On the Relative Usefulness of Fireballs
Beniamino Accattoli, Claudio Sacerdoti Coen

To cite this version:
Beniamino Accattoli, Claudio Sacerdoti Coen. On the Relative Usefulness of Fireballs. 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, Jul 2015, Kyoto, Japan. 10.1109/LICS.2015.23. hal-01244833
On the Relative Usefulness of Fireballs

Beniamino Accattoli
INRIA & LIX/École Polytechnique
1 rue Honoré d’Estienne d’Orves, Palaiseau, France
Email: beniamino.accattoli@inria.fr

Claudio Sacerdoti Coen
Department of Computer Science and Engineering
University of Bologna
Mura Anteo Zamboni 7, Bologna (BO), Italy
Email: claudio.sacerdoticoen@unibo.it

Abstract—In CSL-LICS 2014, Accattoli and Dal Lago [1] showed that there is an implementation of the ordinary (i.e. strong, pure, call-by-name) λ-calculus into models like RAM machines which is polynomial in the number of β-steps, answering a long-standing question. The key ingredient was the use of a calculus with useful sharing, a new notion whose complexity was shown to be polynomial, but whose implementation was not explored. This paper, meant to be complementary, studies useful sharing in a call-by-value scenario and from a practical point of view. We introduce the Fireball Calculus, a natural extension of call-by-value to open terms, that is an intermediary step towards the strong case, and we present three results. First, we adapt useful sharing, refining the meta-theory. Then, we introduce the GLAMOUR, a simple abstract machine implementing the Fireball Calculus extended with useful sharing. Its key feature is that usefulness of a step is tested—surprisingly—in constant time. Third, we provide a further optimisation that leads to an implementation having only a linear overhead with respect to the number of β-steps.

I. INTRODUCTION

The λ-calculus is an interesting computational model because it is machine-independent, simple to define, and it compactly models functional programming languages. Its definition has only one rule, the β rule, and no data structures. The catch is the fact that the β-rule—which by itself is Turing-complete—is not atomic. Its action, namely \( \lambda x.t \ u \to^\beta t[x\mapsto u] \), can make many copies of an arbitrarily big subprogram \( u \). In other computational models like Turing or RAM machines, an atomic operation can only move the head on the ribbon or access a register. Is β atomic in that sense? Can one count the number of β-steps to the result and then claim that it is a reasonable bound on the complexity of the term? Intuition says no, because β can be nasty, and make the program grow at an exponential rate. This is the size explosion problem.

Useful Sharing: nonetheless, it is possible to take the number of β-steps as an invariant cost model, i.e. as a complexity measure polynomially related to RAM or Turing machines. While this was known for some notable sub-calculi [2]–[6], the first proof for the general case is a recent result by Accattoli and Dal Lago [1]. Similarly to the literature, they circumvent size explosion by factoring the problem via an intermediary model in between λ-calculus and machines. Their model is the linear substitution calculus (LSC) [1], [7], that is a simple λ-calculus with sharing annotations (also known as explicit substitutions) where the substitution process is decomposed in micro steps, replacing one occurrence at a time. In contrast with the literature, the general case is affected by a stronger form of size explosion, requiring an additional and sophisticated layer of sharing, called useful sharing. Roughly, a micro substitution step is useful if it contributes somehow to the creation of a β-redex, and useless otherwise. Useful reduction then selects only useful substitution steps, avoiding the useless ones. In [1], the Useful LSC is shown to be polynomially related to both λ-calculus (in a quadratic way) and RAM machines (with polynomial overhead, conjectured linear). It therefore follows that there is a polynomial relationship \( \lambda \to \text{RAM} \). Pictorially:

\[
\begin{array}{ccc}
\lambda & \text{polynomial} & \to \text{RAM} \\
\text{quadratic} & \text{Useful LSC} & \text{polynomial (linear?)}
\end{array}
\]

Coming back to our questions, the answer of [1] is yes, β is atomic, up to a polynomial overhead. It is natural to wonder how big this overhead is. Is β reasonably atomic? Or is the degree of the polynomial big and does the invariance result only have a theoretical value? In particular, in [1] the definition of useful steps relies on a separate and global test for usefulness, that despite being tractable might not be feasible in practice. Is there an efficient way to implement the Useful LSC? Does useful sharing—i.e. the avoidance of useless duplications—bring a costly overhead? This paper answers these questions. But, in order to stress the practical value of the study, it shifts to a slightly different setting.

The Fireball Calculus: we recast the problem in terms of the new fireball calculus (FBC), essentially the weak call-by-value λ-calculus generalised to handle open terms. It is an intermediary step towards a strong call-by-value λ-calculus, that can be seen as iterated open weak evaluation. A similar approach to strong evaluation is followed also by Grégoire and Leroy in [8]. It avoids some of the complications of the strong case, and at the same time exposes all the subtleties of dealing with open terms.

Free variables are actually formalised using a distinguished syntactic class, that of symbols, noted \( a, b, c \). This approach is technically convenient because it allows restricting to closed terms, so that any variable occurrence \( x \) is bound, while still having free variables, represented as symbols.

The basic idea is that—in the presence of symbols—restricting β-redex to fire only in presence of values is problematic. Consider indeed the following term:

\[ t := ((\lambda x.\lambda y.u)(aa))w \]
where \( w \) is normal. For the usual call-by-value operational semantics \( t \) is normal (because \( aa \) is not a value) while for theoretical reasons (see [9]–[11]) one would like to be able to fire the blocked redex, reducing to \((\lambda y.u\{x\leftarrow aa\})w\), so that a new redex is created and the computation can continue. According to the standard classification of redex creations due to Lévy [12], this is a creation of type 1.

The solution we propose here is to relax the constraint about values, allowing \( \beta \)-redexes to fire whenever the argument is a more general structure, a so-called fireball, defined recursively by extending values with inert terms, i.e. applications of symbols to fireballs. In particular, \( aa \) is inert, so that \( e.g. t \rightarrow (\lambda y.u\{x\leftarrow aa\})w \), as desired.

Functional languages are usually modelled by weak and closed calculi, so it is natural to wonder about the practical relevance of the FBC. Applications are along two axes. On the one hand, the evaluation mechanism at work in proof assistants has to deal with open terms for comparison and unification. For instance, Grégoire and Leroy’s [8], meant to improve the implementation of Coq, relies on inert terms (therein called accumulators). On the other hand, symbols may also be interpreted as constructors, meant to represent data as lists or trees. The dynamics of fireballs is in fact consistent with the way constructors are handled by Standard ML [13] and in several formalisation of core ML, as in [14]. In this paper we omit destructors, whose dynamics is orthogonal to the one of \( \beta \)-reduction, and we expect all results presented here to carry-over with minor changes to a calculus with destructors. Therefore firing redexes involving inert terms is also justified from a practical perspective.

**The Relative Usefulness of Fireballs:** as we explained, the generalisation of values to fireballs is motivated by creations of type 1 induced by the firing of inert terms. There is a subtlety, however. While substituting a value can create a new redex (e.g. as in \((\lambda x.(xI))I \rightarrow (xI)\{x\leftarrow I\} = II\), where \( I \) is the identity—these are called creations of type 3)—substituting a inert term can not. Said differently, duplicating inert terms is useless, and leads to size explosion. Note the tension between different needs: redexes involving inert terms have to be fired (for creations of type 1), and yet the duplication and the substitution of inert terms should be avoided (since they do not give rise to creations of type 3). We solve the tension by turning to sharing, and use the simplicity of the framework to explore the implementation of useful sharing. Both values and inert terms (\( i.e. \) fireballs) in argument position will trigger reduction, and both will be shared just after, but only the substitution of values might be useful, because inert terms are useless. This is what we call the relative usefulness of fireballs. It is also why—in contrast to Grégoire and Leroy—we do not identify fireballs and values.

1 The reader unfamiliar with redex creations should not worry. Creations are a key concept in the study of usefulness—which is why we mention them—but for the present discussion it is enough to know that there exists two kinds of creation (type 1 and the forthcoming type 3, other types will not play a role), no expertise on creations is required.

**The Result:** our main result is an implementation of FBC relying on useful sharing and such that it has only a linear overhead with respect to the number of \( \beta \)-steps. To be precise, the overhead is bilinear, \( i.e. \) linear in the number of \( \beta \)-steps and in the size of the initial term (roughly the size of the input).

The dependency from the size of the initial term is induced by the action of \( \beta \) on whole subterms, rather than on atomic pieces of data as in RAM or Turing machines. Therefore, \( \beta \) is not exactly as atomic as accessing a register or moving the head of a Turing machine, and this is the price for embracing higher-order computations. Bilinearity, however, guarantees that such a price is mild and that the number of \( \beta \) steps—\( i.e. \) of function calls in a functional program—is a faithful measure of the complexity of a program. To sum up, our answer is yes, \( \beta \) is also reasonably atomic.

**A Recipe for Bilinearity, with Three Ingredients:** our proof technique is a tour de force progressively combining together and adapting to the FBC three recent works involving the LSC, namely the already cited invariance of useful sharing of [1], the tight relationship with abstract machines developed by Accattoli, Barenbaum, and Mazza in [15], and the optimisation of the substitution process studied by the present authors in [16]. The next section will give an overview of these works and of how they are here combined, stressing how the proof is more than a simple stratification of techniques. In particular, it was far from evident that the orthogonal solutions introduced by these works could be successfully combined together.

