ and all simulator memory spaces $M$, we have $\forall A \in \tau_{\text{adv}}, \text{Adv}^{\parallel \mathcal{A}}_{\epsilon_{\text{sim}}, \epsilon_{\text{env}}} (\langle \pi_1 \parallel \mathcal{A} (\pi_1) \rangle, \pi_2) \leq \epsilon$ $\Rightarrow$ $\text{Adv}^{\parallel \mathcal{A}}_{\epsilon_{\text{sim}}, \epsilon_{\text{env}}} (\pi_1, \pi_2) \leq \epsilon$

**Appendix Outline.** We quickly outline the structure of the appendix. We show that the standard dummy adversary theorem holds in our UC modeling in Appendix A. We present the type system for our programming language and module system in Appendix B. Then, we present the semantics of our module system. This module semantics takes the form of a module resolution mechanism, which describe how module expressions are evaluated, and is given in Appendix C. Appendix D proves that our type system and module resolution mechanism have the subject reduction property: essentially, evaluating a module expression preserves its type. This is a crucial property, as it proves that module restrictions are preserved by the evaluation of a module using the module resolution mechanism. Then, we define the semantics of our programming language and of the cost judgment in Appendix E. Finally, we present the full set of rules of our Hoare logic for cost and prove their soundness in Appendix F.

**A THE DUMMY ADVERSARY IN UC**

The standard notion of UC emulation [15, 16] enriches the real-world with an explicit adversary $\mathcal{A}$ representing an attacker that has access to the real-world BACKDOORS interface and colludes with the environment to break the protocol. In this case, the real- and ideal- world execution models become structurally identical, in that the environment interacts with the BACKDOORS interface via adversarial entities in both worlds. The order of the quantifiers in the emulation definition is crucial for its compositional properties: it requires that, for all adversaries $\mathcal{A}$, there exists a simulator $S$ such that, for all environments $\mathcal{E}$, the real- and ideal- worlds are indistinguishable. We now show that the same result holds in our setting.

---

10 For this reason the simulator is often called an ideal world adversary; we do not adopt this terminology here to avoid confusion.
We now present the core rules of our module type system, which help the reader, we give a summary of all the syntactic categories is a module with signature \( p \Gamma \) is a list of typing declarations. A typing declaration, denoted \( \delta \), is either a variable, module, abstract module or procedure declaration, with a type.

\[
\delta ::= \text{var } v : \tau | \text{module } p = m : M | \text{module } x = \text{abs} : M \\
| \text{proc } p.f : \xi \rightarrow \tau = \text{body}
\]

\( K ::= \text{open} | \text{param} \)

\( \Gamma ::= \varepsilon | \Gamma, \delta \)

Note that module and procedure declarations can be rooted at an arbitrary path \( p \).

An abstract module declaration module \( x = \text{abs} : M \) states that \( x \) is a module with signature \( M \) whose code is unknown. This is used either for open code, or to represent a functor parameter at typing time. Open modules and parameters are treated differently by the type system: a memory restriction ignores the memory footprint of a functor parameter, and a complexity restriction restricts the number of calls that can be made by parameters’ procedures. Therefore, we annotate an abstract module with its kind, which can be \text{open} or \text{param}. Finally, module and procedure declarations come with the absolute path from the root of the program to the parent module where the declaration is made (variable and abstract modules are always declared at top-level).

For example, the entry \( \text{module } p.x = m : M \) means that there is a sub-module \( m \) named \( x \) and with type \( M \) declared at path \( p \). As usual we require that typing environments do not contain two declarations with the same path. This allows to see a typing environment \( \Gamma \) as a partial function from variable names \( v \), module paths \( p \) or procedure paths \( p.f \) to (base, module, abstract modules or procedure) values and their types, defined as follows:

\[
\begin{align*}
\Gamma(v) &= \tau \quad \text{(if } \Gamma = (\Gamma_1; \text{var } v : \tau; \Gamma_2)) \\
\Gamma(p) &= m : M \quad \text{(if } \Gamma = (\Gamma_1; \text{module } p = m : M; \Gamma_2)) \\
\Gamma(x) &= \text{abs} : M \quad \text{(if } \Gamma = (\Gamma_1; \text{module } x = \text{abs} : M; \Gamma_2)) \\
\Gamma(p.f) &= \text{proc } f(\xi : \tilde{\tau}) = \text{body} \\
& \quad \text{(if } \Gamma = (\Gamma_1; \text{proc } p.f(\xi : \tilde{\tau}) = \text{body}; \Gamma_2))
\end{align*}
\]

and \( \Gamma(z) = \text{undef} \) otherwise. Also, we write \( \Gamma(z) \mid \text{undef} \) when \( \Gamma(z') = \text{undef} \) for any prefix \( z' \) of \( z \).

**Abstract modules.** Abstract modules representing open code (i.e. with kind \text{open} ) are restricted to low-order signatures:

\[
\begin{align*}
\text{M}_1 &::= \text{sig } S_1 \text{ restr } \theta \text{ end } | \text{func}(x : \text{sig } S_1 \text{ restr } \theta \text{ end}) \text{ M}_1 \\
S_1 &::= D_1 ; \ldots ; D_n \\
D_i &::= \text{proc } f(\xi : \tilde{\tau}) = \text{body}
\end{align*}
\]

Basically, we only allow module structures, or functors whose parameters are module structures. This restriction is motivated by the fact that further generality is not necessary for cryptographic proofs (adversaries and simulations usually return base values, not procedures); and, more importantly, this restriction allows the abstract call rule of our instrumented Hoare logic \text{Abs} presented in Figure 6 to remain tractable.

For any \( \text{M}_i \), let \( \text{procs}(\text{M}_i) = \{ f_1 , \ldots , f_n \} \) be the set of procedure names declared in \( \text{M}_i \).

**Typing module paths.** The typing judgment \( \Gamma \vdash p : M \) states that the module path \( p \) refers to a module with type \( M \). Its typing rules, which are given in Figure 14, are standard, except for the functor application typing rule \text{FuncApp}:

\[
\begin{align*}
\Gamma &\vdash p : \text{func}(x : M') \quad \Gamma &\vdash p' : M' \\
\Gamma &\vdash p(p') : M[x \mapsto \text{mem}_T(p')] \\
\end{align*}
\]

A key point here is that we need to substitute \( x \) in the module signature. The substitution function is standard (see Figure 20), except for module restrictions, which are modified as follows:

- a memory restriction restricts the variables that a procedure can access directly – however, memory accesses done through functor parameters are purposely not restricted. Hence, when we instantiate a functor parameter \( x \) by a module path \( p' \), we must add its memory footprint, which is \( \text{mem}_T(p') \). This is handled when substituting \( x \) in a memory restriction:

\[
\lambda_m[x \mapsto \text{mem}_T(p')] = \lambda_m \cup \text{mem}_T(p')
\]

- a complexity restriction gives upper bounds on a procedure execution time, and on the number of calls it can make to its functors’ parameters. When we instantiate a functor, we remove a functor parameter, and therefore remove the corresponding entries in the complexity restrictions.

\[
\begin{align*}
\text{comp}(\text{intr } k : y_1.f_1 : k_1, \ldots , y_j.f_j : k_j | x \mapsto \_ =) \\
&\quad = \begin{cases} \\
e & \text{if } y = x \\
y.f : k & \text{otherwise}
\end{cases}
\end{align*}
\]

\( ^{11} \text{Meaning that the (variable, module or procedure) path } z \text{ is not declared by } \Gamma , \text{ even through a sub-module or functor application.} \)
Expressions (distribution expressions are similar):

\[
e := v \in \mathcal{V} \quad \text{(variable)}
| f(e_1, \ldots, e_n) \quad \text{(if } f \in \mathcal{T}E\text{)}
\]

Statements:

\[
s := \text{abort} \quad \text{(abort)}
| \text{skip} \quad \text{(skip)}
| s_1; s_2 \quad \text{(sequence)}
| x := e \quad \text{(assignment)}
| x \leftarrow d \quad \text{(sampling)}
| x \leftarrow \text{call } f(\vec{e}) \quad \text{(procedure call)}
| \text{if } e \text{ then } s_1 \text{ else } s_2 \quad \text{(conditional)}
| \text{while } e \text{ do } s \quad \text{(loop)}
\]

Procedure body:

\[
\text{body} := \{ \text{var } (\vec{d} : \vec{\tau}); s; \text{ return } e \}\n\]

Module paths:

\[
p := x \quad \text{(mod. ident.)}
| p.x \quad \text{(mod. comp.)}
| p(p) \quad \text{(func. app.)}
\]

Procedure body:

\[
\text{body} := \{ \text{var } (\vec{d} : \vec{\tau}); s; \text{ return } e \}\n\]

Module expressions:

\[
m := p \quad \text{(mod. path)}
| \text{struct } st \text{ end} \quad \text{(structure)}
| \text{func}(x : M) \ m \quad \text{(functor)}
\]

Module declarations:

\[
d := \text{proc } f(\vec{d} : \vec{\tau}) \rightarrow \tau_r = \text{body} \quad \text{(proc.)}
| \text{module } x = m \quad \text{(module)}
\]

Signature structures:

\[
S := D_1; \ldots; D_n \quad \text{(for any } n \in \mathbb{N})
\]

Module signature declarations:

\[
D := \text{proc } f(\vec{d} : \vec{\tau}) \rightarrow \tau_r \quad \text{(procedure decl.)}
| \text{module } x : M \quad \text{(mod. decl.)}
\]

Module signatures:

\[
M := \text{sig } S \text{ restr } \theta \text{ end} \quad \text{(restr. sig. struct.)}
| \text{func}(x : M) \ M' \quad \text{(functor)}
\]

Typing environment declarations:

\[
\delta := \text{var } v : \tau \quad \text{(variable decl.)}
| \text{module } p = m : M \quad \text{(module decl.)}
| \text{module } x = \text{abs}_K : M \quad \text{(abs. mod.)}
| \text{proc } p.f(\vec{d} : \vec{\tau}) \rightarrow \tau_r = \text{body} \quad \text{(proc. decl.)}
\]

Abstract module kind:

\[
K := \text{open} \quad \text{(open module)}
| \text{param} \quad \text{(module parameter)}
\]

Typing Environment:

\[
\Gamma := \epsilon \mid \Gamma, \delta
\]

Module restrictions:

\[
\theta := \epsilon \mid \theta, (f : \lambda) \quad \text{(for any } \lambda \text{)}
| \lambda_m := +\text{all mem}\\{v_1, \ldots, v_l\} \quad \text{(for any } l \in \mathbb{N})
| \{v_1, \ldots, v_l\} \quad \text{(for any } l \in \mathbb{N})
\]

Memory restrictions:

\[
\lambda_c := \top \mid \text{comp}[[\text{intr } k, x_1.f_1 : k_1, \ldots, x_l.f_l : k_l]] \quad \text{(for any } l, k, k_1, \ldots, k_l \in \mathbb{N})
\]

Complexity restrictions:

\[
\lambda_m := +\text{all mem}\\{v_1, \ldots, v_l\} \quad \text{(for any } l \in \mathbb{N})
| \{v_1, \ldots, v_l\} \quad \text{(for any } l \in \mathbb{N})
\]

Low-order module signatures:

\[
M_l := \text{sig } S_l \text{ restr } \theta \text{ end} \quad \text{(restr. sig. struct.)}
| \text{func}(x : M_l) \ M_l \quad \text{(low-order func.)}
\]

Low-order signature structures:

\[
S_l := D_{1l}; \ldots; D_{nl} \quad \text{(for any } n \in \mathbb{N})
\]

Low-order module signature declarations:

\[
D_l := \text{proc } f(\vec{d} : \vec{\tau}) \rightarrow \tau_r \quad \text{(procedure decl.)}
\]

Extended module expressions:

\[
m := m \mid \text{abs}_K x
\]

Figure 13: Syntax of statements and modules.
Module path typing $\Gamma \vdash p : M$.

<table>
<thead>
<tr>
<th>NAME</th>
<th>COMPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma(p) = _ : M$</td>
<td>$\Gamma \vdash p : \text{sig} S_1; \text{module} x : M; S_2$ restr $\theta$ end</td>
</tr>
<tr>
<td>$\Gamma \vdash p : M$</td>
<td>$\Gamma \vdash p.x : M$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FUNCAPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma \vdash p : \text{func}(x : M') M$</td>
</tr>
<tr>
<td>$\Gamma \vdash p(p') : [M[x \mapsto \text{mem}_\Gamma(p')]]$</td>
</tr>
</tbody>
</table>

Module expression typing $\Gamma \vdash p m : M$.

