

# *Don't exhaust, don't waste*

## *Resource-aware soundness for big-step semantics*

RICCARDO BIANCHINI

University of Genoa, Italy  
(email: [riccardo.bianchini@edu.unige.it](mailto:riccardo.bianchini@edu.unige.it))

FRANCESCO DAGNINO

University of Genoa, Italy  
(email: [francesco.dagnino@dibris.unige.it](mailto:francesco.dagnino@dibris.unige.it))

PAOLA GIANNINI

University of Eastern Piedmont, Italy  
(email: [paola.giannini@uniupo.it](mailto:paola.giannini@uniupo.it))

ELENA ZUCCA

University of Genoa, Italy  
(email: [paola.giannini@uniupo.it](mailto:paola.giannini@uniupo.it))

### Abstract

We extend the semantics and type system of a lambda calculus equipped with common constructs to be *resource-aware*. That is, the semantics keeps track of the usage of resources, and is stuck, besides in case of type errors, if either a needed resource is exhausted, or a provided resource would be wasted. In such way, the type system guarantees, besides standard soundness, that for well-typed programs there is a computation where no resource gets either exhausted or wasted.

The extension is parametric on an arbitrary *grade algebra*, modeling an assortment of possible usages, and does not require ad-hoc changes to the underlying language. To this end, the semantics needs to be formalized in big-step style; as a consequence, expressing and proving (resource-aware) soundness is challenging, and is achieved by applying recent techniques based on coinductive reasoning.

### 1 Introduction

An increasing interest has been devoted in research to *resource-awareness*, that is, to formal techniques for reasoning about how programs use external resources, such as files, locks, and memory. The original inspiration for such techniques has been *linear logic*, introduced by Girard [26] in his seminal paper, where logical statements are considered resources which cannot be duplicated or discarded. The idea has been firstly carried to programming languages by *substructural* type systems [38], particularly *linear* and *affine* ones. Such type systems enjoy an extended form of soundness which we call *resource-aware soundness*; that is, they statically approximate not only the expected result of a program, but also how each external resource, handled through a name (free variable), is used: either unused, or used exactly/at most once, in the linear/affine case, respectively, or in an unrestricted way. Note that, differently from linear ones, affine (and unrestricted) resources are *discardable*, meaning that there is no constraint that they should be actually used by the program.

More recently, the notion has been generalized to an arbitrary assortment of usages, formally modeled by *grades*, elements of an algebraic structure (*grade algebra*) defined



© 2026 Copyright held by the owner/author(s).

This work is licensed under a Creative Commons Attribution 4.0 International License.

in slightly different ways in the literature<sup>1</sup> [1, 5, 12, 19, 24, 25, 31, 32, 39]. For instance, grades can be natural numbers counting how many times a resource is used, or even express non-quantitative properties, e.g., that a resource should be used with a given access level. In this way, linear/affine type systems can be generalized to type systems parametric on the grade algebra, and the notion of resource-aware soundness can be generalized as well.

In order to formally express and prove that a type system enjoys resource-aware soundness, the execution model needs to take into account resource consumption. This has been achieved in some recent proposals [8, 13, 35], including the conference version of this paper [9]. The basic feature of the *resource-aware semantics* is that substitution of variables is not performed once and for all, as in the standard  $\beta$ -rule. Instead, program execution happens in an *environment* of available resources, and each variable occurrence is replaced when needed, by consuming in some way the associated resource. In this way, reduction is stuck if *resources are exhausted*, that is, the current availability is not enough to cover the usage required by the program, and this situation is expected to be prevented by the type system. Formally, “enough” means that  $r + s' \preceq s$ , where  $r$  and  $s$  are the required and available amount, respectively, and  $+$ ,  $\preceq$  are the sum and order of the grade algebra. Note that the amount  $s'$  is left available.

In this way, the program cannot consume more resources than those available; however, the converse property does not hold, that is, resources can be *wasted*. For instance, there is no guarantee that a linear resource is actually used.

The advantages of constraints which impose no-waste, such as linear type systems, have been firstly illustrated by Wadler [37] in his seminal paper. They include avoiding garbage collection or reference counting, ensuring the correct use of files<sup>2</sup>, and, in session type systems, prevent a receiver from indefinitely wait on a channel. However, in the existing proposals mentioned above [8, 9, 13, 35], there is no formal way to express that the type system ensures no-waste as well.

In this paper, we provide, to the best of our knowledge, the first statement and proof of resource-aware soundness where well-typedness implies that *all* the following situations (which are stuck in the semantics) are prevented:

- (1) type errors, as in the standard soundness
- (2) resource exhaustion, as in the resource-aware soundness in previous work
- (3) resource wasting (novelty of this work)

We share with the conference paper [9] the aim of adding resource-awareness in a light, abstract and general way, without requiring ad-hoc changes to the underlying language. To achieve this aim, we also share the following features:

- The reference language is an extended lambda calculus, intended to be representative of typical language features. A contribution of our work is that, differently from most graded operational models, we consider a call-by-value semantics. Moreover, we provide an in-depth investigation of *resource consumption in recursive functions*, and our graded type system smoothly includes *equi-recursive types*.
- We keep the original syntax, with *no boxing/unboxing* constructs; to this end, there is no explicit promotion rule, but different grades can be assigned to an expression, assuming different contexts.

<sup>1</sup>Essentially variants of an ordered semiring.

<sup>2</sup>See the example in Section 6.

- The resource-aware semantics is given in *big-step* style, so that no annotations in subterms are needed, again keeping the underlying language unaffected. A consequence of this choice is that proving and even expressing (resource-aware) soundness of the type system becomes challenging, since in big-step semantics non-terminating and stuck computations are indistinguishable [15, 28]. To solve this problem, the big-step judgment is extended to model divergence explicitly, and is defined by a *generalized inference system* [3, 16], where rules are interpreted in an *essentially coinductive*, rather than inductive, way, in the sense that infinite proof trees are allowed, in a controlled way. Our proof of resource-aware soundness is a significant application of these innovative techniques.

On the other hand, as mentioned above, differently from the conference paper [9], we state and prove resource-aware soundness *including no-waste*, thanks to the following novel features:

- Formal definition of no-waste (transitive) usage of an environment of resources, in terms of the associated graph of direct dependencies.
- No-waste refinement of the resource-aware semantics, meaning that a computation is stuck, in addition to the situations (1) and (2), when it would be wasting, i.e., (3).
- Formal characterization of configurations which are no-waste, in the sense that they do not get stuck due to wasting errors.
- Proof that well-typed configurations are no-waste.

We provide first, in Section 2, a gentle introduction to resource-aware semantics by examples. Then, we formally define grade algebras in Section 3. To make the presentation simpler, and modular with respect to the conference version, in Section 4 we present resource-aware reduction as in the conference paper [9], focusing on its general notions. In Section 5 we provide the type system, and in Section 6 more significant examples and discussions. In Section 7 we present the refined resource-aware reduction which ensures no-waste. In Section 8 we prove resource-aware soundness. Section 9 surveys related work, and Section 10 summarizes the contributions and outlines future work. Omitted proofs can be found in the Appendix.

## 2 Preliminary examples

In order to illustrate the key ideas of resource-aware evaluation, we illustrate its expected behaviour on some simple examples.

We assume a minimal syntax of expressions:

$$e ::= x \mid \text{unit} \mid \langle^r e_1, e_2^s \rangle \mid \text{match } e_1 \text{ with } \langle x, y \rangle \rightarrow e_2$$

only comprising variables in an infinite set  $V$ , a constant, and (graded) pairs, with the corresponding destructor. The metavariables  $r$  and  $s$  denote *grades*, which the reader can initially think as natural numbers. Thus, the pair constructor is decorated with a grade for each subterm, intuitively meaning “how many copies” are contained in the compound term. For instance, a pair of shape  $\langle^2 e_1, e_2^2 \rangle$  contains “two copies” of each component, hence to evaluate (one copy of) such pair we need to obtain 2 copies of the results of  $e_1$  and  $e_2$ .

execution model which takes into account resource consumption. To achieve this, the basic feature [8, 13, 35] is that substitution of variables is not performed once and for all, as in the standard  $\beta$ -rule. Instead, program execution happens in an *environment* of available

resources, and each variable occurrence is replaced when needed, by consuming in some way the associated resource. Formally, the resource-aware semantics is defined on *configurations*, that is, pairs  $e \mid \rho$  where the environment  $\rho$  is a finite map associating to each resource (variable), besides its value, a grade modeling its available usage, represented as shown below:

The goal is to provide an execution model that explicitly accounts for resource consumption. To this end, a key idea, following [8, 13, 35], is to avoid performing variable substitution once and for all, as in the standard  $\beta$ -reduction rule. Instead, program execution takes place within an *environment* of available resources. Each occurrence of a variable is replaced only when needed, and doing so consumes the resource associated with that variable. Formally, the resource-aware semantics is defined over *configurations*, which are pairs  $e \mid \rho$ . Here, the environment  $\rho$  is a finite map that associates each resource, i.e., variable, with both its value and a grade representing the amount of usage still available, as illustrated below.

$$\begin{aligned}\rho &::= x_1 : \langle r_1, \mathbf{v}_1 \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n \rangle \\ \mathbf{v} &::= \text{unit} \mid \langle^r \mathbf{v}_1, \mathbf{v}_2^s \rangle\end{aligned}$$

The judgment has shape  $e \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'$ , meaning that the configuration  $e \mid \rho$  produces a value  $\mathbf{v}$  and a final environment  $\rho'$ . The reduction relation is *graded*, that is, indexed by a grade  $r$ , meaning that the resulting value can be used (at most)  $r$  times. The grade of a variable in the environment decreases, each time the variable is used, by the amount specified in the reduction grade. Of course, this can only happen if the current grade of the variable *can* be reduced by such an amount. Otherwise, evaluation is stuck; formally, since we choose to give the reduction relation in big-step style<sup>3</sup>, no judgment can be derived. Correspondingly, introducing a variable means adding a new resource in the environment.

**Example 2.1.** Let us consider the following expressions:

- $e_1 = \text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle \text{unit}, \text{unit} \rangle$
- $e_2 = \text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, \text{unit} \rangle$
- $e_3 = \text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, y \rangle$
- $e_4 = \text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, x \rangle$

to be evaluated in the environment  $\rho = p : \langle 1, \mathbf{v} \rangle$  with  $\mathbf{v} = \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$ . Assume, as said above, that grades are natural numbers, as will be formally defined in Example 3.3(1). In order to lighten the notation, 1 annotations are considered the default, hence omitted. Moreover, in figures we abbreviate `unit` by `u`. In the first proof tree in Fig. 1 we show the evaluation of  $e_1$ . The resource `p` is consumed, and its available amount (1) is “transferred” to both the resources `x` and `y`, which are added to the environment<sup>4</sup>, and not consumed.

Evaluating  $e_2$  and  $e_3$  works in much the same way, except that for  $e_2$  the resource `x` gets consumed during the process and the evaluation of  $e_3$  uses up all the available resources. Finally, the evaluation of  $e_4$  is stuck, that is, no proof tree can be constructed: indeed, when the second occurrence of `x` is found, the resource is exhausted, as shown in the second (incomplete) proof tree in Fig. 1. A result could be obtained, instead, if the original grade of `p` was greater than 1, e.g., 2, since in this case `x` (and `y`) would be added with grade 2, or, alternatively, if the value associated to `p` in the environment was, e.g.,  $\mathbf{v} = \langle^2 \mathbf{v}_1, \mathbf{v}_2 \rangle$ . Indeed, we expect a component of a pair  $\langle^r \mathbf{v}_1, \mathbf{v}_2^s \rangle$  to be extracted with a grade obtained

<sup>3</sup>The motivation for this choice is given in Section 4.

<sup>4</sup>Modulo renaming, omitted here for simplicity.

$$\begin{array}{c}
\frac{}{p \mid \rho \Rightarrow v \mid p : \langle 0, v \rangle} \text{ (VAR)} \quad \frac{}{\langle u, u \rangle \mid \rho' \Rightarrow \langle u, u \rangle \mid \rho'} \text{ (PAIR)} \quad \begin{array}{l} \rho = p : \langle 1, v \rangle \text{ with } v = \langle v_1, v_2 \rangle \\ \rho_0 = p : \langle 0, v \rangle, y : \langle 1, v_2 \rangle \\ \rho' = \rho_0, x : \langle 1, v_1 \rangle \\ \rho'' = \rho_0, x : \langle 0, v_1 \rangle \end{array} \\
\hline
\text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle u, u \rangle \mid \rho \Rightarrow \langle u, u \rangle \mid \rho' \text{ (MATCH-P)} \\
\\
\frac{}{p \mid \rho \Rightarrow v \mid p : \langle 0, v \rangle} \text{ (VAR)} \quad \frac{}{x \mid \rho' \Rightarrow v_1 \mid \rho''} \text{ (VAR)} \quad \frac{}{x \mid \rho'' \Rightarrow ?} \text{ (VAR)} \\
\hline
\langle x, x \rangle \mid \rho' \Rightarrow ? \text{ (PAIR)} \\
\hline
\text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, x \rangle \mid \rho \Rightarrow ? \text{ (MATCH-P)}
\end{array}$$

Fig. 1. Examples of resource-aware evaluation (counting usages)

by multiplying the grade of the pair with the grade of the component inside the pair, in this example 2·1 and 1·2, respectively.

Until now, we have assumed grades to be natural numbers, modeling *how many times* resources are used. However, a different choice of grades can model a *non-quantitative* usage, that is, track possible *modes* in which a resource can be used. A very simple example are grades expressing access levels; for instance, *private* and *public*, besides the grade 0 which always expresses no usage at all. Such grades are ordered as follows:  $0 \preceq \text{private} \preceq \text{public}$ , meaning that a program which does not use a variable can be safely run in an environment where this variable is available as *private*, and a program which uses a variable as *private* can be safely run in an environment where it is *public*. Of course, the converse does not hold. Moreover, multiplication is the meet, meaning that we obtain an access level which is more restrictive than both.

Note that exactly the same structure could be used to model, e.g., modifiers *readonly* and *mutable* in an imperative setting, rather than access levels. Moreover, the structure can be generalized by adding a 0 element to any distributive lattice, as will be formalized in Example 3.3(5), where we will also discuss the difference with the models of privacy levels in the literature [1].

**Example 2.2.** In Example 2.1, writing *priv* and *pub* (default, omitted in the annotations) for short, we have, e.g., for  $\rho = p : \langle \text{pub}, v \rangle$  with  $v = \langle^{\text{priv}} v_1, v_2 \rangle$ , that the evaluation in mode *pub* of  $e_1$  is analogous to that in Fig. 1; however, the evaluation in mode *pub* of  $e_2$ ,  $e_3$ , and  $e_4$  is stuck, since it needs to use the resource  $x$ , which gets a grade *priv* = *priv*·*pub*, hence cannot be used in mode *pub* since *pub*  $\not\preceq$  *priv*, as we show in the first (incomplete) proof tree for  $e_2$  in Fig. 2. On the other hand, evaluation in mode *priv* can be safely performed; indeed, resource  $p$  can be used in mode *priv* since *priv*  $\preceq$  *pub*, as shown in the second proof tree in Fig. 2.

In both the previous examples, reduction gets stuck when *a needed resource is exhausted*, as will be formalized in Section 4. In Section 7, we introduce a refined notion of reduction that also gets stuck when *a resource is wasted*, that is, when some resource that *should have been used* is left over after program execution.

This cannot happen with the choices of grades considered until now. That is because the grade 0, representing no usage, is less or equal than all grades, that is, can be overapproximated by any amount of usage. In other words, there are no grades which impose that a resource *should be used*. An example where, instead, there is such a constraint, are natural numbers

$$\begin{array}{c}
\frac{}{p \mid \rho \Rightarrow v \mid \rho} \quad \frac{\frac{}{x \mid \rho' \Rightarrow ?}}{\langle x, u \rangle \mid \rho' \Rightarrow ?} \quad \begin{array}{l} \rho = p : \langle \text{pub}, \mathbf{v} \rangle \text{ with } \mathbf{v} = \langle \text{priv } \mathbf{v}_1, \mathbf{v}_2 \rangle \\ \rho' = p : \langle \text{pub}, \mathbf{v} \rangle, x : \langle \text{priv}, \mathbf{v}_1 \rangle, y : \langle \text{pub}, \mathbf{v}_2 \rangle \end{array} \\
\hline
\text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, u \rangle \mid \rho \Rightarrow ?
\end{array}$$
  

$$\begin{array}{c}
\frac{}{p \mid \rho \Rightarrow v \mid p : \langle \text{pub}, \mathbf{v} \rangle} \quad \frac{\frac{}{x \mid \rho' \Rightarrow_{\text{priv } \mathbf{v}_1} \rho'}{\langle x, y \rangle \mid \rho' \Rightarrow_{\text{priv } \langle \mathbf{v}_1, \mathbf{v}_2 \rangle} \rho'} \quad \frac{}{y \mid \rho' \Rightarrow_{\text{priv } \mathbf{v}_2} \rho'}}{\langle x, y \rangle \mid \rho' \Rightarrow_{\text{priv } \langle \mathbf{v}_1, \mathbf{v}_2 \rangle} \rho'} \\
\hline
\text{match } p \text{ with } \langle x, y \rangle \rightarrow \langle x, y \rangle \mid \rho \Rightarrow_{\text{priv } \langle \mathbf{v}_1, \mathbf{v}_2 \rangle} \rho'
\end{array}$$

Fig. 2. Examples of resource-aware evaluation (access levels)

where the considered order is equality, as formalized in Example 3.3(1). This means that a resource with grade, e.g., 1, should be used *exactly once*: neither more than once, nor unused. Formally, 0 is *not* less than 1. The grades which impose a lower bound on usage are called *non-discardable*, see Definition 3.8 in the following.

Let us consider what would happen in Example 2.1 with these grades. We expect that only  $e_3$  can be successfully evaluated, since only in this case the resources are all exhausted; the evaluations of  $e_1$  and  $e_2$ , instead, would waste both  $x$  and  $y$ , and only  $y$ , respectively, hence they are not allowed. Instead the evaluation of  $e_4$  gets stuck due to resource exhaustion exactly as before. The formal definition of a reduction which is no-waste, hence gets stuck for  $e_1$  and  $e_2$ , requires some more elaborated definitions, which will be developed in Section 7.

### 3 Algebraic preliminaries: a taxonomy of grade algebras

In this section we introduce the algebraic structures we will use throughout the paper. At the core of our work there are *grades*, namely, annotations in terms and types expressing how or how much resources can be used during the computation. As we will see, we need some operations and relations to properly combine and compare grades in the resource-aware semantics and type system, hence we assume grades to form an algebraic structure called a *grade algebra* defined below. Such a structure is a slight variant of others in the literature [1, 5, 12, 13, 24, 25, 31, 32, 39], which are all instances of ordered semirings.

**Definition 3.1** (Ordered Semiring). An *ordered semiring* is a tuple  $R = \langle |R|, \preceq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  such that:

- $\langle |R|, \preceq \rangle$  is a partially ordered set;
- $\langle |R|, +, \mathbf{0} \rangle$  is a commutative monoid;
- $\langle |R|, \cdot, \mathbf{1} \rangle$  is a monoid;

and the following axioms are satisfied:

- $r \cdot (s + t) = r \cdot s + r \cdot t$  and  $(s + t) \cdot r = s \cdot r + t \cdot r$ , for all  $r, s, t \in |R|$ ;
- $r \cdot \mathbf{0} = \mathbf{0}$  and  $\mathbf{0} \cdot r = \mathbf{0}$ , for all  $r \in |R|$ ;
- if  $r \preceq r'$  and  $s \preceq s'$  then  $r + s \preceq r' + s'$  and  $r \cdot s \preceq r' \cdot s'$ , for all  $r, r', s, s' \in |R|$ ;

Essentially, an ordered semiring is a semiring with a partial order on its carrier which makes addition and multiplication monotonic with respect to it. Roughly, addition and multiplication (which is not necessarily commutative) provide parallel and sequential composition of usages,

**1** models the unitary or default usage and **0** models no use. Finally, the partial order models overapproximation in the resource usage, giving flexibility. For instance we can have different usage in the branches of an if-then-else construct.

In an ordered semiring there can be elements  $r \preceq \mathbf{0}$ , which, however, make no sense in our context, since **0** models no usage. Hence, in a grade algebra we forbid such grades.

**Definition 3.2** (Grade Algebra). An ordered semiring  $R = \langle |R|, \preceq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  is a *grade algebra* if  $r \preceq \mathbf{0}$  implies  $r = \mathbf{0}$ , for all  $r \in |R|$ .

This property is not technically needed, but it is intuitively expected to hold, and allows to simplify some definitions. Moreover, it can be forced in any ordered semiring, just noting that the set  $I_{\preceq \mathbf{0}} = \{r \in |R| \mid r \preceq \mathbf{0}\}$  is a two-sided ideal and so the quotient semiring  $R/I_{\preceq \mathbf{0}}$  is well-defined and is a grade algebra.

We now give some examples of grade algebras adapted from the literature.

**Example 3.3.**

- (1) The simplest way of measuring resource usage is by counting and can be done using natural numbers with their usual operations. We consider two grade algebras over natural numbers: one for *bounded counting*  $\text{Nat}^{\leq} = \langle \mathbb{N}, \leq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$ , taking the natural ordering, and another for *exact counting*  $\text{Nat}^= = \langle \mathbb{N}, =, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$ , taking equality as order, thus basically forbidding approximations of resource usage.
- (2) The *linearity* grade algebra  $\langle \{0, 1, \infty\}, \leq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  is obtained from  $\text{Nat}^=$  above by identifying all natural numbers strictly greater than 1 and taking as order  $0 \leq \infty$  and  $1 \leq \infty$ ; the *affinity* grade algebra only differs for the order, which is  $0 \leq 1 \leq \infty$ .
- (3) In the trivial grade algebra  $\text{Triv}$  the carrier is a singleton set  $|\text{Triv}| = \{\mathbf{0}\}$ , the partial order is the equality, addition and multiplication are defined in the trivial way and  $\mathbf{0}_{\text{Triv}} = \mathbf{1}_{\text{Triv}} = \mathbf{0}$ .
- (4) The grade algebra of extended non-negative real numbers is  $R_{\geq 0}^{\infty} = \langle [0, \infty], \leq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$ , where usual order and operations are extended to  $\infty$  in the expected way.
- (5) A distributive lattice  $L = \langle |L|, \leq, \vee, \wedge, \perp, \top \rangle$ , where  $\leq$  is the order,  $\vee$  and  $\wedge$  the join and meet, and  $\perp$  and  $\top$  the bottom and top element, respectively, is a grade algebra. These grade algebras do not carry quantitative information, as the addition is idempotent, but rather express how/in which mode a resource can be used. They are called *informational* by Abel and Bernardy [1].
- (6) Given the grade algebras  $R = \langle |R|, \preceq_R, +_R, \cdot_R, \mathbf{0}_R, \mathbf{1}_R \rangle$  and  $S = \langle |S|, \preceq_S, +_S, \cdot_S, \mathbf{0}_S, \mathbf{1}_S \rangle$ , the *product*  $R \times S = \langle \{\langle r, s \rangle \mid r \in |R| \wedge s \in |S|\}, \preceq, +, \cdot, \langle \mathbf{0}_R, \mathbf{0}_S \rangle, \langle \mathbf{1}_R, \mathbf{1}_S \rangle \rangle$ , where operations are the pairwise application of the operations for  $R$  and  $S$ , is a grade algebra.
- (7) Given a grade algebra  $R = \langle |R|, \preceq_R, +_R, \cdot_R, \mathbf{0}_R, \mathbf{1}_R \rangle$ , set  $R^{\infty} = \langle |R| + \{\infty\}, \preceq, +, \cdot, \mathbf{0}_R, \mathbf{1}_R \rangle$  where  $\preceq$  extends  $\preceq_R$  by adding  $r \preceq \infty$  for all  $r \in |R|$  and  $+$  and  $\cdot$  extend  $+_R$  and  $\cdot_R$  by  $r + \infty = \infty + r = \infty$ , for all  $r \in |R^{\infty}|$ , and  $r \cdot \infty = \infty \cdot r = \infty$ , for all  $r \in |R^{\infty}|$  with  $r \neq \mathbf{0}_R$ , and  $\mathbf{0}_R \cdot \infty = \infty \cdot \mathbf{0}_R = \mathbf{0}_R$ . Then,  $R^{\infty}$  is a grade algebra, where  $\infty$  models *unrestricted usage*.
- (8) Given  $R$  as above, set  $|\text{Int}(R)| = \{\langle r, s \rangle \in |R| \times |R| \mid r \preceq_R s\}$ , the set of *intervals* between two points in  $|R|$ , with  $\langle r, s \rangle \preceq \langle r', s' \rangle$  iff  $r' \preceq_R r$  and  $s \preceq_R s'$ . Then,  $\text{Int}(R) = \langle |\text{Int}(R)|, \preceq, +, \cdot, \langle \mathbf{0}_R, \mathbf{0}_R \rangle, \langle \mathbf{1}_R, \mathbf{1}_R \rangle \rangle$  is a grade algebra, with  $+$  and  $\cdot$  defined pointwise.

We say that a grade algebra is *trivial* if it is isomorphic to  $\text{Triv}$ , that is, it contains a single point. It is easy to see that a grade algebra is trivial iff  $\mathbf{1} \preceq \mathbf{0}$ , as this implies  $r \preceq \mathbf{0}$ , hence  $r = \mathbf{0}$ , for all  $r \in |R|$ , by the axioms of ordered semiring and Definition 3.2.

A grade algebra is still a quite wild structure, notably we can get  $\mathbf{0}$  by summing or multiplying non-zero grades. This does not match the intuition that  $\mathbf{0}$  represents no usage at all, hence a combination of non-zero usages cannot give no usage, as expressed by the following definition.

**Definition 3.4.** Let  $R = \langle |R|, \preceq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  be a grade algebra. We say that

- $R$  is *integral* if  $r \cdot s = \mathbf{0}$  implies  $r = \mathbf{0}$  or  $s = \mathbf{0}$ , for all  $r, s \in |R|$ ;
- $R$  is *reduced* if  $r + s = \mathbf{0}$  implies  $r = s = \mathbf{0}$ , for all  $r, s \in |R|$ .

The grade algebras considered as examples in the paper will be integral and reduced. Besides the modeling reasons mentioned above, the requirement to be integral is technically useful, e.g., in Lemma 5.3(2).

All the grade algebras in Example 3.3 are reduced, provided that the parameters are reduced, for (6)-(8). Similarly, they are all integral except (5) and (6). Indeed, in the former there can be elements different from  $\perp$  whose meet is  $\perp$  (e.g., disjoint subsets in the powerset lattice), while in the latter there are pairs  $\langle r, \mathbf{0} \rangle$  and  $\langle \mathbf{0}, s \rangle$  whose product is  $\langle \mathbf{0}, \mathbf{0} \rangle$  even if both  $r \neq \mathbf{0}$  and  $s \neq \mathbf{0}$ . Fortunately, there is an easy construction making a grade algebra both reduced and integral.

**Definition 3.5.** Set  $R = \langle |R|, \preceq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  an ordered semiring. We denote by  $R_0$  the ordered semiring  $\langle |R| + \{\hat{\mathbf{0}}\}, \preceq, +, \cdot, \hat{\mathbf{0}}, \mathbf{1} \rangle$  where we add a new point  $\hat{\mathbf{0}}$  and extend order and operations as follows:

$$\begin{aligned} \hat{\mathbf{0}} &\preceq r \text{ iff } \mathbf{0} \preceq r, \\ r + \hat{\mathbf{0}} &= \hat{\mathbf{0}} + r = r, \\ r \cdot \hat{\mathbf{0}} &= \hat{\mathbf{0}} \cdot r = \hat{\mathbf{0}}, \text{ for all } r \in |R| + \{\hat{\mathbf{0}}\}. \end{aligned}$$

It is easy to check that the following proposition holds.

**Proposition 3.6.** *If  $R = \langle |R|, \preceq, +, \cdot, \mathbf{0}, \mathbf{1} \rangle$  is a grade algebra, then  $R_0$  is a reduced and integral grade algebra.*

Applying this construction to (5) and (6) we get reduced and integral grade algebras.

For the former, note that we get an informational grade algebra where the grade meaning the “lowest” mode of usage is different from the zero grade, meaning no usage at all. For instance, two access levels are modeled by a grade algebra where  $\mathbf{0} \preceq \text{private} \preceq \text{public}$ . This is different from models of privacy levels in the literature [1], where  $\mathbf{0}$  coincides with the lowest mode of usage. Indeed, in such models the meaning of the zero grade is “irrelevant”. That is, the usage of the resource does not affect the result of the computation, hence we cannot infer any information about the resource by observing such result: in this sense the resource is private.

For (6), the result is not yet satisfactory. Indeed, the resulting grade algebra still has spurious elements which are difficult to interpret. Thus we consider the following refined construction.

