A resource modality for RAII
Guillaume Combette, Guillaume Munch-Maccagnoni

To cite this version:

HAL Id: hal-01806634
https://inria.hal.science/hal-01806634
Submitted on 4 Jun 2018

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

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A resource modality for RAII

Guillaume Combette (CNRS, ENS Lyon)
Guillaume.Combette@ens-lyon.fr

Guillaume Munch-Maccagnoni (Inria, LS2N CNRS)
Guillaume.Munch-Maccagnoni@inria.fr

31st May 2018

1 RAII and move semantics

Stroustrup’s “Resource acquisition is initialisation” idiom (RAII, Stroustrup 1994) attaches destructors to types in C++, called whenever the lifetime of a variable ends, either by the end of its scope being reached, by an exception being raised, or by a control operator (return, break) being called. It is used in C++ to ensure the basic exception-safety guarantee (Stroustrup, 2001). Unlike finalizers called by a tracing garbage collector, destructors are called at fixed and predictable times.

RAII allows a form of resource management, for ensuring for instance that dynamically-allocated memory is always freed by the end of a scope. It is also used to ensure that locks are always freed, connections are always closed, etc. Doing so amounts to treat locks and connections as resources. Thus, a main point of RAII is that destructors may perform effects.

The extension of C++ with move semantics (Hinnant, Dimov, and Abrahams, 2002) allowed to express the moving of non-copiable resources. Moving a resource alters its lifetime: it can change the order in which destructors are called, or transfer the duty of calling the destructor to a different scope. Notably it allowed the definition of a non-copiable smart pointer for automatic resource management (unique_ptr) expressing ownership.

Baker (1994a,b, 1995) has proposed a synthesis of the notion of resource from systems programming with that of resources from linear logic (Girard, 1987). Arguably, it contained an early description of move semantics (it mentioned in particular the compatibility of moving with C++-style destructors). Although these articles described many of the ideas behind the resource management model of the C++11 (Stroustrup, Sutter, and Dos Reis, 2015) and Rust (Anderson, Bergstrom, Goregaokar, Matthews, McAllister, Moffitt, and Sapin, 2016) languages, they appear in advance of their time and rarely mentioned. In this presentation, we substantiate a link between C++-style destructors and linear logic.

2 A resource modality for RAII

We consider \( \mathcal{L} \) any distributive symmetric monoidal closed category (such as in particular any standard model of linear logic). For any \( E \in \mathcal{L} \), there is a monad \( - \oplus E \). It has been noticed in Hasegawa
that this monad lacks in general a strength, and therefore cannot be used to model exceptions like in a cartesian setting (Moggi, 1991). Intuitively, the operations bind and raise (or throw) need to dispose of variables in their context.

The main idea to model exceptions in \( \mathcal{L} \) is to consider the slice category \( \mathcal{L}/I \) where \( I \) is the monoidal unit. We recall that the slice category \( \mathcal{C}/X \) of a category \( \mathcal{C} \) for \( X \in \mathcal{C} \) has objects \( (A, \delta) \) for \( A \in \mathcal{C} \) and \( \delta \in \mathcal{C}(A, X) \), and morphisms those in \( \mathcal{C} \) that preserve the second component. In particular, \( (X, \text{id}_X) \) is terminal, and so \( \mathcal{L}/I \) is affine. When an object \( A \in \mathcal{L} \) interprets a type and \( \delta \in \mathcal{L}(A, I) \) interprets a derivation, we think of \( (A, \delta) \) as another type obtained by attaching the destructor \( \delta \) to the type \( A \).

We are more generally interested in the case where we are given a strong monad \((T, \eta, \mu, \sigma)\) on \( \mathcal{L} \).

We consider the slice category \( \mathcal{L}/TI \) and think of objects \( (A, \tilde{\delta}) = (A \otimes B, m \circ \delta \otimes \delta') \). The forgetful functor \( U : \mathcal{L}/M \to \mathcal{L} \) is strict monoidal.

Now, the object \( TI \) has a monoid structure given by \( \mu_I \circ \sigma_{TI, I} : TI \otimes TI \to TI \) and \( \eta_I : I \to TI \).

This \( \mathcal{L}/TI \) has a monoidal structure and strict monoidal forgetful functor \( U : \mathcal{L}/TI \to \mathcal{L} \). \( \mathcal{L}/TI \) has a terminal object \( (TI, \text{id}_{TI}) \). Notice that if \( \mathcal{L} \) is symmetric, the symmetry does not necessarily lift to a symmetry on \( \mathcal{L}/TI \). This is the case though whenever \( T \) is commutative. Otherwise, there is a definite order in the application of destructors: the destructor of \( P \otimes Q \) first calls the destructor of \( Q \) and then the destructor of \( P \).

We notice that the functor \( U \) has a right adjoint if and only if \( \mathcal{L} \) has the products \(- \times TI\) (as is the case in any model of multiplicative-additive intuitionistic linear logic). One therefore has a monoidal adjunction \( \mathcal{L}/TI \dashv \mathcal{L} \), giving rise to a resource modality \( S = UR \) on \( \mathcal{L} \) in the sense of Melliès (2009). When \( \mathcal{L} \) has finite products, this adjunction has the structure of a (non-commutative) linear call-by-push-value model (Curien, Fiore, and Munch-Maccagnoni, 2016). In particular, its deductive system given by the oblique morphisms of the adjunction (Munch-Maccagnoni, 2014), still expresses multiplicative-additive intuitionistic linear logic, though with fewer identities between derivations, reflecting the presence of an evaluation order. The deductive system includes a symmetry \( A \otimes B \vdash B \otimes A \) found in

\[
\mathcal{L}(UA \otimes UB, UB \otimes UA) \cong \mathcal{L}/TI(A \otimes B, RU(B \otimes A)) ,
\]

in words, moving resources is available as an effectful operation.

In this setting, we study the monad \( T(E = T(- \otimes E)) \) on \( \mathcal{L} \) and strength-like maps \( \theta_{P, A} : UP \otimes TEA \to T(E(UP \otimes A)) \) defined for \( P \in \mathcal{L}/TI \) and \( A \in \mathcal{L} \).

3 Resource management modes as polarities

We will conclude with considerations of programming language design following from the analogy:

smart pointer \( \sim \) resource modality

---

1https://mathoverflow.net/a/229371
which is suggested by Chirimar, Gunter, and Riecke, 1996 (a resource modality for a reference-counted garbage collection) and the previous section (a resource modality for `unique_ptr`).

We propose to extend it into an analogy:

resource management mode ∼ polarity

where the notion of polarities (Girard, 1991, 1993) suggests a way of mixing different resource management modes as kinds in a functional programming language, presented recently in a companion article (Munch-Maccagnoni, 2018).

References