Remark B.1. We omit the rules $\Gamma \vdash M$ to check that a module signature $M$ is well-formed.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Struct</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma \vdash p_a : M$</td>
<td>$\Gamma \vdash p, p_a : M$</td>
</tr>
<tr>
<td>$\Gamma \vdash p : M_0$</td>
<td>$\Gamma \vdash p : M_0\tau$</td>
</tr>
<tr>
<td>$\Gamma \vdash \text{func}(x : M_0 : M_0) : \text{func}(x : M_0 : M)$</td>
<td>$\Gamma \vdash p : M_0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Func</th>
<th>Sub</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma \vdash (x)_{_\text{ndef}}$</td>
<td>$\Gamma \vdash p : M_0$</td>
</tr>
<tr>
<td>$\Gamma \vdash \text{module} x = \text{abs}_{\text{param}} \tau_0 \tau_1$</td>
<td>$\Gamma \vdash p.m = M_0$</td>
</tr>
<tr>
<td>$\Gamma \vdash \text{func}(x : M_0 : M_0) : \text{func}(x : M_0 : M)$</td>
<td>$\Gamma \vdash p : M_0$</td>
</tr>
</tbody>
</table>

Restriction checking $\Gamma \vdash \{ \text{var} \langle \tilde{e}_1 : \tilde{E}_1 \rangle ; s \}; \text{return } e \} \triangleright \theta$.

<table>
<thead>
<tr>
<th>RestrCheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma \vdash \text{body} \triangleright \lambda_m$</td>
</tr>
<tr>
<td>$\Gamma \vdash \text{body} \triangleright \lambda_m \land \lambda_c$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RestrMemExt</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma \vdash s \triangleright \lambda_m$</td>
</tr>
<tr>
<td>$\Gamma \vdash e \triangleright \lambda_m$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RestrMemExt</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{mem}_\Gamma(s) \subseteq \lambda_m$</td>
</tr>
<tr>
<td>$\text{var}_\Gamma(e) \subseteq \lambda_m$</td>
</tr>
</tbody>
</table>

RestrComplTop

<table>
<thead>
<tr>
<th>RestrCompl</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E \vdash { \top } s { \psi</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RestrCompl</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E \vdash { :, : s }; \text{return } r } \triangleright \lambda_c$</td>
</tr>
</tbody>
</table>

Notes: the relation $\subseteq$ checks the inclusion of a memory restriction into another, and is defined in Figure 18.

Also, $\text{mem}_\Gamma(s)$ computes an over-approximation of a instruction’s memory footprint, and is defined in Figure 19.

Figure 15: Restriction checking rules.

```
| module A = |
| module B = |

| module C = |
| module E = A.B |
| module F = B |
```

Figure 16: Example of valid and invalid paths.

```
| module A = |
| module B = |
| module C = |
| module E = |
```

Figure 17: Example of procedures typing.

declaration of an abstract module of kind $\text{param}$, only of open modules of kind $\text{open}$, which are never substituted, only instantiated). Instead, we only need to show closure under such substitution for typing judgment (not Hoare logic derivations), which makes the proof simpler.

B.2 Additional Typing Rules

The memory restriction union $\sqcup$, intersection $\sqcap$ and the memory restriction subset $\subseteq$ operations are defined in Figure 18. In Figure 19, we present our sub-typing rules, our typing rules for statements and expressions, and the definition of the function $\text{mem}_\Gamma(p)$ which computes the memory footprint of $p$ in $\Gamma$. Note that we need two different rules to type function paths: T-Proc1 does a lookup of the procedure as a component of an already typed module; and T-Proc2 does a lookup of the procedure in the typing environment,
in case the procedure is declared in one of the parent modules of the current sub-module being typed (consequently, these modules are not yet fully typed).

Example B.1. Consider the modules and procedures given in Figure 17. When typing \( h \), the typing environment contains one module declaration and one procedure declaration:

\[
\Gamma = (\text{module A.B = } \_:: \text{struct proc } f() \rightarrow \text{unit end}; (\text{proc A.C.g() } \rightarrow \text{unit } = \ldots))
\]

Here, the call to \( f \) in \( h \) is typed using the T-Proc1 rule, while the call to \( g \) is typed using T-Proc2.

C MODULE RESOLUTION

Our module resolution mechanism, given in Figure 21, allows to evaluate any module expression \( m \) in a typing environment \( \Gamma \) (mostly, it takes care of functor applications). Essentially, this defines the semantics of our module system, and will be used to give the semantics of our programming language in Appendix E.

Extended module resolution. Because a module expression \( m \) is evaluated in a typing environment \( \Gamma \) that can contain abstract modules (representing open code or functor parameters), the resolved module \( \text{res}_T(\_m) \) may not be a module expression according to the syntactic categories defined in Figure 13. We let extended module expressions be the elements of the form:

\[
m := m | \text{abs}_x^y
\]

Note that it would not make much sense to extend the syntax of module expressions to allow them to contain abstract modules, as abstract modules of kind \text{param} are reserved to the type system; and \text{open} modules must be introduced at the logical level (in the ambient higher-order logic).

Module resolution. The resolution function \( \text{res}_T(\_m) \) evaluates a module path, in \( \Gamma \), into a (resolved) extended module expression, which can be a module structure, a functor, or an (potentially applied) abstract module. Mostly, \( \text{res}_T(\_m) \) take care of functor application through the rules:

\[
\begin{align*}
\text{res}_T(p(p')) &= \text{res}_T(m_0[x \mapsto p']) & (\text{if } \text{res}_T(p) = \text{func}(x : M) m_0) \\
\text{res}_T(p(p')) &= (\text{abs}_x^y)(\text{res}_T(p')(p_0)) & (\text{if } \text{res}_T(p) = (\text{abs}_x^y)(p_0))
\end{align*}
\]

(the full definition is in Figure 21). In the concrete functor case, we must substitute the module identifier \( x \) into a path \( p' \) in a module expression \( m_0 \).

Example C.1. Consider a typing environment \( \Gamma \), and the path \( x.y(z)(v)(w) \), which must be read as (((x,y,z)(v))(w)). Then, assuming that \( \Gamma(z) = \text{absopen } z, \Gamma(v) = m_v, \Gamma(w) = \text{absparam } w \) and:

\[
\Gamma(x) = \text{struct module } y = \text{func}(u : \ldots) \text{ end}
\]

where \( m_v \) is some module expression, then \( \text{res}_T(x.y(z)(v)(w)) = (\text{absopen } z)(v, w) \).

We define the module procedure resolution function \( f \cdot \text{res}_T(\_m, f) \). A resolved module procedure \( f \cdot \text{res}_T(\_m, f) \) is: i) either a concrete procedure declaration (\( \text{proc } f(t) \rightarrow \tau_r = \text{body} \)); ii) or the procedure component \( f \) of a resolved (potentially applied) abstract module \( \text{abs}_x^y(f(p)) \).

Soundness. Then, we need show that our module resolution mechanism has the subject reduction property. Unfortunately, this does not hold, because of sub-modules declarations, as shown in the following example.

Example C.2. Consider a well-typed typing environment \( \vdash \Gamma \), and a module path \( p \) where:

\[
\Gamma \vdash p : \text{sig } S_1; \text{module } x : M_1; \text{ restr } \_ \text{ end}
\]

We are going to assume that some kind of subject reduction property holds for \( p \). More precisely, we assume that:

\[
f \cdot \text{res}_T(p) = (\text{struct } S_1; \text{module } x = m_1; \text{ end})
\]
Module signature and structure sub-typing \( \vdash \mathcal{M}_1 <: \mathcal{M}_2 \) and \( \vdash \mathcal{S}_1 <: \mathcal{S}_2 \).

We omit the reflexivity and transitivity rules.

\[ \frac{\vdash \mathcal{S}_1 <: \mathcal{S}_2 \quad \vdash \theta_1 <: \theta_2}{\vdash \text{sig } \mathcal{S}_1 \text{ restr } \theta_1 \text{ end } <: \text{sig } \mathcal{S}_2 \text{ restr } \theta_2 \text{ end}} \]

\[ \frac{\vdash \mathcal{M}_1' <: \mathcal{M}_0 \quad \vdash \mathcal{M} <: \mathcal{M}'}{\vdash \text{func}(\mathcal{M}_0) \mathcal{M} <: \text{func}(\mathcal{M}_0') \mathcal{M}'} \]

\[ \forall i \in \{1; \ldots; n\}, \vdash \mathcal{D}_i <: \mathcal{D}_i' \]

\[ \vdash \text{module } x : \mathcal{M}_1 <: \text{module } x : \mathcal{M}_2 \]

Statements and function paths typing \( \Gamma \vdash s \) and \( \Gamma \vdash f : \_ \).

**T-Abort**
\[ \Gamma \vdash \text{abort} \quad \Gamma \vdash s \]

**T-Skip**
\[ \Gamma \vdash \text{skip} \quad \Gamma \vdash s \]

**T-Seq**
\[ \Gamma \vdash \text{x} : \tau \quad \Gamma \vdash e : \tau \quad \Gamma \vdash \text{x} \leftarrow e \]

**T-Call**
\[ \Gamma \vdash f : \text{proc } \mathcal{F} \left( \hat{v} : \hat{\tau} \right) \rightarrow \tau_r \quad \Gamma \vdash \text{x} : \tau_r \quad \Gamma \vdash \hat{v} : \hat{\tau} \quad \Gamma \vdash \text{x} \leftarrow \text{call } f(\hat{v}) \]

**T-Proc1**
\[ \Gamma \vdash p : \text{sig } (S_1 ; \text{proc } \mathcal{F} \left( \hat{v} : \hat{\tau} \right) \rightarrow \tau_r ; S_2) \quad \text{restr } \theta \quad \Gamma \vdash \text{x} \leftarrow \text{call } f(\hat{v}) \]

**T-Proc2**
\[ \Gamma \vdash (\mathcal{P}, p) \equiv (\text{proc } f(\mathcal{V} : \mathcal{V} \rightarrow \tau_r) \rightarrow \tau_r) \quad \Gamma \vdash p \vdash f(\mathcal{V} : \mathcal{V} \rightarrow \tau_r) \]

**T-Assign**
\[ \Gamma \vdash \text{x} : \tau \quad \Gamma \vdash e : \tau \quad \Gamma \vdash \text{x} \leftarrow e \]

**T-While**
\[ \Gamma \vdash e : \text{bool} \quad \Gamma \vdash s_1 \quad \Gamma \vdash s_2 \quad \Gamma \vdash \text{while } e \text{ do } s \]

**T-If**
\[ \Gamma \vdash e : \text{bool} \quad \Gamma \vdash s_1 \quad \Gamma \vdash s_2 \quad \Gamma \vdash \text{if } e \text{ then } s_1 \text{ else } s_2 \]

Expressions typing \( \Gamma \vdash e : \tau \).

**ExprApp**
\[ \text{type}(f) = \tau_1 \times \cdots \times \tau_n \rightarrow \tau \quad \forall i \in \{1; \ldots; n\}, \Gamma \vdash e_i : \tau_i \quad \Gamma \vdash f(\langle e_1, \ldots, e_n \rangle) : \tau \]

**ExprVar**
\[ \Gamma \vdash (\mathcal{V}) = \tau \quad \Gamma \vdash \mathcal{V} : \tau \]

Restriction entailment \( \vdash \theta <: \theta' \).

We omit the transitivity and reflexivity rules for \( \vdash \theta <: \theta' \).