**This Paper:** the paper is meant to be self-contained, and mostly follows a didactic style. For the first half we warm up by discussing design choices, the difficulty of the problem, and the abstract architecture. The second half focuses on the results. We also suggest reading the introductions of [1], [15], [16], as they provide intuitions about concepts that here are only hinted at. Although not essential, they will certainly soften the reading of this work. Omitted proofs are in the companion technical report [17] and related work is discussed in Sect. III.

II. A RECIPE WITH THREE INGREDIENTS

This section gives a sketch of how the bilinear implementation is built by mixing together tools from three different studies on the LSC.

1) Useful Fireballs: we start by introducing the Useful Fireball Calculus (Useful FBC), akin to the Useful LSC, and provide the proof that the relationship \( FBC \rightarrow \text{Useful FBC} \), analogously to the arrow \( \lambda \rightarrow \text{Useful LSC} \), has a quadratic overhead. Essentially, this step provides us with the following diagram:

\[
\begin{array}{ccc}
\text{FBC} & \quad \text{quadratic} \quad & \text{RAM} \\
\downarrow & & \downarrow \\
\text{Useful FBC} & & \\
\end{array}
\]

We go beyond simply adapting the study of [1], as the use of evaluation contexts (typical of call-by-value scenarios) leads to the new notion of useful evaluation context, that simplifies the technical study of useful sharing. Another key point is the
relative usefulness of fireballs, according to their nature: only values are properly subject to the useful discipline, i.e. are duplicated only when they contribute somehow to β-redexes, while inert terms are never duplicated.

2) Distilling Useful Fireballs: actually, we do not follow [1] for the study of the arrow Useful FBC → RAM. We rather refine the whole picture, by introducing a further intermediary model, an abstract machine, mediating between the Useful FBC and RAM. We adopt the distillation technique of [15], that establishes a fine-grained and modular view of abstract machines as strategies in the LSC up to a notion of structural equivalence on terms. The general pattern arising from [15] is that for call-by-name/value/need weak and closed calculi the quadratic overhead is due to malicious chains of renamings, i.e. of substitutions of variables for variables, and that the substitution overhead reduces to linear if the evaluation is modified so that variables are never substituted, i.e. if values do not include variables.

For the fireball calculus the question is tricky. First of all a disclaimer: with variables we refer to occurrences of bound variables and not to symbols/free variables. Now, our initial definition of the calculus will exclude variables from fireballs, but useful sharing will force us to somehow reintroduce them. Our way out is an optimised form of substitution that unchains renamings and whose overhead is proved linear by a simple amortised analysis. Such a third ingredient is first mixed with both the Useful FBC and the GLAMOUr, obtaining the Unchaining FBC and the Unchaining GLAMOUr, and then used to prove our main result, an implementation FBC → RAM having an overhead linear in the number of β steps and in the size of the initial term:

\[
\begin{array}{c}
\text{FBC} \quad \text{\longrightarrow} \quad \text{\texttt{RAM}} \\
\text{Useful FBC} \quad \text{\longrightarrow} \quad \text{GLAMOUr AM}
\end{array}
\]

This is the most interesting and original step of our study. First, it shows that distilleries are compatible with open terms and useful sharing. Second, while in [15] distilleries were mainly used to revisit machines in the literature, here the distillation principles are used to guide the design of a new abstract machine. Third, useful sharing is handled via a refinement of an ordinary abstract machine relying on a basic form of labelling. The most surprising fact is that such a labelling (together with invariants induced by the call-by-value scenario) allows a straightforward and very efficient implementation of useful sharing. While the calculus is based on separate and global tests for the usefulness of a substitution step, the labelling allows the machine to do on-the-fly and local tests, requiring only constant time (!). It then turns out that implementing usefulness is much easier than analysing it. Summing up, useful sharing is easy to implement and thus a remarkable case of a theoretically born concept with relevant practical consequences.

3) Unchaining Substitutions: at this point, it is natural to wonder if the bottleneck given by the side of the diagram FBC → Useful FBC, due to the overhead of the decomposition of substitutions, can be removed. The bound on the overhead is in fact tight, and yet the answer is yes, if one refines the actors of the play. Our previous work [16], showed that (in ordinary weak and closed settings) the quadratic overhead is due to malicious chains of renamings, i.e. of substitutions of variables for variables, and that the substitution overhead reduces to linear if the evaluation is modified so that variables are never substituted, i.e. if values do not include variables.

In this step, the original content is that the unchaining optimisation—while inspired by [16]—is subtler to define than in [16], as bound variables cannot be simply removed from the definition of fireballs, because of usefulness. Moreover, we also show how such an optimisation can be implemented at the machine level.

The next section discusses related work. Then there will be a long preliminary part providing basic definitions, an abstract decomposition of the implementation, and a quick study of both a calculus, the Explicit FBC, and a machine, the Open GLAM, without useful sharing. Both the calculus and the machine will not have any good asymptotical property, but they will be simple enough to familiarise the reader with the framework and with the many involved notions.

III. RELATED WORK

In the literature, invariance results for the weak call-by-value λ-calculus have been proved three times, independently. First, by Blelloch and Greiner [2], while studying cost models for parallel evaluation. Then by Sands, Gustavsson and Moran [3], while studying speedups for functional languages, and finally by Dal Lago and Martini [4], who addressed the invariance thesis for λ-calculus. Among them, [3] is the closest one, as it also provides an abstract machine and bounds its overhead. These works however concern closed terms, and so
they deal with a much simpler case. Other simple call-by-name cases are studied in [5] and [6]. The difficult case of the strong \( \lambda \)-calculus has been studied in [1], which is also the only reference for useful sharing.

The LSC is a variation over a \( \lambda \)-calculus with ES by Robin Milner [18], [19], obtained by plugging in some of the ideas of the structural \( \lambda \)-calculus by Accattoli and Kesner [20], introduced as a syntactic reformulation of linear logic proof nets. The LSC is similar to calculi studied by De Bruijn [21] and Nederpelt [22]. Its first appearances are in [6], [23], but its inception is actually due to Accattoli and Kesner.

Many abstract machines can be rephrased as strategies in \( \lambda \)-calculi with explicit substitutions (ES), see at least [24]–[29].

The related work that is by far closer to ours is the already cited study by Grégoire and Leroy of an abstract machine for call-by-value weak and open reduction in [8]. We developed our setting independently, and yet the FBC is remarkably close to their calculus, in particular our inert terms are essentially their accumulators. The difference is that our work is complexity-oriented while theirs is implementation-oriented. The on the one hand they do not recognise the relative usefulness of fireballs, and so their machine is not invariant, i.e. our machine is more efficient and on some terms even exponentially faster. On the other hand, they extend the language up to the calculus of constructions, present a compilation to bytecode, and certify in Coq the correctness of the implementation.

The abstract machines in this paper use global environments, an approach followed only by a minority of authors (e.g. [3], [15], [30], [31]) and essentially identifying the environment with a store. The distillation technique was developed to better understand the relationship between the KAM and weak linear head reduction pointed out by Danos & Regnier [32]. The idea of distinguishing between operational content and search for the redex in an abstract machine is not new, as it underlies in particular the refocusing semantics of Danvy and Nielsen [33]. Distilleries however bring an original refinement where logic, rewriting, and complexity enlighten the picture, leading to formal bounds on machine overheads.

Our unchaining optimisation is a lazy variant of an optimisation that repeatedly appeared in the literature, often with reference to space consumption and space leaks, for instance in [3] as well as in Wand’s [34] (section 2), Friedman et al.’s [35] (section 4), and Sestoft’s [36] (section 4).

## IV. THE FIREBALL CALCULUS

The setting is the one of the call-by-value \( \lambda \)-calculus extended with symbols \( a, b, c \), meant to denote free variables (or constructors). The syntax is:

- **Terms** \( t, u, w, r \) ::= \( x \mid a \mid \lambda x.t \mid tu \)
- **Values** \( v, v' \) ::= \( \lambda x.t \)

with the usual notions of free and bound variables, capture-avoiding substitution \( t[x \leftarrow u] \), and closed (i.e. without free variables) term. We will often restrict to consider closed terms, the idea being that an open term as \( x(\lambda y.zy) \) is rather represented as the closed term \( a(\lambda y.by) \).

The ordinary (i.e. without symbols) call-by-value \( \lambda \)-calculus has a nice operational characterisation of values:

*closed normal forms are values*

Now, the introduction of symbols breaks this property, because there are closed normal forms as \( a(\lambda x.x) \) that are not values.

In order to restore the situation, we generalise values to fireballs\(^2\), that are either values \( v \) or inert terms \( A \), i.e. symbols possibly applied to fireballs. Associating to the left, fireballs and inerts are compactly defined by

- **Fireballs** \( f, g, h \) ::= \( v \mid A \)
- **Inert Terms** \( A, B, C \) ::= \( af_1 \ldots f_n \ n \geq 0 \)

For instance, \( \lambda x.y \) and \( a \) are fireballs, as well as \( a(\lambda x.x) \), \( ab \), and \( (a(\lambda x.x))(bc)(\lambda y.zy) \). Fireballs can also be defined more atomically by mixing values and inert terms as follows:

\[
\begin{align*}
f & ::= \ v \mid A \quad A & ::= \ a \mid Af
\end{align*}
\]

Note that \( AB \) and \( AA \) are always inert.