**Example 3.7.** Let  $R$  and  $S$  be non-trivial, reduced and integral grade algebras. The *smash product* of  $R$  and  $S$  is  $R \otimes S = \langle |R \otimes S|, \preceq, +, \cdot, \hat{\mathbf{0}}, \langle \mathbf{1}_R, \mathbf{1}_S \rangle \rangle$ , where  $|R \otimes S| = |(R \times S)_0| \setminus \{|R| \times$

$$\begin{array}{ll}
v ::= x \mid \text{recf}.\lambda x.e \mid \text{unit} \mid \langle^r v_1, v_2^s \rangle \mid \text{inl}^r v \mid \text{inr}^r v & \text{value expression} \\
e ::= \text{return } v \mid \text{let } x = e_1 \text{ in } e_2 \mid v_1 v_2 & \text{expression} \\
\quad \mid \text{match } v \text{ with unit} \rightarrow e & \\
\quad \mid \text{match } v \text{ with } \langle x, y \rangle \rightarrow e & \\
\quad \mid \text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 &
\end{array}$$

Fig. 3. Fine-grained syntax

$\{0_S\} \cup \{0_R\} \times |S|$ ,  $\preceq$ ,  $+$  and  $\cdot$  are the restrictions of the order and operations of  $(R \times S)_0$ , as in Definition 3.5, to the subset  $|R \oslash S|$ , and  $\hat{0}$  is the zero of  $(R \times S)_0$ . It is easy to see  $R \oslash S$  is a non-trivial, reduced and integral grade algebra.

Finally, to express no-wasting, as will be done in Section 7, we need the following definition.

**Definition 3.8** (Discardable grade and affine grade algebra). In a grade algebra  $R$ , a grade  $r$  such that  $0 \preceq r$  is said *discardable*. A grade algebra is said to be *affine* if  $0 \preceq r$  holds for all  $r \in |R|$ , that is, all grades are discardable.

Intuitively, resources with discardable grades can be safely wasted, since they can be reduced to  $0$  through the approximation order. For instance, in the linearity grade algebra of Example 3.3(2), the element  $\infty$  can be discarded, while the element  $1$  cannot. Note that the affinity condition is equivalent to requiring just  $0 \preceq 1$  again thanks to the axioms of ordered semiring. Instances of affine grade algebras from Example 3.3 are bounded usage (1), the extended non-negative real numbers (4) and distributive lattices (5), while exact usage (1) and linearity (2) are not affine.

The subset of discardable elements in a grade algebra<sup>5</sup> forms a *two-sided ideal*. This means that the following two properties hold:

- if  $0 \preceq r$  and  $0 \preceq s$ , then  $0 \preceq r + s$ ,
- if  $0 \preceq r$ , then  $0 \preceq r \cdot s$  and  $0 \preceq s \cdot r$ , for every  $s \in |R|$ .

These properties easily follow from the monotonicity of  $+$  and  $\cdot$  and from the fact that multiplying by  $0$  yields  $0$ .

#### 4 Resource-aware semantics

We define, for a standard functional calculus, an instrumented semantics which keeps track of resource usage, hence, in particular, it gets stuck if some needed resource is insufficient.

The syntax, shown in Fig. 3, is given in a fine-grained style. This long-standing approach [29] is used to clearly separate effect-free from effectful expressions (*computations*), and to make the evaluation strategy, relevant for the latter, explicit through the sequencing construct (*let-in*), rather than fixed a-priori. In our calculus, the computational effect is *divergence*, so the effectful expressions are possibly diverging, whereas those effect-free will be called *value expressions*<sup>6</sup>. Note that, as customary, expressions are defined on top of value expressions, whereas the converse does not hold; this stratification makes the technical development modular, as will be detailed in the following.

<sup>5</sup>Actually in any ordered semiring.

<sup>6</sup>They are often called just “values” in literature, though, as already noted in [29], they are not values in the operational sense, that is, results of the evaluation; here we keep the two notions distinct. Values turn out to be value expressions with no free variables, except those under a lambda.

The constructs are pretty standard: the `unit` constant, pairs, left and right injections, and three variants of `match` construct playing as destructors of units, pairs, and injections, respectively. Instead of standard lambda expressions and a `fix` operator for recursion, we have a single construct `rec f.  $\lambda x. e$` , meaning a function with parameter  $x$  and body  $e$  which can recursively call itself through the variable  $f$ . Standard lambda expressions can be recovered as those where  $f$  does not occur free in  $e$ , that is, when the function is non-recursive, and we will use the abbreviation  $\lambda x. e$  for such expressions. The motivation for such unique construct is that in the resource-aware semantics there is no immediate parallel substitution as in standard rules for application and `fix`, but occurrences of free variables are replaced one at a time, when needed, by their value stored in an environment. Thus, application of a (possibly recursive) function can be nicely modeled by generalizing what is expected for a non-recursive one, that is, it leads to the evaluation of the body in an environment where both  $f$  and  $x$  are added as resources, as formalized in rule (APP) in Fig. 4.

As anticipated, the pair and injection constructors are decorated with a grade for each subterm, intuitively meaning “how many copies” are contained in the compound term. For instance, taking as grades the natural numbers as in Example 3.3(1), a pair of shape  $\langle^2 e_1, e_2^2\rangle$  contains “two copies” of each component. In the resource-aware semantics, this is reflected by the fact that, to evaluate (one copy of) such pair, we need to obtain 2 copies of the results of  $e_1$  and  $e_2$ ; correspondingly, when matching such result with a pair of variables, both are made available in the environment with grade 2.

We will sometimes use, rather than `match  $e_1$  with unit  $\rightarrow e_2$` , the alternative syntax  $e_1; e_2$ , emphasising that there is a sequential evaluation of the two subterms.

The resource-aware semantics is formally defined in Fig. 4. Corresponding to the two syntactic categories, the semantics is expressed by two distinct judgments,  $v \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'$  in the top section, and  $e \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'$  in the bottom section. Note that there is no mutual recursion: the latter is defined on top of the former. Hence, the metarules in Fig. 4 can be equivalently seen as

- a single inductive definition
- a stratified definition, where the judgment  $e \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'$  is inductively defined, assuming the definition of  $v \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'$ .

For simplicity, we use the same notation for the two judgments, and in the bottom section of Fig. 4 we write both judgments as premises, taking the first view. However, the stratified view will be useful later to allow a modular technical development, notably for the construction adding divergence given in Section 8.

Rules for value expressions just replace variables by values; the reduction cannot diverge, but is resource-consuming, hence it can get stuck.

In particular, in (VAR), which is the key rule where resources are consumed, a variable is replaced by its associated value, and its grade  $s$  decreases to  $s'$ , burning an amount  $r$  of resource which has to be at least the reduction grade. The side condition  $r + s' \preceq s$  ensures that the initial grade is allowed to consume the  $r$  amount, leaving a residual grade  $s'$ . Note that such a condition could hold for different residual grades. Hence, reduction is largely non-deterministic; it will be the responsibility of the type system to ensure that there is at least one reduction which does not get stuck.

$$\begin{array}{c}
\text{(VAR)} \frac{}{x|\rho, x : \langle s, \mathbf{v} \rangle \Rightarrow_r \mathbf{v}|\rho, x : \langle s', \mathbf{v} \rangle} \quad r + s' \preceq s \quad \text{(FUN)} \frac{}{\text{recf}.\lambda x.e|\rho \Rightarrow_r \text{recf}.\lambda x.e|\rho} \\
\\
\text{(UNIT)} \frac{}{\text{unit}|\rho \Rightarrow_r \text{unit}|\rho} \quad \text{(PAIR)} \frac{v_1|\rho \Rightarrow_{r \cdot r_1} \mathbf{v}_1|\rho_1 \quad v_2|\rho_1 \Rightarrow_{r \cdot r_2} \mathbf{v}_2|\rho_2}{\langle r_1 v_1, v_2 r_2 \rangle |\rho \Rightarrow_r \langle r_1 \mathbf{v}_1, \mathbf{v}_2 r_2 \rangle |\rho_2} \\
\\
\text{(INL)} \frac{v|\rho \Rightarrow_{r \cdot s} \mathbf{v}|\rho'}{\text{inl}^s v|\rho \Rightarrow_r \text{inl}^s \mathbf{v}|\rho'} \quad \text{(INR)} \frac{v|\rho \Rightarrow_{r \cdot s} \mathbf{v}|\rho'}{\text{inr}^s v|\rho \Rightarrow_r \text{inr}^s \mathbf{v}|\rho'} \\
\\
\hline
\text{(RET)} \frac{v|\rho \Rightarrow_s \mathbf{v}|\rho'}{\text{return } v \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'} \quad r \preceq s \neq \mathbf{0} \quad \text{(LET)} \frac{e_1|\rho \Rightarrow_s \mathbf{v} \mid \rho'' \quad e_2[x'/x]|\rho'', x' : \langle s, \mathbf{v} \rangle \Rightarrow_r \mathbf{v}'|\rho'}{\text{let } x = e_1 \text{ in } e_2|\rho \Rightarrow_r \mathbf{v}'|\rho'} \quad x' \text{ fresh} \\
\\
\text{(APP)} \frac{v_1|\rho \Rightarrow_s \text{recf}.\lambda x.e|\rho_1 \quad v_2|\rho_1 \Rightarrow_t \mathbf{v}_2|\rho_2 \quad e[f'/f][x'/x] \mid \rho_2, f' : \langle s_2, \text{recf}.\lambda x.e \rangle, x' : \langle t, \mathbf{v}_2 \rangle \Rightarrow_r \mathbf{v} \mid \rho' \quad \begin{array}{l} s_1 + s_2 \preceq s \\ s_1 \neq \mathbf{0} \\ f', x' \text{ fresh} \end{array}}{v_1 v_2 \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'} \\
\\
\text{(MATCH-U)} \frac{v|\rho \Rightarrow_s \text{unit}|\rho'' \quad e \mid \rho'' \Rightarrow_r \mathbf{v} \mid \rho'}{\text{match } v \text{ with unit} \rightarrow e \mid \rho \Rightarrow_r \mathbf{v} \mid \rho} \quad s \neq \mathbf{0} \\
\\
\text{(MATCH-P)} \frac{v|\rho \Rightarrow_s \langle r_1 \mathbf{v}_1, \mathbf{v}_2 r_2 \rangle |\rho'' \quad e[x'/x][y'/y] \mid \rho'', x' : \langle s \cdot r_1, \mathbf{v}_1 \rangle, y' : \langle s \cdot r_2, \mathbf{v}_2 \rangle \Rightarrow_r \mathbf{v} \mid \rho' \quad \begin{array}{l} s \neq \mathbf{0} \\ x', y' \text{ fresh} \end{array}}{\text{match } v \text{ with } \langle x, y \rangle \rightarrow e \mid \rho \Rightarrow_r \mathbf{v} \mid \rho'} \\
\\
\text{(MATCH-L)} \frac{v|\rho \Rightarrow_t \text{inl}^s \mathbf{v}|\rho'' \quad e_1[y/x_1] \mid \rho'', y : \langle t \cdot s, \mathbf{v} \rangle \Rightarrow_r \mathbf{v}' \mid \rho' \quad \begin{array}{l} t \neq \mathbf{0} \\ y \text{ fresh} \end{array}}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_r \mathbf{v}' \mid \rho'} \\
\\
\text{(MATCH-R)} \frac{v|\rho \Rightarrow_t \text{inr}^s \mathbf{v}|\rho'' \quad e_2[y/x_1] \mid \rho'', y : \langle t \cdot s, \mathbf{v} \rangle \Rightarrow_r \mathbf{v}' \mid \rho' \quad \begin{array}{l} t \neq \mathbf{0} \\ y \text{ fresh} \end{array}}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_r \mathbf{v}' \mid \rho'}
\end{array}$$

Fig. 4. Resource-aware semantics

The other rules for value expressions propagate rule (VAR) to subterms which are variables. In rules for “data containers” (PAIR), (IN-L), and (IN-R), the components are evaluated with the evaluation grade of the compound value expression, multiplied by that of the component.

Whereas evaluation of value expressions may have grade  $\mathbf{0}$ , when they are actually *used*, that is, are subterms of expressions, they should be evaluated with a non-zero grade, as required by a side condition in the corresponding rules in the bottom section of Fig. 4.

In rule (RET), the evaluation grade of the value expression should be enough to cover the current evaluation grade. In rule (LET), expressions  $e_1$  and  $e_2$  are evaluated sequentially, the latter in an environment where the local variable  $x$  has been added as available resource,

modulo renaming with a fresh variable to avoid clashes, with the value and grade obtained by the evaluation of  $e_1$ .

In rule (APP), an application  $v_1 v_2$  is evaluated by first consuming the resources needed to obtain a value from  $v_1$  and  $v_2$ , with the former expected to be a (possibly recursive) function. Then, the function body is evaluated in an environment where the function name and the parameter have been added as available resources, modulo renaming with fresh variables. The function should be produced in a “number of copies”, that is, with a grade  $s$ , enough to cover both all the future recursive calls ( $s_2$ ) and the current use ( $s_1$ ); in particular, for a non-recursive call,  $s_2$  could be  $\mathbf{0}$ . Instead, the current use should be non-zero since we are actually using the function.

Note also that, in this rule as in others, there is no required relation between the reduction grades of some premises (in this case,  $s$  and  $t$ ) and that of the consequence, here  $r$ . Of course, depending on the choice of such grades, reduction could either proceed or get stuck due to resource exhaustion; the role of the type system is exactly to show that there is a choice which prevents the latter case.

Rules for match constructs, namely (MATCH-U), (MATCH-P), (MATCH-L), and (MATCH-R), all follow the same pattern. The resources needed to obtain a value from the value expression to be matched are consumed, and then the continuation is evaluated. In rule (MATCH-U), there is no value-passing from the matching expression to the continuation, hence their evaluation grades are independent. In rule (MATCH-P), instead, the continuation is evaluated in an environment where the two variables in the pattern have been added as available resources, again modulo renaming. The values associated to the two variables are the ones of the corresponding component of the expression to be matched, whereas the grades are the evaluation grade of the expression, multiplied by the grade of the component. Rules (MATCH-L) and (MATCH-R) are analogous.

Besides the standard typing errors, an evaluation graded  $r$  can get stuck (formally, no judgment can be derived) when rule (VAR) cannot be applied since its side condition does not hold. Informally, some resource (variable) is exhausted, that is, can no longer be replaced by its value. Also note that the instrumented reduction is non-deterministic, due to rule (VAR). That is, when a resource is needed, it can be consumed in different ways; hence, soundness of the type system will be *soundness-may*, meaning that *there exists* a computation which does not get stuck.

We end this section by illustrating resource consumption in a non-terminating computation.

**Example 4.1.** Consider the function  $\text{div} = \text{rec } f. \lambda x. y; f x$ , which clearly diverges on any argument, by using infinitely many times the external resource  $y$ . In Fig. 5 we show the (incomplete) proof tree for the evaluation of an application  $y; f x$ , in an environment where  $f$  denotes the function  $\text{div}$ , and  $y$  and  $x$  denote  $\text{unit}$ . For simplicity, as in previous examples, we omit  $\mathbf{1}$  grades, and renaming of variables; moreover, we abbreviate by  $\langle r, s, t \rangle$  the environment  $y : \langle r, \text{unit} \rangle, f : \langle s, \text{div} \rangle, x : \langle t, \text{unit} \rangle$ .

In this way, we can focus on the key feature that the (tentative) proof tree shows: the body of  $\text{div}$  is evaluated infinitely many times, in a sequence of environments, starting from the root, where the grades of the external resource  $y$ , assuming that each time it is consumed by  $\mathbf{1}$ , are as follows:

$$r_0 = r_1 + \mathbf{1} \quad r_1 = r_2 + \mathbf{1} \quad \dots \quad r_k = r_{k+1} + \mathbf{1} \quad \dots$$

$$\frac{y; \langle r_0, s_0, \mathbf{1} \rangle \Rightarrow u \mid \langle r_1, s_0, \mathbf{1} \rangle}{\frac{f \mid \langle r_1, s_0, \mathbf{1} \rangle \Rightarrow_{s_0} \text{div} \mid \langle r_1, \mathbf{0}, \mathbf{1} \rangle \quad x \mid \langle r_1, \mathbf{0}, \mathbf{1} \rangle \Rightarrow u \mid \langle r_1, \mathbf{0}, \mathbf{0} \rangle \quad y; f x \mid \langle r_1, s_1, \mathbf{1} \rangle \Rightarrow ?}{f x \mid \langle r_1, s_0, \mathbf{1} \rangle \Rightarrow ?} \text{ (APF)}} \text{ (MATCH-U)}$$

Fig. 5. Example of resource-aware evaluation: consumption/divergency

In the case of the resource  $f$ , at each recursive call, the function must be produced with a grade which is the sum of its current usage (assumed again to be  $\mathbf{1}$ ) and the grade which will be associated to (a fresh copy of)  $f$  in the environment, to evaluate the body. As a consequence, we also get:

$$s_0 = s_1 + \mathbf{1} \quad s_1 = s_2 + \mathbf{1} \quad \dots \quad s_k = s_{k+1} + \mathbf{1} \quad \dots$$

Let us now see what happens depending on the underlying grade algebra, considering  $y$  (an analogous reasoning applies to  $f$ ). Taking the grade algebra of natural numbers of Example 3.3(1), it is easy to see that the above sequence of constraints can be equivalently expressed as:

$$r_1 = r_0 - 1 \quad r_2 = r_1 - 1 \quad \dots \quad r_{k+1} = r_k - 1 \quad \dots$$

Thus, in a finite number of steps, the grade of  $y$  in the environment becomes 0, hence the proof tree cannot be continued since we can no longer extract the associated value by rule (VAR). In other words, the computation is stuck due to resource consumption.

Assume now to take, instead, natural numbers extended with  $\infty$ , as defined in Example 3.3(7). In this case, if we start with  $r_0 = \infty$ , intuitively meaning that  $y$  can be used infinitely many times, evaluation can proceed forever by taking  $r_k = \infty$  for all  $k$ . The same happens if we take a non-quantitative grade algebra, e.g., that of access levels; we can have  $r_k = \text{public}$  for all  $k$ . However, interpreting the rules in Fig. 4 in the standard inductive way, the semantics we get *does not* formalize such non-terminating evaluation, since we only consider judgments with a *finite* proof tree. We will see in Section 8 how to extend the semantics to model non-terminating computations as well.

## 5 Resource-aware type system

Types, defined in Fig. 6, are those expected for the constructs in the syntax: functional,  $\text{Unit}$ , (tensor) product, sum, and (equi-)recursive types, obtained by interpreting the productions *coinductively*, so that infinite<sup>7</sup> terms are allowed. However, they are *graded*, that is, decorated with a grade, and the type subterms are graded. Moreover, accordingly with the fact that functions are possibly recursive, arrows in functional types are decorated with a grade as well, called the *recursion grade* in the following, expressing the recursive usage of the function; thus, functional types decorated with  $\mathbf{0}$  are non-recursive.

In (type-and-grade) contexts, also defined in Fig. 6, order is immaterial and  $x_i \neq x_j$  for  $i \neq j$ ; hence, they represent maps from variables to pairs consisting of a grade, sometimes called *coeffect* [12, 33, 34] when used in this position, and a (non-graded) type. We write  $\text{dom}(\Gamma)$  for  $\{x_1, \dots, x_n\}$ . Equivalently, a type-and-grade context can be seen as a pair consisting of the standard type context  $x_1 : \tau_1 \dots, x_n : \tau_n$ , and the grade context  $x_1 : r_1, \dots, x_n : r_n$ , the latter representing a function  $\gamma$  from variables into grades with finite support, that is,  $\gamma(x) \neq \mathbf{0}$  for

<sup>7</sup>More precisely, *regular* terms, that is, those with finitely many distinct subterms.

|                  |                                                                        |                          |
|------------------|------------------------------------------------------------------------|--------------------------|
| $\tau, \sigma$   | $::= T \rightarrow_s S \mid \mathbf{Unit} \mid T \otimes S \mid T + S$ | non-graded type          |
| $T, S$           | $::= \tau^r$                                                           | graded type              |
| $\gamma$         | $::= x_1 : r_1, \dots, x_n : r_n$                                      | grade context            |
| $\Gamma, \Delta$ | $::= x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$                    | (type-and-grade) context |

Fig. 6. Types and (type-and-grade) contexts

finitely many  $x \in V$ . Grade contexts will play a key role in Section 7 to express the no-waste version of the semantics.

We define the following operations on contexts:

- a partial order  $\preceq$

$$\begin{aligned}
 & \emptyset \preceq \emptyset \\
 & x :_s \tau, \Gamma \preceq x :_r \tau, \Delta \quad \text{if } s \preceq r \text{ and } \Gamma \preceq \Delta \\
 & \Gamma \preceq x :_r \tau, \Delta \quad \text{if } x \notin \text{dom}(\Gamma) \text{ and } \Gamma \preceq \Delta \text{ and } \mathbf{0} \preceq r
 \end{aligned}$$

- a sum  $+$

$$\begin{aligned}
 & \emptyset + \Gamma = \Gamma \\
 & (x :_s \tau, \Gamma) + (x :_r \tau, \Delta) = x :_{s+r} \tau, (\Gamma + \Delta) \\
 & (x :_s \tau, \Gamma) + \Delta = x :_s \tau, (\Gamma + \Delta) \quad \text{if } x \notin \text{dom}(\Delta)
 \end{aligned}$$

- a scalar multiplication  $\cdot$

$$s \cdot \emptyset = \emptyset \quad s \cdot (x :_r \tau, \Gamma) = x :_{s \cdot r} \tau, (s \cdot \Gamma)$$

These operations on type-and-grade contexts are obtained by lifting the corresponding operations on grade contexts, which are the pointwise extension of those on grades, to handle types. In this step, the addition becomes partial since a variable in the domain of both contexts is required to have the same type.

**Remark 5.1.** It is important to note that, when overapproximating contexts with the partial order, new resources can be added only with a discardable grade. For instance, in the linearity grade algebra of Example 3.3(2),  $\Gamma \not\preceq (\Gamma, y :_1 \sigma)$ . In other words, the partial order models *no-waste* approximation.

In Fig. 7, we give the typing rules, which are *parameterized* on the underlying grade algebra. As for instrumented reduction, the resource-aware type system is formalized by two judgments,  $\Gamma \vdash v : T$  and  $\Gamma \vdash e : T$ , for value expressions and expressions, respectively. However, differently from reduction, the two judgments are mutually recursive, due to rule (T-FUN), hence the metarules in Fig. 7 define a unique judgment which is their union. We only comment on the most significant points. In rule (T-SUB-V) and (T-SUB), the context can be made more general, and the grade of the type more specific. This means that, on one hand, variables can get less constraining grades. For instance, assuming affinity grades as in Example 3.3(2), an expression which can be typechecked assuming to use a given variable at most once (grade 1) can be typechecked with no constraints (grade  $\omega$ ). On the other hand, an expression can get a more constraining grade. For instance, an expression of grade  $\omega$  can be used where a grade 1 is required.

$$\begin{array}{c}
\text{(T-SUB-V)} \frac{\Gamma \vdash v : \tau^r \quad s \preceq r}{\Delta \vdash v : \tau^s \quad \Gamma \preceq \Delta} \quad \text{(T-VAR)} \frac{}{x :_r \tau \vdash x : \tau^r} \\
\\
\text{(T-FUN)} \frac{\Gamma, f :_s \tau_1^{r_1} \rightarrow_s \tau_2^{r_2}, x :_{r_1} \tau_1 \vdash e : \tau_2^{r_2}}{r \cdot \Gamma \vdash \text{recf}.\lambda x.e : (\tau_1^{r_1} \rightarrow_s \tau_2^{r_2})^r} \quad \text{(T-UNIT)} \frac{}{\mathbf{0} \vdash \text{unit} : \text{Unit}^r} \\
\\
\text{(T-PAIR)} \frac{\Gamma_1 \vdash v_1 : \tau_1^{r_1} \quad \Gamma_2 \vdash v_2 : \tau_2^{r_2}}{r \cdot (\Gamma_1 + \Gamma_2) \vdash \langle v_1, v_2 \rangle : (\tau_1^{r_1} \otimes \tau_2^{r_2})^r} \\
\\
\text{(T-INL)} \frac{\Gamma \vdash v : \tau_1^{r_1}}{r \cdot \Gamma \vdash \text{inl}^{r_1} v : (\tau_1^{r_1} + \tau_2^{r_2})^r} \quad \text{(T-INR)} \frac{\Gamma \vdash v : \tau_2^{r_2}}{r \cdot \Gamma \vdash \text{inr}^{r_2} v : (\tau_1^{r_1} + \tau_2^{r_2})^r} \\
\hline
\\
\text{(T-SUB)} \frac{\Gamma \vdash e : \tau^r \quad s \preceq r}{\Delta \vdash e : \tau^s \quad \Gamma \preceq \Delta} \quad \text{(T-RET)} \frac{\Gamma \vdash v : \tau^r}{\Gamma \vdash \text{return } v : \tau^r} \quad r \neq \mathbf{0} \\
\\
\text{(T-LET)} \frac{\Gamma_1 \vdash e_1 : \tau_1^{r_1} \quad \Gamma_2, x :_{r_1} \tau_1 \vdash e_2 : \tau_2^{r_2}}{\Gamma_1 + \Gamma_2 \vdash \text{let } x = e_1 \text{ in } e_2 : \tau_2^{r_2}} \\
\\
\text{(T-APP)} \frac{\Gamma_1 \vdash v_1 : (\tau_1^{r_1} \rightarrow_s \tau_2^{r_2})^{(r+r \cdot s)} \quad \Gamma_2 \vdash v_2 : \tau_1^{r \cdot r_1}}{\Gamma_1 + \Gamma_2 \vdash v_1 v_2 : \tau_2^{r \cdot r_2}} \quad r \neq \mathbf{0} \\
\\
\text{(T-MATCH-U)} \frac{\Gamma_1 \vdash v : \text{Unit}^r \quad \Gamma_2 \vdash e : T}{\Gamma_1 + \Gamma_2 \vdash \text{match } v \text{ with unit} \rightarrow e : T} \quad r \neq \mathbf{0} \\
\\
\text{(T-MATCH-P)} \frac{\Gamma_1 \vdash v : (\tau_1^{r_1} \otimes \tau_2^{r_2})^r \quad \Gamma_2, x :_{r \cdot r_1} \tau, y :_{r \cdot r_2} \tau_2 \vdash e : T}{\Gamma_1 + \Gamma_2 \vdash \text{match } v \text{ with } \langle x, y \rangle \rightarrow e : T} \quad r \neq \mathbf{0} \\
\\
\text{(T-MATCH-IN)} \frac{\Gamma_1 \vdash v : (\tau_1^{r_1} + \tau_2^{r_2})^r \quad \Gamma_2, x :_{r \cdot r_1} \tau_1 \vdash e_1 : T \quad \Gamma_2, x :_{r \cdot r_2} \tau_2 \vdash e_2 : T}{\Gamma_1 + \Gamma_2 \vdash \text{match } v \text{ with inl } x \rightarrow e_1 \text{ or inr } x \rightarrow e_2 : T} \quad r \neq \mathbf{0}
\end{array}$$

Fig. 7. Typing rules

If we take  $r = \mathbf{1}$ , then rule (T-VAR) is the standard rule for variable in graded systems, where the grade context is the map where the given variable is used once, and no other variable is used. Here, more generally, the variable can get an arbitrary grade  $r$ , provided that the context is multiplied by  $r$ . The same “local promotion” can be applied in the other structural rules for value expressions.

In rule (T-FUN), a (possibly recursive) function can get a graded functional type, provided that its body can get the result type in the context enriched by assigning the functional type to the function name, and the parameter type to the parameter. As mentioned, we expect the recursion grade  $s$  to be  $\mathbf{0}$  for a non-recursive function; for a recursive function, we expect  $s$  to be an “infinite” grade, in a sense which will be clarified in Example 5.2 below.

In the rules in the bottom section, when a value expression is used as subterm of an expression, its grade is required to be non-zero, since it is evaluated in the computation, hence its resource consumption should be taken into account.

$$\begin{array}{c}
\frac{}{y :_{r'} U \vdash y : U^{r'}} \text{(T-VAR)} \quad \frac{}{f :_{r+r \cdot s} \tau \vdash f : \tau^{r+r \cdot s}} \text{(T-VAR)} \quad \frac{}{x :_{r \cdot r_1} U \vdash x : U^{r \cdot r_1}} \text{(T-VAR)} \\
\frac{}{f :_{r+r \cdot s} \tau, x :_{r \cdot r_1} U \vdash fx : U^{r \cdot r_2}} \text{(T-APP)} \quad \frac{}{r \neq 0} \text{(T-MATCH-U)} \\
\frac{}{y :_{r'} U, f :_{r+r \cdot s} \tau, x :_{r \cdot r_1} U \vdash y;fx : U^{r \cdot r_2}} \text{(T-FUN)} \quad \frac{}{\tau = U^{r_1} \rightarrow_s U^{r_2}} \text{(T-FUN)} \\
\frac{}{y :_{r'} U \vdash \text{rec } f. \lambda x. y; fx : \tau} \text{(T-FUN)}
\end{array}$$

Fig. 8. Example of type derivation: recursive function

In rule (T-APP), the function should be produced with a grade which is the sum of that required for the current usage ( $r$ ) and that corresponding to the recursive calls: the latter are the grade required for a single usage multiplied by the recursion grade ( $s$ ). For a non-recursive function ( $s = 0$ ), the rule turns out to be as expected for a usual application.