**\bot-Proc**
\[ \forall f \in \text{dom}(\theta, \theta'), \vdash \theta[f] <: \theta'[f] \]

**\bot-Split**
\[ \vdash \lambda_m <: \lambda_m', \lambda_e <: \lambda_e' \quad \vdash \lambda_m \wedge \lambda_e <: \lambda_m' \wedge \lambda_e' \quad \vdash \lambda <: \top \quad \vdash \lambda_m <: \lambda_m' \quad \vdash \lambda_e <: \top \]

**\bot-Compl**
\[ k \leq k' \quad \forall i, k_i \leq k_i' \]

\[ \text{compl[intr} : l, x_1; f_1 : k_1; \ldots; x_n; f_n : k_n]\]

Memory restriction.

\[ \text{mem}_\mathcal{F}(\text{abort}) = \emptyset \quad \text{mem}_\mathcal{F}(\text{skip}) = \emptyset \]

\[ \text{mem}_\mathcal{F}(x \leftarrow e) = \{x\} \cup \text{vars}(e) \quad \text{mem}_\mathcal{F}(x \leftarrow d) = \{x\} \]

\[ \text{mem}_\mathcal{F}(\text{if } e \text{ then } s_1 \text{ else } s_2) = \text{vars}(e) \cup \text{mem}_\mathcal{F}(s_1) \cup \text{mem}_\mathcal{F}(s_1) \]

\[ \text{mem}_\mathcal{F}(x \leftarrow \text{call } p.f(\hat{v})) = \{x\} \cup \text{mem}_\mathcal{F}(p.f) \cup \text{vars}(\hat{v}) \]

\[ \text{mem}_\mathcal{F}(p.f) = (\text{mem}_\mathcal{F}(s)) \cup \text{vars}(r) \cup \{\hat{v}; \hat{v_i}\} \]

When \( \text{f-res}_\mathcal{F}(p.f) = (\text{proc } f(\mathcal{V} : \mathcal{V} \rightarrow \tau_r) \rightarrow \tau_r) \):

\[ \text{mem}_\mathcal{F}(p.f) = (\text{mem}_\mathcal{F}(s)) \cup \mathcal{V}_i \cup \text{vars}(\mathcal{V}) \]

When \( \text{f-res}_\mathcal{F}(p.f) = (\text{absK } x(p_0).f, K = \text{open} \text{ and } \Gamma(x) = \text{absK } : \text{func}(\mathcal{V}) \text{ sig } \_ \text{ restr } \theta \text{ end}) \):

\[ \text{mem}_\mathcal{F}(p.f) = \theta[f] \cup \text{mem}_\mathcal{F}(p_0) \]

When \( \text{f-res}_\mathcal{F}(p.f) = (\text{absParam } x)(p_0).f) \):

\[ \text{mem}_\mathcal{F}(p.f) = \text{mem}_\mathcal{F}(p_0) \]

Figure 19: Additional typing rules and operations.
Then, we know that $p$ and that we have a derivation:

\[
\text{module resolution function w.r.t. the typing judgment } \Gamma \text{ can have:}
\]

\[
\text{inst} \text{ not have:}
\]

\[\begin{align*}
1 & \Rightarrow S(d : \text{module } y_1); \ldots ; D_n : \text{module } y_m) \Rightarrow \text{abort if } e_1; 1 & \Rightarrow \text{return } s_1; \text{else } s_2; \text{end}
\end{align*}\]

Consequently, it is not well-typed in $\Gamma \vdash \text{abort}$; $\text{return } s_1; \text{else } s_2; \text{end}$. Figure 20: Substitution functions.

Instead, we introduce another typing judgment, noted $\Gamma \vdash m : M$, which is similar to the typing judgment $\Gamma \vdash p : M$ of Figure 14, but is used to type a module expression in an environment which has already been typed, while $\Gamma \vdash p : M$ is used to type a module declaration in an environment where some modules have not yet been fully typed. We postpone its definition to Appendix D. Using this alternative typing judgment notion, we can state the subject reduction property we want (the proof is postponed to Appendix D).

Lemma C.1 (Subject reduction). If $\Gamma \vdash E$ and $\Gamma \vdash m : M$ then $\Gamma \vdash \text{res}_{E}(m) : M$ whenever $\text{res}_{E}(m)$ is well-defined.

D \quad \text{SUBJECT REDUCTION PROPERTY OF MODULE RESOLUTION}

The goal of this section is to prove that the module resolution mechanism of Figure 21 has the subject reduction property (Lemma C.1), which we recall below:
Module path resolution $\text{res}_T(p)$ to module expression

$\text{res}_T(p) = \text{res}_T(m)$ (if $\Gamma(p) = \bar{m}$)

$\text{res}_T(p,x) = \text{res}_T(m)$ (if $\text{res}_T(p) = \text{struct} s; \text{module} x = m; M_1$)

$\text{res}_T(p(x)) = \text{res}_T(m)$ (if $\text{res}_T(p) = \text{abs}_K x(p_0')$)

Module expression resolution $\text{res}_T(m)$

$\text{res}_T(\text{func}(x : M) m) = \text{func}(x : M) m$

$\text{res}_T((\text{abs}_K x)(\bar{p})) = (\text{abs}_K x)(\bar{p})$

Module procedure resolution $\text{f-res}_T(m,f)$

(\text{note that this includes resolution for paths } \text{f-res}_T(p,f))

$\text{f-res}_T(p,f) = (\text{proc } f(\bar{v} : \bar{T}) \to \tau_r = \text{body})$

$\text{f-res}_T(\text{struct} s; \text{proc} f(\bar{v} : \bar{T}) \to \tau_r = \text{body})$

$\text{f-res}_T((\text{abs}_K x)(\bar{p})).f = (\text{res}_T(m) = (\text{abs}_K x)(\bar{p}))$

Module structure typing $\Gamma \vdash \tau \text{ st : } S.$

$\text{body} = \{ \text{var } (\tilde{v}_1 : \tilde{T}_1); s, \text{ return } r \}$

$\text{f-res}_T(p,f) = \text{body}

$\text{f-res}_T(\text{struct} s; \text{proc} f(\bar{v} : \bar{T}) \to \tau_r = \text{body})$

$\text{f-res}_T((\text{abs}_K x)(\bar{p})).f = (\text{res}_T(m) = (\text{abs}_K x)(\bar{p}))$

Module expression typing $\Gamma \vdash \bar{m} : M.$

$\text{D-Resolve}$

$\Gamma \vdash \bar{p} : M$

$\text{D-Struct}$

$\Gamma \vdash \text{struct} s; \text{sig} S \text{ restr } \theta : S$

$\text{D-Func}$

$\Gamma \vdash \bar{m} : M$

$\Gamma \vdash \text{func}(x : M) m : \text{func}(x : M_0) M$

$\text{D-Sub}$

$\Gamma \vdash \bar{m} : M_0$

$\Gamma \vdash \bar{m} : M$

$\text{D-Abs}$

$\Gamma \vdash (\text{abs}_K x)(\bar{p}) : \text{func}(y : M) M$

$\Gamma \vdash (\text{abs}_K x)(\bar{p}) : \text{func}(y : M) M$

$\text{D-Compt}$

$\Gamma \vdash \text{sig} S; \text{module} x : M, S_2 \text{ restr } \theta : S$

$\text{D-FuncApp}$

$\Gamma \vdash m : \text{func}(x : M) M$

$\Gamma \vdash \text{func}(x : M) m : \text{func}(x : M_0) M$

$\text{D-EnvSeq}$

$\Gamma \vdash \Gamma_1 \Gamma_2$

$\Gamma \vdash \varepsilon$

$\text{D-EnvMod}$

$\Gamma \vdash \text{module} x : M$

$\Gamma \vdash \text{module} x : M$

$\text{D-EnvVar}$

$\Gamma \vdash (\text{var } u : \tau)$

$\Gamma \vdash (\text{var } u : \tau)$

$\text{D-Jump}$

$\Gamma \vdash (\text{module} x = M)$

$\Gamma \vdash (\text{module} x = M)$

$\text{D-EnvAbs}$

$\Gamma \vdash (\text{abs}_K x : M)$

$\Gamma \vdash (\text{abs}_K x : M)$

Figure 21: Resolution functions for paths, module expressions and module procedure.

Lemma (Subject reduction). If $\Gamma \vdash E$ and $\Gamma \vdash m : M$ then $\Gamma \vdash \text{res}_E(m) : M$ whenever $\text{res}_E(m)$ is well-defined.

Essentially, this lemma states that evaluating a module expression preserves its type. This is a crucial property that allows to show that memory and complexity restrictions are preserved by the evaluation of a module using the module resolution mechanism. That is, the module expression resulting from the evaluation of another module expression has the same memory footprint, and satisfies the same complexity restrictions.

Proof outline. The proof is essentially the proof that simply typed $\lambda$-calculus has the subject reduction properties, with some consequent additional work to handle module restrictions.

The rest of this section is organized as follows: we define the typing rules for $\Gamma \vdash : M$ in Appendix D.1, and prove the link between $\Gamma \vdash m : M$ and $\Gamma \vdash_\theta m : M$; we present an alternative, more computational, way of defining the module resolution procedure in Appendix D.2; finally, we prove that the module resolution procedure has the subject reduction property in Appendix D.3.

D.1 Typing in Typed Environments

During the resolution of a module expression $m$, we may have to resolve applied module paths of the form $m(p')$. This is done by first evaluating $p$ into a function or an abstract module, and then performing the application. Consequently, we can have intermediate expressions of the form $m(p)$. Similarly, when resolving a module component access $p.x$, we first resolve $p$ into a module structure and then access its component $x$. This yields intermediate expressions of the form $m.x$.

Example D.1. We recall Example C.1 which we presented in Section 3. We recall that $\Gamma$ is a typing environment $\Gamma$ such that:

$\Gamma(x) = \text{struct} \text{ module } y = \text{func}(u : \_ ) \text{ end }$

$\Gamma(z) = \text{abs}_\text{open} z$

$\Gamma(v) = m_v$

$\Gamma(w) = \text{abs}_\text{open} w$

where $m_v$ is some module expression. The resolution of the module expression $x.y(z)(v)(w)$ in $\Gamma$ is as follows:

$x.y(z)(v)(w)$

\Rightarrow_\text{res. step} \text{ (struct module } y = \text{func}(u : \_ ) \text{ end } \gamma(z)(v)(w)$
We introduce a new notion of lookup in a typing environment, well-formed.

For example, assume that:

- we descend in sub-module declarations to retrieve the type of declaration corresponding to
- if it contains no duplicate declarations, and it contains only well-formed environments. Essentially, a typing environment structure and module environment typing rules given in Figure 14,

We give the rules for typing in already typed environment in

It is enough to allow only top-level applications of module expressions to module paths and module component accesses.

We give the rules for typing in already typed environment in

We recall that given a module path \( p \), \( \Gamma \) returns the typing declaration corresponding to \( p \) in \( \Gamma \), if it exists. Note that this does not descend in sub-module declarations to retrieve the type of \( p \).

For example, assume that:

\[
\Gamma = \text{module } p = \text{struct module } x = m \text{ end}:
\]

\[\text{(sig module } x : M \text{ restr } \_ \text{ end)}\]

then \( \Gamma(p) = _\_ \text{(sig module } y : M \text{ restr } \_ \text{ end)} \), but \( \Gamma(p.y) \) is not defined.

We introduce a new notion of lookup in a typing environment, \( \Gamma[p] \), which descends in sub-module declarations. It also descends below functor definitions, in the case where the functor argument is a module identifier. Continuing the example above, we have \( \Gamma[p.y] = m : M \). Formally:

**Definition D.3.** For every well-formed typing environment \( \Gamma \) and module path \( p \), we let:

\[
\begin{align*}
\Gamma[p] &= m : M & \text{(if } \Gamma(p) = m : M) \\
\Gamma[p(x)] &= m : M & \text{(if } \Gamma[p] = \text{func}(x : M_0) m : \text{func}(x : M_0) M) \\
\end{align*}
\]

where the functor rule is module alpha-renaming. Moreover, if:

\[
\begin{align*}
\Gamma[p] &= \text{struct } \_ : \text{module } x = m; \_ \text{ end} \\
& \text{then:} \\
\Gamma[p.x] &= m : M \\
\end{align*}
\]

The following proposition allows to replace a typing environment \( \Gamma_0 \) by \( \Gamma_1 \), as long as they coincide w.r.t. \([p]\) on every \( p \) such that \( \Gamma_0[p] \) is well-defined.

**PROPOSITION D.2.** For every well-formed environments \( \Gamma_0 \) and \( \Gamma_1 \), if \( \Gamma_0[p] = \Gamma_1[p] \) for every \( p \) such that \( \Gamma_0[p] \) is well-defined, then for any \( m \) and \( M \), if \( \Gamma_0 \vdash m : M \) then \( \Gamma_1 \vdash m : M \).

**Proof.** This is immediate by induction over the typing derivations \( \Gamma_0 \vdash m : M \).

**Example D.2.** The following two typing environments \( \Gamma_0 \) and \( \Gamma_1 \) verify the proposition hypothesis:

\[
\begin{align*}
\Gamma_0 &= \text{module } p.x = m : M; \text{module } p.y = m' : M' \\
\Gamma_1 &= \text{module } \_ = m; \text{module } \_ = m' \text{ end} \\
& \text{end} \\
& \text{end} \\
& \text{end}
\end{align*}
\]

We can strengthen the context.

**PROPOSITION D.3.** For any well-formed environment \( \Gamma \), if \( (\Gamma, \Gamma_1) \) is well-formed then \( \Gamma, \Gamma_1 \vdash m : M \) whenever \( \Gamma \vdash m : M \).

**Proof.** This is straightforward by induction over the typing derivation \( \Gamma \vdash m : M \).

We can replay a typing derivation if we have a finer type for a module declaration in the context.