Next, we generalise the call-by-value rule \( (\lambda x.t)v \rightarrow_{\beta} t[x \leftarrow v] \) to substitute fireballs \( f \) rather than values \( v \). First of all, we define a notion of evaluation context (noted \( F \) rather than \( E \), reserved to forthcoming global environments), mimicking right-to-left CBV evaluation:

**Evaluation Contexts** \( F ::= \langle \rangle \mid tF \mid Ff \)

note the case \( Ff \), that in CBV would be \( Fv \). Last, we define the \( \tau \) (fireball) rule \( \rightarrow_\tau \) as follows

**Rule at Top Level**

**Contextual closure**

\[
\begin{align*}
(\lambda x.t)f \rightarrow_\tau t[x \leftarrow f] \quad F(t) \rightarrow_\tau F(u) & \text{ if } t \rightarrow_\tau u
\end{align*}
\]

Our definitions lead to:

**Theorem 1.**

1) Closed normal forms are fireballs.

2) \( \rightarrow_\tau \) is deterministic.

In the introduction we motivated the notion of fireball both from theoretical and practical points of view. Theorem 1.1 provides a further, strong justification: it expresses a sort of internal harmony of the FBC, allowing to see it as the canonical completion of call-by-value to the open setting.

## V. SIZE EXPLOSION

Size explosion is the side effect of a discrepancy between the dynamics and the representation of terms. The usual substitution \( t[x \leftarrow u] \) makes copies of \( u \) for all the occurrences of \( x \), even if \( u \) is useless, i.e. it is normal and it does not create redexes after substitution. These copies are the burden leading to the exponential growth of the size. To illustrate the problem, let’s build a size exploding family of terms.

Note that a inert term \( A \), when applied to itself still is an inert term \( AA \). In particular, it still is a fireball, and so it can

\(^2\)About fireball: the first choice was fire-able, but then the spell checker suggested fireball.
be used as an argument for redexes. We can then easily build a term of size linear in \( n \) that in \( n \) steps evaluates a complete binary tree \( A^{2^n} \). Namely, define the family of terms \( t_n \) for \( n \geq 1 \):

\[
\begin{align*}
    t_1 & := \lambda x_1.(x_1x_1) \\
    t_{n+1} & := \lambda x_{n+1}.(t_n(x_{n+1}x_{n+1}))
\end{align*}
\]

Now consider \( t_nA \), that for a fixed \( A \) has size linear in \( n \). The next proposition shows that \( t_nA \) reduces in \( n \) steps to \( A^{2^n} \), causing size explosion.

**Proposition 1** (Size Explosion in the FBC), \( t_nA \rightarrow^n A^{2^n} \).

**Proof:** by induction on \( n \). Let \( B := A^2 = AA \). Cases:

\[
\begin{align*}
    t_1 & := (\lambda x_1.(x_1x_1))A \rightarrow^1 A^2 \\
    t_{n+1} & := (\lambda x_{n+1}.(t_n(x_{n+1}x_{n+1})))A \rightarrow^1 A^2 \\
    t_nA^2 & = t_nB \rightarrow^1 (i.h.) \\
    B^{2^n} & = A^{2^{n+1}} \quad \blacksquare
\end{align*}
\]

**VI. FIREBALLS AND EXPLICIT SUBSTITUTIONS**

In a ordinary weak scenario, sharing of subterms prevents size explosion. In the FBC however this is no longer true, as we show in this section. Sharing of subterms is here represented in a variation over the Linear Substitution Calculus, a formalism with explicit substitutions coming from a linear logic interpretation of the \( \lambda \)-calculus. At the dynamic level, the small-step operational semantics of the FBC is refined into a micro-step one, where explicit substitutions replace one variable occurrence at a time, similarly to abstract machines.

The terms of the Explicit Fireball Calculus (Explicit FBC) are:

\[
\begin{align*}
t, u, w, r & ::= x | a | \lambda x.t | tu | t[x\leftarrow u]
\end{align*}
\]

where \( t[x\leftarrow u] \) is the explicit substitution (ES) of \( u \) for \( x \) in \( t \), that is an alternative notation for let \( x = u \) in \( t \), and where \( x \) becomes bound in \( t \) and \( u \). We silently work modulo \( \alpha \)-equivalence of these bound variables, e.g. \( (xy)[y\leftarrow t]\{x\leftarrow y\} = (yz)[z\leftarrow t] \). We use \( \mathcal{F}v(t) \) for the set of free variables of \( t \).

**Contexts:** the dynamics of explicit substitutions is defined using (one-hole) contexts. Weak contexts subsume all the kinds of context in the paper, and are defined by

\[
W, W' ::= (\cdot) | tW | Wt | W[x\leftarrow t] | t[x\leftarrow W]
\]

The plugging \( W(t) \) of a term \( t \) into a context \( W \) is defined as \( \langle \cdot \rangle(t) := t, (\lambda x.W)(t) := \lambda x.(W(t)) \), and so on. As usual, plugging in a context can capture variables, e.g.

\[
(\langle \cdot \rangle y)[y\leftarrow t] = (\langle \cdot \rangle y)[y\leftarrow t].
\]

The plugging \( W(W') \) into a context \( W \) is defined analogously. Since all kinds of context we will deal with will be weak, the definition of plugging applies uniformly to all of them.

A special and frequently used class of contexts is that of substitution contexts \( L ::= (\cdot) | L[x\leftarrow t] \).

Switching from the FBC to the Explicit FBC the syntactic categories of inert terms \( A \), fireballs \( f \) and evaluation contexts \( F \) are generalised in Table I as to include substitution contexts \( L \). Note that fireballs may now contain substitutions, but not at top level, because it is technically convenient to give a separate status to a fireball \( f \) in a substitution context \( L \); terms of the form \( L(f) \) are called answers. An initial term is a closed term with no explicit substitutions.

**Rewriting Rules**:

- Fireball rule \( \rightarrow_f \) is replaced by \( \rightarrow_a \), defined as the union of the two rules \( \rightarrow_a \) and \( \rightarrow_e \) in Table I:

  1) **Multiplicative** \( \rightarrow_a \): a version of \( \rightarrow_f \) where \( \lambda x.t \) and \( f \) can have substitution contexts \( L \) and \( L' \) around, and the substitution is delayed.

  2) **Exponential** \( \rightarrow_e \): the substitution or exponential rule \( \rightarrow_e \) replaces exactly one occurrence of a variable \( x \) currently under evaluation (in \( F \)) with its definiendum \( f \) given by the substitution. Note the apparently strange position of \( L \) in the reduct. It is correct: \( L \) has to commute outside to bind both copies of \( f \), otherwise the rule would create free variables.

The name of the rules are due to the linear logic interpretation of the LSC.

**Unfolding**:

The shared representation is related to the usual one via the crucial notion of unfolding, producing the \( \lambda \)-term \( t_1 \) denoted by \( t \) and defined by:

\[
\begin{align*}
x_1 \downarrow & := x \\
(\lambda x.t) \downarrow & := \lambda x.t_1 \\
(tu) \downarrow & := t[u_1] \\
(t[x\leftarrow u]) \downarrow & := t[x\leftarrow u_1]
\end{align*}
\]

Note that \( r_n \downarrow := A^{2^n} \).

As for the FBC, evaluation is well-defined:

**Theorem 2.**

1) Closed normal forms are answers, i.e. fireballs in substitution contexts.

2) \( \rightarrow_e \) is deterministic.

**Structural Equivalence**:

The calculus is endowed with a structural equivalence, noted \( = \), whose property is to be a strong bisimulation with respect to \( \rightarrow_e \). It is the least
Proof: by induction on \( n \). Let \( B := A^2 = A A \). Cases:

\[
\begin{align*}
    t_1 &= (\lambda x_1. (x_1 x_1)) A \rightarrow^e_n (x_1 x_1)[x_1 \vdash A] \rightarrow^e_n (x_1 A)[x_1 \vdash A] \rightarrow^e_n \langle x_1 A \rangle[x_1 \vdash A] = A^2[x_1 \vdash A] \\
    t_{n+1} &= (\lambda x_{n+1}. (t_n (x_{n+1} x_{n+1}))) A \rightarrow^e_n (t_n A^2)[x_1 \vdash A] = L(t_n B) (\rightarrow^e_n A^2)^n (i.h.) \\
    L'(\langle B^2 \rangle) &= L'(\langle A^2^n \rangle) \quad \blacksquare
\end{align*}
\]

Before introducing useful evaluation—that will liberate us from size explosion—we are going to fully set up the architecture of the problem, by explaining 1) how ES implement a calculus, 2) how an abstract machine implements a calculus with ES, and 3) how to define an abstract machine for the inefficient Explicit FBC. Only by then (Sect. XI) we will start optimising the framework, first with useful sharing and then by eliminating renaming chains.

VII. TWO LEVELS IMPLEMENTATION

Here we explain how the the small-step strategy \( \rightarrow_t \) of the FBC is implemented by a micro-step strategy \( \rightarrow \). We are looking for an appropriate strategy \( \rightarrow \) with ES which is polynomially related to both \( \rightarrow_t \) and an abstract machine. Then we need two theorems:

1) **High-Level Implementation**: \( \rightarrow_t \) terminates iff \( \rightarrow \) terminates. Moreover, \( \rightarrow_t \) is implemented by \( \rightarrow \) with only a polynomial overhead. Namely, \( t \rightarrow^e_k u \) iff \( t \rightarrow^h_k u \), with \( k \) polynomial in \( h \);

2) **Low-Level Implementation**: \( \rightarrow \) is implemented on an abstract machine with an overhead in time which is polynomial in both \( k \) and the size of \( t \).