**Example 5.2.** As an example of type derivation, we consider the function  $\text{div} = \text{rec } f. \lambda x. y; fx$  introduced in Example 4.1. In Fig. 8, we show a (parametric) proof tree deriving for  $\text{div}$  a type of the shape  $(\text{Unit}^{r_1} \rightarrow_s \text{Unit}^{r_2})$ , in a context providing the external resource  $y$ . Consider, first of all, the condition that the recursion grade  $s$  should satisfy, that is  $(r + r \cdot s) \preceq s$ , for some  $r \neq 0$ , meaning that it should be enough to cover the recursive call in the body and all the further recursive calls.<sup>8</sup> Assuming the grade algebra of natural numbers of Example 3.3(1), there is no grade  $s$  satisfying this condition. In other words, the type system correctly rejects the function since its application would get stuck due to resource consumption, as illustrated in Example 4.1. On the other hand, for, e.g.,  $s = \infty$ , with natural numbers extended as in Example 3.3(7),  $(r + r \cdot s) \preceq s$  would hold for any  $r \neq 0$ , hence the function would be well-typed. Moreover, there would be no constraints on the parameter and return type, since the conditions  $r \cdot r_1 \preceq r_1$  and  $r_2 \preceq r \cdot r_2$  would be always satisfied taking  $r = 1$ . Assuming the grade algebra of access levels introduced before Example 2.2, where  $\mathbf{1} = \text{public}$ , for  $s = \text{public}$  the condition is satisfied analogously, again with no constraints on  $r_1$  and  $r_2$ . For  $s = \text{private}$ , instead, it only holds for  $r = \text{private}$ , hence the condition  $r_2 \preceq r \cdot r_2$  prevents the return type of the function to be public, accordingly with the intuition that a function used in private mode cannot return a public result. In such cases, the type system correctly accepts the function since its application to a value never gets stuck. Finally note that, to type an application of the function, e.g., to derive that  $\text{div } u$  has type  $U^{r_2}$ ,  $\text{div}$  should get grade  $\mathbf{1} + s$ , hence the grade of the external resource  $y$  should be  $(\mathbf{1} + s) \cdot r'$ , that is, it should be usable infinitely many times as well.

A similar reasoning applies in general; namely, for recursive calls in a function's body we get a condition of shape  $(r + r \cdot s) \preceq s$ , with  $r \neq 0$ , forcing the grade  $s$  of the function to be “infinite”. Brunel et al. [12] and the subsequent work of Abel et al. [2] assume the existence of fixed-point operators whose typing rules explicitly impose a restriction analogous to ours. In our system, instead, this restriction arises from the application of the typing rules. As already observed by Brunel et al. [12], the condition  $(r + r \cdot s) \preceq s$ , with  $r \neq 0$ , forces the grade  $s$  of the function to be “infinite”. This happens regardless of whether the recursive

<sup>8</sup>Note that  $r$  is arbitrary, since there is no sound default grade, and it is only required to be non-zero since the function is actually used.

function is actually always diverging, as in the example above, or terminating on some/all arguments. On the other hand, in the latter case the resource-aware semantics does terminate, as expected, provided that the initial amount of resources is sufficient to cover the (finite number of) recursive calls. This behavior is perfectly reasonable, since the type system is a static overapproximation of the evaluation. We will show an example of this terminating resource-aware evaluation in Section 6 (Fig. 12).

The following lemmas show that the promotion rule, usually explicitly stated in graded type systems, is admissible in our system (Lemma 5.3), and also a converse holds for value expressions (Lemma 5.4). Note that we can promote an expression only using a non-zero grade, to ensure that non-zero constraints on grades in typing rules for expressions are preserved.<sup>9</sup> These lemmas also show that we can assign to a value expression any grade provided that the context is appropriately adjusted: by demotion we can always derive  $\mathbf{1}$  (taking  $r = \mathbf{1}$ ) and then by promotion any grade.

**Lemma 5.3 (Promotion).**

- (1) If  $\Gamma \vdash v : \tau^r$  then  $s \cdot \Gamma \vdash v : \tau^{s \cdot r}$
- (2) If  $\Gamma \vdash e : \tau^r$  and  $s \neq \mathbf{0}$ , then  $s \cdot \Gamma \vdash e : \tau^{s \cdot r}$ .

PROOF. By induction on the typing rules. We show only some cases.

(T-SUB-V) We have  $\Delta \vdash v : \tau^{s'}$ ,  $\Gamma \vdash v : \tau^r$ ,  $r \preceq s'$  and  $\Delta \preceq \Gamma$ . By induction hypothesis  $s \cdot \Delta \vdash v : \tau^{s \cdot s'}$ . By monotonicity  $s \cdot r \preceq s \cdot s'$  and  $s \cdot \Delta \preceq s \cdot \Gamma$ , so, by (T-SUB) we get  $s \cdot \Gamma \vdash v : \tau^{s \cdot r}$ , that is, the thesis.

(T-VAR) By rule (T-VAR) we get the thesis.

(T-FUN) We have  $\Gamma = r \cdot \Gamma'$ ,  $v = \text{rec } f. \lambda x. e'$ ,  $\tau = \tau_1^{r_1} \rightarrow_{s'} \tau_2^{r_2}$  and  $\Gamma', f :_{s'} \tau_1^{r_1} \rightarrow_{s'} \tau_2^{r_2}, x :_{r_1} \tau_1 \vdash e' : \tau_2^{r_2}$ . By rule (T-FUN),  $(s \cdot r) \cdot \Gamma' \vdash v : \tau^{s \cdot r}$ . From  $(s \cdot r) \cdot \Gamma' = s \cdot (r \cdot \Gamma') = s \cdot \Gamma$  we get the thesis.

(T-PAIR), (T-INL) and (T-INR) Similar to (T-FUN).

(T-SUB) We have  $\Delta \vdash e : \tau^{s'}$ ,  $\Gamma \vdash e : \tau^r$ ,  $r \preceq s'$  and  $\Delta \preceq \Gamma$ . By induction hypothesis  $s \cdot \Delta \vdash e : \tau^{s \cdot s'}$ . By monotonicity  $s \cdot r \preceq s \cdot s'$  and  $s \cdot \Delta \preceq s \cdot \Gamma$ , so, by (T-SUB) we get  $s \cdot \Gamma \vdash e : \tau^{s \cdot r}$ , that is, the thesis.

(T-APP) We have  $\Gamma_1 + \Gamma_2 \vdash v_1 v_2 : \tau_2^{r' \cdot r_2}$ . By induction hypothesis  $s \cdot \Gamma_1 \vdash v_1 : (\tau_1^{r_1} \rightarrow_{s'} \tau_2^{r_2})^{s \cdot (r' + r' \cdot s')}$  and  $s \cdot \Gamma_2 \vdash v_2 : \tau_2^{s \cdot r' \cdot r_1}$ . Since  $s \neq \mathbf{0}$  and  $r' \neq \mathbf{0}$  and, since the algebra is integral,  $s \cdot r \neq \mathbf{0}$ . By rule (T-APP),  $s \cdot (\Gamma_1 + \Gamma_2) \vdash v_1 v_2 : \tau_2^{s \cdot r' \cdot r_2}$ , that is, the thesis.

(T-MATCH-P) By induction hypothesis  $s \cdot \Gamma_1 \vdash v : (\tau_1^{r_1} \otimes \tau_2^{r_2})^{s \cdot s'}$  and  $s \cdot \Gamma_2, x :_{(s \cdot s') \cdot r_1} \tau, y :_{(s \cdot s') \cdot r_2} \tau_2 \vdash e : \tau^{s \cdot r}$ . Since  $s \neq \mathbf{0}$  and  $s' \neq \mathbf{0}$  and, since the algebra is integral,  $s \cdot s' \neq \mathbf{0}$ . By rule (T-MATCH-P),  $s \cdot (\Gamma_1 + \Gamma_2) \vdash \text{match } v \text{ with } \langle x, y \rangle \rightarrow e : \tau^{s \cdot r}$ , that is, the thesis.  $\square$

**Lemma 5.4 (Demotion).** If  $\Gamma \vdash v : \tau^{s \cdot r}$  then  $s \cdot \Gamma' \preceq \Gamma$  and  $\Gamma' \vdash v : \tau^r$ , for some  $\Gamma'$ .

PROOF. By case analysis on  $v$ . We show only some cases.

$v = x$  By Lemma 12.1(1)  $x :_{r'} \tau \preceq \Gamma$  and  $s \cdot r \preceq r'$ . Let  $\Gamma' = x :_r \tau$ . By monotonicity of  $\cdot$  and, by transitivity of  $\preceq$ ,  $(s \cdot r) \cdot x :_{\mathbf{1}} \tau = s \cdot \Gamma' \preceq \Gamma$ . By (T-VAR)  $\Gamma' \vdash x : \tau^r$ .

<sup>9</sup>Without assuming the grade algebra to be integral, we would need to use grades which are not zero-divisors.

$$\begin{array}{c}
\text{(T-ENV)} \quad \frac{\Gamma_i \vdash \mathbf{v}_i : \tau_i^1 \quad \forall i \in 1..n}{\Gamma \vdash x_1 : \langle r_1, \mathbf{v}_1 \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n \rangle \triangleright \Delta} \quad \Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n \\
\text{(T-CONF)} \quad \frac{\Delta \vdash E : T \quad \Gamma \vdash \rho \triangleright \Delta}{\Gamma \vdash E \mid \rho : T} \quad E ::= v \mid e
\end{array}$$

Fig. 9. Typing rules for environments and configurations

$v = \langle^{r_1} v_1, v_2^{r_2} \rangle$  By Lemma 12.1(4)  $r' \cdot (\Gamma_1 + \Gamma_2) \preceq \Gamma$  and  $s \cdot r \preceq r'$  and  $\Gamma_1 \vdash v_1 : \tau_1^{r_1}$  and  $\Gamma_2 \vdash v_2 : \tau_2^{r_2}$ . Let  $\Gamma' = r \cdot (\Gamma_1 + \Gamma_2)$ . By monotonicity of  $\cdot$  and by transitivity of  $\preceq$  we have  $s \cdot \Gamma' \preceq \Gamma$ . By (T-PAIR)  $\Gamma' \vdash v : \tau^r$ .

□

In Fig. 9 we give the typing rules for environments and configurations.

The typing judgement for environments has shape  $\Gamma \vdash \rho \triangleright \Delta$ . In rule (T-ENV),  $\Gamma$  is the context *extracted* from the environment, in the sense that, if typechecking succeeds, each variable will get exactly its grade, and the type of its value, in  $\rho$ . In other words,  $\Gamma$  gives type and grade information about the resources (variables) provided by the environment. The context  $\Gamma$  should be enough to cover both the sum of the contexts needed to typecheck each provided resource, and a *residual* context  $\Delta$  left for the program (last side condition). The typing judgment for configurations has shape  $\Gamma \vdash E \mid \rho : T$ , with  $E$  either value expression or expression. In rule (T-CONF), the residual context obtained by typechecking the environment should be exactly that required by the program.

**Remark 5.5.** Note that, in this way, rule (T-CONF) imposes *no-waste*. For instance, taking the linearity grade algebra of Example 3.3(2),  $\Gamma$  cannot offer resources which are unused in both the expression and the codomain of the environment. Hence, e.g.,  $x \mid x : \langle \infty, \mathbf{unit} \rangle, y : \langle 1, \mathbf{unit} \rangle$ , is ill-typed, since the linear resource  $y$  is wasted, even though in the resource-aware semantics such configuration safely reduces to  $\mathbf{unit} \mid x : \langle \infty, \mathbf{unit} \rangle, y : \langle 1, \mathbf{unit} \rangle$ . In other words, the type system checks that available (non-discardable) resources are fully consumed, whereas in the instrumented semantics there is no such check. This mismatch between type system and semantics can be eliminated in two ways:

- as done by Bianchini et al. [9], with the more permissive typing rule for configurations shown below:

$$\text{(T-CONF)} \quad \frac{\Delta \vdash E : T \quad \Gamma \vdash \rho \triangleright \widehat{\Gamma}}{\Gamma \vdash E \mid \rho : T} \quad E ::= v \mid e \quad \Delta + \widehat{\Gamma} + \Theta \preceq \Gamma$$

The additional context  $\Theta$  allows the environment to contain resources which will be wasted; e.g., the configuration  $x \mid x : \langle \infty, \mathbf{unit} \rangle, y : \langle 1, \mathbf{unit} \rangle$  becomes well-typed with  $\Theta = y :_1 \mathbf{Unit}$ .

- Conversely, we can refine the instrumented semantics to check no-waste as well; e.g., the configuration  $x \mid x : \langle \infty, \mathbf{unit} \rangle, y : \langle 1, \mathbf{unit} \rangle$  is stuck. This is the approach we will develop in Section 7.

## 6 Programming examples and discussions

In this section, for readability, we use the surface syntax and, moreover, assume some standard additional constructs and syntactic conventions. Notably, we generalize (tensor) product types

```

Bool = true + false
Nat = zero + succ:Nat
NatList = empty + cons:(Nat ⊗ NatList)
OptNat = none + some:Nat

not: Bool -> Bool
not = \b.match b with true -> false or false -> true

even: Nat ->∞ Bool
even = rec ev.\n.match n with zero -> true or succ m -> not (ev m)

_+_ : Nat ->∞ Nat -> Nat
_+_ = rec sum.\n.\m. match n with zero -> m or succ x -> succ (sum x m)

double: Nat2 -> Nat
double n = n + n

*_ : Nat ->∞ Nat∞ -> Nat
*_ = rec mult.\n.\m.match n with zero -> zero or succ x -> (mult x m) + m

length : NatList ->∞ Nat
length = rec len.
  \ls.match ls with empty -> zero
  or cons ls1 -> match ls1 with <_,tl> -> succ (len tl)

get : NatList ->∞ Nat -> OptNat
get = rec g.
  \ls.\i.match ls with empty -> none
  or cons ls1 ->
    match ls1 with <hd,tl> -> match i with zero -> some hd
    or succ j -> g j tl

```

Fig. 10. Examples of type and function definitions

to tuple types, with the obvious extended syntax, and sum types to variant types, written  $\ell_1:T_1 + \dots + \ell_n:T_n$  for some *tags*  $\ell_1, \dots, \ell_n$ . Injections are generalized to tagged variants  $\ell^r e$ , and the corresponding match constructs are of shape  $\text{match } e \text{ with } \ell_1 x_1 \text{ or } \dots \text{ or } \ell_n x_n$ . We write just  $\ell$  as an abbreviation for an addend  $\ell:\text{Unit}^0$  in a variant type, and also for the corresponding tagged variants  $\ell^0 \text{unit}$  and patterns  $\ell x$  in a matching construct. Moreover, we will use type and function definitions (that is, synonyms for function and type expressions), and, as customary, represent (equi-)recursive types by equations. Finally, we will omit **1** annotations as in the previous examples, and we will consider **0** as default, hence omitted, as recursion grade (that is, functions are by default non-recursive).

**Natural numbers and lists.** The encoding of Booleans, natural numbers, lists of natural numbers, and optional natural numbers, is given at the top of Fig. 10 followed by the definition of some standard functions. Assume, firstly, the grade algebra of natural numbers with bounded usage, Example 3.3(1), extended with  $\infty$ , as in Example 3.3(7), needed as annotation

of recursive functions, as has been illustrated in Example 5.2; we discuss below what happens taking exact usage instead.

As a first comment, note that in types of recursive functions the recursion grade needs to be  $\infty$ , as expected. On the other hand, most function parameters are graded 1, since they are used at most once in each branch of the function’s body. The second parameter of the function `*`, instead, needs to be graded  $\infty$ . Indeed, it is used in the body of the function both as argument of `sum`, and *inside* the recursive call. Hence, its grade  $r$  should satisfy the equation  $(1 + r) \leq r$ , analogously to what happens for the recursive grade; compare with the parameter of function `double`, which is used twice as well, and can be graded 2. In the following alternative definitions:

```
double: Nat1 -> Nat
double n = n * succ succ zero
```

```
double: Nat∞ -> Nat
double n = succ succ zero * n
```

the parameter needs to be graded differently depending on whether it is used as either first or second argument of `*`. In other words, the resource-aware type system captures, as expected, non-extensional properties.

Assume now the grade algebra of natural numbers with exact usage, again extended with  $\infty$ . Interestingly enough, the functions `length` and `get` above are no longer typable.

In `length`, this is due to the fact that, when the list is non-empty, the head is unused, whereas it should be used exactly once as the tail, since the grade of a pair is “propagated” to both the components. The function would be typable assuming for lists the type  $\text{NatList} = \text{empty} + \text{cons} : (\text{Nat}^0 \otimes \text{NatList})$ , which, however, would mean to essentially handle a list as a natural number.

Function `get`, analogously, cannot be typed since, in the last line, only one component of a non-empty list (either the head or the tail) is used in a branch of the match, whereas both should be used exactly once. Both functions could be typed, instead, grading with  $\infty$  the list parameter; this would mean to allow an arbitrary usage in the body. These examples suggest that, in a grade algebra with exact usage, such as that of natural numbers, or the simpler linearity grade algebra, see Example 3.3(2), there is often no middle way between imposing severe limitations on code, to ensure linearity (or, in general, exactness), and allowing code which is essentially non-graded.

**Cartesian product.** The product type we consider in Fig. 6 is the *tensor* product, also called *multiplicative*, following Linear Logic terminology [26]. In the destructor construct for such a type, both components are simultaneously extracted, each one with a grade which is (a multiple of) that of the pair, see the semantic<sup>10</sup> rule (MATCH-P) in Fig. 4. Thus, as shown in the examples above, programs which discard the use of either component cannot be typed in a non-affine grade algebra. Correspondingly, the resource consumption for constructing a (multiplicative) pair is the *sum* of those for constructing the two components, corresponding to a sequential evaluation, see rule (PAIR) in Fig. 4. The *Cartesian* product, instead, formalized in Fig. 11, has one destructor for each component, so that which is not extracted is discarded. Correspondingly, the resource consumption for constructing a pair

<sup>10</sup>Typing rules follow the same pattern.

$$\begin{aligned}
v & ::= \dots \mid [^{r_1} v_1, v_2^{r_2}] \mid \pi_1 v \mid \pi_2 v \\
\tau, \sigma & ::= \dots \mid T \times S
\end{aligned}$$

$$\begin{aligned}
(\text{APAIR}) \quad & \frac{v_1 \mid \rho \Rightarrow_{r \cdot r_1} \mathbf{v}_1 \mid \rho' \quad v_2 \mid \rho \Rightarrow_{r \cdot r_2} \mathbf{v}_2 \mid \rho'}{[^{r_1} v_1, v_2^{r_2}] \mid \rho \Rightarrow_r [^{r_1} \mathbf{v}_1, \mathbf{v}_2^{r_2}] \mid \rho'} \quad (\text{PROJ}) \quad \frac{v \mid \rho \Rightarrow_s [^{r_1} \mathbf{v}_1, \mathbf{v}_2^{r_2}] \mid \rho' \quad i \in \{1, 2\}}{\pi_i v \mid \rho \Rightarrow_r \mathbf{v}_i \mid \rho'} \quad r \preceq s \cdot r_i \\
(\text{T-APAIR}) \quad & \frac{\Gamma \vdash v_1 : \tau_1^{r_1} \quad \Gamma \vdash v_2 : \tau_2^{r_2}}{r \cdot \Gamma \vdash [^{r_1} v_1, v_2^{r_2}] : (\tau_1^{r_1} \times \tau_2^{r_2})^r} \quad (\text{T-PROJ}) \quad \frac{\Gamma \vdash v : (\tau_1^{r_1} \times \tau_2^{r_2})^r}{\Gamma \vdash \pi_i v : \tau_i^{r \cdot r_i}} \quad r \neq \mathbf{0}
\end{aligned}$$

Fig. 11. Cartesian product

$$\begin{array}{c}
\frac{}{\text{ev} \mid \langle 1, 1, z \rangle \Rightarrow_1 \text{even} \mid \langle 0, 1, z \rangle} \quad \frac{}{\mathbf{n} \mid \langle 0, 1, z \rangle \Rightarrow z \mid \langle 0, 0, z \rangle} \quad \frac{\mathbf{t} \mid \langle 0, 0, z \rangle \Rightarrow \mathbf{t} \mid \langle 0, 0, z \rangle}{\text{if-}z(z, \mathbf{t}, \text{sn} \rightarrow \text{not}(\text{ev} \mathbf{n})) \mid \langle 0, 0, z \rangle \Rightarrow \mathbf{t} \mid \langle 0, 0, z \rangle} \\
\hline
\text{ev} \mathbf{n} \mid \langle 1, 1, z \rangle \Rightarrow \mathbf{t} \mid \langle 0, 0, z \rangle \\
\hline
\frac{}{\text{ev} \mid \langle n, 1, s^n z \rangle \Rightarrow_n \text{even} \mid \langle n-1, 1, z \rangle} \quad \frac{}{\mathbf{n} \mid \langle n-1, 1, z \rangle \Rightarrow z \mid \langle n-1, 0, z \rangle} \quad \frac{\text{not}(\text{ev} \mathbf{n}) \mid \langle n-1, 1, z \rangle \Rightarrow \bar{b} \mid \langle 0, 0, z \rangle}{\text{if-}z(z, \mathbf{t}, \text{sn} \rightarrow \text{not}(\text{ev} \mathbf{n})) \mid \langle n-1, 1, z \rangle \Rightarrow b \mid \langle 0, 0, z \rangle} \\
\hline
\text{ev} \mathbf{n} \mid \langle n, 1, s^n z \rangle \Rightarrow b \mid \langle 0, 0, z \rangle
\end{array}$$

Fig. 12. Example of resource-aware evaluation: terminating recursion. (Labels of rules are omitted.)

is an *upper bound* of those for constructing the two components, corresponding in a sense to a non-deterministic evaluation. The get example, rewritten using the constructs of the Cartesian product, becomes typable even in a non-affine grade algebra. In an affine grade algebra, programs can always be rewritten replacing the cartesian product with the tensor, and conversely; in particular,  $\pi_i v$  can be encoded as `match v with  $\langle x_1, x_2 \rangle \rightarrow x_i$` , even though, as said above, resources are consumed differently (sum versus upper bound). An interesting remark is that record/object calculi, where generally width subtyping is allowed, meaning that components can be discarded at runtime, and object construction happens by sequential evaluation of the fields, need to be modeled by multiplicative product and affine grades. In future work we plan to investigate object calculi which are *linear*, or, more generally, use resources in an exact way.

**Terminating recursion.** As anticipated, even though the type system can only derive, for recursive functions, recursion grades which are “infinite”, their calls which terminate in standard semantics can terminate also in resource-aware semantics, provided that the initial amount of the function resource is enough to cover the (finite number of) recursive calls, as shown in Fig. 12.

For brevity, we write  $z$ ,  $s$ , and  $\mathbf{t}$  for zero, succ, and true, respectively, `if- $z(v, e_1, s x \rightarrow e_2)$`  for `match v with  $z \rightarrow e_1$  or  $s x \rightarrow e_2$` , and  $\langle r, s, v \rangle$  for the environment  $\text{ev} : \langle r, \text{even} \rangle, \mathbf{n} : \langle s, \mathbf{v} \rangle$ . In the top part of the figure we show the proof tree for the evaluation of `ev n` in the base case, that is, in an environment where the value of  $\mathbf{n}$  is zero. In this case, both `ev` and  $\mathbf{n}$  can be graded 1, since they are used only once. In the bottom part, we show the proof tree in an environment where the value of  $\mathbf{n}$  is  $s^n z$ , for  $n \neq 0$ . Here,  $b$  stands for either true or false, and  $\bar{b}$  for its complement.

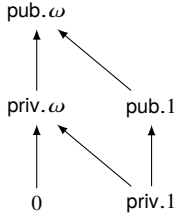


Fig. 13. Grade algebra of access levels and linearity

```

Result = success + failure
OptChar = none + some:Charpriv.ω
fnType = Charpriv.ω → (ok:Charpriv.ω + error)

open:Stringpub.ω → FileHandle
read:FileHandle → (OptCharpriv.ω ⊗ FileHandle)
write:(Charpriv.ω ⊗ FileHandle) → FileHandle
close:FileHandle → Unit0

```

Fig. 14. Types of data and filesystem interface

```

1 fileRW:FileHandle →pub.ω FileHandle → fnTypepub.ω → Resultpub.ω =
2 rec fileRdWr.
3   \inF.\outF.\fn.
4     match (read inF) with <oC,inF1> ->
5       match oC with none ->
6         close inF1;close outF;success
7       or (some c) ->
8         match (fn c) with (ok c1) ->
9           let outF1 = write <c1,outF> in
10            fileRdWr inF1 outF1 fn
11       or error ->
12         close inF1;close outF;failure

```

Fig. 15. Processing data from/to files

**Processing data from/to files.** The following example illustrates how we can simultaneously track access levels, as introduced in Example 2.2, and linearity information. Linearity grades guarantee the correct use of files, whereas access levels are used to ensure that data are handled without leaking information. We combine the two grade algebras with the smash product of Example 3.7. So there are five grades: 0 (meaning unused), priv.1 and pub.1 (meaning used linearly in either priv or pub mode), and priv.ω, pub.ω (meaning used an arbitrary number of times in either priv or pub mode). The partial order is graphically shown in Fig. 13. The neutral element for multiplication is pub.1, which therefore will be omitted.

In Fig. 14 are the types of the data, the processing function and the functions of a filesystem interface, assuming types Char, String, and FileHandle to be given. The type Result indicates success or failure. The type OptChar represents the presence or absence of a Char and is used in the function reading from a file; fnType is the type of a function processing a private Char and returning either a private Char or error. The signatures of the functions of the filesystem interface specify that file handlers are used in a linear way. Hence, after opening a file and doing a number of read or write operations, the file must be closed.

In the code of Fig. 15 we use, rather than  $\text{match } e_1 \text{ with unit} \rightarrow e_2$ , the alternative syntax  $e_1; e_2$  mentioned in Section 4. The function fileRW takes as parameters an input and an output file handler and a function that processes the character read from the input file. The

result indicates whether all the characters of the input file have been successfully processed and written in the output file or there was an error in processing some character.

The function starts by reading a character from the input file. If `read` returns `none`, then all the characters from the input file have been read and so both files are closed and the function returns `success` (lines 5—6). Closing the files is necessary in order to typecheck this branch of the match. If `read` returns a character (lines 7—12), then the processing function `fn` is applied to that character. Then, if `fn` returns a character, then this result is written to the output file using the file handler passed as a parameter and, finally, the function is recursively called with the file handlers returned by the `read` and `write` functions as arguments. If, instead, `fn` returns `error`, then both files are closed and the function returns `failure` (lines 11—12).

Observe that, given the order of Fig. 13, we have  $0 \not\leq \text{pub}.1$ . Therefore the variables of type `FileHandle`, which have grade `pub.1`, must be used exactly once in every branch of the matches in their scope.

A call to `fileRW` could be: `fileRW (open "inFile") (open "outFile") (rec f.\x.x)`. Note that, with

$$\text{write} : (\text{Char}^{\text{pub}.\omega} \otimes \text{FileHandle}) \rightarrow \text{FileHandle}$$

the function `fileRW` would not be well-typed, since a `priv` character cannot be the input of `write`. On the other hand, using subsumption, we can apply `fileRW` to a processing function with type

$$\text{Char}^{\text{priv}.\omega} \rightarrow (\text{ok} : \text{Char}^{\text{pub}.\omega} + \text{error})$$

Finally, in the type of `fileRW`, the grade of the first arrow says that the function is recursive and it is internally used in an unrestricted way. The function could also be typed with:

$$\text{FileHandle} \rightarrow_{\text{priv}.\omega} \text{FileHandle} \rightarrow \text{fnType}^{\text{pub}.\omega} \rightarrow \text{Result}^{\text{priv}.\omega}$$

However, in this case its final result would be private and therefore less usable.

## 7 No-waste semantics

This section is structured as follows. We first informally describe no-waste usage in Section 7.1. In Section 7.2 we give some preliminary definitions and results related to *grade graphs*, needed in the following sections. In Section 7.3 we define the no-waste refinement of the resource-aware semantics, and examples of reduction are shown in Section 7.4. Finally, in Section 7.5 we prove the related results. Notably, the refined semantics actually ensures no-waste (Theorem 7.20), garbage in the environment is discardable (Proposition 7.23), and well-typed configurations are no-waste (Theorem 7.27).

### 7.1 No-waste usage

In the resource-aware semantics in Fig. 4, a program cannot consume more resources than those available. That is, reduction is stuck if the current availability of a resource is not enough to cover the required usage by the program, and this situation is expected to be prevented by the type system.

However, the converse property does not hold, that is, resources can be *wasted*, even though, see Remark 5.5 at the end of Section 5, the type system prevents this situation as well. For instance, assuming linearity grades, the configuration  $x \mid x : \langle 1, \text{unit} \rangle, y : \langle 1, \text{unit} \rangle$ , where both  $x$  and  $y$  are provided as linear, reduces (with grade 1) to  $\text{unit} \mid y : \langle 1, \text{unit} \rangle$ , by

|               |                                                                                                 |                                |
|---------------|-------------------------------------------------------------------------------------------------|--------------------------------|
| $\rho$        | $::= x_1 : \langle r_1, \mathcal{V}_1 \rangle, \dots, x_n : \langle r_n, \mathcal{V}_n \rangle$ | environment                    |
| $\mathcal{V}$ | $::= \mathbf{v}^\gamma$                                                                         | (annotated) value              |
| $\gamma$      | $::= x_1 : r_1, \dots, x_n : r_n$                                                               | grade context                  |
| $E$           | $::= v \mid e$                                                                                  | value expression or expression |

Fig. 16. Environments and (annotated) values

wasting the resource  $y$ . In this section, we provide a refinement of resource-aware semantics where *resources cannot be wasted*, hence the configuration above is stuck. In this way, resource-aware soundness including no-waste can be stated and proved.