**PROPOSITION D.4.** For any well-formed environment \( \Gamma \), if

\[
\Gamma, \text{module } p = m : M, \Gamma_1 \vdash m_0 : M_0
\]

then for any \( \Gamma, \Gamma' \vdash M' <= M \), we have

\[
\Gamma, \text{module } \_ = m' : M', \Gamma_1 \vdash m_0 : M_0
\]

**Proof.** We show this by induction over the typing derivation \( \Gamma, \text{module } p = m : M, \Gamma_1 \vdash m_0 : M_0 \), by replacing any application of the \( \text{D-ALIAS} \) typing rule on a path starting by \( p \), i.e. of the form \( p(p_0, \ldots, p_n) \), \( p' \), by an application of \( \text{D-ALIAS} \) on \( p \), followed by \( \text{D-SUB} \) and by the applications of \( \text{D-FUNAPP} \) and \( \text{D-COMPNT} \) to replay the path typing derivation of \( \Gamma \vdash p(p_0, \ldots, p_n) \).
Lemma D.5. For every well-formed typing environment $\Gamma$ such that $\Gamma(p) \vdash \text{undef}$:

- if $\Gamma \vdash p \vdash m : M$ then there exists $M'$ well-formed in $\Gamma$ such that $\vdash M' < : M$

\[ \Gamma; \text{module } p = m : M' \vdash m : M' \]

- if $\Gamma \vdash p, \theta (d_1, \ldots, d_n) : (D_1, \ldots, D_n)$ then there exists $D'_1, \ldots, D'_n$ well-formed such that $\vdash D'_i < : D_i$ for every $i$ and:

\[ \Gamma; \delta_1, \ldots, \delta_n \vdash \theta (d_1, \ldots, d_n) : (D_1, \ldots, D_n) \]

where for every $i$:

\[ \delta_i = \text{module } p.x = m : M \]

if $D'_i = (\text{module } x : M)$ and $d_i = (\text{module } x = m)$, and

\[ \delta_i = \text{proc } p.f.(\bar{v} : \bar{\tau}) \rightarrow \tau_r = \text{body} \]

if $d_i = (\text{proc } f.(\bar{v} : \bar{\tau}) \rightarrow \tau_r = \text{body})$.

Proof. The proof is by induction over the typing derivations in hypothesis.

- the Alias and StructEmp cases are immediate. Note that we use the hypothesis $\Gamma(p) \vdash \text{undef}$ in the Alias case, to ensure that the path lookup in $\Gamma$ is still well-formed.

- we show the Struct case by applying the induction hypothesis, and using Proposition D.2.

- for ModDecl we have $\Gamma(x) \vdash \text{undef}$ in the ModDecl case, to ensure that the path lookup in $\Gamma$ is still well-formed.

- we show the ModDecl case by applying the induction hypothesis, and using Proposition D.2.

- for ModDecl we have $\Gamma(x) \vdash \text{undef}$ in the ModDecl case, to ensure that the path lookup in $\Gamma$ is still well-formed.

Figure 23: The relation $\vdash_r$.

- for Sub, we have:

\[ \begin{array}{c}
\text{Sub} \\
\Gamma \vdash p \vdash m_0 \\
M_0 \vdash M_0 < : M
\end{array} \]

By induction hypothesis, we have a derivation of $\Gamma$, module $p : M_0 \vdash M_0' : M_0$ such that $\vdash M_0' < : M_0$. Using the sub-typing transitivity rule, we have that $\vdash M_0' < : M$. This concludes this case.

- for Func we have $m = \text{func}(x : M_0) m'$ and $M = \text{func}(x : M_0) M'$, and the derivation:

\[ \begin{array}{c}
\text{Func} \\
\Gamma \vdash M_0 \\
\Gamma \vdash \text{func}(x : M_0) m' : \text{func}(x : M_0) M'
\end{array} \]

By induction hypothesis, we have a derivation of $\Gamma$, module $p : M_0 \vdash \text{func}(x : M_0) m'$ and $M = \text{func}(x : M_0) M'$.

By applying the D-Func rule, there is a derivation of:

\[ \begin{array}{c}
\Gamma, \text{module } p \vdash \text{func}(x : M_0) m' : \text{func}(x : M_0) M'
\end{array} \]

By Proposition D.2, there is a derivation of:

\[ \begin{array}{c}
\Gamma, \text{module } p = (\text{func}(x : M_0) m') : (\text{func}(x : M_0) M') \vdash M'
\end{array} \]

We extend sub-typing judgments to typing environments, by requiring that $\vdash I_0 < I_1$ whenever $I_0$ and $I_1$ are of the same length, and any declaration in $I_0$ is a sub-type of the corresponding declaration in $I_1$.

Lemma D.6. If $\vdash I \vdash p \vdash \text{env}$ such that $\vdash I' < : I$.

Proof. We use Lemma D.5 to replace the EnvMod rules by D-EnvMod rules. We omit the details.

D.2 Module Resolution as a Rewrite Relation

We define in Figure 23 the relation $\vdash_r$ on partially resolved module expressions. This relation is exactly the evaluation strategy used by the module resolution procedure defined in Figure 21.

We let $\bar{m}$ be the normal form of $m$ w.r.t. the reflexive and transitive closure of $\vdash_r$, if it exists.

We now state a property of $\vdash_r$ in the case where $\Gamma$ is an environment, i.e. top-level module declarations are not module aliases.
we state the following substitution lemmas.

Moreover, for any well-formed module path, if $\text{res}_E(m)$ is well-defined then $\text{res}_E(m) = \tilde{m}$.

Proof. The fact that $\rightarrow_T$ is deterministic is straightforward from the definition of $\rightarrow_T$ in Figure 23: indeed, we only need to observe that well-formed module expressions cannot have two module declarations with the same name.

Moreover, for any $m_1$ and $m_2$, if $m_1 \rightarrow_T m_2$ and $m_1$ is well-formed then so is $m_2$. Hence if $\rightarrow_T$ terminates on a well-formed $m$ then $\tilde{m}$ exists.

Let $E$ be a well-typed environment. We show the second point by induction over the length of the computation of $\text{res}_E(m)$. In the environment lookup case, we use the fact that $E(p)$ is either a module structure, functor or an abstract module, and is therefore in $\rightarrow_E$-normal form. We omit the rest of the proof.

\section{D.3 Subject Reduction}

Before proving that our system has the subject reduction property, we state the following substitution lemmas.

\textbf{Lemma D.8 (Substitution 1).} We have the following substitution properties:

- if $\theta_1 \mathrel{\ll} \theta_2$ then $\theta_1[x \mapsto \lambda_m] \mathrel{\ll} \theta_2[x \mapsto \lambda_m]$.
- if $\lambda_1 \mathrel{\ll} \lambda_2$ then $\lambda_1[x \mapsto \lambda_m] \mathrel{\ll} \lambda_2[x \mapsto \lambda_m]$.
- if $\Gamma \vdash m_0 \mathrel{\ll} m'_0$ then $\Gamma[x \mapsto \lambda_m] \mathrel{\ll} m'_0[x \mapsto \lambda_m]$.

Proof. The properties above are shown by induction over their respective typing derivation.

\textbf{Lemma D.9 (Substitution 2).} For every:

$$\Gamma_1; \text{module } x \equiv \text{abs}_{\text{param}} : M; \Gamma_2$$

which is a well-formed typing environment, if:

$$\Gamma_1; \text{module } x \equiv \text{abs}_{\text{param}} : M; \Gamma_2 \vdash e : \tau$$

then:

$$\Gamma_1; \Gamma_2[x \mapsto \lambda_m] \vdash e : \tau$$

Proof. The proof is immediate by induction over the typing derivation, since module types in the typing environment are not used when typing expressions.

\textbf{Proposition D.10.} For any well-formed typing environment $\Gamma$, if $\Gamma \vdash p : M$ and $\text{mem}_\Gamma(p) = \lambda_m$ then:

$$\text{mem}_\Gamma(F[x \mapsto p]) \subseteq (\{ \text{mem}_\Gamma; \text{module } x \equiv \text{abs}_{\text{param}}; \text{M}(\Gamma)(x \mapsto \lambda_m)\})$$

\textbf{Lemma D.11 (Substitution 3).} For every well-formed environment $\Gamma$ of the form:

$$\Gamma_1 ; \text{module } x \equiv \text{abs}_{\text{param}} : M; \Gamma_2$$

for every module path $p$ such that $\Gamma_1 \vdash m \mathrel{\ll} M$, if $\text{mem}_\Gamma(p) = \lambda_m$ then:

- if $\Gamma \vdash m : M_0$ then:
  $$\Gamma_1; \Gamma_2[x \mapsto \lambda_m] \vdash m[x \mapsto p] : M_0[x \mapsto \lambda_m]$$
- if $\Gamma \vdash \{ \text{var}(\tilde{c}_i ; \tilde{n}_i); s; \text{return } e \} ; \Lambda$ then:
  $$\Gamma_1; \Gamma_2[x \mapsto \lambda_m] \vdash \{ \text{var}(\tilde{c}_i ; \tilde{n}_i); s[x \mapsto p]; \text{return } e \} ; \lambda[x \mapsto \lambda_m]$$

Proof. We prove the two properties above simultaneously, by induction over the corresponding typing derivations. The proof is straightforward (we omit the details).

Note that we do not need to show closure under substitution of module parameters in Hoare derivations, only in typing derivations (see Remark B.1).

\textbf{Lemma D.12.} If $\Gamma \vdash E$ and $\Gamma \vdash m : M$ then if $m \rightarrow_T m'$ then $\Gamma \vdash m' : M$.

Proof. W.I.O.G., we assume that the typing derivations $\Gamma \vdash E$ and $\Gamma \vdash m : M$ never apply the $D\text{-Sub}$ typing rules twice in a row (using the transitivity rule for sub-typing judgments). To simplify derivations, we also assume that $D\text{-Sub}$ is applied once between each typing rule application (using the sub-typing reflexivity rule if necessary).

We do a case analysis on the reduction $m \rightarrow_T m'$.

- if $x \rightarrow_T E(x)$. We check that we must have a derivation of the following form:

\begin{align*}
\text{D- Alias} & \quad \Gamma \vdash \_ : M_0 \\
\text{D-Sub} & \quad \Gamma \vdash x : M_0 \quad \vdash M_0 \mathrel{\ll} M \\
& \quad \Gamma \vdash x : M \\
\end{align*}

Using the fact that $\Gamma \vdash E$, we know that $E = (E_0; \text{module } x \equiv m : M_0; E_2)$ and $\Gamma \vdash m : M_0$. We conclude by applying $D\text{-Sub}$.

- if $m.x \rightarrow_T m'$. We check that we must have a derivation of the following form:

\begin{align*}
\text{D- Compnt} & \quad \Gamma \vdash m : \text{sig } S_1; \text{module } x : M_0; S_2 \text{ restr } \theta \text{ end} \\
\text{D- Sub} & \quad \Gamma \vdash m.x : M_0 \quad \vdash M_0 \mathrel{\ll} M \\
& \quad \Gamma \vdash m.x : M \\
\end{align*}

and:

\begin{align*}
\text{D- Struct+} & \quad \ldots \\
\text{D- Sub} & \quad \Gamma \vdash m : \text{sig } S_1; \text{module } x : M_0; S'_2 \text{ restr } \theta \text{ end} \\
& \quad \vdash M'_0 \mathrel{\ll} M_0 \quad \ldots \\
\text{D- Sub} & \quad \Gamma \vdash m : \text{sig } S_1; \text{module } x : M_0; S_2 \text{ restr } \theta \text{ end} \\
\end{align*}

Hence we have a derivation of $\Gamma \vdash m' : M'$. We conclude by sub-typing, using the fact that we can derive $M' \mathrel{\ll} M$.

- if $m.x \rightarrow_T m'.x$ where $m \rightarrow_T m'$, we know that our derivation is of the form:

\begin{align*}
\text{D- Compnt} & \quad \Gamma \vdash m : \text{sig } S_1; \text{module } x : M_0; S_2 \text{ restr } \theta \text{ end} \\
\text{D- Sub} & \quad \Gamma \vdash m.x : M_0 \quad \vdash M_0 \mathrel{\ll} M \\
& \quad \Gamma \vdash m.x : M \\
\end{align*}

By induction hypothesis, we have a derivation of:

$$\Gamma \vdash m' : \text{sig } S_1; \text{module } x : M_0; S_2 \text{ restr } \theta \text{ end}$$

We conclude immediately using $D\text{- Compnt}$ and $D\text{- Sub}$.