We will actually be more accurate, giving linear or quadratic bounds, but this is the general setting.

A. High-Level Implementation

First, terminology and notations. Derivations \( d \), \( e \), \ldots are sequences of rewriting steps. With \(|d|_l|, |d|_m \), and \(|d|_o \) we denote respectively the length, the number of multiplicative, and exponential steps of \( d \).

**Definition 1.** Let \( \rightarrow_f \) be a deterministic strategy on FBC-terms and \( \rightarrow \) a deterministic strategy for terms with ES. The pair \((\rightarrow_f, \rightarrow)\) is a **high-level implementation system** if whenever \( t \) is a \( \lambda \)-term and \( d : t \rightarrow^* u \) then:

1) **Normal Form**: if \( u \) is a \( \rightarrow^* \)-normal form then \( u \downarrow \) is a \( \rightarrow_t \)-normal form.

2) **Projection**: \( d \downarrow : t \rightarrow^*_t u \downarrow \) and \(|d|_l = |d|_o|.

Moreover, it is

1) **locally bounded**: if the length of a sequence of substitution \( \varepsilon \)-steps from \( u \) is linear in the number \(|d|_m \) of \( \varepsilon \)-steps in \( d \);

2) **globally bounded**: if \(|d|_o \) is linear in \(|d|_m|.

The normal form and projection properties address the qualitative part, i.e. the part about termination. The normal form property guarantees that \( \rightarrow \) does not stop prematurely, so that when \( \rightarrow \) terminates \( \rightarrow_f \) cannot keep going. The projection property guarantees that termination of \( \rightarrow \) implies termination of \( \rightarrow \). The two properties actually state a stronger fact: \( \rightarrow_f \) steps can be identified with the \( \rightarrow^e_n \)-steps of the \( \rightarrow \) strategy.

The local and global bounds allow to bound the overhead introduced by the Explicit FBC wrt the FBC, because by relating \( \rightarrow \rightarrow^e_n \) steps, they relate \(|d|_l| \) and \(|d|_l| \), since \( \rightarrow \rightarrow^e_n \) steps can be identified.

The high-level part can now be proved abstractly.

**Theorem 3** (High-Level Implementation). Let \( t \) be an ordinary \( \lambda \)-term and \((\rightarrow_f, \rightarrow)\) a high-level implementation system.

1) **Normalisation**: \( t \rightarrow^* \) normalising iff it is \( \rightarrow \)-normalising.

2) **Projection**: if \( d : t \rightarrow^* u \) then \( d \downarrow : t \rightarrow^* t \downarrow \).

Moreover, the overhead of \( \rightarrow \) is, depending on the system:

1) **locally bounded**: quadratic, i.e. \(|d|_l = O(|d|_m^2|).

2) **globally bounded**: linear, i.e. \(|d|_l = O(|d|_m|).

Let us see our framework at work:

**Theorem 4.** \((\rightarrow_f, \rightarrow)\) is a high-level implementation system.

Note the absence of complexity bounds. In fact, \((\rightarrow_f, \rightarrow)\) is not even locally bounded. Let \( t^n \) here be defined by \( t^1 = t \) and \( t^{n+1} = t^n t \), and \( u_n := (\lambda x. x^n) A \). Then \( d : u_n \rightarrow^e_n A^n[x \vdash A] \) is a counter-example to local boundedness. Moreover, the Explicit FBC also suffers of size explosion, i.e. implementing a single step may take exponential time. In Sect. XI useful sharing will solve these issues.

B. Low-Level Implementation: Abstract Machines

Introducing Distilleries: an abstract machine \( M \) is meant to implement a strategy \( \rightarrow \) via a **distillation**, i.e. a decoding function \( \cdot \). A machine has a state \( s \), given by a code \( T \), i.e. a \( \lambda \)-term \( t \) without ES and not considered up to \( \alpha \)-equivalence, and
some data-structures like stacks, dumps, environments, and eventually heaps. The data-structures are used to implement the search of the next \( \sim \) -redex and some form of parsimonious substitution, and they distill to evaluation contexts for \( \sim \). Every state \( s \) decodes to a term \( s_\shortmid \), having the shape \( F(t) \), where \( t \) is a \( \lambda \)-term and \( F \) is some kind of evaluation context.

A machine computes using transitions, whose union is noted \( \sim \), of two types. The principal one, noted \( \sim_p \), corresponds to the firing of a rule defining \( \sim \). In doing so, the machine can differ from the calculus implemented by a transformation to the behaviour, even at the level of complexity, because they commute with evaluation.

To preserve correctness, structural equivalence \( \equiv \) is required to commute with evaluation \( \sim \), i.e. to satisfy

\[
\begin{align*}
t \sim r \quad &\equiv \quad \exists q \text{ s.t. } u \sim r \quad \equiv \quad \equiv \\

\end{align*}
\]

for each of the rules of \( \sim \), preserving the kind of rule. In fact, this means that \( \equiv \) is a strong bisimulation (i.e. one step to one step) with respect to \( \sim \). Strong bisimulations formalise transformations which are transparent with respect to the behaviour, even at the level of complexity, because they can be retarded without affecting the length of evaluation.

**Lemma 1 (\( \equiv \) Postponement).** If \( \equiv \) is a strong bisimulation and \( t \rightarrow \cup \equiv^* u \) then \( t \rightarrow^* \equiv u \) and the number and kind of steps of \( \sim \) in the two reduction sequences is the same.

We can finally introduce distilleries, i.e. systems where a strategy \( \sim \) simulates a machine \( M \) up to structural equivalence \( \equiv \) (via the decoding \( \tilde{\shortmid} \)).

**Definition 2.** A distillery \( D = (M, \sim, \equiv, \tilde{\shortmid}) \) is given by:

1. An abstract machine \( M \), given by
   a) a deterministic labeled transition system \( \sim \) on states \( s \);
   b) a distinguished class of states deemed initial, in bijection with closed \( \lambda \)-terms and from which one obtains the reachable states by applying \( \sim^* \);
   c) a partition of the labels of the transition system \( \sim \) as:
      - principal transitions, noted \( \sim_p \);
      - commutative transitions, noted \( \sim_c \);
2. a deterministic strategy \( \sim \);
3. a structural equivalence \( \equiv \) on terms s.t. it is a strong bisimulation with respect to \( \sim \);
4. a distillation \( \tilde{\shortmid} \), i.e. a decoding function from states to terms, s.t. on reachable states:
   - Principal: \( s \sim_p s' \) implies \( s \rightarrow s' \);
   - Commutative: \( s \sim_c s' \) implies \( s \equiv s' \).

We will soon prove that a distillery implies a simulation theorem, but we want a stronger form of relationship. Additional hypothesis are required to obtain the converse simulation, handle explicit substitution, and talk about complexity bounds.

Some terminology first. An execution \( \rho \) is a sequence of transition from an initial state. With \( |\rho|_p \), \( |\rho|_c \), and \( |\rho|_e \) we denote respectively the length, the number of principal, and commutative transitions of \( \rho \). The size of a term is noted \( |t| \).

**Definition 3 (Distillation Qualities).** A distillery is

- Reflective when on reachable states:
   - Termination: \( \sim_c \) terminates;
   - Progress: if \( s \rightarrow s' \) then \( \rho \) is not final.
- Explicit when
  - Partition: principal transitions are partitioned into multiplicative \( \sim_m \) and exponential \( \sim_e \), like for the strategy \( \sim \).
  - Explicit decoding: the partition is preserved by the decoding, i.e.
    - Multiplicative: \( s \sim_m s' \) implies \( s \rightarrow s'= s' \)
    - Exponential: \( s \sim_e s' \) implies \( s \equiv s'= s' \)
- Bilinear when it is reflective and
  - Execution Length: given an execution \( \rho \) from an initial term \( t \), the number of commutative steps \( |\rho|_c \) is linear in both \( |t| \) and \( |\rho|_p \) (with a slightly stronger dependency on \( |t| \), due to the time needed to recognise a normal form), i.e. if \( |\rho|_c \equiv O(1+|\rho|_p \cdot |t|) \).
  - Commutative: \( \sim_e \) is implementable on RAM in a constant number of steps;
  - Principal: \( \sim_p \) is implementable on RAM in \( O(|t|) \) steps.

A reflective distillery is enough to obtain a bisimulation between the strategy \( \sim \) and the machine \( M \), that is strong up to structural equivalence \( \equiv \). With \( |\rho|_p \) and \( |\rho|_e \) we denote respectively the number of multiplicative and exponential transitions of \( \rho \).

**Theorem 5 (Correctness and Completeness).** Let \( D \) be a reflective distillery and \( s \) an initial state.

1. Strong Simulation: for every execution \( \rho : s \rightarrow^* s' \) there is a derivation \( d : s \rightarrow^* s' \) s.t. \( |\rho|_p = |d| \).
2. Reverse Strong Simulation: for every derivation \( d : s \rightarrow^* t \) there is an execution \( \rho : s \rightarrow^* s' \) s.t. \( t \equiv s' \) and \( |\rho|_p = |d| \).

Moreover, if \( D \) is explicit then \( |\rho|_e = |d|_e \) and \( |\rho|_e = |d|_e \).

Bilinearity, instead, is crucial for the low-level theorem.