To formally express that “resources cannot be wasted”, we will rely on the *no-waste relation*  $\gamma \preceq_{\text{nw}}^* \rho$ , meaning that the resources provided by  $\rho$  are (transitively) used with no-waste by  $\gamma$ . The formal definition of the no-waste relation will be provided in Definition 7.18 (Section 7.3); the following examples illustrate its expected behaviour.

**Example 7.1.** In the simple case when values in the environment are closed, as in the example above, there is no need of transitivity; for instance,  $x : 1, y : 1 \preceq_{\text{nw}}^* x : \langle 1, \text{unit} \rangle, y : \langle 1, \text{unit} \rangle$  holds, whereas  $x : 1, y : 0 \preceq_{\text{nw}}^* x : \langle 1, \text{unit} \rangle, y : \langle 1, \text{unit} \rangle$  does not hold, since for linearity grades  $0 \not\leq 1$ .

On the other hand, when values have free variables, dependencies in the environment should be taken into account. To this end, as shown in Fig. 16, the no-waste semantics is instrumented by *annotating* values with a grade context “declaring” the *direct usage* of resources in the value, so that transitive usage can be computed.

**Example 7.2.** For instance,  $x : 1 \preceq_{\text{nw}}^* x : \langle 1, (\lambda_. \langle y, z \rangle)^{y:1, z:1}, y : \langle 1, \text{unit}^\emptyset \rangle, z : \langle 1, \text{unit}^\emptyset \rangle \rangle$  holds, since  $x : 1$  directly uses  $x$ , and transitively  $y$  and  $z$ , exactly once. Note that the relation of no-waste usage, being based on the partial order, still allows approximation which is no-waste, see Remark 5.1. Hence, for instance,  $x : 1 \preceq_{\text{nw}}^* x : \langle 1, \text{unit}^\emptyset \rangle, y : \langle \infty, \text{unit}^\emptyset \rangle$  holds, since the resource  $y$ , which is not used by the grade context, is discardable.

Set  $\text{fv}(\mathbf{v})$  to be the free variables of  $\mathbf{v}$ , defined in the standard way. We assume environments to be *closed*, that is, for each  $x : \langle r, \mathbf{v}^\gamma \rangle \in \rho$ ,  $\text{fv}(\mathbf{v}) \subseteq \text{dom}(\rho)$ .

The grade context annotating a value is meant to be a “guess” about the resource consumption which would be actually triggered when the value is used. Reduction will be non-stuck when the guess is correct (and no standard typing errors occur); as expected, the type system will check such correctness. We only assume that, in an annotated value  $\mathbf{v}^\gamma$ ,  $\gamma$  is *honest* for  $\mathbf{v}$ , that is, it does not declare a resource consumption which could not possibly be triggered, as formally defined below:

**Definition 7.3 (Honest).** A grade context  $\gamma$  is honest for  $E$  if  $\mathbf{0} \not\leq \gamma(x)$  implies  $x \in \text{fv}(E)$ .

For instance,  $(\lambda_. y)^{y:1, z:1}$  is an ill-formed value, since  $z$  is not a free variable of the term, whereas the grade context says that it is used exactly once. The honesty condition is intuitively reasonable, and allows us to prove the important property that garbage, that is, resources which are not reachable from the program, can be discarded (Proposition 7.23).

The no-waste relation  $\gamma \preceq_{\text{nw}}^* \rho$  informally introduced by the above examples will be formalized in Section 7.3. However, such formalization requires some technical definitions and results which will be provided in Section 7.2. Notably, to express the property, the first step

is the notion of the *grade graph*  $G_\rho$  extracted from an environment  $\rho$ . Intuitively,  $G_\rho$  expresses the (direct) dependencies among variables in  $\rho$ , that is, for each pair  $x$  and  $y$ , how  $y$  is used in (the grade context annotating) the value associated to  $x$ . For instance, considering the first environment of Example 7.2, that is,  $\rho = x : \langle 1, (\lambda \_ . \langle y, z \rangle)^{y:1, z:1}, y : \langle 1, \text{unit}^0 \rangle, z : \langle 1, \text{unit}^0 \rangle \rangle$ , we expect to have  $G_\rho(x, y) = G_\rho(x, z) = 1$ , and  $G_\rho$  to give 0 on all the other pairs.

## 7.2 Grade graphs: an algebraic digression

As anticipated, the aim of this section is to provide the technical definitions and results needed in the following sections. In detail:

- (1) Definition of *grade graphs* (Definition 7.4).
- (2) Grade graphs are a special case of *grade matrices* (Definition 7.11). The *reflexive and transitive closure*  $G^\star$  of an (acyclic) grade graph  $G$  (Definition 7.9) is a grade matrix.
- (3) *Fixed-point characterization* of the closure:  $G^\star = \mathbb{I} + G^\star \cdot G$  (Corollary 7.15).
- (4) *Induction principle*: for each  $\gamma$ ,  $\gamma \cdot G^\star$  is the least fixed point of the transformation  $\phi_\gamma(\gamma') = \gamma + \gamma' \cdot G$  (Proposition 7.16).

The key points where these notions will be used are the following:

- The no-waste relation is defined in terms of  $G^\star$  (Definition 7.18).
- Resource balance (Theorem 7.21) relies on the fixed point characterization, and the result that well-typed configurations and results are no-waste (Theorem 7.27) relies on the induction principle.

### 7.2.1 Grade graphs

Recall that we denote by  $V$  the set of variables and that, for a function  $f : X \rightarrow |R|$ , the support of  $f$  is the set  $S_f = \{x \in X \mid f(x) \neq \mathbf{0}\}$ .

**Definition 7.4** (Grade graph). A *grade graph* is a function  $G : V \times V \rightarrow |R|$  with finite support.

The finite support condition ensures that  $G(x, y) \neq \mathbf{0}$  for finitely many pairs  $\langle x, y \rangle \in V \times V$ . As the name suggests, these functions can be represented by finite graphs where nodes are variables and edges are labeled by grades, analogously to functions from variables into grades with finite support which are represented by grade contexts. More precisely, given a grade graph  $G$ , we have an edge from  $x$  to  $y$  with label  $r$  exactly when  $G(x, y) = r$ . Intuitively, such an edge means that  $x$  depends on “ $r$  copies” of  $y$ ; for  $r = \mathbf{0}$ ,  $x$  does *not* depend on  $y$ , and the edge can be omitted. Finally, again following graph terminology, we will call *source* in  $G$  a node (variable)  $y$  such that  $G(x, y) = \mathbf{0}$  for all  $x$ . We will write  $V(G)$  for the set of *non-source* nodes, i.e., those with at least one incoming edge:

$$V(G) = \{y \in V \mid G(x, y) \neq \mathbf{0} \text{ for some } x \in V\}$$

Since  $G$  has finite support, the set  $V(G)$  is clearly finite, as its cardinality is bounded by that of  $S_G$ .

**Example 7.5.** Consider the grade graph  $G$  with support  $\{x, y, z\}$  defined by:

$$\begin{array}{cccccc} G(x, y) = 2 & G(x, z) = 1 & G(y, x) = 0 & G(y, z) = 1 & G(z, x) = G(z, y) = \\ 0 \end{array}$$

We have  $V(G) = \{y, z\}$ . This grade graph could correspond, for instance, to the environment:

$$x : \langle \_, (\lambda \_. \langle y, z \rangle)^{y:2, z:1} \rangle, y : \langle \_, (\lambda \_. z)^{z:1} \rangle, z : \langle \_, \mathbf{unit}^0 \rangle$$

where we left the grades unspecified as they are not relevant.

In order to model transitive dependencies, we have to consider paths in a grade graph. The next definition introduces path-related notions, adapting them from the standard graph-theoretic ones.

**Definition 7.6** (Paths, cycles and acyclic grade graphs). A *path* is a sequence  $p = x_1 \dots x_n$ , with  $n \geq 1$ ;  $x_1, x_n$  are denoted  $\text{in}(p)$  and  $\text{out}(p)$ , respectively. We set  $|p| = n - 1$  the *length* of the path  $p$ .<sup>11</sup> A path  $x_1 \dots x_n$  is a *cycle* if  $n > 1$  and  $x_1 = x_n$ . A grade graph  $G$  induces a function  $G : V^+ \rightarrow R$  inductively defined as follows:

$$\begin{aligned} G(x) &= \mathbf{1} \\ G(x \cdot p) &= G(x, \text{in}(p)) \cdot G(p) \end{aligned}$$

Then,  $G$  is *acyclic* if, for all cycles  $p$ ,  $G(p) = \mathbf{0}$ .

**Example 7.7.** For the grade graph of Example 7.5 the paths having non zero grade are:

$$\begin{aligned} G(x) = G(y) = G(z) &= \mathbf{1} & G(xy) &= \mathbf{2} & G(xz) &= \mathbf{1} & G(xyz) &= \mathbf{2} & G(yz) &= \\ & \mathbf{1} \end{aligned}$$

As expected,  $G$  is acyclic.

We will write  $P(x, y)$  for the set of paths  $p$  such that  $\text{in}(p) = x$  and  $\text{out}(p) = y$ . The following are immediate consequences of the above definitions.

**Proposition 7.8.** Let  $G$  be a grade graph,  $x, y \in V$ . Set  $P_{\neq \mathbf{0}}^G(x, y) = \{p \in P(x, y) \mid G(p) \neq \mathbf{0}\}$ .

- (1) If  $p = x_1 \dots x_{n+1} \in P(x, y)$  with  $n \geq 1$  and there is  $j \in 2..n+1$  such that  $x_j \notin V(G)$ , then  $G(p) = \mathbf{0}$ .
- (2) If  $x \neq y$  and  $y \notin V(G)$ , then  $P_{\neq \mathbf{0}}^G(x, y) = \emptyset$ .
- (3) If  $G$  is acyclic and  $n$  is the cardinality of  $V(G)$ , then  $|p| \geq n + 1$  implies  $G(p) = \mathbf{0}$ .
- (4) If  $G$  is acyclic, then the set  $P_{\neq \mathbf{0}}^G(x, y)$  is finite.

### 7.2.2 Reflexive and transitive closure

For acyclic grade graphs we can define the reflexive and transitive closure, as detailed below.

**Definition 7.9** (Reflexive and transitive closure of a grade graph). Let  $G$  be an acyclic grade graph. Its *reflexive and transitive closure*, denoted  $G^*$ , is defined as follows:

$$\text{for all } x, y \in V, G^*(x, y) = \sum_{p \in P(x, y)} G(p)$$

The definition of  $G^*(x, y)$ , for each pair of nodes  $x, y$ , requires a summation over an infinite set. However, Proposition 7.8(4) ensures that only finitely many addends are different from  $\mathbf{0}$ , hence the summation is well-defined.

**Example 7.10.** Given  $G$  of Example 7.5 and Example 7.7,  $G^*$  is:

<sup>11</sup>Note that the length counts the number of edges which is the number of nodes minus 1.

$$\begin{aligned}
G^*(x, x) &= G^*(y, y) = G^*(z, z) = 1 \\
G^*(x, y) &= G(xy) + G(xzy) = 2 + 0 = 2 \\
G^*(x, z) &= G(xz) + G(xyz) = 1 + 2 = 3 \\
G^*(y, x) &= G(yx) + G(yzx) = 0 + 0 = 0 \\
G^*(y, z) &= G(yz) + G(yxz) = 1 + 0 = 1 \\
G^*(z, x) &= G(zx) + G(zyx) = 0 + 0 = 0 \\
G^*(z, y) &= G(zy) + G(zxy) = 0 + 0 = 0
\end{aligned}$$

Since  $G$  is acyclic, by Proposition 7.8(3) we can consider only paths of length strictly less than 4.

Note that the reflexive and transitive closure of a grade graph  $G$  is *neither acyclic, nor a grade graph*. Indeed, we have  $G^*(x, x) = 1$  for all  $x \in V$ , hence cycles of the form  $x \cdot x$  have a non-zero grade and  $S_{G^*}$  is infinite.

However,  $G^*$  is an instance of a more general notion, which we call *grade matrix*. Whereas for grade graphs we require a function  $M : V \times V \rightarrow |R|$  to have finite support (in the graph view, finitely many non-isolated nodes), for grade matrices we require a weaker constraint, namely, that every row has finite support (every node has finitely many non-zero outgoing edges), as formalized below.

Let  $M : V \times V \rightarrow |R|$  be a function. For every variable  $x \in V$ , we define the function  $M_x : V \rightarrow |R|$  as follows:  $M_x(y) = M(x, y)$ .

**Definition 7.11** (Grade matrix). A *grade matrix* is a function  $M : V \times V \rightarrow |R|$  such that, for every variable  $x \in V$ ,  $M_x$  has a finite support, i.e., it is a grade context.

The grade context  $G_x$  is the row expressing the direct dependencies of  $x$ . Note that grade contexts turn out to be grade matrices with only one row, and grade graphs are grade matrices with a finite number of non-zero entries. As expected,  $G^*$  is a grade matrix. Indeed, thanks to Proposition 7.8(2), for all variables  $x \in V$ , we have  $S_{G_x^*} \subseteq V(G) \cup \{x\}$ , which thus is finite.

Grade matrices support the standard operations of *addition* and (*row-by-column*) *multiplication*, as formally detailed below.

Addition is the pointwise extension of the addition on grades. It is immediate to see that the result is still a grade matrix, and that on grade contexts we get the addition as previously defined.

Row-by-column multiplication is a summation of multiplications. For finite matrices, this summation has a finite number of addends. We show that this still holds for matrices where each row has a finite number of non-zero entries, leading, in turn, to a grade matrix. To this end, consider first the multiplication of a grade matrix  $M$  by a single row, i.e., a grade context  $\gamma$ , on the left, giving the grade context  $\gamma \cdot M$  defined by<sup>12</sup>:

$$\text{for all } x \in V, (\gamma \cdot M)(x) = \sum_{y \in V} \gamma(y) \cdot M(y, x)$$

The infinite summation above has only finitely many non-zero addends, as  $\gamma$  has a finite support, hence it is well-defined. Moreover, it is easy to see that  $\gamma \cdot M = \sum_{x \in S_\gamma} \gamma(x) \cdot M_x$ , hence it is a well-defined grade context.

Now, given the grade matrices  $M_1, M_2$ , we set

$$\text{for all } x, y \in V, (M_1 \cdot M_2)(x, y) = (M_{1x} \cdot M_2)(y) = \sum_{z \in V} M_1(x, z) \cdot M_2(z, y)$$

<sup>12</sup>Vector-matrix multiplication is also used by Vollmer et al. [36].

This is obviously well-defined because we have  $(M_1 \cdot M_2)_x = M_{1x} \cdot M_2$  which has a finite support, being a grade context. It is easy to see that this operation is associative and monotone and has as neutral element the identity grade matrix  $\mathbb{I}$  defined by

$$\mathbb{I}(x, y) = \begin{cases} \mathbf{1} & \text{if } x = y \\ \mathbf{0} & \text{otherwise} \end{cases}$$

Altogether, taking as ordering the pointwise extension of the ordering on grades, grade matrices with addition carry an ordered commutative monoid structure, and with multiplication another ordered monoid structure.

### 7.2.3 Fixed point characterization and induction principle

The main theorems on grade graphs (the fixed point characterization of the closure and the induction principle) rely on the fact that the closure can be expressed by a finite summation (Lemma 7.14). To prove this we need some preliminary results.

The following lemma states that, being the graph acyclic, multiplying a row with the matrix expressing transitive dependencies we get zero on the component corresponding to the variable  $x$  itself. Equivalently, the matrix obtained by multiplying the graph  $G$  with the matrix of transitive dependencies has  $\mathbf{0}$  on the diagonal.

**Lemma 7.12.** *If  $G$  is acyclic, then  $(G \cdot G^*)(x, x) = (G_x \cdot G^*)(x) = \mathbf{0}$ .*

Intuitively, this happens because the grade matrix  $G \cdot G^*$  considers transitive dependencies through non-empty paths and, since the graph is acyclic, there are no non-empty paths from a variable to itself.

Given a grade graph  $G$ , in the following we will write  $G^n$  to denote the multiplication of  $G$  with itself  $n$  times. Moreover, we will denote by  $P_n(x, y)$  the subset of  $P(x, y)$  of those paths of length  $n$ .

**Proposition 7.13.** *Let  $G$  be a grade graph. For all  $n \in \mathbb{N}$  and  $x, y \in V$ , we have  $G^n(x, y) = \sum_{p \in P_n(x, y)} G(p)$ .*

Combining Proposition 7.13 and Proposition 7.8(3), it is immediate to see that, if  $n$  is the cardinality of  $V(G)$ , then  $G^k$  is the zero grade matrix, for all  $k \geq n + 1$ . As a consequence we get the following result.

**Lemma 7.14.** *Let  $G$  be an acyclic grade graph and let  $n$  be the cardinality of  $V(G)$ . Then the following holds:*

$$G^* = \sum_{i=0}^n G^i$$

PROOF. Using Proposition 7.13, we get the following

$$G^*(x, y) = \sum_{p \in P(x, y)} G(p) = \sum_{k \in \mathbb{N}} \sum_{p \in P_k(x, y)} G(p) = \sum_{k \in \mathbb{N}} G^k(x, y)$$

As already noticed, by Proposition 7.8(3), we have that  $G^k(x, y) = \mathbf{0}$  for all  $k \geq n + 1$ , hence we have the thesis.  $\square$

Considering the grade graph  $G$  of Example 7.5,  $G^0 = \mathbb{I}$ ,  $G^1 = G$  and in  $G^2 = G \cdot G$  the only non zero grade is  $G^2(x, z) = 2$ . Indeed, as seen in Example 7.7, the only path of length 2 with

non zero grade is  $xyz$  and  $G(xyz) = 2$ . Finally,  $G^\star = G^0 + G^1 + G^2$  coincides with  $G^\star$  as described in Example 7.10.

We can now prove the main results of this section. The first one states that the reflexive and transitive closure behaves similarly to the Kleene closure, by satisfying an analogous equation.

**Corollary 7.15.** *Let  $G$  be an acyclic grade graph. Then,  $G^\star = \mathbb{I} + G^\star \cdot G = \mathbb{I} + G \cdot G^\star$ .*

PROOF. Let  $n$  be the cardinality of  $V(G)$ . The thesis is immediate by Lemma 7.14:

$$\mathbb{I} + G^\star \cdot G = G^0 + \sum_{k \in 0..n} G^{k+1} = \sum_{k \in 0..n} G^k + G^{n+1} = G^\star$$

because  $G^{n+1}$  is the zero grade matrix.  $\square$

The second main result is the following induction principle, allowing to show that an upper bound holds for  $\gamma \cdot G^\star$  by proving that it holds for  $\gamma + (\gamma' \cdot G)$ .

**Proposition 7.16.** *Given an acyclic graph  $G$ , and two grade contexts  $\gamma, \gamma'$ :*

$$\gamma + (\gamma' \cdot G) \preceq \gamma' \text{ implies } \gamma \cdot G^\star \preceq \gamma'.$$

PROOF. By a straightforward induction on  $k \in \mathbb{N}$ , we can prove that  $\gamma_1 \cdot (\sum_{i \in 0..k} G^i) + \gamma_2 \cdot G^{k+1} \preceq \gamma_2$ , for all  $k \in \mathbb{N}$ . Taking  $n$  to be the cardinality of  $V(G)$ , by Lemma 7.14, we get the thesis because  $G^\star = \sum_{i \in 0..n} G^i$  and  $G^{n+1}$  is the zero matrix.  $\square$

Note that the above property means that, for every grade context  $\gamma$ , the monotone function on grade contexts  $\phi_\gamma(\gamma') = \gamma + \gamma' \cdot G$  has a least pre-fixed point given by  $\gamma \cdot G^\star$ . Actually, this is also a fixed point thanks to Corollary 7.15.

### 7.3 No-waste semantics

In this section we provide the no-waste refinement of the resource-aware semantics. First of all, we define the grade context and grade graph extracted from an environment. Recall from Fig. 16 that in the no-waste setting values in the environment are annotated with a grade context.

**Definition 7.17.** Given an environment  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$

- the grade context  $\gamma_\rho$  is  $x_1 : r_1, \dots, x_n : r_n$
- the grade graph  $G_\rho$  has support  $\{x_1, \dots, x_n\}$  and is defined by  $(G_\rho)_{x_i} = \gamma_i$ , for  $i \in 1..n$ .

Intuitively, the grade context  $\gamma_\rho$  expresses the availability of each resource (variable) in the environment, whereas the grade graph  $G_\rho$  collects the direct dependencies among such variables.

In the following, we will assume acyclic environments, in the sense that there is no dependency path from a variable to itself. Formally, this means that we assume that the grade graph  $G_\rho$  is acyclic (see Definition 7.6). It is important to note this *does not* prevent provided resources to be recursive; indeed, this is handled in the semantics by adding a resource, under a fresh name, for each recursive call, as seen in rule (APP) in Fig. 4 and the example in Fig. 12. We discuss at the end of the section whether allowing cyclic environments rather than modeling recursion, essentially, by unfolding, makes some relevant difference, and how to adjust the technical treatment.

As the reader can expect, the reflexive and transitive closure  $G_\rho^\star$  of the grade graph extracted from an environment  $\rho$  expresses the (*full*) *dependencies* among resources in  $\text{dom}(\rho)$ . Indeed, for each  $x, y \in \text{dom}(\rho)$ , a dependency path from  $x$  to  $y$  expresses *one* transitive (graded) usage of  $y$  from (the value associated to)  $x$ ; thus, the sum of the weights of such paths represents the whole usage of  $y$  from  $x$ .

We can finally define the relation between grade contexts and environments modeling no-waste usage.

**Definition 7.18** (No-waste usage). The grade context  $\gamma$  (*transitively*) *uses*  $\rho$  *with no waste*, written  $\gamma \preceq_{\text{nw}}^\star \rho$ , if  $\gamma \cdot G_\rho^\star \preceq \gamma_\rho$ .

The relation  $\gamma \preceq_{\text{nw}}^\star \rho$  says that the resources provided by  $\rho$  are (transitively) used with no-waste by  $\gamma$ . Indeed, for each resource  $x$ ,  $(\gamma \cdot G_\rho^\star)(x)$  gives the (transitive) usage of  $x$  from  $\gamma$ , obtained as the sum of the usages of  $x$  from any variable  $y$ , each one multiplied by the direct usage of  $x$  in  $\gamma$ . On the other hand,  $\gamma_\rho(x)$  gives the availability of  $x$  in  $\rho$ . As previously illustrated in Examples 7.1 and 7.2, the relation of no-waste usage only allows the approximation given by the partial order; in cases where the partial order is the equality, as in the grade algebra of exact counting defined in Example 3.3(1), usage and availability are required to coincide.

For example, consider the environment

$$\rho = x : \langle 1, (\lambda_{-}.\langle y, z \rangle)^{y:2, z:1} \rangle, y : \langle 4, (\lambda_{-}.z)^{z:1} \rangle, z : \langle 5, \text{unit}^\emptyset \rangle$$

whose grade graph  $G_\rho$  is defined in Example 7.5 with reflexive and transitive closure  $G_\rho^\star$  presented in Example 7.10. The grade context  $\gamma = x : 1, y : 2$  uses  $\rho$  with no waste, since  $\gamma \cdot G_\rho^\star = \gamma_\rho$ . Indeed

- $x$  is used once only in  $\gamma$
- $y$  is used twice in  $\gamma$  and twice through  $x$
- $z$  is not used in  $\gamma$  but it is used through  $x$  three times, one directly and two by the use of  $y$ , and twice by  $y$  since each use of  $y$  in  $\gamma$  uses  $z$  once.

We can now formally define the no-waste semantics. The reduction judgement for expressions has shape  $e \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'$ , and is defined in Fig. 17 on top of an analogous one for value expressions. As noted for the previous semantics in Fig. 4, for simplicity we use the same notation for the two judgments, and in the bottom section of Fig. 17 we write both judgments as premises.

In the reduction rules,  $\rho_1 + \rho_2$  denotes the *sum* of environments, defined as follows, analogously to the sum of contexts in Section 5:

$$\begin{aligned} \emptyset + \rho &= \rho \\ (x : \langle s, \mathcal{V} \rangle, \rho_1) + (x : \langle r, \mathcal{V} \rangle, \rho_2) &= x : \langle s + r, \mathcal{V} \rangle, (\rho_1 + \rho_2) \\ (x : \langle s, \mathcal{V} \rangle, \rho_1) + \rho_2 &= x : \langle s, \mathcal{V} \rangle, (\rho_1 + \rho_2) \quad \text{if } x \notin \text{dom}(\rho_2) \end{aligned}$$

We use an analogous notation for grade contexts. Note that, similarly to the sum of contexts, sum of environments is partial, since a variable in the domain of both is required to have the same associated value.

The distinguishing features with respect to the previous resource-aware semantics are the following:

$$\begin{array}{c}
\text{(VAR)} \frac{\mathcal{V} = \mathbf{v}^\gamma}{x \mid \rho, x : \langle s, \mathcal{V} \rangle \Rightarrow_r \mathcal{V} \mid \rho, x : \langle s', \mathcal{V} \rangle} \quad r + s' \preceq s \quad r \cdot \gamma \preceq_{\text{nw}}^* \rho, x : \langle s', \mathcal{V} \rangle \\
\\
\text{(FUN)} \frac{}{\text{recf}.\lambda x.e \mid \rho \Rightarrow_r (\text{recf}.\lambda x.e)^\gamma \mid \rho} \quad r \cdot \gamma \preceq_{\text{nw}}^* \rho \quad \text{(UNIT)} \frac{}{\text{unit} \mid \rho \Rightarrow_r \text{unit}^\gamma \mid \rho} \quad r \cdot \gamma \preceq_{\text{nw}}^* \rho \\
\\
\text{(PAIR)} \frac{v_1 \mid \rho_1 \Rightarrow_{r \cdot r_1} \mathbf{v}_1^{\gamma_1} \mid \rho'_1 \quad v_2 \mid \rho_2 \Rightarrow_{r \cdot r_2} \mathbf{v}_2^{\gamma_2} \mid \rho'_2 \quad \gamma = r_1 \cdot \gamma_1 + r_2 \cdot \gamma_2}{\langle r_1 v_1, v_2 r_2 \rangle \mid \rho \Rightarrow_r \langle r_1 \mathbf{v}_1, \mathbf{v}_2 r_2 \rangle^\gamma \mid \rho'_1 + \rho'_2} \quad \rho_1 + \rho_2 \preceq \rho \\
\\
\text{(INL)} \frac{v \mid \rho \Rightarrow_{r \cdot s} \mathbf{v}^\gamma \mid \rho'}{\text{inl}^r v \mid \rho \Rightarrow_r (\text{inl}^r \mathbf{v})^{s \cdot \gamma} \mid \rho'} \quad \text{(INR)} \frac{v \mid \rho \Rightarrow_{r \cdot s} \mathbf{v}^\gamma \mid \rho'}{\text{inr}^r v \mid \rho \Rightarrow_r (\text{inr}^r \mathbf{v})^{s \cdot \gamma} \mid \rho'} \\
\\
\text{(RET)} \frac{v \mid \rho \Rightarrow_s \mathcal{V} \mid \rho'}{\text{return } v \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad r \preceq s \neq \mathbf{0} \\
\\
\text{(LET)} \frac{e_1 \mid \rho_1 \Rightarrow_s \mathcal{V}_1 \mid \rho'_1 \quad e_2[x'/x] \mid (\rho'_1 + \rho_2), x' : \langle s, \mathcal{V}_1 \rangle \Rightarrow_r \mathcal{V} \mid \rho'}{\text{let } x = e_1 \text{ in } e_2 \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad \rho_1 + \rho_2 \preceq \rho \quad x' \text{ fresh} \\
\\
\text{(APP)} \frac{v_1 \mid \rho_1 \Rightarrow_s \text{recf}.\lambda x.e^{\gamma_1} \mid \rho'_1 \quad v_2 \mid \rho_2 \Rightarrow_t \mathcal{V}_2 \mid \rho'_2 \quad e[x'/x][f'/f] \mid (\rho'_1 + \rho'_2), x' : \langle t, \mathcal{V}_2 \rangle, f' : \langle s_2, \text{recf}.\lambda x.e^{\gamma_1} \rangle \Rightarrow_r \mathcal{V} \mid \rho'}{v_1 v_2 \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad \begin{array}{l} s_1 + s_2 \preceq s \\ s_1 \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \\ f', x' \text{ fresh} \end{array} \\
\\
\text{(MATCH-U)} \frac{v \mid \rho_1 \Rightarrow_s \text{unit}^\gamma \mid \rho'_1 \quad e \mid (\rho'_1 + \rho_2) \Rightarrow_r \mathcal{V} \mid \rho'}{\text{match } v \text{ with unit} \rightarrow e \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad \begin{array}{l} s \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \end{array} \\
\\
\text{(MATCH-P)} \frac{v \mid \rho_1 \Rightarrow_s \langle r_1 \mathbf{v}_1, \mathbf{v}_2 r_2 \rangle^\gamma \mid \rho'_1 \quad e[x'/x][y'/y] \mid \rho, x' : \langle s \cdot r_1, \mathbf{v}_1^{\gamma_1} \rangle, y' : \langle s \cdot r_2, \mathbf{v}_2^{\gamma_2} \rangle \Rightarrow_r \mathcal{V} \mid \rho'}{\text{match } v \text{ with } \langle x, y \rangle \rightarrow e \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad \begin{array}{l} s \neq \mathbf{0} \\ \gamma \preceq r_1 \cdot \gamma_1 + r_2 \cdot \gamma_2 \\ \rho_1 + \rho_2 \preceq \rho \\ x, y \text{ fresh} \end{array} \\
\\
\text{(MATCH-L)} \frac{v \mid \rho_1 \Rightarrow_t (\text{inl}^s \mathbf{v}_1)^\gamma \mid \rho'_1 \quad e_1[y/x_1] \mid (\rho'_1 + \rho_2), y : \langle s \cdot r, \mathbf{v}_1^{\gamma_1} \rangle \Rightarrow_r \mathcal{V} \mid \rho'}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_t \mathcal{V} \mid \rho'} \quad \begin{array}{l} t \neq \mathbf{0} \\ \gamma \preceq s \cdot \gamma_1 \\ \rho_1 + \rho_2 \preceq \rho \\ y \text{ fresh} \end{array} \\
\\
\text{(MATCH-R)} \frac{v \mid \rho_1 \Rightarrow_s (\text{inr}^s \mathbf{v}_1)^\gamma \mid \rho'_1 \quad e_2[y/x_2] \mid (\rho'_1 + \rho_2), y : \langle s \cdot r, \mathbf{v}_1^{\gamma_1} \rangle \Rightarrow_t \mathcal{V} \mid \rho'}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_t \mathcal{V} \mid \rho'} \quad \begin{array}{l} t \neq \mathbf{0} \\ \gamma \preceq s \cdot \gamma_1 \\ \rho_1 + \rho_2 \preceq \rho \\ y \text{ fresh} \end{array}
\end{array}$$

Fig. 17. No-waste semantics

- (1) Configurations obtained as results, of shape  $\mathbf{v}^\gamma \mid \rho$ , are enforced to be *no-waste*, that is, the resources left in  $\rho$  should be only those needed (modulo approximation) by the (grade context  $\gamma$  annotating the) value  $\mathbf{v}$ .
- (2) When reducing a term with more than one subterm, the available resources are *split* among subterms, analogously to what happens in resource-aware type systems.