- the case where $m(p) \rightarrow_T m'(p)$ with $m \rightarrow_T m'$ is the same.
- if $m(p) \rightarrow_T m_0[x \mapsto p]$ where $m = \text{func}(x : M_0) m_0$, we have a derivation of the form:

\begin{align*}
\text{D- FuncApp} & \quad \Gamma \vdash m : \text{func}(x : M_0) M' \quad \Gamma \vdash p : M'_0 \\
\text{D- Sub} & \quad \Gamma \vdash m(p)[x \mapsto \lambda_m] \quad \vdash M'[x \mapsto \lambda_m] \mathrel{\ll} M \\
& \quad \Gamma \vdash m(p) : M \\
\end{align*}
where $\lambda_m = \text{mem}_T(p')$. Since $m = \text{func}(x : M_p)$, we must have a derivation of the form:

$$
\Gamma \vdash M_p \quad \Gamma(x)_\text{undefined} \triangleright
\begin{aligned}
\text{D-FNC} & \quad \Gamma, \text{module } x = \text{absparam} : M_p \vdash m_0 : M'' \\
\text{D-SUB} & \quad \Gamma \vdash \text{func}(x : M_p) m_0 : \text{func}(x : M_p) M'' \\
\end{aligned}
$$

Since $\Gamma \vdash p : M'_p$ and $\vdash M'_p : M_p$, we know that we have a derivation of $\Gamma \vdash p : M_p$. Since:

$$
\begin{aligned}
\Gamma \vdash \text{func}(x : M_p) m_0 : \text{func}(x : M_p) M''
\end{aligned}
$$

is derivable, we apply Lemma D.11 to get a derivation of:

$$
\Gamma \vdash m_0[x \mapsto p] : M''[x \mapsto \lambda_m]
$$

Using Lemma D.8, we know that since $\vdash M'' : M'$, we have a derivation of:

$$
\Gamma \vdash m_0[x \mapsto p] : M'[x \mapsto \lambda_m]
$$

• the case where $m(p) \rightarrow \Gamma(\text{absfun}(\bar{\rho}_0), p)$ and $\bar{m} = (\text{absfun}(\bar{\rho}_0)$ is immediate.

We recall and prove Lemma C.1:

**Lemma (Subject Reduction).** If $\Gamma \vdash E$ and $\Gamma \vdash m : M$ then $\Gamma \vdash \text{res}_E(m) : M$ whenever $\text{res}_E(m)$ is well-defined.

**Proof.** From Proposition D.7, we know that $\text{res}_E(m) = m \downarrow E$. From Lemma D.12, we know that the type of the module expression is preserved. This concludes this proof.

## E INSTRUMENTED SEMANTICS

We now define the denotational semantics of our programming language and cost judgments. We quickly introduce the main aspects of our semantics below, before defining it formally in the rest of the section. We use this semantics to state and prove our main soundness theorem in Appendix F.

**Program semantics.** The semantics $\llbracket s \rrbracket_{E,p}^\nu$ of our language depends on the initial memory $\nu$, the environment $E$, and on the interpretation $p$ of $E$'s abstract modules. Essentially, $\llbracket s \rrbracket_{E,p}^\nu$ is a discrete distribution over $M \times \mathbb{N}$, where the integer component is the cost of evaluating $s$ in $(E, p)$, starting from the memory $\nu$. Then, the $E$-cost of an instruction $s$ under memory $\nu$ and interpretation of $E$'s abstract modules $p$, denoted by $\text{cost}_s^E(\nu, p) \in \mathbb{N} \cup \{+\infty\}$, is the maximum execution cost in any final memory, defined as:

$$
\text{cost}_s^E(\nu, p) = \inf \left\{ c' \mid \text{Pr}(\text{Pr}(\_c) \leftarrow \llbracket s \rrbracket_{E,p}^\nu, c \leq c') = 1 \right\}
$$

**Judgments semantics.** Basically, the judgment $E \vdash \{\phi\} s \{\psi \mid t\}$ states that: i) the memory $\nu$ obtained after executing $s$ in an initial memory $\nu \in \phi$ must satisfy $\psi$; and ii) the complexity of the instruction $s$ is upper-bound by the complexity of the concrete code in $s$, plus the sum over all abstract oracles $A.f$ of the number of calls to $A.f$ times the intrinsic complexity of $A.f$. Formally:

$$
\text{cost}_s^{E,p}(\nu) \leq t[\text{conc}] + \sum_{f \in \text{procs}(E(A))} t[A.f] \cdot \text{compl}_{A.f}^{E,p}
$$

where $\text{compl}_{A.f}^{E,p}$ is the intrinsic complexity of the procedure $A.f$, i.e. its complexity excluding calls to $A$'s functor parameters.

**Outline of this Section.** We present the semantics of our programs in Appendix E.1. Then, we define the semantics of our cost judgments. This requires two additional complexity measures: the number of calls a program execution makes to some abstract procedure, and the intrinsic cost of a program execution (i.e. the cost of the program without the cost of parameters calls). These additional complexity measures are defined in Appendix E.2. Finally, we give the semantics of our cost judgment in Appendix E.3.

### E.1 Semantics

For any set $A$, we denote by $D(A)$ the set of discrete sub-distributions over $A$ — i.e. the set of function $\mu : A \rightarrow [0,1]$ with discrete support s.t. $\mu$ is summable and $|\mu| = \sum \mu(x) \leq 1$. For $x \in A$, the Dirac distribution at $x$ is written $\delta^A_x$ or $1_A$ when $A$ is clear from the context. If $\mu \in D(A)$ and $\nu : A \rightarrow D(B)$, the expected distribution of $\nu'[\mu]$ when ranging over $\mu$, written $E_{\nu}[\mu][\nu'][\nu]$ or $E[\nu'][\nu]$ is defined as $E_{\nu}[\mu]' = b \in B \sum_{a \in A} \mu(a) \mu'(a)(b)$. For $\mu \in D(A)$ and $f : A \rightarrow B$, the marginal of $\nu'(\mu')$, $f'$, written $f'(\mu') \in D(B)$, is defined as $f'(\mu') = b \in B \sum_{a \in A} f(a)(b) \mu'(a)$. We write $\pi_{n_1}^n$ for resp. the first and second marginal — i.e. when $f$ is resp. the first and second projection. For any base type $\tau \in E$, we assume an interpretation domain $\mathbb{V}_\tau$. We let $\mathbb{V}$ be the set of all possible $\mathbb{V}_\tau \in E$. A memory $\nu \in M$ is a function from $\mathbb{V}$ to $\mathbb{V}$. We write $\nu[x]$ for $\nu(x)$. For $\nu \in M$ and $v \in \mathbb{V}$, we write $\nu[x \mapsto v]$ for the memory that maps $x$ to $v$ and $y$ to $\nu[y]$ for $y \neq x$.

**Expressions semantics.** For any operator $f \in \mathbb{T}_E$ with type $\tau_1 \times \cdots \times \tau_n \rightarrow \tau$, we assume its semantic $\llbracket f \rrbracket : \mathbb{V}_{\tau_1} \times \cdots \times \mathbb{V}_{\tau_n} \rightarrow \mathbb{V}_\tau$, and the cost of its evaluation $\text{ct}_E(f \cdot \nu) : \mathbb{V}_{\tau_1} \times \cdots \times \mathbb{V}_{\tau_n} \rightarrow \mathbb{N}$. The semantics $\llbracket e \rrbracket_{\nu} : M \rightarrow \mathbb{V}$ of a well-typed expression $e$ in a memory $\nu$ is defined inductively by:

$$
\llbracket e \rrbracket_{\nu} =
\begin{cases}
\nu(x) & \text{if } e = x \in \mathbb{V} \\
[\llbracket f \rrbracket(\llbracket e_1 \rrbracket), \ldots, \llbracket e_n \rrbracket) & \text{if } e = f(e_1, \ldots, e_n)
\end{cases}
$$

And the cost of the evaluation of a well-typed expression $\text{ct}_E(e, \cdot) : M \rightarrow \mathbb{N}$ is defined by:

$$
\text{ct}_E(e, \nu) =
\begin{cases}
1 & \text{if } e = x \in \mathbb{V} \\
\text{ct}_E + \sum_{1 \leq i \leq n} \text{ct}_E(e_i, \nu) & \text{if } e = f(e_1, \ldots, e_n)
\end{cases}
$$

For technical reasons, we assume that there exists one operator with a non-zero cost. For any distribution operator $d \in \mathbb{T}_D$ with type $\tau_1 \times \cdots \times \tau_n \rightarrow \tau$, we assume its semantics $\llbracket d \rrbracket : \mathbb{V}_{\tau_1} \times \cdots \times \mathbb{V}_{\tau_n} \rightarrow \mathbb{D}(\mathbb{V}_\nu)$, and the cost of its evaluation $\text{ct}_D(d \cdot \nu) : \mathbb{V}_{\tau_1} \times \cdots \times \mathbb{V}_{\tau_n} \rightarrow \mathbb{N}$. We define similarly $\llbracket d \rrbracket : M \rightarrow \mathbb{D}(\mathbb{V})$ and $\text{ct}_D(d \cdot \nu) : M \rightarrow \mathbb{N}$.

**Environment and $E$-pre-interpretation.** To give the semantics of a program in an environment $E$, we need an interpretation of $E$'s abstract modules. An $E$-pre-interpretation is a function $p$ from $E$’s abstract modules to module expressions, with the correct types, some of our lemmas do not hold if all programs have a cost of zero.
where every complexity restriction $x$ (module expression. Note that this subsumes the syntax of state-

Moreover, if $\rho \leftarrow x$ by $c$ such that $\rho$ is subsumed by the module signature $M$ (in any memory) $\nu$ (open $\nu$ defines 

**Figure 25:** Function call counting semantics $\gamma.g \llbracket \_ \rrbracket_v^{E, \rho}$.

The $E$-cost of an instruction $s$ under memory $v$ and $E$-pre-interpretation $\rho$, denoted by $\text{cost}^{E, \rho}_v(s) \in \mathbb{N} \cup \{+\infty\}$, is defined as:

$$\text{cost}^{E, \rho}_v(s) = \sup(\text{supp}(\pi^2_v([s]_v^{E, \rho})))$$

where supp is the support of a distribution (this definition is equivalent to the one given in Section 4.3).

### E.2 Instrumented Semantics

We present two other instrumented semantics: $\gamma.g \llbracket [s]_v^{E, \rho}$ counts the number of times $s$ calls an abstract procedure $y.g$, and $\llbracket [s]_v^{E, \rho}$ measures the intrinsic cost of an instruction (i.e. without counting the cost of function calls in a functor parameters).

**Function call counting.** The function call counting semantics $\gamma.g \llbracket [s]_v^{E, \rho}$, given in Figure 25, evaluates the instruction $s$ under the memory $v$ and $E$-pre-interpretation $\rho$, counting the number of calls to the abstract procedure $y.g$.

The maximum number of calls of an instruction $s$ or module procedure $m.f$ to $y.g$ in $(E, \rho)$ is:

$$\#\text{calls}^{E, \rho}_v(s) = \max(\#\text{calls}^{E, \rho}_{y.g, v}(s))$$

(expression of $\max$ over $v \in M$)

The type of a module expression $x$ is $\text{absopen}(x)(\overline{p})$, which allows one to define the semantics of a call to an abstract procedure $\text{absopen}(x)(\overline{p}).f$ as the semantics of a call to $\rho(x)(\overline{p}).f$.

**Definition E.1.** Let $\text{erase}_{\text{comp}}(M)$ be the module signature $M$ where every complexity restriction $\lambda_v$ has been erased, by replacing it by $\top$. Then $\rho$ is a $E$-pre-interpretation if and only if for every $x$ such that $E \vdash E_1$; module $x = \text{absopen} : M_1; E_2$, we have $E_1 \vdash E_2\rho(x) : \text{erase}_{\text{comp}}(M_1)$.

Note that we type $\rho(x)$ in $E_1$, which lets the interpretation of $x$ use any module or abstract module declared before in $E$.

**Programs semantics.** If $\mu \in D(M \times \mathbb{N})$ and $n \in \mathbb{N}$, we write $\mu \circ n$ for the distribution $f^n(\mu)$ where $f : (m,c) \mapsto (m,c+1)$. Let $E$ be a well-typed environment, and $s$ be a well-typed instruction in $E$, i.e. such that $E \vdash s$. The $E$-denotational semantics of an instruction $s$ under the memory $v$ and $E$-pre-interpretation $\rho$, written $\llbracket s \rrbracket_{E, v}^{E, \rho} \in D(M \times \mathbb{N})$, is defined in Figure 24.
Intrinsic cost. The \( (E, \rho) \)-denotational semantics of an instruction \( s \) with intrinsic cost under memory \( v \) and parameters \( \bar{x} \), written \( [s]_v^{E, \rho, \bar{x}} \) is the cost of the execution of \( s \) under \( v \) in \( \rho \), without counting the costs of function calls to the parameters \( \bar{x} \). Formally, \( [\cdot]_v^{E, \rho, \bar{x}} \) is defined exactly like \( [\cdot]_v^{E, \rho, \bar{x}} \) in Figure 24, except for the abstract procedure call case, which is replaced by:

\[
i [x \leftarrow \text{call } m.f(\bar{e})]_v^{E, \rho, \bar{x}} = \begin{cases} E_{(\nu', \epsilon') - \text{call } \rho(x)(\bar{e}), E}^{E, \rho, \bar{x}}(\nu', \epsilon(\bar{e}, \nu)) & \text{ if } z \in \bar{x} \\
i[x \leftarrow \text{call } \rho(x)(\bar{e}), E]_v^{E, \rho, \bar{x}} & \text{ if } z \notin \bar{x}
\end{cases}
\]

where \( \text{f-res}_E(m.f) = (\text{absopen } z)(\bar{p}) \cdot f \).