**Theorem 6 (Low-Level Implementation Theorem).** Let \( \rightarrow \) be a strategy on terms with ES and \( D = (M, \sim, \equiv, \tilde{\shortmid}) \) a bilinear distillery. Then a \( \rightarrow \) -derivation \( d \) is implementable on RAM machines in \( O((1+|d|) \cdot |t|) \) steps, i.e. bilinear in the size of the initial term \( t \) and the length of the derivation \( |d| \).

Proof: given \( d : t \rightarrow^* u \) by Theorem 5.2 there is an execution \( \rho : s \rightarrow^* s' \) s.t. \( u \equiv s' \) and \( |\rho|_p = |d| \). The number
of RAM steps to implement ρ is the sum of the number for the commutative and the principal transitions. By bilinearity, |ρ|c = O((1 + |ρ|p)·|t|) and so all the commutative transitions in ρ require O((1 + |ρ|p)·|t|) steps, because a single one takes a constant number of steps. Again by bilinearity, each principal one requires O(|t|) steps, and so all the principal transitions together require O(|ρ|p·|t|) steps.

We will discuss three distilleries, summarised in Table IV (page 11), and two of them will be bilinear. The machines will be sophisticated, so that we will first present a machine for the simpler case without symbols, the number of commutative and the principal transitions. By bilinearity, the saved subterm. Indeed, when the argument, i.e. ϵ, current stack item is pushed on the stack, and the machine stays for data-structures, decoding and transitions.

**Open GLAM:** the machine transitions are given in Table II. Note that the multiplicative one ⊸, new entry in the environment, while the exponential one ⊸e performs a clashing-avoiding substitution from the environment. The idea is that the principal transitions ⊸π and ⊸ε implement ⊸, while the commutative transitions ⊸c1, ⊸c2, and ⊸c3, locate and expose the next redex following a right-to-left strategy.

The commutative rule ⊸c1 forces evaluation to be right-to-left on applications: the machine processes first the argument π, saving the left sub term τ on the dump together with its current stack π. The role of ⊸c2 and ⊸c3 is to backtrack to the saved subterm. Indeed, when the argument, i.e. the current code, is finally put in normal form, encoded by a stack item φ, the stack item is pushed on the stack, and the machine backtracks to the pair on the dump.

**The Machine:** the machine level, terms are replaced by codes, i.e. terms not considered up to α-equivalence. To distinguish codes from terms, we over-line codes like in ⁷. States (noted s, s′, . . . ) of the abstract machine are made out of a context dump D, a code t, an argument stack π, and a global environment E, defined by the grammars in Table II. To save space, sometimes we write [x→t]E for [x→t] : E. Note that stacks may contain pairs (τ, π) of a code and a stack, used to code the application of τ to the stack π. This representation allows to implement commutative rules in constant time.

The Machine: open GLAM will be surprisingly simple (Sect. XII), and yet tests of usefulness will only require constant time.

**Open GLAM stays for Open Global LAM,** in turn referring to a similar machine, based on local environments, introduced in [15] and called LAM—standing for Leroy Abstract Machine. The Open GLAM differs from the LAM in two respects: 1) it uses global rather than local environments, and 2) it has an additional rule (⊡c1) to handle open terms (i.e. symbols).

Data-Structures: at the machine level, terms are replaced by codes, i.e. terms not considered up to α-equivalence. To distinguish codes from terms, we over-line codes like in ⁷. States (noted s, s′, . . . ) of the abstract machine are made out of a context dump D, a code t, an argument stack π, and a global environment E, defined by the grammars in Table II. To save space, sometimes we write [x→t]E for [x→t] : E. Note that stacks may contain pairs (τ, π) of a code and a stack, used to code the application of τ to the stack π. This representation allows to implement commutative rules in constant time.
Lemma 2 (Open GLAM Invariants). Let \( s = (D, u, \pi, E) \) be a state reachable from an initial code \( \overline{t} \). Then:

1) Closure: \( s \) is closed and well-named;
2) Value: values in components of \( s \) are subterms of \( \overline{t} \);
3) Fireball: every term in \( \pi \), in \( E \), and in every stack in \( D \) is a fireball;
4) Contextual Decoding: \( E, D, \pi, \) and \( F \) are evaluation contexts;

The invariants are used to prove the following theorem.

Theorem 7 (Open GLAM Distillation). (Open GLAM, \( \alpha\), \( \forall \), \( \exists \)) is a reflective explicit distillery. In particular, let \( s \) be a reachable state reachable:

1) Commutative: if \( s \vdash_{s_1, s_2} s' \) then \( s = s' \);
2) Multiplicative: if \( s \vdash_{s} s' \) then \( s \vdash_{s} s' \);
3) Exponential: if \( s \vdash_{s} s' \) then \( s \vdash_{s} s' \).

Since the Explicit FBC suffers from size explosion, an exponential step (and thus an exponential transition) may duplicate a subterm that is exponentially bigger than the input. Then (Open GLAM, \( \alpha\), \( \forall \), \( \exists \)) does not satisfy bilinearity, for which every exponential transition has to be linear in the input.

IX. INTERLUDE: RELATIVE UNFOLDINGS

Now we define some notions for weak contexts that will be implicitly instantiated to all kind of contexts in the paper. In particular, we define substitution over contexts, and then use it to define the unfolding of a context, and the more general notion of relative unfolding.

Implicit substitution on weak contexts \( W \) is defined by

\[
\langle \cdot \rangle \{ x \leftarrow u \} := \langle \cdot \rangle
\]

\[
(tW) \{ x \leftarrow u \} := t\{ x \leftarrow u \} W \{ x \leftarrow u \}
\]

\[
(Wt) \{ x \leftarrow u \} := W \{ x \leftarrow u \} t \{ x \leftarrow u \}
\]

\[
W[y \leftarrow t \{ x \leftarrow u \}] \{ x \leftarrow u \} := W \{ x \leftarrow u \} [y \leftarrow t \{ x \leftarrow u \}]
\]

\[
t[y \leftarrow W \{ x \leftarrow u \}] \{ x \leftarrow u \} := t \{ x \leftarrow u \} [y \leftarrow W \{ x \leftarrow u \}]
\]

Lemma 3. Let \( t \) be a term and \( W \) a weak context. Then \( W(t) \{ x \leftarrow u \} = W \{ x \leftarrow u \} (t \{ x \leftarrow u \}) \).

Now, we would like to extend the unfolding to contexts, but in order to do so we have to restrict the notion of context. Indeed, whenever the hole of a context is inside an ES, the unfolding may erase or duplicate the hole, producing a term or a multi-context, which we do not want. Thus, we turn to (weak) shallow contexts, defined by:

\[
S, S', S'' := \langle \cdot \rangle \mid St \mid tS \mid S[x \leftarrow t].
\]

(Note the absence of the production \( t[x \leftarrow S] \)).

Now, we define in Table III context unfolding \( S \downarrow \) unfolding \( t \downarrow \) of a term \( t \) relative to a shallow context \( S \) and unfolding \( S' \downarrow \) of a shallow context \( S' \) relative to a shallow context \( S \).

Relative unfoldings have a number of properties, summed up in the companion technical report [17]. Last, a definition that will be important in the next section.

Definition 4 (Applicative Context). A shallow context \( S \) is applicative when its hole is applied to a sub term \( u \), i.e. if \( S = S'(Lu) \).

X. INTRODUCING USEFUL SHARING

Beware: this and the next sections will heavily use contexts and notions about them as defined in Sect. VI and Sect. IX, in particular the notions of shallow context, applicative context, and relative unfolding.

Introducing Useful Reduction: note that the substitution steps in the size exploding family do not create redexes. We want to restrict the calculus so that these useless steps are avoided. The idea of useful sharing, is to trigger an exponential redex only if it will somehow contribute to create a multiplicative redex. Essentially, one wants only the exponential steps

\[
F(x)[x \leftarrow L(f)] \Rightarrow \alpha L(F(f)[x \leftarrow f])
\]

s.t. \( F \) is applicable and \( f \) is a value, so that the firing creates a multiplicative redex. Such a change of approach, however, has consequences on the whole design of the system. Indeed, since some substitutions are delayed, the present requirements for the rules might not be met. Consider:

\[
(\lambda x. t) y[y \leftarrow ab]
\]
we want to avoid substituting \( ab \) for the argument \( y \), but we also want that evaluation does not stop, i.e. that \((\lambda x. t)[y := ab] \rightarrow_{\alpha} t[x := y][y := ab]\). To accomodate such a dynamics, our definitions have to be up to unfolding, i.e. fireballs have to be replaced by terms unfolding to fireballs. There are 4 subtle things about useful reduction.

1) Multiplicatives and Variables: the idea is that the multiplicative rule becomes

\[ L(\lambda x. t) L'(u) \rightarrow_{\alpha} L(t[x := L'(u)]) \]

where it is the unfolding \( L'(\langle u \rangle) \) of the argument \( L'(u) \) that is a fireball, and not necessarily \( L'(u) \) itself. Note that sometimes variables are valid arguments of multiplicative redexes, and consequently substitutions may contain variables.

2) Exponentials and Future Creations: the exponential rule involves contexts, and is trickier to make it useful. A first approximation of useful exponential step is

\[ F(x)[x := L(u)] \rightarrow_{\alpha} L(F(u)[x := u]) \]

where \( L(\langle u \rangle) \) is a value (i.e. it is not inert) and \( F \) is applicative, so that—after eventually many substitution steps, when \( x \) becomes \( u \)—a multiplicative redex will pop out.