In this way, a configuration  $E \mid \rho$  can be successfully reduced only if it is possible to inductively split  $\rho$ , until reaching the leaves of the proof tree, so that, in every leaf, the the part of environment occurring in every leaf is used with no waste, that is, a no-waste result is obtained. In this way, altogether the whole  $\rho$  is used with no waste.

Examples illustrating when successful reduction is possible and when it is not are given in Section 7.4.

Rules which are axioms, that is, (VAR), (FUN), and (UNIT), are designed to accomplish (1). The most significant case is (VAR), where a variable occurrence is replaced by the associated value.

As in the previous rule in Fig. 4, its current amount should be enough to cover that required by the reduction grade (second side condition). However, there is the additional side condition that the result should be no-waste; since it is produced in  $r$  copies, this condition should hold for a grade context obtained by multiplying by  $r$  that declared in the annotated value. Note that this condition implies that the residual amount  $s'$  *should be discardable*, that is,  $\mathbf{0} \preceq s'$ . Indeed, set  $\rho' = \rho, x : \langle s', \mathcal{V} \rangle$ , we know that  $(r \cdot \gamma) \cdot \mathbf{G}_{\rho'}^* \preceq \gamma_{\rho'}$ , hence, in particular  $((r \cdot \gamma) \cdot \mathbf{G}_{\rho'}^*)(x) \preceq s'$ . Since  $\gamma = \mathbf{G}_x$ , by Lemma 7.12 we get  $\gamma \cdot \mathbf{G}_{\rho'}^*(x) = \mathbf{0}$ , hence  $(r \cdot \gamma) \cdot \mathbf{G}_{\rho'}^*(x) = \mathbf{0}$  as well.

With this formulation, a resource can be used only if its current amount is enough to cover the required use, and no resource amount would be wasted. An alternative formulation could even *remove garbage*, see Proposition 7.23 in the following.

The side condition requiring the result to be no-waste is also added to the other axioms (FUN) and (UNIT). Since no resource is consumed, the condition is checked on the initial environment.

Rules handling constructs with more than one subterm, that is, (PAIR), (LET), (APP), and all the (MATCH) rules, are designed to accomplish (2). For instance, in rule (PAIR), the environment, rather than being sequentially used by the two components as in the previous rule in Fig. 4, is split in two parts, used to evaluate the first and the second component, respectively. A similar splitting is done in the other mentioned rules.

Besides the standard typing errors, and resource exhaustion, as in the previous resource-aware semantics, reduction can get stuck if some available amount would be wasted. For instance, considering linearity grades, the configuration  $x \mid x : \langle 1, \text{unit}^0 \rangle, y : \langle 1, \text{unit}^0 \rangle$  is stuck. Indeed, rule (VAR) is not applicable since there is no way to obtain a no-waste result. Formally, since  $\gamma = \emptyset$ , it should be  $\emptyset \preceq_{\text{nw}}^* y : \langle 1, \text{unit}^0 \rangle$ ; this does not hold, since, for the resource  $y$ , the usage is 0, the availability is 1, and  $0 \not\preceq 1$ . On the other hand, reduction would be possible with an environment  $x : \langle 1, \text{unit}^0 \rangle, y : \langle \omega, \text{unit}^0 \rangle$ , and the final result would be  $\text{unit}^0 \mid y : \langle \omega, \text{unit}^0 \rangle$ , or even  $\text{unit}^0 \mid \emptyset$  in a semantics removing garbage.

When the environment is split in two parts, there are generally many possible ways to do the splitting; depending on such choices, when reaching the base cases, the corresponding axiom could either be applicable or not. This is an additional source of non-determinism besides those already present in the previous semantics. Hence, as already mentioned, soundness of the type system will be *soundness-may*<sup>13</sup>, meaning that, for a well-typed configuration, *there*

<sup>13</sup>The terminology of *may* and *must* properties is very general and comes originally from De Nicola and Hennessy [20]; the specific names *soundness-may* and *soundness-must* were introduced by Dagnino [17], Dagnino et al. [18] in the context of big-step semantics.

exists a computation which does not get stuck; in particular, there exists a way to split the environment at each node such that the proof tree can be successfully completed.

#### 7.4 Examples of reduction

Consider the configuration  $y\langle^3x, x^5\rangle \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle$ , where  $\mathbf{f} = \lambda z.x; z$ , with the grade algebra for bounded counting of Example 3.3(1). The configuration can be reduced, as we show in Fig. 18. In this figure and the following we write  $\mathbf{u}$  for unit to save space, and  $\mathcal{V} = \langle^3\mathbf{u}, \mathbf{u}^5\rangle^0$ . The same reduction is derivable by considering the

$$\begin{aligned}
 \mathcal{D}_1 &= \frac{\frac{}{x \mid x : \langle 3, \mathbf{u}^0\rangle \Rightarrow_3 \mathbf{u}^0 \mid \emptyset} \text{ (VAR)} \quad \frac{}{x \mid x : \langle 5, \mathbf{u}\rangle \Rightarrow_5 \mathbf{u}^0 \mid \emptyset} \text{ (VAR)}}{\langle^3x, x^5\rangle \mid x : \langle 8, \mathbf{u}\rangle \Rightarrow_1 \mathcal{V} \mid \emptyset} \text{ (PAIR)} \\
 \mathcal{D}_2 &= \frac{\frac{}{x \mid x : \langle 1, \mathbf{u}^0\rangle \Rightarrow_1 \mathbf{u}^0 \mid \emptyset} \text{ (VAR)} \quad \frac{}{z \mid z : \langle 1, \mathcal{V}\rangle \Rightarrow_1 \mathcal{V} \mid \emptyset} \text{ (VAR)}}{x; z \mid x : \langle 1, \mathbf{u}^0\rangle, z : \langle 1, \mathcal{V}\rangle \Rightarrow_1 \mathcal{V} \mid \emptyset} \text{ (MATCH-U)} \\
 \mathcal{D} &= \frac{\frac{}{y \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 1, \mathbf{u}^0\rangle \Rightarrow_1 \mathbf{f}^{x:1} \mid x : \langle 1, \mathbf{u}^0\rangle} \text{ (VAR)} \quad \mathcal{D}_1 \quad \mathcal{D}_2}{y\langle^3x, x^5\rangle \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle \Rightarrow_1 \mathcal{V} \mid \emptyset} \text{ (APP)}
 \end{aligned}$$

Fig. 18. Example of non-wasting reduction

grade algebra for exact counting of Example 3.3(1). On the contrary, the configuration  $y\langle^3x, x^5\rangle \mid y : \langle 2, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle$  illustrates how the grade algebra affects the semantics. Indeed, with bounded counting this configuration can be reduced, as shown at the top section of Fig. 19, with  $\mathcal{D}_1$  and  $\mathcal{D}_2$  as in Fig. 18.

$$\begin{aligned}
 \mathcal{D} &= \frac{\frac{}{y \mid y : \langle 2, \mathbf{f}^{x:1}\rangle, x : \langle 1, \mathbf{u}^0\rangle \Rightarrow_1 \mathbf{f}^{x:1} \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 1, \mathbf{u}^0\rangle} \text{ (VAR)} \quad \mathcal{D}_1 \quad \mathcal{D}_2}{y\langle^3x, x^5\rangle \mid y : \langle 2, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle \Rightarrow_1 \mathcal{V} \mid y : \langle 1, \mathbf{f}^{x:1}\rangle} \text{ (APP)} \\
 \hline
 \mathcal{D}'_1 &= \frac{\frac{}{x \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 3, \mathbf{u}^0\rangle \Rightarrow_3 \mathbf{u}^0 \mid y : \langle 1, \mathbf{f}^{x:1}\rangle} \text{ (VAR)} \quad \frac{}{x \mid x : \langle 5, \mathbf{u}\rangle \Rightarrow_5 \mathbf{u}^0 \mid \emptyset} \text{ (VAR)}}{\langle^3x, x^5\rangle \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 8, \mathbf{u}\rangle \Rightarrow_1 \mathcal{V} \mid y : \langle 1, \mathbf{f}^{x:1}\rangle} \text{ (PAIR)} \\
 \mathcal{D}' &= \frac{\frac{}{y \mid y : \langle 1, \mathbf{f}^{x:1}\rangle, x : \langle 1, \mathbf{u}^0\rangle \Rightarrow_1 \mathbf{f}^{x:1} \mid x : \langle 1, \mathbf{u}^0\rangle} \text{ (VAR)} \quad \mathcal{D}'_1 \quad \mathcal{D}_2}{y\langle^3x, x^5\rangle \mid y : \langle 2, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle \Rightarrow_1 \mathcal{V} \mid y : \langle 1, \mathbf{f}^{x:1}\rangle} \text{ (APP)}
 \end{aligned}$$

Fig. 19. Example of wasting reduction

On the other hand, if we consider exact counting, the configuration is stuck, since there is no way to split the environment  $y : \langle 2, \mathbf{f}^{x:1}\rangle, x : \langle 9, \mathbf{u}^0\rangle$  to obtain a proof tree. We consider, for instance, two possibilities.

If we use both the copies of  $y$  to reduce the function, as shown at the top section of Fig. 19, the computation is stuck when we try to apply rule (VAR) in  $\mathcal{D}$ , since  $1 \cdot (x : 1) \not\leq_{\text{nw}}^*$

$y : \langle 1, \mathbf{f}^{x:1} \rangle, x : \langle 1, \mathbf{u}^0 \rangle$  as  $0 \not\leq 1$ . That is, we cannot consume only one copy of  $y$  since the remaining grade would be non-discardable.

If, instead, we allocate one copy of  $y$  to reduce the function and one to reduce its argument, as shown at the bottom section of Fig. 19, the computation is also stuck, when in  $\mathcal{D}_1$  we try to apply one of the instances of rule (VAR). Indeed, here  $y$  is not used and its grade is non-discardable, that is, we would waste  $y$ .

### 7.5 Results

As expected, no-waste semantics can be seen as a refinement of resource-aware semantics. More precisely, given a no-waste reduction, there exist infinitely many resource-aware reductions obtained by adding a “wasted” portion of environment. This is formalized below, where  $\text{erase}(\rho)$  denotes the environment obtained from  $\rho$  by removing annotations from values.

**Theorem 7.19.** *If  $E \mid \rho_1 \Rightarrow_r \mathbf{v}^\gamma \mid \rho_2$  then, for all  $\hat{\rho}$  such that  $\text{erase}(\rho_1) + \hat{\rho}$  is defined,  $E \mid \text{erase}(\rho_1) + \hat{\rho} \Rightarrow_r \mathbf{v} \mid \text{erase}(\rho_2) + \hat{\rho}$ .*

PROOF. Let us write  $\rho \parallel \rho'$  if  $\rho$  and  $\rho'$  are non-conflicting, that is,  $\rho + \rho'$  is defined. First of all note that, if  $E \mid \rho \Rightarrow_r \mathbf{v}^\gamma \mid \rho'$ , and  $\text{erase}(\rho) \parallel \hat{\rho}$  holds, then  $\text{erase}(\rho') \parallel \hat{\rho}$  holds as well, since variables added in  $\rho'$  are fresh.

By induction on the no-waste reduction. We show one base and one inductive case.

(VAR) We have  $x \mid \rho, x : \langle s, \mathcal{V} \rangle \Rightarrow_r \mathcal{V} \mid \rho, x : \langle s', \mathcal{V} \rangle$ , with  $\mathcal{V} = \mathbf{v}^\gamma$  and  $r + s' \preceq s$ . Take an arbitrary  $\hat{\rho}$  such that  $\text{erase}(\rho, x : \langle s, \mathcal{V} \rangle) \parallel \hat{\rho}$ .

If  $x \notin \text{dom}(\hat{\rho})$ , then the side condition  $r + s' \preceq s$  of rule (VAR) in Fig. 4 holds, hence  $x \mid (\text{erase}(\rho), x : \langle s, \mathbf{v} \rangle) + \hat{\rho} \Rightarrow_r \mathbf{v} \mid \text{erase}(\rho), x : \langle s', \mathbf{v} \rangle + \hat{\rho}$ .

If  $\hat{\rho}(x) = \langle r', \mathbf{v} \rangle$ , then the side condition  $r + s' + r' \preceq s + r'$  of rule (VAR) in Fig. 4 holds, hence  $x \mid (\text{erase}(\rho), x : \langle s, \mathbf{v} \rangle) + \hat{\rho} \Rightarrow_r \mathbf{v} \mid \text{erase}(\rho), x : \langle s', \mathbf{v} \rangle + \hat{\rho}$ . In both cases we get the thesis.

(PAIR) We have

- (1)  $v_1 \mid \rho_1 \Rightarrow_{r \cdot r_1} \mathbf{v}_1^{\gamma_1} \mid \rho'_1$
- (2)  $v_2 \mid \rho_2 \Rightarrow_{r \cdot r_2} \mathbf{v}_2^{\gamma_2} \mid \rho'_2$
- (3)  $\langle r_1 v_1, v_2^{r_2} \rangle \mid \rho \Rightarrow_r \langle r_1 \mathbf{v}_1, \mathbf{v}_2^{r_2} \rangle^{\gamma_1 + \gamma_2} \mid \rho'_1 + \rho'_2$
- (4)  $\rho_1 + \rho_2 \preceq \rho$

From (4) we get that  $\text{erase}(\rho_1) \parallel \text{erase}(\rho_2)$  holds. Hence, from (1) by inductive hypothesis, taking as additional environment  $\text{erase}(\rho_2)$ , we get

$$v_1 \mid \text{erase}(\rho_1) + \text{erase}(\rho_2) \Rightarrow_{r \cdot r_1} \mathbf{v}_1 \mid \text{erase}(\rho'_1) + \text{erase}(\rho_2)$$

Since  $\text{erase}(\rho'_1) \parallel \text{erase}(\rho_2)$ , from (2) by inductive hypothesis, taking as additional environment  $\text{erase}(\rho'_1)$ , we get

$$v_2 \mid \text{erase}(\rho_2) + \text{erase}(\rho'_1) \Rightarrow_{r \cdot r_1} \mathbf{v}_1 \mid \text{erase}(\rho'_2) + \text{erase}(\rho'_1)$$

Hence, we can apply rule (PAIR) in Fig. 4:

$$\langle r_1 v_1, v_2^{r_2} \rangle \mid \rho \Rightarrow_r \langle r_1 \mathbf{v}_1, \mathbf{v}_2^{r_2} \rangle \mid \text{erase}(\rho'_1) + \text{erase}(\rho'_2)$$

and we get the thesis. □

We state now the main result of this section: the reduction relation is no-waste. We say that  $E \mid \rho$  is no-waste, written  $\vdash_{\text{nw}} E \mid \rho$ , if  $\gamma \preceq_{\text{nw}}^* \rho$  holds for some  $\gamma$  honest for  $E$ .

**Theorem 7.20** (Semantics is no-waste). *If  $E \mid \rho \Rightarrow_r \mathbf{v}^{\gamma'} \mid \rho'$  then  $\vdash_{\text{nw}} E \mid \rho$ , and  $r \cdot \gamma' \preceq_{\text{nw}}^* \rho'$ .*

Here,  $r \cdot \gamma' \preceq_{\text{nw}}^* \rho'$  states that, as required, *only no-waste results are produced*; since the final result is produced in  $r$  copies, the no-waste condition holds for a grade context obtained by multiplying by  $r$  that declared in the annotated value.

In addition, the theorem provides a *characterization of configurations which do not get stuck due to wasting errors*. In other words, configurations such that  $\vdash_{\text{nw}} E \mid \rho$  does not hold are stuck, since they cannot be reduced to a no-waste result.

Let us consider the configuration  $x \mid x : \langle 1, (\lambda_{-} \langle^1 y, z^1 \rangle)^{y:1, z:1}, y : \langle 1, \text{unit}^0 \rangle, z : \langle 1, \text{unit}^0 \rangle \rangle$ . Assuming linearity grades, this configuration is non-stuck, since there exists a grade context (a way to assign grades to the variables), notably,  $x : 1$ , which uses with no-waste the environment. Indeed, the three resources need to be used with grade 1, and such grade context uses, with grade 1, directly  $x$ , and transitively  $y$  and  $z$ . On the contrary, the configuration  $x \mid x : \langle 1, (\lambda_{-} y)^{y:1}, y : \langle 1, \text{unit}^0 \rangle, z : \langle 1, \text{unit}^0 \rangle \rangle$  is stuck, since *there is no grade context* such that the no-waste condition holds. Indeed, since  $z$  is no longer transitively used, it is should be directly used in the grade context, but this would not be honest for the value expression  $x$ .

Of course we expect, and will prove, that well-typed configurations are no-waste; however, note that the characterization above is purely semantic, and, as usual, it can hold for ill-typed configurations. For instance, assuming to have booleans and conditional, which can be encoded as shown in Fig. 10, the configuration  $\text{if true then } x \text{ else unit} \mid x : \langle 1, \text{unit}^0 \rangle$  is no-waste, since  $x : 1 \preceq_{\text{nw}}^* x : \langle 1, \text{unit} \rangle$  holds, and indeed can be safely reduced to  $\text{unit}^0 \mid \emptyset$ . However, this configuration is ill-typed, since the else alternative does not use  $x$ .

Theorem 7.20 is an immediate corollary of the following one.

**Theorem 7.21** (Resource balance). *If  $E \mid \rho \Rightarrow_r \mathbf{v}^{\gamma'} \mid \rho'$  then there exist  $\gamma, \gamma^c, \gamma^a$ , with  $\gamma$  honest for  $E$ ,  $\gamma(x) = \mathbf{0}$  for each  $x \notin \text{dom}(\rho)$ , and  $\gamma^a(x) = \mathbf{0}$  for all  $x \in \text{dom}(\rho)$ , such that the following conditions hold.*

- (1)  $r \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* \preceq \gamma_{\rho'}$
- (2)  $\gamma \cdot \mathbf{G}_{\rho}^* \preceq \gamma_{\rho}$
- (3)  $\gamma_{\rho'} + \gamma^c \preceq \gamma_{\rho} + \gamma^a$
- (4)  $\gamma \cdot \mathbf{G}_{\rho}^* + \gamma^a \preceq r \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* + \gamma^c$

Notably, Item 1 shows that the result is no-waste, and  $\gamma$  in Item 2 is the grade context used to prove that the configuration is no-waste. The grade contexts  $\gamma^c$  and  $\gamma^a$  denote, respectively, *consumed* and *added* resources during the computation, which are used to express balance (in)equations in Items 3 and 4. Added resources are always fresh, hence  $\gamma^a(x) = \mathbf{0}$  for all  $x \in \text{dom}(\rho)$  is expected to hold. The inequation of Item 3 states that remaining resources plus those consumed during the computation cannot exceed the sum of initially available resources and those added by the evaluation. This is analogous to a resource-balance result proved by Choudhury et al. [13], but here it is expressed in purely semantic terms. Item 4 provides a strict version formulated using the more precise information carried by the grade graphs of the environments and is the key property to prove the no-waste result.

$$\begin{array}{c}
\text{(T-VAL)} \quad \frac{\Gamma \vdash \mathbf{v} : \tau^1}{r \cdot \Gamma \vdash \mathbf{v}^\gamma : \tau^r} \quad \gamma \preceq \gamma_\Gamma \\
\\
\text{(T-ENV)} \quad \frac{\Gamma_i \vdash \mathcal{V}_i : \tau_i^{r_i} \quad \forall i \in 1..n}{\Gamma \vdash x_1 : \langle r_1, \mathcal{V}_1 \rangle, \dots, x_n : \langle r_n, \mathcal{V}_n \rangle \triangleright \Delta} \quad \Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n \\
\Gamma_1 + \dots + \Gamma_n + \Delta \preceq \Gamma \\
\\
\text{(T-CONF)} \quad \frac{\Delta \vdash E : T \quad \Gamma \vdash \rho \triangleright \Delta}{\Gamma \vdash E \mid \rho : T} \quad \text{(T-RES)} \quad \frac{\Delta \vdash \mathcal{V} : T \quad \Gamma \vdash \rho \triangleright \Delta}{\Gamma \vdash \mathcal{V} \mid \rho : T}
\end{array}$$

Fig. 20. Typing rules for (annotated) values, environments, configurations, and results

The no-waste property implies, in particular, that any resource in the environment which is not reachable from the program (garbage) is discardable, as formalized below. As mentioned before, such a resource could be discarded in a semantics removing garbage.

Let us denote by  $\star_\rho$  the *reachability relation* in  $\rho$ , that is, the reflexive and transitive closure of the relation  $\rightarrow_\rho$  defined by:

$$x \rightarrow_\rho y \text{ if } \rho(x) = \langle -, \mathbf{v}^\gamma \rangle \text{ and } y \in \text{fv}(\mathbf{v})$$

The following lemma states that, as expected, the existence of a non-discardable path implies reachability.

**Lemma 7.22.** *If  $\mathbf{0} \not\leq G_\rho(p)$ , then  $\text{in}(p) \star_\rho \text{out}(p)$ .*

PROOF. By induction on the length of  $p$ . If  $p = x$ , then  $x \star_\rho x$  by reflexivity. Otherwise,  $p = x \cdot p'$ , hence  $\rho(x) = \langle -, \mathbf{v}^\gamma \rangle$ . From  $\mathbf{0} \not\leq G_\rho(x \cdot p)$  we get  $\mathbf{0} \not\leq G(x, \text{in}(p'))$  and  $\mathbf{0} \not\leq G_\rho(p')$ . Being  $\gamma$  honest for  $\mathbf{v}$ , we get  $\text{in}(p') \in \text{fv}(\mathbf{v})$ , hence  $x \rightarrow_\rho \text{in}(p')$ , and we get the thesis by applying the inductive hypothesis to  $\mathbf{0} \not\leq G_\rho(p')$ , and then by transitivity.  $\square$

We write  $X \star_\rho y$  if  $x \star_\rho y$  holds for some  $x \in X$ .

**Proposition 7.23** (No-waste  $\Rightarrow$  Garbage is Discardable). *If  $E \preceq_{\text{nw}}^* \rho$  holds:*

$$\text{fv}(E) \not\rightarrow_\rho x \text{ implies } \mathbf{0} \preceq \gamma_\rho(x).$$

PROOF. Set  $r = \gamma_\rho(x)$ . We prove that  $\mathbf{0} \not\leq r$  implies  $\text{fv}(E) \star_\rho x$ . For some  $\gamma$  honest for  $E$ , we have  $\gamma \cdot G_\rho^*(x) \preceq r$ . Since  $\mathbf{0} \not\leq r$ , it is necessarily  $\mathbf{0} \not\leq \gamma \cdot G_\rho^*(x)$ , that is,  $\mathbf{0} \not\leq \sum_{y \in \text{V}} \gamma(y) \cdot G_\rho^*(y, x)$ . Hence  $\mathbf{0} \not\leq \gamma(y) \cdot G_\rho^*(y, x)$  for some  $y$ , and this implies  $\mathbf{0} \not\leq \gamma(y)$  and  $\mathbf{0} \not\leq G_\rho^*(y, x)$ , hence there is a path  $p$  from  $y$  to  $x$  with  $\mathbf{0} \not\leq G_\rho(p)$ . Being  $\gamma$  honest for  $E$ , we get  $y \in \text{fv}(E)$ , hence  $x \rightarrow_\rho y$ , and by Lemma 7.22 and transitivity we get the thesis.  $\square$

Let us consider the type system in Section 5, with the only difference that, as shown in Fig. 20, annotations in values are taken into account. That is, rule (T-VAL) checks that annotations are (overapproximated by) the direct usage obtained by typechecking the value. Moreover, since annotated values are not value expressions, we have to add a typing rule for results. Here  $\gamma_\Gamma$  is the grade context extracted from  $\Gamma$ , i.e.,  $\gamma_\Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$  for  $\Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$ .

We prove now that well-typed configurations and results are no-waste (Theorem 7.27). To this end, the key property is Proposition 7.25, stating that, given a well-typed environment,

the grade context extracted from the residual context uses the environment with no waste. In other words, the resources left in the environment should be only those needed (modulo approximation) by the residual context. Thanks to the induction principle, proved in Proposition 7.16, this property is implied by the following Proposition 7.24, related to grade graph rather than its closure, which can be proved by routine reasoning on the typing rules.

**Proposition 7.24.** *If  $\Gamma \vdash \rho \triangleright \Delta$  then  $\gamma_\Delta + \gamma_\rho \cdot \mathbf{G}_\rho \preceq \gamma_\rho$ .*

**Proposition 7.25.** *If  $\Gamma \vdash \rho \triangleright \Delta$  then  $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ .*

PROOF. It is an immediate consequence of Propositions 7.16 and 7.24.  $\square$

The next lemma shows that the grade context extracted from the typing context of a well-typed expression is always honest for it.

**Lemma 7.26.** *If  $\Gamma \vdash E : T$  and  $\mathbf{0} \not\preceq \gamma_\Gamma(x)$  then  $x \in \text{fv}(E)$ .*

PROOF. By induction on the typing rules.  $\square$

**Theorem 7.27** (Well-typedness implies no-waste).

- (1) *If  $\Gamma \vdash E \mid \rho : T$  then  $\vdash_{\text{nw}} E \mid \rho$ .*
- (2) *If  $\Gamma \vdash \mathbf{v}^\gamma \mid \rho : \tau^r$  then  $r \cdot \gamma \preceq_{\text{nw}}^\star \rho$ .*

PROOF. (1) We have to show that  $\gamma \preceq_{\text{nw}}^\star \rho$  for some  $\gamma$  honest for  $E$ . To derive  $\Gamma \vdash E \mid \rho : T$ , we have necessarily applied rule (T-CONF), hence  $\Delta \vdash E : T$  and  $\Gamma \vdash \rho \triangleright \Delta$  hold for some  $\Delta$ . By Proposition 7.25 we have  $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ , that is,  $\gamma_\Delta \preceq_{\text{nw}}^\star \rho$ . Moreover,  $\gamma_\Delta$  is honest for  $E$  by Lemma 7.26.

(2) To derive  $\Gamma \vdash \mathbf{v}^\gamma \mid \rho : \tau^r$ , we have necessarily applied rule (T-RES), hence  $\Delta \vdash \mathbf{v}^\gamma : \tau^r$  and  $\Gamma \vdash \rho \triangleright \Delta$  hold for some  $\Delta$ . Moreover, to derive  $\Delta \vdash \mathbf{v}^\gamma : \tau^r$  we have necessarily applied rule (T-VAL), hence  $\Delta = r \cdot \Delta'$  and  $\gamma \preceq \gamma_{\Delta'}$ . Moreover, by definition  $\gamma_\Delta = r \cdot \gamma_{\Delta'}$ , hence  $r \cdot \gamma \preceq \gamma_\Delta$ . By Proposition 7.25 we have  $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ , hence  $(r \cdot \gamma) \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ , that is,  $r \cdot \gamma \preceq_{\text{nw}}^\star \rho$ .  $\square$

We end this section by briefly discussing the acyclicity assumption on environments. Technically, this allows us to give Definition 7.9, where an infinite sum of path grades can be reduced to a finite one thanks to Proposition 7.8(4). However, infinite sums would be well-defined as well by assuming suitable conditions on the grade algebra [21–23, 27]. A more serious problem is that the proof of Proposition 7.16 relies on acyclicity; that is, there is no guarantee that the condition ensured by well-typedness ( $\gamma_\Delta + \gamma_\rho \cdot \mathbf{G}_\rho \preceq \gamma_\rho$ ) implies the no-waste condition ( $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ ). In a sense, the meaning of no-waste in presence of cyclic environments is unclear. Consider a cyclic resource which is “garbage”, that is, not reachable from the program, as in, e.g.,  $\mathbf{v} \mid x : \langle r, \lambda z. x^{x:1} \rangle$ , with  $\mathbf{v}$  closed. This configuration would be well-typed for an arbitrary grade  $r$ , since the resource is “auto-consuming”. We will investigate meaning and formalization of no-waste for cyclic resources in future work.