Remark that both semantics coincide on their first component. Indeed, for any \( E \cdot \rho \)-pre-interpretation \( \rho \):

\[
\forall v s. \pi_1^s([s]_v^{E, \rho, \bar{x}}) = \pi_1^s([s]_v^{E, \rho, \bar{x}})
\]

The \( (E, \rho) \)-intrinsic cost \( i\text{-cost}_{E, \rho, \bar{x}}(\cdot) \) of an instruction \( s \) is:

\[
i\text{-cost}_{E, \rho, \bar{x}}(s) = \sup(\pi_2^s([s]_v^{E, \rho, \bar{x}}))
\]

The intrinsic cost of a procedure \( m.f \), with parameters \( \bar{x} \), is:

- If \( \text{f-res}_E(m.f) = (\text{proc } f(\nu : \bar{e}) \rightarrow \tau_r = \{ \_ ; s \} \\text{ return } r \} \) then:

  \[
i\text{-cost}_{E, \rho, \bar{x}}(m.f) = i\text{-cost}_{E, \rho, \bar{x}}(s) + c_f(r, v)
\]

- If \( \text{f-res}_E(m.f) = (\text{absopen } x)(\bar{p}) \cdot f \) then:

  \[
i\text{-cost}_{E, \rho, \bar{x}}(m.f) = i\text{-cost}_{E, \rho, \bar{x}}(\rho(x)(\bar{p}), f)
\]

And the intrinsic cost in any memory of an instruction \( s \) or a module procedure \( m.f \) is:

\[
i\text{-cost}_{E, \rho, \bar{x}}(s) = \max_{v \in M} i\text{-cost}_{E, \rho, \bar{x}}(s)
\]

\[
i\text{-cost}_{E, \rho, \bar{x}}(m.f) = \max_{v \in M} i\text{-cost}_{E, \rho, \bar{x}}(m.f)
\]

Interpretations. We now define when a pre-interpretation is an interpretation.

**Definition E.2.** Let \( E \) be an well-typed environment. A \( E \)-pre-interpretation \( \rho \) is an \( E \)-interpretation if for every module identifier \( x \) such that \( E = E_1 \cdot \text{module } x = \text{absopen } : M_1 : E_2 \) where:

\[
M_1 = \text{func}(\bar{z} : \bar{M}) \text{ sig } S_1 \text{ restr } \emptyset \text{ end}
\]

and for every procedure \( f \in \text{procs}(S) \), for every valuation \( \bar{m} \) of the function’s parameters such that, for every \( 1 \leq i \leq |\bar{z}| \), if we let \( z_i = \bar{z}[i], m_i = \bar{m}[i] \) and \( M_i = \bar{M}[i] = \text{sig } \_ \text{ restr } \lambda_1 \& \_ \text{ end} \),

\[
E \vdash \text{(module } z_i = m_i : \text{erase}_M(M_1))
\]

and

\[
\forall g \in \text{procs}(M_1), \text{cost}^{E, \rho}(m_i, g) \leq \lambda_1
\]

(with the convention that \( j \leq T \) for any integer \( j \)) then the execution of \( f \) in any memory verifies the complexity restriction in \( \theta[f] \).

Formally, let \( E' = E \cdot \text{module } \bar{z} = \text{absopen } \cdot M \) and \( \rho' = \rho(\bar{z} : \bar{m}) \), and:

\[
\theta[f] = \_ \& \lambda_c = \text{compl}^{E, \rho'}(\text{intr } \cdot k, y_1.f_1 : k_1, \ldots, y_l.f_l : k_l)
\]

Then for every \( 1 \leq j \leq l \),

\[
\#\text{calls}^{E, \rho'}(y_j.f_j, \bar{z}, f) \leq k_j \text{ and } i\text{-cost}^{E, \rho', \bar{z}}(x(\bar{z}), f) \leq k
\]

### E.3 Soundness of our Proof System

We now have all the tools to define the semantics of our expression and program cost judgments.

**Definition E.3.** The judgment \( \vdash \{ \phi \} e \leq t_e \) stands for:

\[
\forall v \in \phi, c_E(e, v) \leq t_e
\]

**Definition E.4.** The judgment \( E \vdash \{ \phi \} s \{ \psi \mid t \} \) means that for any \( E \cdot \rho \)-interpretation \( \rho \) and \( v \in \phi \):

\[
\sup(\pi_1^s([s]_v^{E, \rho, \bar{x}})) \subseteq \psi \wedge \text{cost}_{E, \rho}(s) \leq t[\text{conc}] + \sum_{f \in \text{procs}(E(A))} A_t \cdot f \cdot \text{compl}^{E, \rho}_F
\]

Basically, the complexity of the instruction \( s \) is upper-bounded by the complexity of the concrete code in \( s \), plus the sum over all abstract oracles \( A.f \) of the number of calls to \( A.f \) times the intrinsic complexity of \( A.f \).

### F HOARE LOGIC FOR COST

We present the full set of rules of our Hoare logic for cost and state their soundness.

**Hoare logic rules.** Our Hoare logic for cost comprises the basic rules in Figure 26, the abstract call rule in Figure 6, and the instantiation rule in Figure 27.

The basic rules in Figure 26 are essentially Hoare logic rules with some additional components to handle the cost aspects of the logic. Some examples of basic rules: the if rule handles the conditional program construct, and has already been presented in Section 4.2.

\footnote{Indeed, since \( M_1 \) is a low-order signature, \( M_1 \) must be a module structure signature.}
If the rule forced to take \( R \) and \( E \) into \( \{ \phi \} s \{ \psi \} t \).

\( E \vdash \{ \phi \} s \{ \psi \} t \)

\( \phi \Rightarrow \psi \Rightarrow \psi \Rightarrow \psi' \Rightarrow \psi' \leq t \)

\( E \vdash \{ \phi \} s \{ \psi \} t \)

This allows us to instantiate an abstract module \( x \) by a concrete module \( m \).

Assume that we can upper-bound the cost of a statement \( s \) by \( t_s \), when \( x \) is abstract:

\( E \), module \( x = \text{absopen} : M_1 \vdash \{ \phi \} s \{ \psi \} t \)

Then we can instantiate \( x \) by a concrete module \( m \) as long as \( m \) complies with the module signature \( M_1 \), which is checked through two conditions.

First, we check that \( m \) has the correct module type, except for complexity restrictions, through the premise \( E \vdash m \text{erase}_{\text{comp}}(M_1) \).

Then, we check that \( m \) satisfies the complexity restriction \( \theta \) in \( M_1 \), by requiring that for any procedure \( f \) of \( m \):

\( E \), module \( z = \text{absopen} : M \vdash \{ \psi \} t \)

where \( t_f \) must respect \( \theta(f) \), which is guaranteed by \( t_f \leq \text{comp}(\theta(f)) \), which does two checks:

- first, it ensures that the number of calls to any functor parameter \( z_0 \) of \( x \) done by \( m.f \) is upper-bounded by \( \theta(f)[z_0] \).
- then, it verifies that the bound of \( x \)'s intrinsic cost \( \theta(f)[\text{intr}] \) upper-bounds the cost of the execution of \( m.f \), excluding functor parameter calls, through the condition:

\( t_f[\text{conc}] + \sum_{h \in \text{procs}_{(A)}} t_f[A.h] \cdot \text{intr}_{A.h} \leq \theta(f)[\text{intr}] \)

where \( \text{intr}_{A.h} \) is the upper-bound on \( A.h \) intrinsic cost declared in \( E \) (if \( A.h \) declares no intrinsic bound in \( E \), then \( \text{intr}_{A.h} \) is undefined (hence \( A.h \) execution time can be arbitrarily large), and the \textbf{Instantiation} rule cannot be applied). In other words, the concrete execution time \( t_f[\text{conc}] \) of \( x.f \) plus the abstract execution time of \( x.f \) (excluding functor parameters, already accounted for), must be bounded by \( \theta(f)[\text{intr}] \).

The final cost \( T_{\text{inst}} \) (in Figure 27) is the sum of the cost \( t_s \) of \( s \) (which excludes the cost of \( x \)'s procedures), plus the sum, for any procedure \( f \) of \( m \), of the number of times \( s \) called \( x.f \) (which is \( t_s[x.f] \)), times the cost of \( x.f \) (which is \( t_f \)).

**Soundness.** We now prove the soundness of our Hoare logic rules. We recall Theorem 4.1.

**Theorem.** The proof rules in Figures 6, 26 and 27 are sound.

We focus on the two most complicated rules of our system, Abs (Section F.1) and Instantiation (Section F.2). The soundness of the remaining rules is straightforward to show (we omit the proof).

First, some notation. We extend the program semantics \( [[\_]]_{E,\rho}^p \) to function paths, by letting \( [[F]]_{E,\rho}^p \) be the execution of \( F \)'s body without the procedure’s arguments evaluation phase:

\( [[F]]_{E,\rho}^p = \text{exec}_{E,\rho}^p[\text{exec}_{E,\rho}^p[\_]] \quad \text{if } \text{f-res}_{E}^p(F) = \text{(proc } f(\_ : \bar{r} : \to) \quad \text{ret } r \quad \text{)} \)

\( [[F]]_{E,\rho}^p = \text{exec}_{E,\rho}^p[\text{exec}_{E,\rho}^p[\_]] \quad \text{if } \text{f-res}_{E}^p(F) = \text{(absopen } x(\bar{p}) : f) \)

The cost of \( F \) is defined as expected, by taking the maximum over all memories of the support of the second marginal of \( [[F]]_{E,\rho}^p \):
Finally, cost judgment \( E \vdash \{ \phi \} F \{ \psi \mid t \} \) on function path have the same semantics than cost judgment on statements, i.e. for every well-typed environment \( E \), for every \( E \)-interpretation \( \rho \) and \( \nu \in \phi \):
\[
\text{supp}(\pi_1^E([F]_V^E, \rho)) \subseteq \psi \wedge
\text{cost}^E_\rho(F) \leq t[\text{conc}] + \sum_{A \in (E)} \text{tr}[A, f] \cdot \text{comp}^E_\rho(A, f)
\]
(4)

F.1 Abstract Call Rule Soundness

We now prove that the abstract call rule \( \text{Abs} \) in Figure 6 is sound.

First, remark that since the rule \( \text{Abs} \) uses a different upper-bound \( t_{H,g}(k) \) on the cost of the \( k \)-th call to the oracle \( H,g \), and since the fact that we are in the \( k \)-th call is characterized by the invariant \( I \), we must prove both properties (the invariant on the memories, and the upper-bound on the complexity of the call) simultaneously. The proofs is by induction on the size of \( E \) of the procedure \( \rho(x), f \) called, where procedure calls are inline. Formally, for every environment \( E \) and \( E \)-pre-interpretation \( \rho \), we define:
\[
\begin{align*}
\text{size}^E_\rho(\text{abort}) &= 1 \\
\text{size}^E_\rho(\text{skip}) &= 1 \\
\text{size}^E_\rho(s_1; s_2) &= 1 + \text{size}^E_\rho(s_1) + \text{size}^E_\rho(s_2) \\
\text{size}^E_\rho(x \leftarrow e) &= 1 = 1 \\
\text{size}^E_\rho(x \leftarrow d) &= 1 = 1 \\
\text{size}^E_\rho(\text{call } F(\bar{\nu})) &= 1 + \text{size}^E_\rho(s) \\
&\quad (\text{if } f\text{-res}_E(F) = \text{proc } f \_ \_ \_ \_ = \{ s; \_ \_ \} ) \\
\text{size}^E_\rho(\text{if } e \text{ then } s_1 \text{ else } s_2) &= 1 + \text{size}^E_\rho(s_1) + \text{size}^E_\rho(s_2) \\
\text{size}^E_\rho(\text{while } e \text{ do } s) &= 1 + \text{size}^E_\rho(s)
\end{align*}
\]

Note that we do not care about the size of the expressions appearing in the statement.

We now define and prove our (generalized) induction property, which we need to prove the soundness of \( \text{Abs} \) after.