Note that an useful exponential step does not always immediately create a multiplicative redex. Consider the following step (where \( I \) is the identity):

\[ (xI)[x := y][y := I] \rightarrow_{\alpha} (yI)[x := y][y := I] \quad (1) \]

No multiplicative redex has been created yet, but step (1) is useful because the next exponential step creates a multiplicative redex (note how such lookahead is captured by working up to unfoldings):

\[ (yI)[x := y][y := I] \rightarrow_{\alpha} (II)[x := y][y := I] \]

3) Evaluation and Evaluable Contexts: the delaying of useless subtitutions impacts also on the notion of evaluation context \( F \), used in the exponential rule. For instance, the following exponential step should be useful

\[ ((xI)y)[x := I][y := ab] \rightarrow_{\alpha} ((II)y)[x := I][y := ab] \]

but the context \(((xI)y)[x := I][y := ab]\) isolating \( x \) is not an evaluation context, it only unfolds to one. We then need a notion of evaluation context up to unfolding. The intuition is that a shallow context \( S \) is evaluable if \( S_{\downarrow} \) is an evaluation context (see Sect. IX for the definition of context unfolding), and it is useful if it is evaluable and applicative. The exponential rule then should rather be:

\[ S(x)[x := L(u)] \rightarrow_{\alpha} L(S(u)[x := u]) \]

where \( u_{\downarrow} \) is a value and \( S \) is useful.

4) Context Closure vs Global Rules: such a definition, while close to the right one, still misses a fundamental point, i.e. the global nature of useful steps. Evaluation rules are indeed defined by a further closure by contexts, i.e. a step takes place in a certain shallow context \( S' \). Of course, \( S' \) has to be evaluable, but there is more. Such a context, in fact, may also give an essential contribution to the usefulness of a step. Let us give an example. Consider the exponential step

\[ (xx)[x := y] \rightarrow_{\alpha} (yx)[x := y] \]

By itself it is not useful, since \( y \) is not a value nor unfolds to one. If we plug that redex in the context \( S := \langle \cdot \rangle[y := I] \), however, \( y \) unfolds to a value in \( S \), as \( y|_{S} = y|_{\langle \cdot \rangle[y := \lambda z.z]} = \lambda z. z \), and the step becomes:

\[ (xx)[x := y][y := \lambda z.z] \rightarrow_{\alpha} (yx)[x := y][y := \lambda z.z] \quad (2) \]

As before, no multiplicative redex has been created yet, but step (2) is useful because it is essential for the creation given by the next exponential step:

\[ (yx)[x := y][y := \lambda z.z] \rightarrow_{\alpha} ((\lambda z. z)x)[x := y][y := \lambda z.z] \]

Note, indeed, that \((\lambda z. z)x\) gives a useful multiplicative redex, because \( x \) unfolds to a fireball in its context \((\cdot)[x := y][y := \lambda z.z]\).

Summing up, the useful or useless character of a step depends crucially on the surrounding context. Therefore useful rules have to be global: rather than given as axioms closed by evaluable contexts, they will involve the surrounding context itself and impose conditions about it.

The Useful FBC, presented in the next section, formalises these ideas. We will prove it to be a locally bounded implementation of \( \rightarrow_{\alpha} \), obtaining our fist high-level implementation theorem.

**XI. THE USEFUL FIREBALL CALCULUS**

For the Useful FBC, terms, values, and substitution contexts are unchanged (with respect to the Explicit FBC), and we use shallow contexts \( S \) as defined in Sect. IX. An initial term is still a closed term with no explicit substitutions.

The new key notion is that of evaluable context.

**Definition 5** (Evaluable and Usefule Contexts). Evaluable (shallow) contexts are defined by the inference system in Table V. A context is useful if it is evaluable and applicative (being applicative is easily seen to be preserved by unfolding).

Point 1 of the following Lemma 4 guarantees that evaluable contexts capture the intended semantics suggested in the previous section. Point 2 instead provides an equivalent inductive formulation that does not mention relative unfoldings. The definition in Table V can be thought has been from the outside, while the lemma give a characterisation from the inside, relating subterms to their surrounding sub-context.

**Lemma 4.**

1) If \( S \) is evaluable then \( S_{\downarrow} \) is an evaluation context.

2) \( S \) is evaluable iff \( u_{\downarrow} \) is a fireball whenever \( S = S'(\langle u \rangle) \) or \( S = S'(\langle x := u \rangle) \).
The state context, however, now is noted to a fireball in its context. Note also that in the Open GLAM by:  

1) Backtracking instead of performing a useless substitution: there are two new backtracking cases \( \equiv_{c_1} \) and \( \equiv_{c_3} \) (that in the Open GLAM were handled by the exponential transition), corresponding to avoided useless duplications: \( \equiv_{c_1} \) backtracks when the entry \( \phi \) to substitute is marked \( A \) (as it unfolds to a inert term) and \( \equiv_{c_3} \) backtracks when the term is marked \( v \) but the stack is empty (i.e., the context is not applicative).

2) Substituting only when it is useful: the exponential transition is applied only when the term to substitute has label \( v \) and the stack is non-empty.

Lemma 5 (GLAMOUR Invariants). Let \( s = (D, \pi, \pi, E) \) be a state reachable from an initial code \( \overline{I} \). Then:

1) Closure: \( s \) is closed and well named;
2) Value: values in components of \( s \) are subterms of \( \overline{I} \);
3) Fireball: \( \overline{I}_{uc} \) is a fireball (of kind \( 1 \)) for every code \( \overline{I} \) in \( \pi, E \), and \( \overline{I}_{uc} \) in every stack of \( D \);
4) Evaluability: \( E, \overline{D}_{uc}, \overline{P}_{uc}, \overline{A}_{uc} \), and \( S_{uc} \) are evaluable contexts;
5) Environment Size: the length of the global environment \( E \) is bound by \( |\rho|_{uc} \).

Theorem 9 (GLAMOUR Distillation). \((GLAMOUR, \equiv_{uc}, \equiv_{uc})\) is a reflective explicit distillery. In particular, let \( s \) be a reachable state:

1) Commutative: if \( s \equiv_{c_1, c_2, c_3, c_4} s' \) then \( s = s' \);
2) Multiplicative: if \( s \equiv_{uc} s' \) then \( s \equiv_{uc} s' \);
3) Exponential: if \( s \equiv_{uc} s' \) then \( s \equiv_{uc} s' \).

In fact, the distillery is even bilinear, as we now show. The proof employs the following definition of size of a state.

Definition 6. The size of codes and states is defined by:

\[
|x| = |a| := 1 \quad |\overline{I}| := |\overline{I}| + |\overline{I}| + 1 \quad |\lambda x.\overline{I}| := |\overline{I}| + 1 \\
|(D, \overline{I}, \pi, E)| := |
\overline{I}| + \sum_{(\pi, \pi') \in D} |\overline{I}| 
\]

Lemma 6 (Size Bounded). Let \( s = (D, \overline{I}, \pi, E) \) be a state reached by an execution \( \rho \) of initial code \( \overline{I} \). Then \( |s| \leq (1 + |\rho|_{uc})|\overline{I}| - |\rho|_{uc} \).

Proof: by induction over the length of the derivation. The property trivially holds for the empty derivation. Case analysis over the last machine transition. Commutative rule \( \equiv_{c_1} \): the rule splits the code \( \overline{I} \) between the dump and the code, and the measure—as well as the rhs of the formula—decreases by 1 because the rule consumes the application node. Commutative rules \( \equiv_{c_2, c_3, c_4, c_5} \): these rules consume the current code, so they...
Table VI
TRANSITIONS OF THE GLAMOUR

<table>
<thead>
<tr>
<th>D</th>
<th>?π</th>
<th>π</th>
<th>E</th>
<th>~c₁</th>
<th>D : ⟨⃗t, π⟩</th>
<th>?π</th>
<th>0</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>λx.⃗t</td>
<td>φ : π</td>
<td>E</td>
<td>~ua</td>
<td>D</td>
<td>0</td>
<td>π</td>
<td>[x φ]</td>
</tr>
<tr>
<td>D : ⟨⃗t, π⟩</td>
<td>λπ. ⃗t</td>
<td>π</td>
<td>E</td>
<td>~c₂</td>
<td>D</td>
<td>?π</td>
<td>π</td>
<td>E</td>
</tr>
<tr>
<td>D : ⟨⃗t, π⟩</td>
<td>a</td>
<td>π'</td>
<td>E</td>
<td>~c₃</td>
<td>D</td>
<td>?π</td>
<td>π</td>
<td>E</td>
</tr>
<tr>
<td>D : ⟨⃗t, π⟩</td>
<td>x</td>
<td>π'</td>
<td>E₁[x φ₁]E₂</td>
<td>~c₂</td>
<td>D</td>
<td>?π</td>
<td>π'</td>
<td>E₁[x φ₁]E₂</td>
</tr>
<tr>
<td>D : ⟨⃗t, π⟩</td>
<td>x</td>
<td>ε</td>
<td>E₁[x φ₁]E₂</td>
<td>~c₃</td>
<td>D</td>
<td>?π</td>
<td>π'</td>
<td>E₁[x φ₁]E₂</td>
</tr>
<tr>
<td>D</td>
<td>x</td>
<td>φ' : π</td>
<td>E₁[x φ₁]E₂</td>
<td>~ua</td>
<td>D</td>
<td>?π</td>
<td>π' : π</td>
<td>E₁[x φ₁]E₂</td>
</tr>
</tbody>
</table>

where π' is any code α-equivalent to π that preserves well-naming of the machine.