## 8 Type soundness

In this section, we prove our main result: soundness of the type system with respect to the no-waste semantics<sup>14</sup>. That is, for well-typed expressions there is a computation which

<sup>14</sup>Thanks to Theorem 7.19, this implies soundness with respect to the semantics in Fig. 4 as well.

is not stuck for any reason, including resource exhaustion and waste. Note that this is a *may* flavour of soundness [17, 18, 20], which is the only one we can prove in this context, because the semantics is non-deterministic. We analyse separately type soundness for value expressions and expressions. In the following, we will say that two judgements  $\Gamma_1 \vdash \rho_1 \triangleright \Delta_1$  and  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$  are *consistent* if in their derivations the values associated with variables in the common domain of  $\rho_1$  and  $\rho_2$  are typed with the same type and typing context. Formally, this means that for all  $x \in \text{dom}(\rho_1) \cap \text{dom}(\rho_2)$ , there are  $\mathcal{V} = \mathbf{v}^\gamma$ ,  $\tau$  and  $\Delta$  such that  $\rho_1(x) = \langle \_, \mathcal{V} \rangle$ ,  $\rho_2(x) = \langle \_, \mathcal{V} \rangle$ ,  $\Gamma_1(x) = \langle \_, \tau \rangle$ ,  $\Gamma_2(x) = \langle \_, \tau \rangle$ , and in the derivations of both judgements there is a premise  $\Delta \vdash \mathbf{v} : \tau^1$ . Similarly, we say that two typing judgements for configurations are consistent if so are the judgements of the environments they contain.

**Type soundness for value expressions.** Since reduction of value expressions cannot diverge, type soundness means that well-typed value expressions reduce to a value, as stated below.

**Theorem 8.1** (Soundness for value expressions). *If  $\Gamma \vdash v \mid \rho : \tau^r$ , then  $v \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'$  for some  $\mathcal{V}, \rho'$ .*

This is a corollary of the following extended formulation which can be proved inductively on the structure of value expressions, relying on standard lemmas.

**Theorem 8.2** (Soundness for value expressions (extended)). *If  $\Gamma \vdash v \mid \rho : \tau^r$  then  $v \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'$  and  $\Gamma' \vdash \mathcal{V} \mid \rho' : \tau^r$  consistent with  $\Gamma \vdash v \mid \rho : \tau^r$ , for some  $\mathcal{V}, \rho', \Gamma'$ .*

Note that, even though reduction of value expressions just performs substitution, in a resource-aware semantics this is a significant event, since it implies consuming some amount of resources. Theorem 8.1 states that no resource exhaustion or waste can happen.

**Adding divergence.** For expressions, instead, big-step semantics, as those defined in Fig. 4 and Fig. 17, suffer from the long-known drawback [15, 28] that non-terminating and stuck computations are indistinguishable, since in both cases no finite proof tree of a judgment can be constructed. This is an issue for our aim: to prove that for a well-typed expression there is a computation which does not get stuck, that is, either produces a value or diverges. To solve this problem, we extend the big-step semantics to explicitly model diverging computations, proceeding as follows, with  $c ::= e \mid \rho$ .

- the shape of the judgment for expressions is generalized to  $c \Rightarrow_r \mathbf{r}$ , where the *result*  $\mathbf{r}$  is either a pair consisting of a value and a final environment, or *divergence* ( $\infty$ );
- this judgment is defined through a *generalized inference system*, shown in Fig. 21, consisting of the *rules* from (RET) to (MATCH-U/MATCH-U-DIV), and the *corule* (CO-DIV) (differences with respect to the previous semantics in the bottom section of Fig. 17 are emphasized in grey<sup>15</sup>).

The key point here is that, in generalized inference systems, rules are interpreted in an *essentially coinductive*, rather than inductive, way. For details on generalized inference systems we refer to the works by Ancona et al. [3], Dagnino [16]; here, for the reader's convenience, we provide a self-contained presentation, instantiating general definitions on our specific case.

<sup>15</sup>Recall that, since the evaluation judgment is stratified, premises involving the judgment for value expressions can be equivalently considered as side conditions.

$$\begin{array}{c}
\mathbf{R} ::= \mathcal{V} \mid \rho \quad \text{result} \\
\mid \infty
\end{array}$$


---


$$\begin{array}{c}
(\text{RET}) \frac{v \mid \rho \Rightarrow_s \mathcal{V} \mid \rho'}{\text{return } v \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'} \quad r \preceq s \neq \mathbf{0} \\
\\
(\text{LET-DIV1}) \frac{e_1 \mid \rho \Rightarrow_s \infty}{\text{let } x = e_1 \text{ in } e_2 \mid \rho \Rightarrow_r \infty} \\
\\
(\text{LET/LET-DIV2}) \frac{e_1 \mid \rho_1 \Rightarrow_s \mathcal{V}_1 \mid \rho'_1 \quad e_2[x'/x] \mid (\rho'_1 + \rho_2), x' : \langle s, \mathcal{V}_1 \rangle \Rightarrow_r \mathbf{R}}{\text{let } x = e_1 \text{ in } e_2 \mid \rho \Rightarrow_r \mathbf{R}} \quad \begin{array}{l} \rho_1 + \rho_2 \preceq \rho \\ x' \text{ fresh} \end{array} \\
\\
(\text{APP/APP-DIV}) \frac{v_1 \mid \rho_1 \Rightarrow_s \text{recf}. \lambda x. e^{\gamma_1} \mid \rho'_1 \quad v_2 \mid \rho_2 \Rightarrow_t \mathcal{V}_2 \mid \rho'_2 \quad e[x'/x][f'/f] \mid (\rho'_1 + \rho'_2), x' : \langle t, \mathcal{V}_2 \rangle, f' : \langle s_2, \text{recf}. \lambda x. e^{\gamma_1} \rangle \Rightarrow_r \mathbf{R}}{v_1 v_2 \mid \rho \Rightarrow_r \mathbf{R}} \quad \begin{array}{l} s_1 + s_2 \preceq s \\ s_1 \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \\ f', x' \text{ fresh} \end{array} \\
\\
(\text{MATCH-U/MATCH-U-DIV}) \frac{v \mid \rho_1 \Rightarrow_s \text{unit}^{\gamma} \mid \rho'_1 \quad e \mid (\rho'_1 + \rho_2) \Rightarrow_r \mathbf{R} \quad s \neq \mathbf{0}}{\text{match } v \text{ with unit} \rightarrow e \mid \rho \Rightarrow_r \mathbf{R}} \quad \rho_1 + \rho_2 \preceq \rho \\
\\
(\text{MATCH-P/MATCH-P-DIV}) \frac{v \mid \rho_1 \Rightarrow_s \langle r_1 v_1, v_2 r_2 \rangle^{\gamma_1 + \gamma_2} \mid \rho'_1 \quad e[x'/x][y'/y] \mid \rho, x' : \langle s \cdot r_1, v_1^{\gamma_1} \rangle, y' : \langle s \cdot r_2, v_2^{\gamma_2} \rangle \Rightarrow_r \mathbf{R}}{\text{match } v \text{ with } \langle x, y \rangle \rightarrow e \mid \rho \Rightarrow_r \mathbf{R}} \quad \begin{array}{l} s \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \\ x, y \text{ fresh} \end{array} \\
\\
(\text{MATCH-L/MATCH-L-DIV}) \frac{v \mid \rho_1 \Rightarrow_t \text{inl}^s v_1^{\gamma_1} \mid \rho'_1 \quad e_1[y/x_1] \mid (\rho'_1 + \rho_2), y : \langle s \cdot r, v_1^{\gamma_1} \rangle \Rightarrow_r \mathbf{R}}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_t \mathbf{R}} \quad \begin{array}{l} t \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \\ y \text{ fresh} \end{array} \\
\\
(\text{MATCH-R/MATCH-R-DIV}) \frac{v \mid \rho_1 \Rightarrow_s \text{inr}^r v_1^{\gamma_1} \mid \rho'_1 \quad e_2[y/x_2] \mid (\rho'_1 + \rho_2), y : \langle s \cdot r, v_1^{\gamma_1} \rangle \Rightarrow_t \mathbf{R}}{\text{match } v \text{ with inl } x_1 \rightarrow e_1 \text{ or inr } x_2 \rightarrow e_2 \mid \rho \Rightarrow_t \mathbf{R}} \quad \begin{array}{l} t \neq \mathbf{0} \\ \rho_1 + \rho_2 \preceq \rho \\ y \text{ fresh} \end{array} \\
\\
(\text{CO-DIV}) \frac{}{e \mid \rho \Rightarrow_r \infty}
\end{array}$$

Fig. 21. Adding divergence

Rules in Fig. 21 handle divergence propagation. Notably, for each rule in the bottom section of Fig. 17, we add a divergence propagation rule for each of the possibly diverging premises. The only rule with two possibly diverging premises is (LET). Hence, divergence propagation for an expression  $\text{let } x = e_1 \text{ in } e_2$  is obtained by two (meta)rules: (LET-DIV1) when  $e_1$  diverges, and (LET-DIV2) when  $e_1$  converges and  $e_2$  diverges; in Fig. 21, for brevity, this second metarule is merged with (LET), using the metavariable  $\mathbf{R}$ . All the other rules have only one possibly diverging premise, so one divergence propagation rule is added and merged with the original metarule, analogously to (LET-DIV2).

In generalized inference systems, infinite proof trees are allowed. Hence, judgments  $c \Rightarrow_r \infty$  can be derived, as desired, even though there is no axiom introducing them, thus distinguishing diverging computations (infinite proof tree) from stuck computations (no proof tree). However, a purely coinductive interpretation would allow the derivation of spurious judgements [4, 15, 28]. To address this issue, generalized inference systems may include

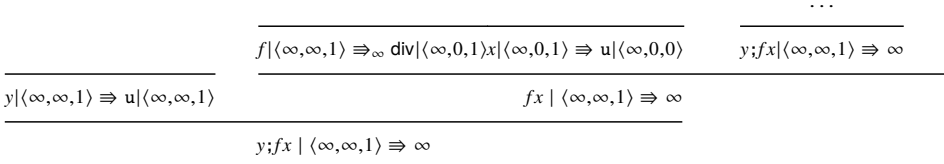


Fig. 22. Example of resource-aware evaluation: divergency with no exhaustion

*corules*, written with a thick line, only (co-DIV) in our case, which refine the coinductive interpretation, filtering out some (undesired) infinite derivations. Intuitively, the meaning of (co-DIV) is to allow infinite derivations only for divergence (see Example 8.4 below). Formally, we have the following definition instantiated from those by Ancona et al. [3], Dagnino [16].

**Definition 8.3.** A judgment  $c \Rightarrow_r R$  is derivable in the generalized inference system in Fig. 21, written  $\vdash_\infty c \Rightarrow_r R$ , if it has an infinite proof tree constructed using the rules where, moreover, each node has a *finite* proof tree constructed using the rules *plus the corule*.

**Example 8.4.** Let us consider again the expression  $y;fx$  of Example 4.1. Now, its non-terminating evaluation in the environment  $y : \langle \infty, \text{unit} \rangle, f : \langle \infty, \text{div} \rangle, x : \langle 1, \text{unit} \rangle$ , abbreviated  $\langle \infty, \infty, 1 \rangle$  using the previous convention, is formalized by the infinite proof tree in Fig. 22, where instantiations of (meta)rules (MATCH-U) and (APP) have been replaced by those of the corresponding divergence propagation rule. It is immediate to see that each node in such infinite proof tree has a finite proof tree constructed using the rules plus the corule: the only nodes which have no finite proof tree constructed using the rules are those in the infinite path, of shape either  $y;fx | \langle \infty, \infty, 1 \rangle \Rightarrow \infty$  or  $fx | \langle \infty, \infty, 1 \rangle \Rightarrow \infty$ , and such judgments are directly derivable by the corule. On the other hand, infinite proof trees obtained by using (MATCH-U) and (APP) would derive  $y;fx | \langle \infty, \infty, 1 \rangle \Rightarrow \mathcal{V} | \langle \infty, \infty, 1 \rangle$  for any  $\mathcal{V}$ . However, such judgments *have no* finite proof tree using also the corule, which allows only to introduce divergence, since there is no rule deriving a value with divergence as a premise.

The transformation from the inductive big-step semantics in Fig. 17 to that handling divergence in Fig. 21 is an instance of a general construction, taking as input an arbitrary big-step semantics, fully formalized, and proved to be correct, by Dagnino [17]. In particular, the construction is *conservative*, that is, the semantics of converging computations is not affected, as stated in the following result, which is an instance of Theorem 6.3 by Dagnino [17].

**Definition 8.5.** Let  $\vdash c \Rightarrow_r \mathcal{V} | \rho$  denote that the judgment can be derived by the rules in the bottom section of Fig. 17, interpreted inductively.

**Theorem 8.6** (Conservativity).  $\vdash_\infty c \Rightarrow_r \mathcal{V} | \rho'$  if and only if  $\vdash c \Rightarrow_r \mathcal{V} | \rho'$ .

Note that to achieve this result corules are essential since, as observed in Example 8.4, a purely coinductive interpretation allows for infinite proof trees deriving values.

**Type soundness for expressions.** The definition of the semantics by the generalized inference system in Fig. 21 allows a very simple and clean formulation of type soundness: well-typed configurations always reduce to a result (which can be possibly divergence). Formally:

**Theorem 8.7** (Soundness). If  $\Gamma \vdash c : \tau'$ , then  $\vdash_\infty c \Rightarrow_r R$  for some  $R$ .

We describe now the structure of the proof, which is interesting in itself; indeed, the semantics being big-step, there is no consolidated proof technique as the long-time known progress plus subject reduction for the small-step case [40].

The proof is driven by coinductive reasoning on the semantic rules, following a schema firstly adopted by Ancona et al. [4], as detailed below. First of all, it is convenient to turn to the following equivalent formulation of type soundness, stating that well-typed configurations which do not converge necessarily diverge.

**Theorem 8.8** (Completeness- $\infty$ ). *If  $\Gamma \vdash c : \tau^r$ , and there is no  $\mathcal{V} \mid \rho$  s.t.  $\vdash_\infty c \Rightarrow_r \mathcal{V} \mid \rho$ , then  $\vdash_\infty c \Rightarrow_r \infty$ .*

Indeed, with this formulation soundness of the type system can be seen as *completeness* of the set of judgements  $c \Rightarrow_r \infty$  which are derivable with respect to the set of pairs  $\langle c, r \rangle$  such that  $c$  is well-typed with grade  $r$ , and does not converge. The standard technique to prove completeness of a coinductive definition with respect to a specification  $S$  is the coinduction principle, that is, by showing that  $S$  is *consistent* with respect to the coinductive definition. This means that each element of  $S$  should be the consequence of a rule whose premises are in  $S$  as well. In our case, since the definition of  $\vdash_\infty c \Rightarrow_r \infty$  is not purely coinductive, but refined by the corule, completeness needs to be proved by the *bounded coinduction* principle [3, 16], a generalization of the coinduction principle. Namely, besides proving that  $S$  is consistent, we have to prove that  $S$  is *bounded*, that is, each element of  $S$  can be derived by the inference system consisting of the rules *and the corules*, in our case, only (co-DIV), interpreted inductively.

The proof of Theorem 8.8 modularly relies on two results. The former (Theorem 8.9) is the instantiation of a general result proved by Ancona et al. [4] (Theorem 3.3) by bounded coinduction. For the reader's convenience, to illustrate the proof technique in a self-contained way, we report here statement and proof for our specific case. Namely, Theorem 8.9 states completeness of diverging configurations with respect to any family of configurations which satisfies the *progress- $\infty$  property* (this name is chosen to suggest that, for a non-converging well-typed configuration, the construction of a proof tree can never get stuck). The latter (Theorem 8.10) is the progress- $\infty$  property for our type system.

**Theorem 8.9** (Progress- $\infty \Rightarrow$  Completeness- $\infty$ ). *For each grade  $r$ , let  $C_r$  be a set of configurations, and set  $C_r^\infty = \{c \in C_r \mid \nexists \mathcal{V} \mid \rho \text{ such that } \vdash c \Rightarrow_r \mathcal{V} \mid \rho\}$ . If the following condition holds:<sup>16</sup>*

*(PROGRESS- $\infty$ )  $c \in C_r^\infty$  implies that  $c \Rightarrow_r \infty$  is the consequence of a rule where, for all premises of shape  $c' \Rightarrow_s \infty$ ,  $c' \in C_s^\infty$ , and, for all premises of shape  $c' \Rightarrow_s R$ , with  $R \neq \infty$ ,  $\vdash c' \Rightarrow_s R$ .*

*then  $c \in C_r^\infty$  implies  $\vdash_\infty c \Rightarrow_r \infty$ .*

**PROOF.** We set  $S = \{c \Rightarrow_r \infty \mid c \in C_r^\infty\} \cup \{c \Rightarrow_r R \mid R \neq \infty, \vdash c \Rightarrow_r R\}$ , and prove that, for each  $c \Rightarrow_r R \in S$ , we have  $\vdash_\infty c \Rightarrow_r R$ , by bounded coinduction. We have to prove two conditions.

- (1)  $S$  is consistent, that is, each  $c \Rightarrow_r R$  in  $S$  is the consequence of a rule whose premises are in  $S$  as well. We reason by cases:

<sup>16</sup>Keep in mind that  $c \Rightarrow_r R$  denotes just the judgment (a triple), whereas  $\vdash c \Rightarrow_r R$  and  $\vdash_\infty c \Rightarrow_r R$  denote derivability of the judgment (Definition 8.5 and Definition 8.3, respectively).

- For each  $c \Rightarrow_r \infty \in S$ , by the (PROGRESS- $\infty$ ) hypothesis it is the consequence of a rule where, for all premises of shape  $c' \Rightarrow_s \infty$ ,  $c' \in C_s^\infty$ , hence  $c' \Rightarrow_s \infty \in S$ , and, for all premises of shape  $c' \Rightarrow_s R$ , with  $R \neq \infty$ ,  $\vdash c' \Rightarrow_s R$ , hence  $c' \Rightarrow_s R \in S$  as well.
  - For each  $c \Rightarrow_r \mathcal{V} \mid \rho \in S$ , we have  $\vdash c \Rightarrow_r \mathcal{V} \mid \rho$ , hence this judgment is the consequence of a rule in Fig. 17 where for each premise, necessarily of shape  $c' \Rightarrow_{r'} \mathcal{V}' \mid \rho'$ , we have  $\vdash c' \Rightarrow_{r'} \mathcal{V}' \mid \rho'$ , hence  $c' \Rightarrow_{r'} \mathcal{V}' \mid \rho' \in S$ .
- (2)  $S$  is bounded, that is, each  $c \Rightarrow_r R$  in  $S$  can be inductively derived (has a finite proof tree) using the rules and the corule in Fig. 21. This is trivial, since, for  $R = \infty$ , the judgment can be directly derived by (CO-DIV), and, for  $R \neq \infty$ , since  $\vdash c \Rightarrow_r R$ , this holds by definition.

□

Thanks to the theorem above, to prove type soundness (formulated as in Theorem 8.8) it is enough to prove the progress- $\infty$  property for well-typed configurations which do not converge.

Set  $WT_r = \{c \mid \Gamma \vdash c : \tau^r \text{ for some } \Gamma, \tau\}$ , and, accordingly with the notation in Theorem 8.9,  $WT_r^\infty = \{c \mid c \in WT_r \text{ and } \nexists \mathcal{V} \mid \rho \text{ such that } \vdash_\infty c \Rightarrow_r \mathcal{V} \mid \rho\}$ .

**Theorem 8.10** (Progress- $\infty$ ). *If  $c \in WT_r^\infty$ , then  $c \Rightarrow_r \infty$  is the consequence of a rule where, for all premises of shape  $c' \Rightarrow_s \infty$ ,  $c' \in WT_s^\infty$ , and, for all premises of shape  $c' \Rightarrow_s R$ , with  $R \neq \infty$ ,  $\vdash c' \Rightarrow_s R$ .*

We derive this theorem from the next one, which needs the following notations:

- We use the metavariable  $\tilde{\rho}$  for environments where grades have been erased, hence they are maps from variables into values.
- We write  $\text{erase}(\rho)$  for the environment obtained from  $\rho$  by erasing grades and grade contexts.
- The reduction relation  $\Rightarrow$  over pairs  $v \mid \tilde{\rho}$  and  $e \mid \tilde{\rho}$  is defined by the metarules in Fig. 17 where we remove side conditions involving grades and grade contexts. That is, such relation models standard semantics.

The following theorem states that, if a configuration is well-typed, and (ignoring the grades) reduces to a result, then there is a corresponding graded reduction, leading to a result which is well-typed as well.

**Theorem 8.11.** *If  $\Gamma \vdash e \mid \rho : \tau^r$  and, set  $\tilde{\rho} = \text{erase}(\rho)$ ,  $e \mid \tilde{\rho} \Rightarrow v \mid \tilde{\rho}'$ , then there exist  $\rho', \gamma$  and  $\Gamma'$  such that  $e \mid \rho \Rightarrow_r v^\gamma \mid \rho'$  with  $\text{erase}(\rho') = \tilde{\rho}'$ , and  $\Gamma' \vdash v^\gamma \mid \rho' : \tau^r$  consistent with  $\Gamma \vdash e \mid \rho : \tau^r$ .*

## 9 Related work

As mentioned, the contributions closest to this work, since they present a resource-aware semantics, are those by Bianchini et al. [8], Choudhury et al. [13], Torczon et al. [35], and the conference version of this paper [9]. Choudhury et al. [13] develop GRAD, a graded dependent type system that includes functions, tensor products, additive sums, and a unit type. The instrumented semantics is defined on typed terms, with the only aim to show the role of the type system.

In the work of Bianchini et al. [8], which adopts a Java-like language, the semantics, also given in small-step style, is defined *independently* of the type system, in order to provide a simple execution model taking into account usage of resources. In the conference version of this paper [9], the language and type system coincide with those of the current paper, and the reduction semantics is big-step. As a consequence, annotating subterms is no longer necessary; however, differently from the semantics considered here, this reduction allows resource waste.

The work of Torczon et al. [35] also employs a big-step semantics. Values are closures that “save” the environment in the presence of delayed evaluation, similarly to our annotated values. In that setting, resource annotations can only count down, and provide an upper bound on the resources required for the computation.

The type system presented in this paper follows the same design principles of those introduced in Bianchini et al. [6, 7], which are, however, based on a Java-like underlying calculus. Those works also address two interesting issues not considered here. The first is the definition of a canonical construction yielding a unique grade algebra of *heterogeneous* grades from a family of grade algebras, thus enabling different notions of resource usage to coexist within the same program. The second is the provision of linguistic support for specifying *user-defined* grades; for instance, grade annotations could be written themselves in Java, analogously to what happens for exceptions.

More generally, in the study of resource-aware type systems, *coeffects*, that is, grades used as annotations in contexts, were first introduced and later further analyzed by Petricek et al. [33, 34]. They develop a generic coeffect system which augments the simply-typed  $\lambda$ -calculus with context annotations indexed by *coeffect shapes*. The framework is highly abstract, and the authors focus on two instances: structural (per-variable) and flat (whole context) coeffects, which are obtained by specific choices of coeffect shapes.

Subsequently, the notion has been generalized to an arbitrary assortment of usages, formally modeled by *grades*, elements of an algebraic structure (*grade algebra*) defined in slightly different ways in literature<sup>17</sup> [1, 5, 12, 19, 24, 25, 31, 32, 39]. For instance, grades can be natural numbers counting how many times a resource is used, or even express non-quantitative properties, e.g., that a resource should be used with a given privacy level. In this way, linear/affine type systems can be generalized to type systems parametric on the grade algebra, and the notion of resource-aware soundness can be generalized as well.

Most of the subsequent literature has focused on structural coeffects (grades), for which there is a clear algebraic description in terms of semirings. This was first noticed by Brunel et al. [12], who developed a framework for structural coeffects for a functional language, and by Ghica and Smith [25]. This approach is inspired by a generalization of the exponential modality of linear logic, see, e.g., [11]. That is, the distinction between linear and unrestricted variables of linear systems is generalized to have variables decorated by coeffects (grades), that determine how much they can be used.

In this setting, many advances have been made to combine grades with other programming features, such as computational effects [19, 24, 32], dependent types [5, 13, 31], and polymorphism [1]. In all these papers, tracking usage through grades has practical benefits like erasure of irrelevant terms and compiler optimizations.

---

<sup>17</sup>Essentially variants of an ordered semiring.

McBride [31], Wood and Atkey [39] observed that contexts in a structural coeffect system form a module over the semiring of grades, even though they restrict themselves to free modules, that is, to structural coeffect systems. Recently, Bianchini et al. [10] show a significant non-structural instance, namely, a coeffect system to track sharing in the imperative paradigm.

## 10 Conclusion

We illustrated, on a paradigmatic calculus, how to enrich the semantics and type system of a language, parametrically on an arbitrary grade algebra, so as to express and prove resource-aware soundness including no-waste. To this end, we defined two instrumented semantics, the latter being a refinement of the former. In both formulations, the resources consumed by a computation are explicitly tracked, and programs cannot consume more resources than those available. In the refined formulation, in addition, programs cannot waste resources. Since the instrumented semantics are non-deterministic, *soundness-may* needs to be proved, that is, for a well-typed program there is a computation which is non-stuck, as formally stated in Theorem 8.7, since, besides type errors, both resource exhaustion and waste are prevented.

More precisely, a non-stuck computation either terminates or diverges. In either case, resource exhaustion never happens. However, the property that no resources remain in the result (except for those that can be discarded) can only be meaningfully stated for terminating computations. We leave to future work the investigation of a possible notion of no-waste for a non terminating computation.

The resource-aware semantics is given in big-step style, extending the judgment to explicitly model divergence. We prove (resource-aware) soundness, by a significant, complex application of a schema previously introduced by Ancona et al. [4].

Most works on graded type systems introduce box/unbox operators in the syntax. Hence, programs typed with the type system proposed in this paper could not even be *written* in these systems. A formal comparison with a calculus/type system based on boxing/unboxing is a challenging topic for future work. However, it is not obvious how to make such a comparison, since works which present calculi with a similar expressive power to ours, e.g., those by Brunel et al. [12] and Dal Lago and Gavazzo [19], do not include an instrumented semantics, so we should as a first step develop such a semantics.

We briefly discussed at the end of Section 7.5 the relevance of the acyclicity assumption on environments. Besides being reasonable in the simple language considered in this paper, we expect such an assumption to still hold when adding more realistic language features, provided that the calculus remains pure. Indeed, cycles are typically introduced by assignment. An extension of our approach to the imperative case is interesting also because a different notion of resource usage should likely be considered, e.g., rather than any time a variable occurrence needs to be replaced, any time memory needs to be accessed, even possibly distinguishing read from write accesses. In this way, we could characterize as grades some properties which are of paramount importance in the imperative context, such as *mutability/immortality* or *uniqueness* opposed to *linearity*, revisiting what is discussed by Marshall et al. [30].

Finally, some more general topics to be investigated are type inference, for which the challenging feature are recursive functions, and combination with *effects*, as investigated by Dal Lago and Gavazzo [19].

Concerning implementation, and mechanization of proofs, which of course would be beneficial developments as well, we just mention the Agda library, available at <https://github.com/LcicC/inference-systems-agda> and described in the paper of Ciccone et al. [14], which allows one to specify (generalized) inference systems. One of the examples provided in such a paper is, as here, a big-step semantics including divergence.

**Acknowledgments.** The authors would like to thank the OOPSLA and JFP anonymous referees who provided useful and detailed comments on previous versions of the paper. This work has the financial support of the University of Eastern Piedmont.