**Lemma F.1.** Let \( I \) a formula, \( E \) a well-typed environment, \( \rho \) an \( E \)-interpretation and \( \bar{x} \) be functor parameters with module types \( \text{abs}^\text{open} \bar{x} : \tilde{M} \) which are module structure signatures (i.e. not functors). For every statement \( s \) well-typed in \( E \) with additional functor parameters \( \text{abs}^\text{param} \bar{x} : \tilde{M} \), and satisfying a memory restriction \( \lambda_\bar{x}^S \):
\[
\Gamma \vdash s \quad \Gamma \vdash s \succ \lambda_\bar{x}^S \quad \text{where} \quad \Gamma = E, \text{module } \bar{x} = \text{abs}^\text{param} \bar{x} : \tilde{M}
\]

Then for every valuation \( \bar{\nu} \) of the parameters \( \bar{x} \) well-typed in \( E \) (i.e. \( E \models \bar{x} : \tilde{M} \)), if we let \( E^{\bar{x}} = E, \text{module } \bar{x} = \text{abs}^\text{open} \bar{x} : \tilde{M}, \text{and } \bar{O} \) be an enumeration of the parameters \( \bar{x} \)'s procedures, i.e. of:
\[
\{ y.h \mid y \in \bar{x} \land h \in \text{procs}(\tilde{M}[y]) \}
\]

Then if:
- the memory of the statement \( s \) is independent of \( I \), except for calls to the parameters \( \bar{x} \), i.e.:
  \[
  \lambda_\bar{x}^S \cap \text{FV}(I) = \emptyset
  \]

- for every parameters’ procedure \( H,g \in \text{procs}_E(\bar{x}) \), the \( k \)-th call to \( H,g \) (when \( H \) is instantiated by \( \bar{\nu}[H] \)) preserves the invariant and has a cost upper-bounded by \( t_{H,g}(k) \) for \( k \leq \lambda_c(H,g) \):
  \[
  \forall k \leq \lambda_c(\bar{\nu}), k[H,g] < \lambda_c(H,g) \rightarrow
  E \vdash (I \tilde{k}) \bar{\nu}[H,f \{ I \tilde{k} + 1[H,g] \mid t_{H,g}(\tilde{k}[H,g]) \})
  \]
  (5)
- the number of calls from \( s \) to the parameters’ procedure is upper-bounded by \( \lambda_1(\bar{\nu}) - k \) (for memory satisfying the invariant \( I \tilde{k} \)):
  \[
  \forall k \leq \lambda_1(\bar{\nu}), \forall v \in I \tilde{k}, \forall H,g \in \text{procs}_E(\bar{x}),
  \#	ext{calls}^{E^v, \rho'}_{H,g,v}(s) \leq \lambda_c(H,g) - k[H,g]
  \]
  (6)

For every \( H,g \in \text{procs}_E(\bar{x}) \) and \( j < \lambda_c(H,g) \), we define:
\[
\text{call-cost}^{E^v, \rho'}_{H,g,j}(k) = t_{H,g,j}(k)[\text{conc}] + \sum_{A \in (E)} t_{H,g,j}[A, f] \cdot \text{comp}^{E^v, \rho'}_{A, f}
\]
(7)

\[
\text{cost}^{E^v, \rho'}_v(s) = i \cdot \text{cost}^{E^v, \rho', \bar{x}}_v(s) + \sum_{H,g \in \text{procs}_E(\bar{x})} \sum_{j = k[H,g]}^{\text{call-cost}^{E^v, \rho'}_{H,g,j}(k)}
\]
(8)

That is, the cost of \( s \) executed in \( E^v, \rho' \) and memory \( v \) (satisfying the invariant \( I \tilde{k} \)) is upper-bounded by the intrinsic cost of \( s \) with functors parameters \( \bar{x} \), of the sum over functor parameters’ procedures \( H,g \in \text{procs}_E(\bar{x}) \) of the cost over all calls to \( H,g \) (which ranges from \( k[H,g] \) to \( \text{call-cost}^{E^v, \rho'}_{H,g,v}(s) - 1 \)) of the concrete cost of the \( j \)-th call to \( H,g \) (upper-bounded by \( t_{H,g,j}(\text{conc}) \)), plus the sum, over all abstract procedures \( A.f \) (in the original environment \( E \)), of the number of the \( j \)-th call to \( H,g \) called \( A,f \) (upper-bounded by \( t_{H,g,j}(A,f) \)) times the maximal cost of \( A,f \) (which is \( \text{comp}^{E^v, \rho'}_{A,f} \)).

Proof. We prove this induction over \( \text{size}^E_\rho(s) \). We do a case analysis on \( s \):

- if \( s \) is \text{abort} or \text{skip}, this is immediate.
- if \( s = s_1; s_2 \). Let \( \tilde{k}_1 \leq \lambda_c(\bar{\nu}) \) and \( v \in I \tilde{k}_1 \). We know that:
  \[
  \#	ext{calls}^{E^v, \rho'}_{H,g,v}(s_1) \leq \tilde{k}_1 
  \]
  (9)

Let \( v' \in \text{nums}(\pi_1^E([s_1]_v^{E^v, \rho'})) \), we know that \( \tilde{k}_1 \leq \lambda_c(\bar{\nu}) \). Hence, by induction hypothesis on \( s_2 \), we deduce that:
\[
\#	ext{calls}^{E^v, \rho'}_{H,g,v}(s_2) \leq \tilde{k}_2
\]
(10)
where \( \tilde{k}(\nu') = \tilde{k} + \#\text{calls}^{E',\rho'}(s_1) + \#\text{calls}^{E',\rho'}(s_2) \). Since:
\[
\#\text{calls}^{E',\rho'}(s_1) + \#\text{calls}^{E',\rho'}(s_2) \leq \#\text{calls}^{E',\rho'}(s_1; s_2) \tag{10}
\]
we deduce:
\[
supp(\pi^s_1([s_x]^{E',\rho'})) \subseteq I(\tilde{k} + \#\text{calls}^{E',\rho'}(s_1; s_2))
\]
which concludes the proofs of the first point. It remains to prove that the complexity of \( s_1; s_2 \) is upper-bounded by the wanted quantity. First, we have:
\[
\begin{align*}
\text{cost}^{E',\rho'}(s_1; s_2) &= \text{cost}^{E',\rho'}(s_1) + \max_{\nu' \in \text{supp}(\pi^s_1([s_x]^{E',\rho'}))} \text{cost}^{E',\rho'}(s_2) \\
\text{By applying the induction hypothesis on } s_1 \text{ and } s_2 \text{ with, respectively, } \tilde{k} \text{ and } \tilde{k}_1, \text{ we get:}
\end{align*}
\]
\[
\begin{align*}
\text{cost}^{E',\rho'}(s_1) &\leq i\text{-cost}^{E',\rho'}(s_1) + \sum_{H,g \in \text{procs}(\tilde{k})} \tilde{k}[H,g]-1 \sum_{j=\tilde{k}[H,g]} \text{call-cost}^{E,\rho}(j) \\
\text{and:}
\end{align*}
\]
\[
\begin{align*}
\text{cost}^{E',\rho'}(s_2) &\leq i\text{-cost}^{E',\rho'}(s_2) + \sum_{H,g \in \text{procs}(\tilde{k})} \tilde{k}(\nu'[H,g]-1) \sum_{j=\tilde{k}[H,g]} \text{call-cost}^{E,\rho}(j) \\
\text{Since } i\text{-cost}^{E',\rho'}(s_1; s_2) \text{ is equal to:}
\end{align*}
\]
\[
\begin{align*}
i\text{-cost}^{E',\rho'}(s_1) + \max_{\nu' \in \text{supp}(\pi^s_1([s_x]^{E',\rho'}))} i\text{-cost}^{E',\rho'}(s_2) \\
\text{and using Equ. (10), we deduce that:}
\end{align*}
\]
\[
\begin{align*}
\text{cost}^{E',\rho'}(s_1) + \text{cost}^{E',\rho'}(s_2) &\leq \\
\text{i-cost}^{E',\rho'}(s_1; s_2) + \sum_{H,g \in \text{procs}(\tilde{k})} \tilde{k}[H,g]+\#\text{calls}^{E',\rho'}(s_1; s_2)-1 \sum_{j=\tilde{k}[H,g]} \text{call-cost}^{E,\rho}(j)
\end{align*}
\]
We conclude by taking the max over \( \nu' \) and using Equ. 9.

- If \( s = x \leftarrow e \). Let \( \tilde{k} \leq \lambda_c[\tilde{\rho}] \) and \( \nu \in I(\tilde{k}) \). Since \( \text{mem}_{\tilde{\rho}}(s) \cap \text{FV}(I) = \emptyset \), we know that \( x \notin \text{FV}(I) \). Hence the invariant is preserved, i.e.:
\[
\forall \nu' \in \text{supp}(\pi^s_1([s_x]^{E',\rho'}))), \nu' \in I(\tilde{k})
\]
Since \( \#\text{calls}^{E',\rho'}(s) = 0 \), this proves the first point. Moreover:
\[
\text{cost}^{E',\rho'}(x \leftarrow e) = i\text{-cost}^{E',\rho'}(x \leftarrow e)
\]
which concludes the proof.

- The random assignment \( x \leftarrow d \), conditional if \( e \) then \( s_1 \) else \( s_2 \) and while loop while \( e \) do \( s \) cases are similar. We omit the details.

- If \( s = x \leftarrow \text{call } F(\bar{e}) \) and \( \text{f-res}_{\tilde{\rho}}(F) = (\text{proc } f(\bar{u} : \bar{r}) \rightarrow t_r = \{ \text{var } (\bar{t}_i : \bar{\gamma}_i) ; s' ; \text{ return } e \}) \), then we proceed as in the previous case, applying the induction hypothesis on \( s' \). First, we remark that \( s' \) is smaller than \( s \), since:
\[
\#\text{size}^{E,\rho'}(s') < \#\text{size}^{E,\rho}(x \leftarrow \text{call } F(\bar{e}))
\]
It only remains to check that the induction hypothesis’s hypotheses hold. The last two hypotheses are straightforward to show. It only remains to prove that \( \Gamma \vdash s' \succ \lambda_{\tilde{\rho}}^s \) is derivable. Since \( \Gamma \vdash s > \lambda_{\tilde{\rho}}^s \), we know that \( \text{mem}_{\tilde{\rho}}(s) \subseteq \lambda_{\tilde{\rho}}^s \), where:
\[
\text{mem}_{\tilde{\rho}}(s) = \{ x \mid \text{mem}_{\tilde{\rho}}(s') \cup \text{vars}(\bar{e}) \}
\]
Which concludes this case.

- idem if \( s = x \leftarrow \text{call } F(\bar{e}) \) and \( \text{f-res}_{\tilde{\rho}}(F) = (\text{abs}\text{open } H(\_)).f \) with \( H \notin \bar{e} \).

- If \( s = x \leftarrow \text{call } F(\bar{e}) \) and \( \text{f-res}_{\tilde{\rho}}(F) = (\text{abs}\text{open } H(\bar{p})).g \) with \( H \notin \bar{e} \), then we use the hypothesis that procedures of the interpretation of the modules parameters \( \bar{x} \) preserves the invariant. First, since \( \bar{x} \) have types \( \bar{M} \) and \( \tilde{M} \) are module structure signatures, we know that \( \bar{p} \) is empty (from the fact that \( s \) is well-typed in \( \Gamma \)). Hence \( \text{f-res}_{\tilde{\rho}}(F) = \text{abs}\text{open } H.g \).

Let \( \tilde{k} \leq \lambda_c[\tilde{\rho}] \) and \( \nu \in I(\tilde{k}) \). First, using the hypothesis in Equ. (6), we know that:
\[
\tilde{k}[H,g] + \#\text{call}_{H,g}(x \leftarrow \text{call } F(\bar{e})) \leq \lambda_c[H,g]
\]
Hence \( \tilde{k}[H,g] < \lambda_c[H,g] \). By applying Equ. (5) on \( H,g \), we know that:
\[
\begin{align*}
E &\vdash I(\tilde{k}) \bar{p}[H,g] \{ I(\tilde{k}+1_{H,g}) \mid t_{H,g}(k) \} \\
\text{Since } \rho \text{ is an } E \text{-interpretation, and since } \bar{x} \text{ have type } \bar{M} \text{ where } \tilde{M} \text{ are module structure signatures, we can check that } \rho' \text{ is an } E' \text{-interpretation. Hence, from Equ. (11) and the semantics of the cost judgment given in Equ. (4) we get that:}
\end{align*}
\]
\[
\begin{align*}
supp(\pi^s_1([\bar{p}[H,g]]^{E,\rho'})) \subseteq I(\tilde{k}+1_{H,g}) \\
\text{and:}
\end{align*}
\]
\[
\begin{align*}
\text{cost}^{E,\rho'}(\bar{p}[H,g]) &\leq t_{H,g}(\tilde{k}[H,g])(\text{conc}) \\
&+ \sum_{A \in \text{procs}(A)} t_{H,g}(\tilde{k}[H,g])(A.f) \cdot \text{comp}^{E,\rho}_a(f) \\
&\leq \text{call-cost}^{E,\rho'}(\tilde{k}[H,g])
\end{align*}
\]
Observe that since \( \rho' = \rho, (\bar{x} : \bar{p}) \), we have:
\[
\begin{align*}
\llbracket x \leftarrow \text{call } F(\bar{e}) \rrbracket^{E,\rho'}_v = \llbracket x \leftarrow \text{call } \bar{p}[H,g(\bar{e})] \rrbracket^{E,\rho'}_v
\end{align*}
\]
Hence Equ. (7) follows directly from Equ. (12). It remains to show Equ. (8). First, note that:
\[
\begin{align*}
\text{cost}^{E,\rho'}(x \leftarrow \text{call } F(\bar{e})) &\quad = \\
i\text{-cost}^{E,\rho'}(x \leftarrow \text{call } F(\bar{e})) + \text{cost}^{E,\rho'}(\bar{p}[H,g])
\end{align*}
\]
Since \( \bar{\varphi} \) is well-typed in \( \mathcal{E} \), we know that \( \text{cost}_v^{E',\rho'}(\bar{\varphi}[H],g) \) is equal to the cost of evaluating \( E' \) under \( \rho' \).

\[
\text{cost}_v^{E',\rho'}(x \leftarrow \text{call } f(\bar{\varphi})) = \text{cost}_v^{E,\rho}(x \leftarrow \text{call } f(\bar{\varphi})).
\]

We conclude the proof of Eq. (8) using the inequality above and Eq. (13).