Table VII
IDENTITY, CHAIN, AND CHAIN-STARTING CONTEXT + REWRITING RULES OF THE UNCHAINING FBC

<table>
<thead>
<tr>
<th>I, I'</th>
<th>C, C'</th>
<th>RULE (ALREADY CLOSED BY CONTEXTS)</th>
<th>SIDE CONDITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x</td>
<td>I(x)[x-I]</td>
<td>I(x)[x-I]</td>
<td>S(C)</td>
</tr>
<tr>
<td>S(x)[x-I]</td>
<td>C(x)[x-I]</td>
<td>S(L(λx.t)u) ~oe S(L(λx.t)x[u])</td>
<td>S(⟨⟨·⟩⟩) is useful</td>
</tr>
<tr>
<td>S(y)[y-I]</td>
<td>y-I</td>
<td>S(y-I)</td>
<td>S(S'[x-L(v)] ~oe S(L(S'(v)[x-I][v])</td>
</tr>
<tr>
<td>S(C)</td>
<td>C</td>
<td>S(C)</td>
<td>S(C(x)[x-I] ~oe S(L(C'(v)[x-I])</td>
</tr>
</tbody>
</table>

Because the length n of the chain is bounded by the number of previous multiplicative steps (local bound property), the overall complexity of the machine is quadratic in the number of multiplicative steps. In our previous work [16], we showed that reducing to linear is enough to perform substitution steps in reverse order, modifying the chains while traversing them. The idea is that in the previous example one should rather have a smart reduction ~oE (o stays for optimised, as u is already used for useful reduction) following the chain of substitutions and performing:

(x₁A)[x₁-t₁] ... [xₙ₋₁-t₁] [xₙ-t₁] ~oe
(x₁A)[x₁-t₁] ... [xₙ₋₁-t₁] [xₙ-t₁] ~oe
...
(vA)[x₁-t₁] ... [xₙ₋₁-t₁] [xₙ-t₁] ~oe

Later occurrences of x₁ will no longer trigger the chain, because it has been unchained by traversing it the first time.

Unfortunately, introducing such an optimisation for useful reduction is hard. In the shown example, that has a very simple form, it is quite easy to define what following the chain means. For the distillation machinery to work, however, we need our rewriting rules to be stable by structural equivalence, whose action is a rearrangement of substitutions through the term structure. Then the substitutions [xᵢ-tᵢ] of the example can be spread all over the term, interleaved by applications and other substitutions, and even nested one into the other (like in [xᵢ-tᵢ+1[xᵢ+1-tᵢ+1[xₙ-tₙ+1]]]). This makes the specification of unchaining useful reduction a quite technical affair.

Chain Contexts: reconsider a term like in the example, (xA)[x₁-t₁][x₂-t₂][x₃-t₄][x₄-t₅]. We want the next step to substitute on x₄ so we should give a status to the context C := (xA)[x₁-t₁][x₂-t₂][x₃-t₄] where C is that.

C' := (x[x₁-t₁][x₂-t₂][x₃-x₅]A)[x₅-t₅]
and so this context has to be caught too. We specify these context in Table VII as chain contexts $C$, defined using the auxiliary notion of identity context $I$, that captures a simpler form of chain (note that both notions are not shallow).

Given a chain context $C$, we will need to retrieve the point where the chain started, i.e. the shallow context isolating the variable at the left end of the chain (x1 in the example). We are now going to define an operation associating to every chain context its chain-starting (shallow) context. To see the two as contexts of a same term, we need also to provide the subterm that we will put in $C$ (that will always be a variable). The chain-starting context $C^s$ associated to the chain context $C$ (with respect to $x$) is defined in Table VII.

For our example $C := (x.A)[x_1 \rightarrow x_2][x_2 \rightarrow x_3][x_3 \rightarrow (\cdot)]$ we have $C^s = ((\cdot).A)[x_1 \rightarrow x_2][x_2 \rightarrow x_3][x_3 \rightarrow x_4]$, as expected.

Rewriting Rules: the rules of the Unchaining FBC are in Table VII. Note that the exponential rule splits in two, the ordinary shallow case $\rightarrow_{oes}$ (now constrained to values) and the chain case $\rightarrow_{oe}$ (where the new definition play a role). They could be merged, but for the complexity analysis and the relationship with the next machine is better to distinguish them. We use $\rightarrow_{oe}$ for $\rightarrow_{oes} \cup \rightarrow_{oe}$, and $\rightarrow_{of}$ for $\rightarrow_{oa} \cup \rightarrow_{oe}$. Note the use of $C^s$ in the third side condition.

A. Linearity: Multiplicative vs Exponential Analysis.

To prove that $\rightarrow_{of}$ implements $\rightarrow_t$ with a global bound, and thus with a linear overhead, we need to show that the exponential number of exponential steps ($\rightarrow_{oe}$) in a $\rightarrow_{of}$-derivation is bound by the number of multiplicative steps ($\rightarrow_{oa}$). We need the following invariant.

Lemma 7 (Subterm Invariant). Let $t$ be a $\lambda$-term and $d : t \rightarrow^* u$. Then every value in $u$ is a value in $t$.

A substitution $t[x\rightarrow u]$ is basic if $u$ has the form $L(y)$. The basic size $|t|_b$ of $t$ is the number of its basic substitutions.

Lemma 8 (Steps and Basic Size).

1) If $t \rightarrow_{oes} u$ then $|u|_b = |t|_b$;
2) If $t \rightarrow_{oe} u$ then $|t|_b > 0$ and $|u|_b = |t|_b - 1$;
3) If $t \rightarrow_{oe} u$ then $|u|_b = |t|_b$ or $|u|_b = |t|_b + 1$.

Lemma 9. Let $t$ be initial and $d : t \rightarrow^*_{of} u$. Then $|u|_b \leq |d|_{oa} - |d|_{oe}$.

Proof: by induction on $|d|$. If $|d| = 0$ the statement holds.

If $|d| > 0$ consider the last step $w \rightarrow_{of} u$ of $d$ and the prefix $e : t \rightarrow_{oes} w$ of $d$. By i.h., $|w|_b \leq |e|_{oa} + |e|_{oe}$. Cases of $w \rightarrow_{of} u$.

Shallow Exponential Step $\rightarrow_{oes}$:

$|u|_b \leq_{L.8.1} |w|_b - 1$
$\leq_{i.h.} |e|_{oa} + |e|_{oe} - 1$
$= |e|_{oa} - (|e|_{oe} + 1) = |d|_{oa} - |d|_{oe}$

Chain Exponential Step $\rightarrow_{oe}$:

$|u|_b =_{L.8.2} |w|_b \leq_{i.h.} |e|_{oa} - |e|_{oe} = |d|_{oa} - |d|_{oe}$

$\rightarrow_{oa}^*$:

$|u|_b \leq_{L.8.3} |w|_b + 1$
$\leq_{i.h.} |e|_{oa} - |e|_{oe} + 1$
$= e + 1 - |e|_{oe} = |d|_{oa} - |d|_{oe}$

Corollary 2 (Linear Bound on Chain Exponential Steps). Let $t$ be initial and $d : t \rightarrow^*_{of} u$. Then $|d|_{oe} \leq |d|_{oa}$.

Next, we bound shallow steps.

Lemma 10 (Linear Bound on Shallow Exponential Steps). Let $t$ be initial and $d : t \rightarrow^*_{oe} u$. Then $|d|_{oe} \leq |d|_{oa}$.

Proof: first note that if $t \rightarrow_{oes} u$ then $u \rightarrow_{oa} w$, because by definition $\rightarrow_{oes}$ can fire only if it creates a $\rightarrow_{oa}$-redex. Such a fact and determinism of $\rightarrow_{of}$ together imply $|d|_{oe} \leq |d|_{oa} + 1$, because every $\rightarrow_{oes}$ step is matched by the eventual $\rightarrow_{oe}$ steps that follows it immediately. However, note that in $t$ there are no explicit substitutions so that the first step is necessarily an unmatched $\rightarrow_{oe}$ step. Thus $|d|_{oe} \leq |d|_{oa}$.

Theorem 11 (Linear Bound on Exponential Steps). Let $t$ be initial and $d : t \rightarrow^*_{oe} u$. Then $|d|_{oe} \leq 2 \cdot |d|_{oa}$.

Proof: by definition, $|d|_{oe} = |d|_{oe} + |d|_{oes}$. By Corollary 2, $|d|_{oe} \leq |d|_{oa}$ and by Lemma 10 $|d|_{oes} \leq |d|_{oa}$, and so $|d|_{oe} \leq 2 \cdot |d|_{oa}$.

We presented the interesting bit of the proof of our improved high-level implementation theorem, which follows. The remaining details are in [17].

Theorem 12 (Linear High-Level Implementation). $(\rightarrow_t, \rightarrow_{of})$ is a globally bounded high-level implementation system, and so it has a linear overhead wrt $\rightarrow_t$.

Last, the structural equivalence $\equiv$ is a strong bisimulation also for the Unchaining FBC.

Proposition 5 (≡ is a Strong Bisimulation). Let $x \in \{\text{oam, oae, oem}\}$. Then, $t \equiv u$ and $t \rightarrow_{oe} t'$ implies that there exists $u'$ such that $u \rightarrow_{oa} u'$ and $t' \equiv u'$.