## References

- [1] Andreas Abel and Jean-Philippe Bernardy. 2020. A unified view of modalities in type systems. *Proceedings of ACM on Programming Languages* 4, ICFP (2020), 90:1–90:28. doi:10.1145/3408972
- [2] Andreas Abel, Nils Anders Danielsson, and Oskar Eriksson. 2023. A Graded Modal Dependent Type Theory with a Universe and Erasure, Formalized. *Proceedings of ACM on Programming Languages* 7, ICFP (2023), 920–954. doi:10.1145/3607862
- [3] Davide Ancona, Francesco Dagnino, and Elena Zucca. 2017. Generalizing Inference Systems by Coaxioms. In *European Symposium on Programming, ESOP 2017 (Lecture Notes in Computer Science, Vol. 10201)*, Hongseok Yang (Ed.). Springer, Berlin, 29–55. doi:10.1007/978-3-662-54434-1\_2
- [4] Davide Ancona, Francesco Dagnino, and Elena Zucca. 2017. Reasoning on Divergent Computations with Coaxioms. *Proceedings of ACM on Programming Languages* 1, OOPSLA (2017), 81:1–81:26. doi:10.1145/3133905
- [5] Robert Atkey. 2018. Syntax and Semantics of Quantitative Type Theory. In *IEEE Symposium on Logic in Computer Science, LICS 2018*, Anuj Dawar and Erich Grädel (Eds.). ACM Press, 56–65. doi:10.1145/3209108.3209189
- [6] Riccardo Bianchini, Francesco Dagnino, Paola Giannini, and Elena Zucca. 2022. A Java-Like Calculus with User-Defined Coeffects. In *ICTCS'22 - Italian Conf. on Theoretical Computer Science*, Ugo Dal Lago and Daniele Gorla (Eds.), Vol. 3284. CEUR-WS.org, 66–78. <https://ceur-ws.org/Vol-3284/8563.pdf>
- [7] Riccardo Bianchini, Francesco Dagnino, Paola Giannini, and Elena Zucca. 2023. A Java-like calculus with heterogeneous coeffects. *Theoretical Computer Science* 971 (2023), 114063. doi:10.1016/j.tcs.2023.114063
- [8] Riccardo Bianchini, Francesco Dagnino, Paola Giannini, and Elena Zucca. 2023. Multi-Graded Featherweight Java. In *European Conference on Object-Oriented Programming, ECOOP 2023 (LIPIcs, Vol. 263)*, Karim Ali and Guido Salvaneschi (Eds.). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 3:1–3:27. doi:10.4230/LIPIcs.ECOOP.2023.3
- [9] Riccardo Bianchini, Francesco Dagnino, Paola Giannini, and Elena Zucca. 2023. Resource-Aware Soundness for Big-Step Semantics. *Proceedings of ACM on Programming Languages* 7, OOPSLA2 (2023), 1281–1309. doi:10.1145/3622843
- [10] Riccardo Bianchini, Francesco Dagnino, Paola Giannini, Elena Zucca, and Marco Servetto. 2022. Coeffects for sharing and mutation. *Proceedings of ACM on Programming Languages* 6, OOPSLA (2022), 870–898. doi:10.1145/3563319
- [11] Flavien Breuvar and Michele Pagani. 2015. Modelling Coeffects in the Relational Semantics of Linear Logic. In *24th EACSL Annual Conference on Computer Science Logic, CSL 2015 (LIPIcs, Vol. 41)*, Stephan Kreutzer (Ed.). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 567–581. doi:10.4230/LIPIcs.CSL.2015.567
- [12] Aloïs Brunel, Marco Gaboardi, Damiano Mazza, and Steve Zdancewic. 2014. A Core Quantitative Coeffect Calculus. In *European Symposium on Programming, ESOP 2013 (Lecture Notes in Computer Science, Vol. 8410)*, Zhong Shao (Ed.). Springer, 351–370. doi:10.1007/978-3-642-54833-8\_19
- [13] Pritam Choudhury, Harley Eades III, Richard A. Eisenberg, and Stephanie Weirich. 2021. A graded dependent type system with a usage-aware semantics. *Proceedings of ACM on Programming Languages* 5, POPL (2021), 1–32. doi:10.1145/3434331
- [14] Luca Ciccone, Francesco Dagnino, and Elena Zucca. 2021. Flexible Coinduction in Agda. In *ITP 2021 - International Conference on Interactive Theorem Proving (LIPIcs, Vol. 193)*, Liron Cohen and Cezary Kaliszyk (Eds.). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 13:1–13:19. doi:10.4230/LIPIcs.ITP.2021.13

- [15] Patrick Cousot and Radhia Cousot. 1992. Inductive Definitions, Semantics and Abstract Interpretations. In *ACM Symposium on Principles of Programming Languages, POPL 1992*, Ravi Sethi (Ed.). ACM Press, New York, 83–94. doi:10.1145/143165.143184
- [16] Francesco Dagnino. 2019. Coaxioms: flexible coinductive definitions by inference systems. *Logical Methods in Computer Science* 15, 1 (2019). doi:10.23638/LMCS-15(1:26)2019
- [17] Francesco Dagnino. 2022. A Meta-theory for Big-step Semantics. *ACM Trans. Comput. Log.* 23, 3 (2022), 20:1–20:50. doi:10.1145/3522729
- [18] Francesco Dagnino, Viviana Bono, Elena Zucca, and Mariangiola Dezani-Ciancaglini. 2020. Soundness Conditions for Big-Step Semantics. In *European Symposium on Programming, ESOP 2020 (Lecture Notes in Computer Science, Vol. 12075)*, Peter Müller (Ed.). Springer, 169–196. doi:10.1007/978-3-030-44914-8\_7
- [19] Ugo Dal Lago and Francesco Gavazzo. 2022. A relational theory of effects and coeffects. *Proceedings of ACM on Programming Languages* 6, POPL (2022), 1–28. doi:10.1145/3498692
- [20] Rocco De Nicola and Matthew Hennessy. 1984. Testing Equivalences for Processes. *Theoretical Computer Science* 34, 1 (1984), 83 – 133. doi:10.1016/0304-3975(84)90113-0
- [21] Zoltán Ésik and Werner Kuich. 2004. Inductive star-semirings. *Theoretical Computer Science* 324, 1 (2004), 3–33. doi:10.1016/J.TCS.2004.03.050
- [22] Zoltán Ésik and Hans Leiß. 2005. Algebraically complete semirings and Greibach normal form. *Annals of Pure and Applied Logic* 133, 1-3 (2005), 173–203. doi:10.1016/J.APAL.2004.10.008
- [23] Feng Feng and Young Bae Jun. 2009. Inductive semimodules and the vector modules over them. *Soft Computing* 13, 11 (2009), 1113–1121. doi:10.1007/s00500-008-0384-y
- [24] Marco Gaboardi, Shin-ya Katsumata, Dominic A. Orchard, Flavien Breuvert, and Tarmo Uustalu. 2016. Combining effects and coeffects via grading. In *ACM International Conference on Functional Programming, ICFP 2016*, Jacques Garrigue, Gabriele Keller, and Eijiro Sumii (Eds.). ACM Press, 476–489. doi:10.1145/2951913.2951939
- [25] Dan R. Ghica and Alex I. Smith. 2014. Bounded Linear Types in a Resource Semiring. In *European Symposium on Programming, ESOP 2013 (Lecture Notes in Computer Science, Vol. 8410)*, Zhong Shao (Ed.). Springer, 331–350. doi:10.1007/978-3-642-54833-8\_18
- [26] Jean-Yves Girard. 1987. Linear Logic. *Theoretical Computer Science* 50 (1987), 1–102. doi:10.1016/0304-3975(87)90045-4
- [27] Jonathan S. Golan. 2003. *Complete semirings*. Springer, 39–47 pages. doi:10.1007/978-94-017-0383-3\_3
- [28] Xavier Leroy and Hervé Grall. 2009. Coinductive big-step operational semantics. *Information and Computation* 207, 2 (2009), 284–304. doi:10.1016/j.ic.2007.12.004
- [29] Paul Blain Levy, John Power, and Hayo Thielecke. 2003. Modelling environments in call-by-value programming languages. *Information and Computation* 185, 2 (2003), 182–210. doi:10.1016/S0890-5401(03)00088-9
- [30] Daniel Marshall, Michael Vollmer, and Dominic Orchard. 2022. Linearity and Uniqueness: An Entente Cordiale. In *European Symposium on Programming, ESOP 2022 (Lecture Notes in Computer Science, Vol. 13240)*, Ilya Sergey (Ed.). Springer, 346–375. doi:10.1007/978-3-030-99336-8\_13
- [31] Conor McBride. 2016. I Got Plenty o’ Nuttin’. In *A List of Successes That Can Change the World - Essays Dedicated to Philip Wadler on the Occasion of His 60th Birthday (Lecture Notes in Computer Science, Vol. 9600)*, Sam Lindley, Conor McBride, Philip W. Trinder, and Donald Sannella (Eds.). Springer, 207–233. doi:10.1007/978-3-319-30936-1\_12
- [32] Dominic Orchard, Vilem-Benjamin Liepelt, and Harley Eades III. 2019. Quantitative program reasoning with graded modal types. *Proceedings of ACM on Programming Languages* 3, ICFP (2019), 110:1–110:30. doi:10.1145/3341714
- [33] Tomas Petricek, Dominic A. Orchard, and Alan Mycroft. 2013. Coeffects: Unified Static Analysis of Context-Dependence. In *Automata, Languages and Programming, ICALP 2013 (Lecture Notes in Computer Science, Vol. 7966)*, Fedor V. Fomin, Rusins Freivalds, Marta Z. Kwiatkowska, and David Peleg (Eds.). Springer, 385–397. doi:10.1007/978-3-642-39212-2\_35
- [34] Tomas Petricek, Dominic A. Orchard, and Alan Mycroft. 2014. Coeffects: a calculus of context-dependent computation. In *ACM International Conference on Functional Programming, ICFP 2014*, Johan Jeuring and Manuel M. T. Chakravarty (Eds.). ACM Press, 123–135. doi:10.1145/2628136.2628160
- [35] Cassia Torczon, Emmanuel Suárez Acevedo, Shubh Agrawal, Joey Velez-Ginorio, and Stephanie Weirich. 2024. Effects and Coeffects in Call-by-Push-Value. *Proc. ACM Program. Lang.* 8, OOPSLA2 (2024), 1108–1134. doi:10.1145/3689750

- [36] Victoria Vollmer, Danielle Marshall, Harley Eades III, and Dominic Orchard. 2025. A Mixed Linear and Graded Logic: Proofs, Terms, and Models. In *33rd EACSL Annual Conference on Computer Science Logic, CSL 2015 (LIPIcs, Vol. 326)*, Jörg Endrullis and Sylvain Schmitz (Eds.). Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 32:1–32:21. doi:10.4230/LIPICS.CSL.2025.32
- [37] Philip Wadler. 1990. Linear Types can Change the World!. In *Programming concepts and methods: Proceedings of the IFIP Working Group 2.2, 2.3 Working Conference on Programming Concepts and Methods*, Manfred Broy and Cliff B. Jones (Eds.). North-Holland, 561.
- [38] David Walker. 2005. Substructural Type Systems. In *Advanced Topics in Types and Programming Languages*, Benjamin C. Pierce (Ed.). The MIT Press.
- [39] James Wood and Robert Atkey. 2022. A Framework for Substructural Type Systems. In *European Symposium on Programming, ESOP 2022 (Lecture Notes in Computer Science, Vol. 13240)*, Ilya Sergey (Ed.). Springer, 376–402. doi:10.1007/978-3-030-99336-8\_14
- [40] Andrew K. Wright and Matthias Felleisen. 1994. A Syntactic Approach to Type Soundness. *Information and Computation* 115, 1 (1994), 38–94. doi:10.1006/inco.1994.1093

## 11 Proofs of Section 7

**Proof** [of Proposition 7.8] (1) We have that  $G(p) = \prod_{i \in 1..n} G(x_i, x_{i+1})$ . Then, we derive  $G(p) = \mathbf{0}$ , because  $G(x_{j-1}, x_j)$  is equal to  $\mathbf{0}$ .

(2) Let  $p \in P(x, y)$ , then, because  $x \neq y$  and  $y \notin V(G)$ , by Item 1, we have  $G(p) = \mathbf{0}$ . Hence, this proves that  $p \notin P_{\neq \mathbf{0}}^G(x, y)$ , as needed.

(3) Let  $p = x_1 \cdots x_k \in P(x, y)$  be a path with  $k \geq n + 2$ . Then we have  $G(p) = \prod_{i \in 1..k-1} G(x_i, x_{i+1})$ . We distinguish two cases. If there is  $j \in 2..k$  such that  $x_j \notin V(G)$ , then the thesis follows by Item 1. Otherwise, we have that  $x_2, \dots, x_k \in V(G)$ , but, since  $k \geq n + 2$  and  $V(G)$  has  $n$  elements, there must be a repeated variable, i.e., there are indices  $2 \leq j < h \leq k$  such that  $x_j = x_h$ . Because  $G$  is acyclic, we deduce that  $G(x_j \cdots x_h) = \prod_{i \in j..h-1} G(x_i, x_{i+1}) = \mathbf{0}$  and this implies  $G(p) = \mathbf{0}$ , as needed.

(4) It is an immediate consequence of (3).

**Proof** [of Lemma 7.12] The fact that  $(G \cdot G^*)(x, x) = (G_x \cdot G^*)(x)$  is immediate, hence we only prove that  $(G_x \cdot G^*)(x) = \mathbf{0}$ . By definition, we have

$$(G_x \cdot G^*)(x) = \sum_{y \in V} G_x(y) \cdot G^*(y, x) = \sum_{y \in V} G(x, y) \cdot G^*(y, x)$$

To conclude the proof, it suffices to show that, for each  $y \in V$ ,  $G(x, y) \cdot G^*(y, x) = \mathbf{0}$ . Indeed, we have

$$G(x, y) \cdot G^*(y, x) = G(x, y) \cdot \sum_{p \in P(y, x)} G(p) = \sum_{p \in P(y, x)} G(x, y) \cdot G(p) = \sum_{p \in P(y, x)} G(xp)$$

because  $\text{in}(p) = y$ . Then, since  $\text{out}(p) = x$ , the path  $xp$  is a cycle and so  $G(xp) = \mathbf{0}$ , because  $G$  is acyclic. Therefore, we conclude  $G(x, y) \cdot G^*(y, x) = \mathbf{0}$ , as needed.

**Proof** [of Proposition 7.13] We proceed by induction on  $n$ . If  $n = 0$ , then  $G^0 = \mathbb{I}$  and, since the only paths of length 0 have shape  $x$ , the thesis is immediate. Let  $n = k + 1$ . Using the

induction hypothesis, we derive

$$\begin{aligned}
 G^{k+1}(x, y) &= (G \cdot G^k)(x, y) = \sum_{z \in V} G(x, z) \cdot G^k(z, y) \\
 &= \sum_{z \in V} G(x, z) \cdot \sum_{p \in P_k(z, y)} G(p) = \sum_{z \in V} \sum_{p \in P_k(z, y)} G(x \cdot p) \\
 &= \sum_{p' \in P_{k+1}(x, y)} G(p')
 \end{aligned}$$

where the last step relies on the fact that  $p' \in P_{k+1}(x, y)$  iff  $p' = x \cdot p$  and  $p \in P_k(z, y)$  for some  $z \in V$ .

For the proof of Theorem 7.21, we introduce the following notations:  $\gamma \subseteq \rho$  if  $\gamma(x) = \mathbf{0}$  for each  $x \notin \text{dom}(\rho)$ , that is, the support of  $\gamma$  is a subset of the domain of  $\rho$ ;  $\gamma \parallel \rho$  if  $\gamma^a(x) = \mathbf{0}$  for all  $x \in \text{dom}(\rho)$ , that is, the support of  $\gamma$  and the domain of  $\rho$  are disjoint.

**Lemma 11.1.** *If  $\gamma \subseteq \rho$  then  $\gamma \cdot G_{\rho+\rho'} = \gamma \cdot G_\rho$ .*

**PROOF.** Consider  $x \in \text{dom}(\rho')$ . If  $x \in \text{dom}(\rho)$ , since  $\rho \parallel \rho'$ , we have  $\rho(x) = \_ : \mathcal{V}$  and  $\rho'(x) = \_ : \mathcal{V}$ , hence  $\gamma \cdot G_{\rho+\rho'}(x) = \gamma \cdot G_\rho(x)$ . If  $x \notin \text{dom}(\rho)$  we have  $\gamma \cdot G_{\rho+\rho'}(x) = \mathbf{0}$ . Hence we get the thesis.  $\square$

**Proof** [of Theorem 7.21]

We prove the following generalized statement:

If  $E \mid \rho \Rightarrow_r \mathbf{v}^{\gamma'} \mid \rho'$  then, for each  $r' \preceq r$ , there exist  $\gamma, \gamma^c, \gamma^a$ , with  $\gamma$  honest for  $E$ ,  $\gamma \subseteq \rho$ , and  $\gamma^a \parallel \rho$ , such that the following conditions hold.

- (1)  $r' \cdot \gamma' \cdot G_{\rho'}^* \preceq \gamma_{\rho'}$
- (2)  $\gamma \cdot G_\rho^* \preceq \gamma_\rho$
- (3)  $\gamma_{\rho'} + \gamma^c \preceq \gamma_\rho + \gamma^a$
- (4)  $\gamma \cdot G_\rho^* + \gamma^a \preceq r' \cdot \gamma' \cdot G_{\rho'}^* + \gamma^c$

First, we show that Item 2 is implied by Item 1, Item 3, and Item 4. Indeed

$$\begin{aligned}
 \gamma \cdot G_\rho^* + \gamma^a &\preceq \text{by Item 4} \\
 r' \cdot \gamma' \cdot G_{\rho'}^* + \gamma^c &\preceq \text{by Item 1} \\
 \gamma_{\rho'} + \gamma^c + \gamma^a &\preceq \text{by Item 3} \\
 \gamma_\rho + \gamma^a &
 \end{aligned}$$

Hence,  $\gamma \cdot G_\rho^* + \gamma^a \preceq \gamma_\rho + \gamma^a$ , and this implies  $\gamma \cdot G_\rho^* \preceq \gamma_\rho$  since  $\gamma^a \parallel \rho$ .

Then, we prove Item 1, Item 3, and Item 4 by induction on the reduction relation. We show the most relevant cases.

(VAR) We have

- (1)  $x \mid \rho \Rightarrow_r \mathcal{V} \mid \rho'$  with  $\mathcal{V} = \mathbf{v}^{\gamma'}$ ,  $\rho = \hat{\rho}$ ,  $x : \langle s, \mathcal{V} \rangle$ ,  $\rho' = \hat{\rho}$ ,  $x : \langle s', \mathcal{V} \rangle$
- (2)  $r + s' \preceq s$
- (3)  $r \cdot \gamma' \cdot G_{\rho'}^* \preceq \gamma_{\rho'}$

Take  $r' \preceq r$ . We choose  $\gamma = \gamma^c = x : r'$  and  $\gamma^a = \emptyset$ , hence  $\gamma$  honest for  $x$ ,  $\gamma \subseteq \rho$ , and  $\gamma^a \parallel \rho$  trivially hold.

**Item 1** We have  $r' \cdot \gamma' \cdot G_{\rho'}^* \preceq r \cdot \gamma' \cdot G_{\rho'}^* \preceq \gamma_{\rho'}$  from (3).

**Item 3** We have

$$\begin{aligned}
\gamma_{\rho'} + (x : r') &= \gamma_{\hat{\rho}}, x : s' + (x : r') = \\
\gamma_{\hat{\rho}}, (x : r' + s') &\preceq \gamma_{\hat{\rho}}, (x : r + s') \preceq \text{from (2)} \\
\gamma_{\hat{\rho}}, (x : s) &= \gamma_{\rho}
\end{aligned}$$

**Item 4** Noting that  $(x : r') \cdot \mathbf{G}_{\rho} = r' \cdot \gamma'$ , by Corollary 7.15 we have

$$\begin{aligned}
(x : r') \cdot \mathbf{G}_{\rho}^{\star} &= (x : r') \cdot (\mathbb{I} + \mathbf{G}_{\rho} \cdot \mathbf{G}_{\rho}^{\star}) = (x : r') + (x : r') \cdot \mathbf{G}_{\rho} \cdot \mathbf{G}_{\rho}^{\star} = \\
x : r' + r' \cdot \gamma' \cdot \mathbf{G}_{\rho}^{\star}.
\end{aligned}$$

(PAIR) We have

$$\begin{aligned}
(1) \quad v_1 \mid \rho_1 &\Rightarrow_{r \cdot r_1} \mathbf{v}_1^{\gamma'_1} \mid \rho'_1 \\
(2) \quad v_2 \mid \rho_2 &\Rightarrow_{r \cdot r_2} \mathbf{v}_2^{\gamma'_2} \mid \rho'_2 \\
(3) \quad \langle r_1 v_1, v_2 r_2 \rangle \mid \rho &\Rightarrow_r \langle r_1 \mathbf{v}_1, \mathbf{v}_2 r_2 \rangle^{\gamma'} \mid \rho'_1 + \rho'_2 \text{ with } \gamma' = r_1 \cdot \gamma'_1 + r_2 \cdot \gamma'_2 \\
(4) \quad \rho_1 + \rho_2 &\preceq \rho
\end{aligned}$$

Take  $r' \preceq r$ , hence  $r' \cdot r_1 \preceq r \cdot r_1$  and  $r' \cdot r_2 \preceq r \cdot r_2$ .

By inductive hypothesis we have that there exist  $\gamma_1, \gamma_2, \gamma_1^c, \gamma_2^c, \gamma_1^a, \gamma_2^a$ , with  $\gamma_1$  honest for  $v_1$ ,  $\gamma_2$  honest for  $v_2$ ,  $\gamma_1 \subseteq \rho_1$ ,  $\gamma_2 \subseteq \rho_2$ ,  $\gamma_1^a \parallel \rho_1$ , and  $\gamma_2^a \parallel \rho_2$ , such that

$$\begin{aligned}
1a \quad r' \cdot r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^{\star} &\preceq \gamma_{\rho'_1} \\
1b \quad r' \cdot r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_2}^{\star} &\preceq \gamma_{\rho'_2} \\
2a \quad \gamma_1 \cdot \mathbf{G}_{\rho_1}^{\star} &\preceq \gamma_{\rho_1} \\
2b \quad \gamma_2 \cdot \mathbf{G}_{\rho_2}^{\star} &\preceq \gamma_{\rho_2} \\
3a \quad \gamma_{\rho'_1} + \gamma_1^c &\preceq \gamma_{\rho_1} + \gamma_1^a \\
3b \quad \gamma_{\rho'_2} + \gamma_2^c &\preceq \gamma_{\rho_2} + \gamma_2^a \\
4a \quad \gamma_1 \cdot \mathbf{G}_{\rho_1}^{\star} + \gamma_1^a &\preceq r' \cdot r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^{\star} + \gamma_1^c \\
4b \quad \gamma_2 \cdot \mathbf{G}_{\rho_2}^{\star} + \gamma_2^a &\preceq r' \cdot r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_2}^{\star} + \gamma_2^c
\end{aligned}$$

We choose  $\gamma = \gamma_1 + \gamma_2$ ,  $\gamma^c = \gamma_1^c + \gamma_2^c$ , and  $\gamma^a = \gamma_1^a + \gamma_2^a$ . Clearly  $\gamma$  is honest for  $\langle r_1 v_1, v_2 r_2 \rangle$ ,  $\gamma \subseteq \rho$ , and  $\gamma^a \parallel \rho$ .

**Item 1** We have

$$\begin{aligned}
r' \cdot (r_1 \cdot \gamma'_1 + r_2 \cdot \gamma'_2) \cdot \mathbf{G}_{\rho'_1 + \rho'_2}^{\star} &= \\
r' \cdot r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1 + \rho'_2}^{\star} + r' \cdot r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_1 + \rho'_2}^{\star} &= \text{by Lemma 11.1 since } \gamma'_1 \subseteq \rho'_1 \\
\text{and } \gamma'_2 \subseteq \rho'_2 & \\
r' \cdot r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^{\star} + r' \cdot r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_2}^{\star} &\preceq \text{by [1a] and [1b]} \\
\gamma_{\rho'_1} + \gamma_{\rho'_2} &= \gamma_{\rho'_1 + \rho'_2}
\end{aligned}$$

**Item 3** We have to prove  $\gamma_{\rho'_1 + \rho'_2} + \gamma^c \preceq \gamma_{\rho} + \gamma^a$ . We have:

$$\begin{aligned}
\gamma_{\rho'_1 + \rho'_2} + \gamma_1^c + \gamma_2^c &= \gamma_{\rho'_1} + \gamma_{\rho'_2} + \gamma_1^c + \gamma_2^c \preceq \text{by [3a] and [3b]} \\
\gamma_{\rho_1} + \gamma_1^a + \gamma_{\rho_2} + \gamma_2^a &= \gamma_{\rho_1 + \rho_2} + \gamma^a
\end{aligned}$$

**Item 4** We have to prove  $(\gamma_1 + \gamma_2) \cdot \mathbf{G}_{\rho}^{\star} + \gamma^a \preceq r' \cdot (r_1 \cdot \gamma'_1 + r_2 \cdot \gamma'_2) \cdot \mathbf{G}_{\rho'}^{\star} + \gamma^c$ . We have

$$\begin{aligned}
(\gamma_1 + \gamma_2) \cdot \mathbf{G}_{\rho}^{\star} + \gamma_1^a + \gamma_2^a &= \\
\gamma_1 \cdot \mathbf{G}_{\rho}^{\star} + \gamma_2 \cdot \mathbf{G}_{\rho}^{\star} + \gamma_1^a + \gamma_2^a &= \text{by Lemma 11.1 since } \gamma_1 \subseteq \rho_1 \text{ and } \gamma_2 \subseteq \rho_2 \\
\gamma_1 \cdot \mathbf{G}_{\rho_1}^{\star} + \gamma_2 \cdot \mathbf{G}_{\rho_2}^{\star} + \gamma_1^a + \gamma_2^a &\preceq \text{by [4a] and [4b]} \\
r' \cdot r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^{\star} + \gamma_1^c + r' \cdot r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_2}^{\star} + \gamma_2^c & \\
r' \cdot (r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^{\star} + r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'_2}^{\star}) + \gamma^c &= \text{by Lemma 11.1 since } \gamma'_1 \subseteq \rho'_1 \text{ and } \\
\gamma'_2 \subseteq \rho'_2 &
\end{aligned}$$

$$\begin{aligned} & r' \cdot (r_1 \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'}^* + r_2 \cdot \gamma'_2 \cdot \mathbf{G}_{\rho'}^*) + \gamma^c = \\ & r' \cdot (r_1 \cdot \gamma'_1 + r_2 \cdot \gamma'_2) \cdot \mathbf{G}_{\rho'}^* + \gamma^c \end{aligned}$$

(LET) We have

- (1)  $e_1 \mid \rho_1 \Rightarrow_s \mathbf{v}_1^{\gamma'_1} \mid \rho'_1$
- (2)  $e_2[x'/x] \mid \hat{\rho} \Rightarrow_r \mathbf{v}^{\gamma'} \mid \rho'$  with  $\hat{\rho} = (\rho'_1 + \rho_2)$ ,  $x' : \langle s, \mathbf{v}_1^{\gamma'_1} \rangle$ ,  $x'$  fresh
- (3)  $\text{let } x = e_1 \text{ in } e_2 \mid \rho \Rightarrow_r \mathbf{v}^{\gamma'} \mid \rho'$
- (4)  $\rho_1 + \rho_2 \preceq \rho$

Take  $r' \preceq r$ . By inductive hypothesis we have that, for each  $s' \preceq s$ , there exist  $\gamma_1, \gamma_2, \gamma_1^c, \gamma_2^c, \gamma_1^a, \gamma_2^a$ , with  $\gamma_1$  honest for  $e_1$ ,  $\gamma_2$  honest for  $e_2[x'/x]$ ,  $\gamma_1 \subseteq \rho_1$ ,  $\gamma_2 \subseteq \hat{\rho}$ ,  $\gamma_1^a \parallel \rho_1$ , and  $\gamma_2^a \parallel \hat{\rho}$ , such that

- 1a  $s' \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^* \preceq \gamma_{\rho'_1}$
- 1b  $r' \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* \preceq \gamma_{\rho'}$
- 3a  $\gamma_{\rho'_1} + \gamma_1^c \preceq \gamma_{\rho_1} + \gamma_1^a$
- 3b  $\gamma_{\rho'} + \gamma_2^c \preceq \gamma_{\hat{\rho}} + \gamma_2^a$
- 4a  $\gamma_1 \cdot \mathbf{G}_{\rho_1}^* + \gamma_1^a \preceq s \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^* + \gamma_1^c$
- 4b  $\gamma_2 \cdot \mathbf{G}_{\hat{\rho}}^* + \gamma_2^a \preceq r \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* + \gamma_2^c$

**Item 1** We have to prove  $r' \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* \preceq \gamma_{\rho'}$ , and this is [1b].

**Item 3** We choose  $\gamma^c = \gamma_1^c + \gamma_2^c$ ,  $\gamma^a = \gamma_1^a + \gamma_2^a + x' : s$ . Clearly  $\gamma^a \parallel \rho$ . We have to prove

$$\gamma_{\rho'} + \gamma_1^c + \gamma_2^c \preceq \gamma_{\rho} + \gamma_1^a + \gamma_2^a + x' : s.$$

We have

$$\begin{aligned} & \gamma_{\rho'} + \gamma_1^c + \gamma_2^c \preceq \text{by [3b]} \\ & \gamma_{\hat{\rho}} + \gamma_2^a + \gamma_1^c = \gamma_{\rho'_1} + \gamma_{\rho_2} + (x' : s) + \gamma_2^a + \gamma_1^c \preceq \text{by [3a]} \\ & \gamma_{\rho_1} + \gamma_1^a + \gamma_{\rho_2} + (x' : s) + \gamma_2^a \preceq \gamma_{\rho} + \gamma_1^a + \gamma_2^a + (x' : s) \end{aligned}$$

**Item 4** We have to prove that there exist  $\gamma$  such that

$$\gamma \cdot \mathbf{G}_{\rho}^* + \gamma_1^a + \gamma_2^a + (x' : s') \preceq r' \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* + \gamma_1^c + \gamma_2^c$$

Since  $\gamma_2 \cdot \mathbf{G}_{\rho_2}^* \preceq \gamma_{\rho_2}$  follows from [1b], [3b], and [4b], and  $x'$  is fresh,  $\gamma_2(x') = s' \preceq s$ . Hence, there exists  $\gamma_1$  such that [4a] holds for such  $s'$ , that is,  $\gamma_1 \cdot \mathbf{G}_{\rho_1}^* + \gamma_1^a \preceq s' \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^* + \gamma_1^c$ .