Lemma F.2. The rule \textit{Ans} given in Figure 6 is sound.

\textbf{Proof.} We just apply Lemma F.1 on \( \rho(x), f \). The first two hypotheses of the lemma hold thanks to the premises of the \textit{Ans} rule, and using the fact that our module system has the subject reduction property (Lemma C.1). The third hypothesis follows from the fact that \( \rho \) is an \( \mathcal{E} \)-interpretation.

\section*{F.2 Instantiation Rule Soundness}

We prove the following technical lemma, which allows to extend an \( \mathcal{E} \)-interpretation \( \rho \) into an \( \mathcal{E}' \)-interpretation \( \rho' \). The rule \textit{Abs} is given in Figure 6 is sound.

\textbf{Proof.} Let \( E \) be a well-typed environment, \( M_i \) be low-order module signature s.t.:

\[
M_i = \text{func}(\bar{x} : \bar{M}) \text{ sig } _{\text{restr}} \theta \text{ end}
\]

and \( m \) be a module expression s.t. \( E \vdash m : \text{erase}_{\text{comp}}(M_i) \). Let \( E_a = E, \) module \( x = \text{absopen} : M_i \) and \( \rho \) be an \( \mathcal{E} \)-interpretation. For every \( f \) in \( M_i \), we have:

\[
\text{E}, \text{module } \bar{x} = \text{absopen} : \bar{M} \vdash \{ \tau \} m(\bar{x}), f \{ \tau | t_f \} \wedge t_f \leq \text{comp}\{0 | f\}
\]

then \( \rho_a = \rho, (x \mapsto m) \) is an \( \mathcal{E}_a \)-interpretation. Moreover, for any \( f \) in \( M_i \):

\[
\text{comp}^{E_a,\rho_a}_{x,f} \leq t_f[\text{conc}] + \sum_{h \in \text{procs}_{\mathcal{E}}(A)} t_f[A,h] \cdot \text{comp}^{E_a,\rho_a}_{A,h}
\]

\section*{Restriction to module structures}

First, note that w.l.o.g. we can assume that \( \bar{M} \) are all module structures (i.e. of the form \text{struct } ... end). Basically, we show that we can build another interpretation \( \rho''_a \) extending \( \rho_a \) which satisfies the same hypotheses as \( \rho'_a \), and such that for every \( z \in \bar{x} \), \( \rho''_a(z) \) is a module structure such that, for every \( g \in \text{procs}(\bar{M}[z]) \):

\[
\#\text{calls}_{\bar{x},y}^{E',\rho''_a}(x(\bar{x}),f) = \#\text{calls}_{\bar{x},y}^{E',\rho''_a}(x(\bar{x}),f)
\]


\[\text{and:}
\]

\[
\#	ext{calls}_{\bar{x},y}^{E',\rho''_a}(x(\bar{x}),f) = \#\text{calls}_{\bar{x},y}^{E',\rho''_a}(x(\bar{x}),f)
\]

Moreover, we can easily check that:

\[
\#	ext{calls}_{\bar{x},y}^{E',\rho''_a}(m(\bar{x}),f) = \#\text{calls}_{\bar{x},y}^{E',\rho''_a}(m(\bar{x}),f)
\]

\]
and:

\[ \text{cost}^{E',\rho_N}(\text{m}(\text{x}), f) = \text{cost}^{E',\rho'}(\text{m}(\text{x}), f) + N \cdot \text{calls}^{E',\rho'}(\text{m}(\text{x}), f) \]

From Eqn. (20), we have:

\[ \text{cost}^{E',\rho'}(\text{m}(\text{x}), f) \leq tf[\text{conc}] + \sum_{\text{h} \in \text{procs}_A(A)} tf[\text{A}, h] \cdot \text{compl}_{A, h}^{E',\rho'}(\text{m}(\text{x}), f) \]

Using the inequality above, and Eqn. (19), we have:

\[ N \cdot \sum_{\text{h} \in \text{procs}_A(A)} tf[\text{A}, h] \cdot (\text{compl}_{A, h}^{E',\rho'}(\text{m}(\text{x}), f) - \text{compl}_{A, h}^{E',\rho'}(\text{m}(\text{x}), f)) \]

\[ \leq tf[y.g] \cdot (\text{compl}_{y, g}^{E',\rho'}(\text{m}(\text{x}), f) - \text{compl}_{y, g}^{E',\rho'}(\text{m}(\text{x}), f)) \]

\[ \leq tf[y.g] \cdot N \]

We deduce that \( \text{calls}^{E',\rho'}(\text{m}(\text{x}), f) \leq tf[y.g] \). From Eqn. (14), we get that:

\[ \text{calls}^{E',\rho'}(\text{m}(\text{x}), f) \leq \theta[f[y.g]] \]

This, together with Eqn. (18), proves Eqn. (16).

Finally, to prove that Eqn. (17) and Eqn. 15 hold we do the exactly the same reasoning, this time by adding to the interpretation of \( x \) some code doing nothing and taking time \( N \).

We also prove the following weakening lemma for the intrinsic complexity of a procedure.

**Lemma F.4.** For every well-typed environment \( E, i_f \):

\[ E = E_1; E_2 \quad \text{where} \quad E_1 = E_0; \text{module } x = \text{absopen} : \text{M}_1 \]

and \( E_2 \) contains only module declarations. Then for every \( f \in \text{procs}(\text{M}_1) \) and \( E \)-interpretation \( \rho \), we have \( \text{compl}_{E, f}^{\rho_1} = \text{compl}_{E, f}^{\rho_1} \) where \( \rho_1 \) is the restriction of \( \rho \) to \( E_1 \)’s abstract modules.

**Proof Sketch.** Assume \( \text{M}_1 = (\text{func}(\text{x} : \tilde{\text{M}}) \quad \text{sig end}) \). Let \( E' = (E, \text{module } \tilde{x} = \text{absopen} : \tilde{\text{M}}) \) and \( E'_2 = (E_2, \text{module } \tilde{x} = \text{absopen} : \tilde{\text{M}}) \), we prove that \( \text{compl}_{E, f}^{\rho_1} \leq \text{compl}_{E, f}^{\rho_1} \) and \( \text{compl}_{E, f}^{\rho} \geq \text{compl}_{E, f}^{\rho_1} \).

The latter inequality is straightforward to show, since any \( E'_1 \) interpretation \( \rho_1 \) can be extended into an \( E'_1 \)-interpretation \( \rho' \) that leaves the intrinsic cost of \( x \) unchanged, i.e. such that for any \( y \):

\[ i \cdot \text{cost}^{E',\rho,\tilde{x}}(x, f) = i \cdot \text{cost}^{E',\rho',\tilde{x}}(x, f) \]

To prove the former inequality, we show that any \( E'_1 \)-interpretation \( \rho \) can be transformed into an \( E'_1 \)-interpretation \( \rho' \) such that Eqn. (F.2) holds, by inlining all modules of \( E_2 \) in \( \rho \). We omit the details.

**Lemma F.5.** The rule **Instantiation** given in Figure 27 is sound.

**Proof.** We consider an instance of the rule **Instantiation**. We want to prove that:

\[ E_1 \text{, module } x = m : \text{M}_1 \vdash \{ \psi \} s \{ \psi \mid T_{ins} \} \]

Let \( E_c = (E, \text{module } x = m : \text{M}_1) \) and \( E_a = (E, \text{module } x = \text{absopen} : \text{M}_1) \). We know that:

\[ M_1 = \text{func}(\gamma : \tilde{\text{M}}) \quad \text{sig } S_1 \quad \text{restr } \theta \text{ end} \quad E \vdash x : m \quad \text{erase}_{comp}(M_1) \]

Let \( \rho \) be an \( E_c \)-interpretation and \( \psi \in \phi \), we need to show that for every memory \( v \):

\[ \text{supp}(\pi^E_1([s]^E_{c, \rho} )) \leq \psi \]

\[ \text{cost}^{E',\rho}(v) \leq T_{ins}[\text{conc}] + \sum_{\text{A} \in (E, \rho)} T_{ins}[\text{A}, g] \cdot \text{compl}_{A, g}^{E',\rho} \]

We know that \( M_1 = \text{func}(\gamma : \tilde{\text{M}}) \quad \text{sig } S_1 \quad \text{restr } \theta \text{ end and:} \)

\[ E_a \vdash \{ \psi \} s \{ \psi \mid t_s \} \]

Using Lemma F.3, we know that \( \rho_a = \rho, (x \mapsto m) \) is an \( E_a \)-interpretation. Hence, using Eqn. (23), we deduce that:

\[ \text{supp}(\pi^E_1([s]^E_{a, \rho_a} )) \leq \psi \]

\[ \text{cost}^{E_a,\rho_a}(v) \leq t_s[\text{conc}] + \sum_{\text{A} \in (E_a, \rho_a)} t_s[\text{A}, g] \cdot \text{compl}_{A, g}^{E,\rho_a} \]

Using the fact that \( \rho_a(x) = m \), we can check (by induction over \( \text{size}_{E_a}^{\rho_a}(s) \)) that:

\[ \text{cost}^{E_a,\rho_a}(s) = \text{cost}^{E,\rho}(s) \]

From the left equality above and Eqn. (24), we know that Eqn. (21) holds. It remains to prove Eqn. (22).

From the right equality above and Eqn. (25):

\[ \text{cost}^{E,\rho}(v) \leq t_s[\text{conc}] + \sum_{\text{f} \in \text{procs}(S_1)} t_s[\text{f}, x] \cdot \text{compl}_{A, g}^{E,\rho_a} \]

\[ \leq t_s[\text{conc}] + \sum_{\text{f} \in \text{procs}(S_1)} t_s[\text{f}, x] \cdot \text{compl}_{A, g}^{E,\rho_a} \]

\[ + \sum_{\text{A} \in (E, \rho)} t_s[\text{A}, g] \cdot \text{compl}_{A, g}^{E,\rho_a} \]

We replace \( \text{compl}_{A, g}^{E,\rho_a} \) by \( \text{compl}_{A, g}^{E,\rho} \) for every \( A \in (E_c) \) and \( g \in \text{procs}_A(A) \) using Lemma F.4:

\[ \text{cost}^{E,\rho}(v) \leq t_s[\text{conc}] + \sum_{\text{f} \in \text{procs}(S_1)} t_s[\text{f}, x] \cdot \text{compl}_{A, g}^{E,\rho} \]

\[ + \sum_{\text{A} \in (E, \rho)} t_s[\text{A}, g] \cdot \text{compl}_{A, g}^{E,\rho} \]

Using Lemma F.3, we upper-bound \( \text{compl}_{A, g}^{E,\rho_a} \) for every \( f \in \text{procs}(S_1) \):

\[ \text{compl}_{A, g}^{E,\rho_a} \leq tf[\text{conc}] + \sum_{\text{A} \in (E, \rho)} tf[\text{A}, g] \cdot \text{compl}_{A, g}^{E,\rho} \]
We check that the quantities above are identical when evaluated in $E_c$, hence:

$$\text{compl}_{x,f}^{E_c,\rho} \leq t_f[\text{conc}] + \sum_{A \in (E_c)} \sum_{g \in \text{procs}_{E_c}(A)} t_f[A.g] \cdot \text{compl}_{A,g}^{E_c,\rho}$$

Hence, re-organizing the terms in the sum in Equ. (26):

$$\text{cost}_{E_c,\rho}(s) \leq t_s[\text{conc}] + \sum_{f \in \text{procs}(S_i)} t_s[x.f] \cdot t_f[\text{conc}] + \sum_{A \in (E_c)} \sum_{g \in \text{procs}_{E_c}(A)} (t_s[A.g] + \sum_{f \in \text{procs}(S_i)} t_s[x.f] \cdot t_f[A.g]) \cdot \text{compl}_{A,g}^{E_c,\rho}$$

Which, by definition of $T_{ins}$, is exactly Equ. (22). □