Let us decompose  $\gamma_2$  as  $\gamma_2 = \gamma_2^{\rho} + \gamma_2^{\bar{\rho}}$  such that  $\gamma_2^{\rho} \subseteq \rho$  and  $\gamma_2^{\bar{\rho}} \parallel \rho$ . Moreover:

$$(\star) \quad \gamma_2^{\bar{\rho}} \cdot \mathbf{G}_{\hat{\rho}}^* = (x' : s') + s' \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^*$$

Then, we choose  $\gamma = \gamma_1 + \gamma_2^{\rho}$ , and we have:

$$\begin{aligned} & (\gamma_1 + \gamma_2^{\rho}) \cdot \mathbf{G}_{\rho}^* + \gamma_1^a + \gamma_2^a + (x' : s') = \text{since } \gamma_1 \subseteq \rho_1 \text{ and } \gamma_2^{\rho} \subseteq \hat{\rho} \\ & \gamma_1 \cdot \mathbf{G}_{\rho_1}^* + \gamma_2^{\rho} \cdot \mathbf{G}_{\hat{\rho}}^* + \gamma_1^a + \gamma_2^a + (x' : s') \preceq \text{from [4a]} \\ & s' \cdot \gamma'_1 \cdot \mathbf{G}_{\rho'_1}^* + \gamma_1^c + \gamma_2^{\rho} \cdot \mathbf{G}_{\hat{\rho}}^* + \gamma_2^a + (x' : s') = \text{from } (\star) \\ & \gamma_1^c + \gamma_2 \cdot \mathbf{G}_{\hat{\rho}}^* + \gamma_2^a \preceq \text{from [4b]} \\ & \gamma_1^c + r \cdot \gamma' \cdot \mathbf{G}_{\rho'}^* + \gamma_2^c \end{aligned}$$

**Proof** [of Proposition 7.24] If  $\gamma \vdash \rho \triangleright \Delta$  then  $\gamma_{\Delta} + \gamma_{\rho} \cdot \mathbf{G}_{\rho} \preceq \gamma_{\rho}$ .

Set  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$ . To derive  $\gamma \vdash \rho \triangleright \Delta$  we have necessarily applied rule (T-ENV), and then (T-VAL) to the premises, hence  $\gamma_{\gamma} = x_1 : r_1, \dots, x_n : r_n$ , and, for some  $\gamma_1, \dots, \gamma_n$ , we have  $\gamma_i \preceq \gamma_{\gamma_i}$  for  $i \in 1..n$ , and  $\Delta + \sum_{i \in 1..n} r_i \cdot \gamma_i \preceq \gamma$ . From the last condition,

$\gamma_\Delta + \sum_{i \in 1..n} r_i \cdot \gamma_i \preceq \gamma_\gamma$ , hence, since  $\gamma_\gamma = \gamma_\rho$ , we get  $\gamma_\Delta + \sum_{i \in 1..n} r_i \cdot \gamma_i \preceq \gamma_\rho$ . Finally, we show that  $\sum_{i \in 1..n} r_i \cdot \gamma_i = \gamma_\rho \cdot \mathbf{G}_\rho$ . Indeed, for  $i \in 1..n$ ,  $r_i = \gamma_\rho(x_i)$ , and  $\gamma_i(x) = \mathbf{G}_\rho(x_i, x)$ , hence we have  $(\sum_{i \in 1..n} r_i \cdot \gamma_i)(x) = \sum_{i \in 1..n} \gamma_\rho(x_i) \cdot \mathbf{G}_\rho(x_i, x)$ , which is equal to  $(\gamma_\rho \cdot \mathbf{G}_\rho)(x) = \sum_{y \in V} \gamma_\rho(y) \cdot \mathbf{G}_\rho(y, x)$  since  $\gamma_\rho(y) \neq \mathbf{0}$  implies  $y = x_i$  for some  $i \in 1..n$ .

## 12 Proofs of Section 8

**Lemma 12.1** (Inversion for value expressions).

- (1) If  $\Gamma \vdash x : \tau^r$  then  $\Gamma = x :_{r'} \tau, \Gamma'$  and  $x :_{r'} \tau \preceq \Gamma$  and  $r \preceq r'$ .
- (2) If  $\Gamma \vdash \text{recf}.\lambda x.e : \tau^r$  then  $r' \cdot \Gamma' \preceq \Gamma$  and  $\tau = \tau_1^{r_1} \rightarrow_s \tau_2^{r_2}$  such that  $\Gamma', f :_s \tau_1^{r_1} \rightarrow_s \tau_2^{r_2}, x :_{r_1} \tau_1 \vdash e : \tau_2^{r_2}$  and  $r \preceq r'$ .
- (3) If  $\Gamma \vdash \text{unit} : \tau^r$  then  $\tau = \text{Unit}$  and  $\mathbf{0} \preceq \Gamma$ .
- (4) If  $\Gamma \vdash \langle r_1 v_1, v_2 r_2 \rangle : \tau^r$  then  $r' \cdot (\Gamma_1 + \Gamma_2) \preceq \Gamma$ ,  $\tau = \tau_1^{r_1} \otimes \tau_2^{r_2}$  and  $r \preceq r'$  such that  $\Gamma_1 \vdash v_1 : \tau_1^{r_1}, \Gamma_2 \vdash v_2 : \tau_2^{r_2}$ .
- (5) If  $\Gamma \vdash \text{inl}^{r_1} v : \tau^r$  then  $r' \cdot \Gamma' \preceq \Gamma$ ,  $\tau = \tau_1^{r_1} + \tau_2^{r_2}$  and  $r \preceq r'$  such that  $\Gamma' \vdash v : \tau_1^{r_1}$ .
- (6) If  $\Gamma \vdash \text{inr}^{r_2} v : \tau^r$  then  $r' \cdot \Gamma' \preceq \Gamma$ ,  $\tau = \tau_1^{r_1} + \tau_2^{r_2}$  and  $r \preceq r'$  such that  $\Gamma' \vdash v : \tau_2^{r_2}$ .

**Lemma 12.2** (Canonical Forms).

- (1) If  $\Gamma \vdash v : (\tau_1^{r_1} \rightarrow_s \tau_2^{r_2})^{r_3}$  then  $v = \text{recf}.\lambda x.e$ .
- (2) If  $\Gamma \vdash v : \text{Unit}$  then  $v = \text{unit}$ .
- (3) If  $\Gamma \vdash v : (\tau_1^{r_1} \otimes \tau_2^{r_2})^{r_3}$  then  $v = \langle r_1 v_1, v_2 r_2 \rangle$ .
- (4) If  $\Gamma \vdash v : (\tau_1^{r_1} + \tau_2^{r_2})^r$  then  $v = \text{inl}^{r_1} v_1$  or  $v = \text{inr}^{r_2} v_2$ .

**Lemma 12.3** (Renaming). If  $\Gamma, x :_{r_1} \tau_1 \vdash e : \tau_2^{r_2}$  then  $\Gamma, x' :_{r_1} \tau_1 \vdash e[x'/x] : \tau_2^{r_2}$  with  $x'$  fresh.

**Lemma 12.4.** If  $\gamma = \gamma_1 + \gamma_2$  then  $\gamma \cdot \mathbf{G}_\rho^\star = (\gamma_1 \cdot \mathbf{G}_\rho^\star) + (\gamma_2 \cdot \mathbf{G}_\rho^\star)$ .

**Lemma 12.5.** Given  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$ ,  $\Gamma = x_1 :_{r_1} \tau_1^{r_1}, \dots, x_n :_{r_n} \tau_n^{r_n}$ ,  $\Delta \preceq \Gamma$  and for all  $i \in 1..n$  it exists  $\Gamma_i$  such that  $\Gamma_i \vdash \mathbf{v}_i^{\gamma_i} : \tau_i^{r_i}$  and  $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$  then  $\Gamma \vdash \rho \triangleright \Delta$ .

**Lemma 12.6** (Environment splitting). If  $\Gamma \vdash \rho \triangleright \Delta$  and  $\Delta_1 + \Delta_2 \preceq \Delta$ , then there are  $\rho_1$  and  $\rho_2$  such that  $\rho_1 + \rho_2 \preceq \rho$  and  $\Gamma_1 \vdash \rho_1 \triangleright \Delta_1$  and  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$  and these are consistent.

PROOF. Let  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$  and  $\Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$ . From rule (T-ENV),  $\sum_{i \in 1..n} r_i \cdot \Gamma'_i + \Delta \preceq \Gamma$  where  $\Gamma'_i \vdash \mathbf{v}_i^{\gamma_i} : \tau_i^{\mathbf{1}}$  and  $\gamma_i \preceq \gamma_{\Gamma'_i}$ , by rule (T-VAL).

Let  $\gamma'_i = \gamma_{\Delta_i} \cdot \mathbf{G}_\rho^\star$  and  $\rho_i = x_1 : \langle \gamma'_i(x_1), \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle \gamma'_i(x_n), \mathbf{v}_n^{\gamma_n} \rangle$  for  $i = 1, 2$ . From  $\Delta_1 + \Delta_2 \preceq \Delta$  and  $\gamma_\Delta \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$  we get  $\gamma_{\Delta_1 + \Delta_2} \cdot \mathbf{G}_\rho^\star \preceq \gamma_\rho$ . Therefore  $\rho_1 + \rho_2 \preceq \rho$ . Let  $\Gamma_i = x_1 :_{\gamma'_i(x_1)} \tau_1, \dots, x_n :_{\gamma'_i(x_n)} \tau_n$ , since  $\mathbf{G}_\rho^\star = \mathbf{G}_{\rho_i}^\star$  and by definition  $\gamma_{\rho_i} \cdot \mathbf{G}_\rho^\star = \gamma_{\rho_i} \cdot \mathbf{G}_{\rho_i}^\star = \gamma_{\rho_i}$ , applying Lemma 12.5 we get  $\Gamma_i \vdash \rho_i \triangleright \Delta_i$ .

□

**Proof** [of Theorem 8.2] Let  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$  and  $\Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$ . From rule (T-RES), for some  $\Delta$ , we get  $\Delta \vdash v : \tau^r$  and  $\Gamma \vdash \rho \triangleright \Delta$ . From rule (T-ENV),  $\sum_{i \in 1..n} r_i \cdot \Gamma_i + \Delta \preceq \Gamma$  where  $\Gamma_i \vdash \mathbf{v}_i^{\gamma_i} : \tau_i^{\mathbf{1}}$  and  $\gamma_i \preceq \gamma_{\Gamma_i}$ , by rule (T-VAL).

By induction on the syntax of  $v$ . We show only relevant cases.

$v = x$  From  $\Delta \vdash x : \tau^r$  and  $\Delta \preceq \Gamma$  then  $x = x_k$  for some  $k \in 1..n$  and  $\tau_k = \tau$  and  $r_k = s$  and  $\Delta \vdash x_k : \tau^r$ . By Lemma 12.1(1)  $\Delta = x_k :_{r'} \tau_k, \Delta'$  with  $r \preceq r'$ . Let  $s' = \sum_{i \in 1..n} s_i$  where  $s_i = r_i \cdot r_{i,k}$  and

$$\rho' = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_k : \langle s', \mathbf{v}_k^{\gamma_k} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle.$$

We want to prove that  $\Gamma' \vdash \mathbf{v}^{\gamma_k} \mid \rho' : \tau_k^r$  where  $\Gamma'$  is  $\Gamma$  in which  $r_k$  is substituted by  $s'$ . Let  $\Delta'' = r \cdot \Gamma_k$ , from  $\Gamma_k \vdash \mathbf{v}_k^{\gamma_k} : \tau^1$  we get  $\Delta'' \vdash \mathbf{v}_k^{\gamma_k} : \tau^r$ . Let  $\Gamma_0 = \sum_{i \in 1..n \wedge i \neq k} r_i \cdot \Gamma_i$ . From  $\sum_{i \in 1..n} r_i \cdot \Gamma_i + \Delta = \Gamma'' + s \cdot \Gamma_k + \Delta \preceq \Gamma$  we have that  $r + s' \preceq s$ . Therefore  $\Delta'' + s' \cdot \Gamma_k = (r + s') \cdot \Gamma_k \preceq s \cdot \Gamma_k$  and  $\Delta'' + \Gamma'' + s' \cdot \Gamma_k \preceq \sum_{i \in 1..n} r_i \cdot \Gamma_i + \Delta$ . Since  $\Gamma(x_i) = \Gamma'(x_i)$  for all  $i \in 1..n$  and  $i \neq k$  and  $(\Delta'' + \Gamma'' + s' \cdot \Gamma_k)(x) = s'$  we have that  $\Delta'' + \Gamma'' + s' \cdot \Gamma_k \preceq \Gamma'$ . Applying rule (T-RES) we get  $\Gamma' \vdash \mathbf{v}^{\gamma_k} \mid \rho' : \tau_k^r$ . Finally from Theorem 7.27(2) we get  $r \cdot \gamma_k \preceq_{\text{nw}}^* \rho'$ , so rule (VAR) can be applied and  $x \mid \rho \Rightarrow_r \mathbf{v}^{\gamma_k} \mid \rho'$ .

For function and unit values the result derives from Theorem 7.27(2).

$v = \langle^{s_1} v_1, v_2^{s_2} \rangle$  From  $\Delta \vdash \langle^{s_1} v_1, v_2^{s_2} \rangle : \tau^r$  for some  $\Delta$ . By Lemma 12.1(4) for some  $\Delta_1$  and  $\Delta_2$  and  $r'$  we get  $r' \cdot (\Delta_1 + \Delta_2) \preceq \Delta$ ,  $\tau = \tau_1^{r_1} \otimes \tau_2^{s_2}$  and  $r \preceq r'$  and  $\Delta_i \vdash v_i : \tau_i^{s_i}$  for  $i = 1, 2$ . From  $r' \cdot (\Delta_1 + \Delta_2) \preceq \Delta$  and  $r \preceq r'$  we get  $(r \cdot \Delta_1) + (r \cdot \Delta_2) \preceq \Delta$  and from  $\Gamma \vdash \rho \triangleright \Delta$  and Lemma 12.6 we have that there are  $\rho_1$  and  $\rho_2$  such that  $\rho_1 + \rho_2 \preceq \rho$  and  $\Gamma'_1 \vdash \rho_1 \triangleright r \cdot \Delta_1$  and  $\Gamma'_2 \vdash \rho_2 \triangleright r \cdot \Delta_2$  and these are consistent. Therefore from  $r \cdot \Delta_i \vdash v_i : \tau_i^{r \cdot s_i}$  and  $\Gamma'_i \vdash \rho_i \triangleright r \cdot \Delta_i$ , applying rule (T-CONF) we get  $\Gamma'_i \vdash v_i \mid \rho_i : \tau_i^{r \cdot s_i}$ . By inductive hypotheses  $v_i \mid \rho_i \Rightarrow_{r \cdot s_i} \mathbf{v}_i^{\gamma_i''} \mid \rho_i'$  and therefore  $\langle^{s_1} v_1, v_2^{s_2} \rangle \mid \rho \Rightarrow_r \langle^{s_1} v_1, v_2^{s_2} \rangle^{\gamma_1'' + \gamma_2''} \mid (\rho_1' + \rho_2')$ .

**Lemma 12.7** (Inversion for possibly diverging expressions).

- (1) If  $\Gamma \vdash \text{return } v : \tau^r$  then  $\Gamma' \vdash v : \tau^{r'}$  with  $r \preceq r'$ ,  $\Gamma' \preceq \Gamma$  and  $r' \neq \mathbf{0}$ .
- (2) If  $\Gamma \vdash \text{let } x = e_1 \text{ in } e_2 : \tau^r$  then  $\Gamma_1 \vdash e_1 : \tau_1^{r_1}$  and  $\Gamma_2, x :_{r_1} \tau_1 \vdash e_2 : \tau^{r'}$  and  $\Gamma_1 + \Gamma_2 \preceq \Gamma$  and  $r \preceq r'$ .
- (3) If  $\Gamma \vdash v_1 v_2 : \tau_2^r$  then we have  $\Gamma_1 + \Gamma_2 \preceq \Gamma$  and  $r \preceq r' \cdot r_2$  such that  $\Gamma_1 \vdash v_1 : (\tau_1^{r_1} \rightarrow_s \tau_2^{r_2})^{r' + r' \cdot s}$  and  $\Gamma_2 \vdash v_2 : \tau_1^{r' \cdot r_1}$  and  $r' \neq \mathbf{0}$ .
- (4) If  $\Gamma \vdash \text{match } v \text{ with unit } \rightarrow e : \tau^r$  then we have  $\Gamma_1 + \Gamma_2 \preceq \Gamma$  and  $r \preceq t$  such that  $\Gamma_1 \vdash v : \text{Unit}^{r'}$  and  $\Gamma_2 \vdash e : \tau^t$ .
- (5) If  $\Gamma \vdash \text{match } v \text{ with } \langle x, y \rangle \rightarrow e : \tau^r$  then we have  $\Gamma_1 + \Gamma_2 \preceq \Gamma$  and  $r \preceq t$  such that  $\Gamma_1 \vdash v : (\tau_1^{r_1} \otimes \tau_2^{r_2})^s$  and  $\Gamma_2, x :_{s \cdot r_1} \tau, y :_{s \cdot r_2} \tau_2 \vdash e : \tau^t$  and  $s \neq \mathbf{0}$ .
- (6) If  $\Gamma \vdash \text{match } v \text{ with inl } x \rightarrow e_1 \text{ or inr } x \rightarrow e_2 : \tau^r$  then we have  $\Gamma_1 + \Gamma_2 \preceq \Gamma$  and  $r \preceq s$  such that  $\Gamma_1 \vdash v : (\tau_1^{r_1} + \tau_2^{r_2})^{r'}$ ,  $\Gamma_2, x :_{r' \cdot r_1} \tau_1 \vdash e_1 : \tau^s$ ,  $\Gamma_2, x :_{r' \cdot r_2} \tau_2 \vdash e_2 : \tau^s$  and  $r' \neq \mathbf{0}$ .

**Lemma 12.8** (Environment extension). If  $\Gamma_1 \vdash \rho_1 \triangleright \Delta_1$  and  $\Gamma_2 \vdash \mathcal{V} \mid \rho_2 : \tau^r$  and these are consistent, then  $\rho = \rho_1 + \rho_2$  and  $\Gamma = \Gamma_1 + \Gamma_2$ , then  $\Gamma, x :_r \tau \vdash \rho, x : \langle r, \mathcal{V} \rangle \triangleright \Delta_1, x :_r \tau$ .

PROOF. By consistency, we know that  $\rho = \rho_1 + \rho_2$  and  $\Gamma = \Gamma_1 + \Gamma_2$  are well defined. Let  $\rho = x_1 : \langle r_1, \mathbf{v}_1^{\gamma_1} \rangle, \dots, x_n : \langle r_n, \mathbf{v}_n^{\gamma_n} \rangle$  and  $\Gamma = x_1 :_{r_1} \tau_1, \dots, x_n :_{r_n} \tau_n$  and suppose, without loss of generality, that there are  $\leq h \leq k \leq n + 1$  such that  $\text{dom}(\rho_1) \cap \text{dom}(\rho_2) = \{x_1, \dots, x_{h-1}\}$ ,  $\text{dom}(\rho_1) \setminus \text{dom}(\rho_2) = \{x_h, \dots, x_{k-1}\}$  and  $\text{dom}(\rho_2) \setminus \text{dom}(\rho_1) = \{x_k, \dots, x_n\}$ . Hence, for all  $i \in 1..h - 1$ , we have  $r_i = r'_i + r''_i$  where  $\Gamma_1(x_i) = \langle r'_i, \tau_i \rangle$  and  $\Gamma_2(x_i) = \langle r''_i, \tau_i \rangle$  and similarly for the environments. By Rule (T-CONF), we know that  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$  and  $\Delta_2 \vdash \mathcal{V} : \tau^r$ . By consistency and Rules (T-ENV) and (T-VAL), we deduce that, for all  $i \in 1..n$ ,  $\Theta_i \vdash \mathbf{v}_i : r_i \tau_i$ .

and the following inequalities hold:

$$\begin{aligned}\Delta_1 + \sum_{i=1}^{h-1} r'_i \cdot \Theta_i + \sum_{i=h}^{k-1} r_i \cdot \Theta_i &\preceq \Gamma_1 \\ \Delta_2 + \sum_{i=1}^{h-1} r''_i \cdot \Theta_i + \sum_{i=k}^n r_i \cdot \Theta_i &\preceq \Gamma_2\end{aligned}$$

Combining these inequalities, we derive

$$\Delta_1 + \Delta_2 + \sum_{i=1}^n r_i \cdot \Theta_i \preceq \Gamma_1 + \Gamma_2 = \Gamma$$

Therefore, since  $x \notin \text{dom}(\rho)$ , by Rule (T-ENV) we immediately get the thesis.  $\square$

**Proof** [of Theorem 8.10] We have  $\Gamma \vdash e \mid \rho : \tau^r$ . By rule (T-CONF) we have  $\Gamma \vdash \rho \triangleright \Delta$  and  $\Delta \vdash e : \tau^r$ . Proof is by case analysis on  $e$ . We show only one case for the sake of brevity, since other ones are similar.

$e = \text{let } x = e_1 \text{ in } e_2$  By Lemma 12.7(2) we have  $\Delta_1 \vdash e_1 : \tau_1^{r_1}$  and  $\Delta_2, x :_{r_1} \tau_1 \vdash e_2 : \tau^{r'}$  and  $\Delta_1 + \Delta_2 \preceq \Delta$  and  $r \preceq r'$ . By Lemma 12.6 we have  $\rho_1$  and  $\rho_2$  such that  $\rho_1 + \rho_2 \preceq \rho$  and  $\Gamma_1 \vdash \rho_1 \triangleright \Delta_1$  and  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$ . By rule (T-CONF) we have  $\Gamma_1 \vdash e_1 \mid \rho_1 : \tau_1^{r_1}$ . We have two cases:

- $\nexists \mathcal{V} \mid \rho'_1$  such that  $e_1 \mid \rho_1 \Rightarrow_{r_1} \mathcal{V} \mid \rho'_1$  By applying rule (LET-DIV1) we have the thesis.
- $\exists \mathcal{V} \mid \rho'_1$  such that  $e_1 \mid \rho_1 \Rightarrow_{r_1} \mathcal{V} \mid \rho'_1$

Since we have  $e_1 \mid \rho_1 \Rightarrow_{r_1} \mathcal{V} \mid \rho'_1$  we also have  $e_1 \mid \tilde{\rho}_1 \Rightarrow \mathcal{V} \mid \tilde{\rho}'_1$  with  $\text{erase}(\rho_1) = \tilde{\rho}_1$  and  $\text{erase}(\rho'_1) = \tilde{\rho}'_1$ . By Theorem 8.11 we have  $\Gamma'_1 \vdash \mathcal{V} \mid \rho'_1 : \tau_1^{r_1}$ . Since  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$  and  $\Gamma'_1 \vdash \mathcal{V} \mid \rho'_1 : \tau_1^{r_1}$  and  $\hat{\rho} = \rho_1 + \rho_2$  and  $\Gamma' = \Gamma'_1 + \Gamma_2$ , then  $\Gamma', x :_{r_1} \tau_1 \vdash \hat{\rho}, x : \langle r_1, \mathcal{V} \rangle \triangleright \Delta_2, x :_{r_1} \tau_1$ . By renaming we have  $\Gamma', x' :_{r_1} \tau_1 \vdash \hat{\rho}, x' : \langle r_1, \mathcal{V} \rangle \triangleright \Delta_2, x' :_{r_1} \tau_1$ . By Lemma 12.3 we have  $\Delta_2, x' :_{r_1} \tau_1 \vdash e_2[x'/x] : \tau^{r'}$ . By (T-CONF) and (T-SUB) we have  $\Gamma', x' :_{r_1} \tau_1 \vdash e_2[x'/x] \mid \hat{\rho}, x' : \langle r_1, \mathcal{V} \rangle : \tau^r$ .

If  $\nexists \mathcal{V}_2 \mid \rho_3$  such that  $e_2[x'/x] \mid \hat{\rho}, x' : \langle r_1, \mathcal{V} \rangle \Rightarrow_r \mathcal{V}_2 \mid \rho_3$  then by rule (LET/LET-DIV2) we have the thesis, otherwise we have an absurd, since if  $\mathcal{V}_2 \mid \rho_3$  would exists then, by rule (LET/LET-DIV2) also  $c \Rightarrow_r \mathcal{V}_2 \mid \rho_3$ .

**Proof** [of Theorem 8.11]

By induction on the syntax of  $e$ . We show the case  $e = \text{let } x = e_1 \text{ in } e_2$ .

From rule (T-CONF), for some  $\Delta$ , we get  $\Delta \vdash e : \tau^r$  and  $\Gamma \vdash \rho \triangleright \Delta$ . From  $\Delta \vdash \text{let } x = e_1 \text{ in } e_2 : \tau^r$  and Lemma 12.7(2) we get  $\Delta_1 \vdash e_1 : \tau_1^{s_1}$  and  $\Delta_2, x :_{s_1} \tau_1 \vdash e_2 : \tau^{r'}$  and  $\Delta_1 + \Delta_2 \preceq \Delta$  and  $r \preceq r'$ . From  $\text{let } x = e_1 \text{ in } e_2 \mid \tilde{\rho} \Rightarrow \mathbf{v} \mid \tilde{\rho}'$  we get  $e_1 \mid \rho_1 \Rightarrow \mathbf{v}'_1 \mid \tilde{\rho}'_1$  and  $e_2[x'/x] \mid (\tilde{\rho}'_1 + \tilde{\rho}_2), x : \mathbf{v}'_1 \Rightarrow \mathbf{v} \mid \tilde{\rho}'$  with  $\tilde{\rho}'_1 + \tilde{\rho}_2 = \tilde{\rho}$  with  $\tilde{\rho} = \text{erase}(\rho)$ .

From Lemma 12.6, there are  $\rho_1$  and  $\rho_2$  such that  $\rho_1 + \rho_2 \preceq \rho$  and  $\Gamma_1 \vdash \rho_1 \triangleright \Delta_1$  and  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$  and  $\rho_1$  and  $\rho_2$  are consistent. By rule (T-CONF) we have  $\Gamma_1 \vdash e_1 \mid \rho_1 : \tau_1^{s_1}$ . Applying the inductive hypothesis to  $e_1$ , with  $e_1 \mid \rho_1 \Rightarrow \mathbf{v}'_1 \mid \tilde{\rho}'_1$ , we get that there are  $\rho'_1, \gamma_1$  and  $\Gamma'_1$  such that

- (1)  $e_1 \mid \rho'_1 \Rightarrow_{s_1} \mathbf{v}_1^{\gamma_1} \mid \rho'_1$  with  $\text{erase}(\rho'_1) = \tilde{\rho}'_1$  and
- (2)  $\Gamma'_1 \vdash \mathbf{v}_1^{\gamma_1} \mid \rho'_1 : \tau_1^{s_1}$  and
- (3) and  $\rho_1$  and  $\rho'_1$  are consistent.

From  $\Gamma_2 \vdash \rho_2 \triangleright \Delta_2$ , (2), (3) and Lemma 12.8 we get that,

- (4)  $(\Gamma'_1 + \Gamma_2), x' :_{s_1} \tau_1 \vdash (\rho'_1 + \rho_2), x' : \langle s_1, \mathbf{v}_1^{\gamma_1} \rangle \triangleright \Delta_2, x' :_{s_1} \tau_1$

Let  $e'_2 = e_2[x'/x]$ , from  $\Delta_2, x :_{s_1} \tau_1 \vdash e_2 : \tau^{r'}$  and Lemma 12.3 we get  $\Delta_2, x' :_{s_1} \tau_1 \vdash e_2[x'/x] : \tau^{r'}$  and  $\Delta_2, x' :_{s_1} \tau_1 \vdash e_2[x'/x] : \tau^r$  by rule (T-SUB). Therefore from (4) we get

$$(5) \quad (\Gamma'_1 + \Gamma_2), x' :_{s_1} \tau_1 \vdash e'_2 \mid (\rho'_1 + \rho_2), x' : \langle s_1, \mathbf{v}_1^{\gamma_1} \rangle : \tau^r$$

Let  $\rho'_2 = (\rho'_1 + \rho_2), x' : \langle s_1, \mathbf{v}_1^{\gamma_1} \rangle$ . Applying the inductive hypothesis to  $e'_2$ , (5) with  $e'_2[x'/x] \mid (\tilde{\rho}'_1 + \tilde{\rho}_2), x : \mathbf{v}'_1 \equiv \mathbf{v} \mid \tilde{\rho}'$ , we have that there are  $\rho', \gamma$  and  $\Gamma'$  such that

$$(6) \quad e'_2 \mid \rho'_2 \Rightarrow_r \mathbf{v}^\gamma \mid \rho' \text{ with } \text{erase}(\rho') = \tilde{\rho}' \text{ and}$$

$$(7) \quad \Gamma' \vdash \mathbf{v}^\gamma \mid \rho' : \tau^r \text{ and}$$

$$(8) \quad \rho'_2 \text{ and } \rho' \text{ are consistent.}$$

From (1) and (6) and  $\rho_1 + \rho_2 \preceq \rho$  applying rule (LET) we get  $\text{let } x = e_1 \text{ in } e_2 \mid \rho \Rightarrow_r \mathbf{v}^\gamma \mid \rho'$ . Moreover, from  $\rho_1$  and  $\rho_2$  consistent with  $\rho$ , (3) and definition of  $\rho'_2$  we have that  $\rho$  is consistent with  $\rho'_2$ . Finally, (7) and (8) conclude the proof.