XIV. UNCHAINING GLAMOUR

The Unchaining GLAMOUR machine, in Table VIII, behaves like the GLAMOUR machine until the code is a variable $x_1$ that is hereditarily bound in the global environment to a value via the chain $[x_1 \rightarrow x_2]^n \ldots [x_n \rightarrow v]^n$, and the stack is not empty (i.e. evaluation is in an applicative context). At this point the machine needs to traverse the chain until it finds the final binding $[x_n \rightarrow v]^n$, and then traverse again the chain in the opposite direction replacing every $[x_i \leftarrow x_{i+1}]^n$ entry with $[x_i \leftarrow v]^n$.

The forward traversal of the chain is implemented by a new commutative rule $\rightarrow_{cc}$ that pushes the variables encountered in the chain on a new machine component, called the chain heap. The backward traversal is driven by the next variable popped from the heap, and it is implemented by a new exponential rule (the chain exponential rule, corresponding to that of the calculus). Most of the analyses of the GLAMOUR carry over to the Unchaining GLAMOUR.
Every old grammar is as before, and heaps are simply lists of variables, \( i.e. \) they are defined by \( H ::= \epsilon \mid H : x \).

**Decoding and Invariants:** because of chain heaps and chain contexts, the decoding is provided.

First of all, note that there is a correlation between the chain and the environment, as the variables of a chain heap \( H = x_1 : \ldots : x_n \) need to have corresponding entries \([x_i \mapsto x_i]_{i=1}^{n+1}\).

More precisely, we will show that the following notion of compatibility is an invariant of the machine.

**Definition 7** (Compatibility Heap-Environment). Let \( E \) be an environment and \( H = x_1 : \ldots : x_n \) be a heap. We say that \( H \) is compatible with \( E \) if either \( H \) is empty or \([x_i \mapsto x_i]_{i=1}^{n+1}\) is in \( E \) for \( n < n', [x_n \mapsto x_n'] \in E \), and \([x_i \mapsto x_i'] \in E \) for some \( i' \).

Given a state \( s = (D, H, \overline{t}, \pi, E) \), the dump, the stack and the environment provide a shallow context \( S_s := \langle D(\overline{t}) \rangle E \) that will be shown to be evaluable, as for the GLAMOUR.

If the chain heap \( H \) is not empty, the current code \( \overline{t} \) is somewhere in the middle of a chain inside the environment, and it is not apt to fill the state context \( S_s \). The right code is the variable \( x_1 \) starting the chain heap \( H = x_1 : \ldots : x_n \).

Thus, the term to plug in the state context is \( \overline{t}^H \), given by:

\[
\overline{t}^H := \overline{t} \overline{x} : \ldots : x_n := x_1
\]

Finally, a state decodes to a term as follows: \( \overline{t} := S_s(\overline{t}^H) \).

**Lemma 11** (Unchaining GLAMOUR Invariants). Let \( s = (D, H, \overline{t}, \pi, E) \) be a state reachable from an initial code \( \overline{t} \).

1) Closure: \( s \) is closed and \( s \) is well named;
2) Value: values in components of \( s \) are subterms of \( \overline{t} \);
3) Fireball: \( \overline{t}_{\overline{L}} = \overline{t}^k \) is a fireball (of kind l) for every code \( \overline{t}^k \) in \( \pi \) and \( E \);
4) Evaluability: \( E, \overline{D}_{\overline{L}}^k, \overline{X}_{\overline{E}}^k \) and \( S_s \) are evaluable cont.;
5) Environment Size: the length of the global environment \( E \) is bounded by \( |\rho|_{\overline{m}} \);
6) Compatible Heap: if \( H \neq \epsilon \) then the stack is not empty, \( \pi = x \), and \( H \) is compatible with \( E \).

We need additional decodings to retrieve the chain-starting context \( C \) in the side-condition of \( \overline{\rho}_{\overline{oc}} \) rule, that—unsurprisingly—is given by the chain heap. Let \( s = (D, H : y, \overline{t}, \pi, E) \) be a state s.t. \( H : y \) is compatible with \( E \). Note that compatibility gives \( E = E_1[y \mapsto \overline{t}] \). Define the chain context \( C_s \) and the substitution context \( L_s \) as:

\[
C_s := \langle D(\langle y^H \rangle \overline{t}) \rangle E_1[y \mapsto \langle \cdot \rangle] \quad L_s := E_2
\]

The first point of the following lemma guarantees that \( C_s \) and \( L_s \) are well defined. The second point proves that filling \( L_s(C_s) \) with the current term gives exactly the decoding of the state \( s \).

**Lemma 12** (Heaps and Contexts). Let \( s = (D, H : y, x, \pi, E) \) be a state s.t. \( H : y \) is compatible with \( E \). Then:

1) \( L_s \) is a substitution context and \( C_s \) is a chain context;
2) \( s, t \in S_s(\langle y^H \rangle \overline{t}) \) then \( C_s \) is identical to that of the GLAMOUR, thus we omit it and focus on \( \overline{\rho}_{\overline{oc}} \).

The size \( |H| \) of a chain heap is its length as a list.

**Theorem 13** (Unchaining GLAMOUR Distillation).

(\( \overline{\rho}_{\overline{oc}} \) is a reflective explicit distillery. In particular, let \( s \) be a reachable state:

1) Commutative: if \( s \overline{\rho}_{\overline{c}} \overline{c} \) then \( s = s' \);
2) Multiplicative: if \( s \overline{\rho}_{\overline{c}} \overline{c} \) then \( s = s' \);
3) Shallow Exponential: if \( s \overline{\rho}_{\overline{c}} \overline{c} \) then \( s = s' \);
4) Chain Exponential: if \( s \overline{\rho}_{\overline{c}} \overline{c} \) then \( s = s' \).

A. Bilinearity: Principal vs Commutative Analysis

Bilinearity \( \overline{\rho}_{\overline{c}} \) is identical to that of the GLAMOUR, thus we omit it and focus on \( \overline{\rho}_{\overline{oc}} \).

The size \( |H| \) of a chain heap is its length as a list.

**Lemma 14** (Linearity of \( \overline{\rho}_{\overline{oc}} \)). Let \( s = (D, H, \overline{t}, \pi, E) \) be a state reachable by an execution \( \rho \). Then:

1) \( |\rho|_{\overline{oc}} = |H| + |\rho|_{\overline{oc}} \)
2) \( |H| \leq |\rho|_{\overline{m}} \)
3) \( |\rho|_{\overline{oc}} \leq |\rho|_{\overline{m}} + |\rho|_{\overline{oc}} = O(1 + |\rho|_{\overline{m}} \cdot |\overline{t}|) \)

**Proof:** 1) By induction over \( |\rho| \) and analysis of the last machine transition. The \( \overline{\rho}_{\overline{oc}} \) steps increment the size of the heap. The \( \overline{\rho}_{\overline{oc}} \) steps decrement it. All other steps do not change the heap. 2) By the compatible heap invariant (Lemma 11.6), \( |H| \leq |E| \). By the environment size invariant (Lemma 11.5), \( |E| \leq |\rho|_{\overline{m}} \). Then \( |H| \leq |\rho|_{\overline{m}} \). 3) Plugging Point 2 into Point 1.

**Corollary 3** (Bilinearity of \( \overline{\rho}_{\overline{c}} \)). Let \( s \) be a state reached by an execution \( \rho \) of initial code \( \overline{t} \). Then \( |\rho|_{\overline{c}} \leq (1 + |\rho|_{\overline{c}}) |\overline{t}| + |\rho|_{\overline{m}} + |\rho|_{\overline{oc}} = O(1 + |\rho|_{\overline{m}} \cdot |\overline{t}|) \).

Finally, we obtain the main result of the paper.
Theorem 14 (Useful Implementation).

1) Low-Level Bilinear Implementation: $a \rightarrow_\alpha$-derivation $d$ is implementable on RAM in $O((1 + |d|) \cdot |t|)$ steps.
2) Low + High Bilinear Implementation: $a \rightarrow_\alpha$-derivation $d$ is implementable on RAM in $O((1 + |d|) \cdot |t|)$ steps.

Let us conclude with a remark. Our result requires a compact representation of terms via ES. Because unfolding may exponentially increase the size of a term, it is important to show that common operations like equality checking (up to $\alpha$-conversion) can be implemented efficiently on the compact representation. In other words, ES are succinct data structures, in the sense of Jacobson [37].

Despite quadratic and quasi-linear recent algorithms [6], [38] for testing equality of terms with ES, we discovered that a linear algorithm can be obtained by slightly modifying an algorithm already known quite some time before (1976!): the Paterson-Wegmar linear unification algorithm [39] (better explained in [40]). The algorithm works on first order terms represented as DAGs, and unification boils down to equality checking when no metavariable occurs in the involved terms.

Our terms with ES can not be fed directly to the Paterson-Wegmar algorithm: we represent shared terms via occurrences of variables bound in substitutions, whereas Paterson-Wegmar uses a simple DAG representation. The change of representation can be easily done in linear time in the size of the input.

Moreover, the Paterson-Wegmar algorithm works with standard equality, whereas we are interested in $\alpha$-equivalence. Therefore the algorithm needs to be adapted so that two $\lambda$-bound variables are considered equivalent when they point to binding nodes that have already been determined to be candidates for equality. The details of the adaptation of Paterson-Wegmar are left to a forthcoming publication.

ACKNOWLEDGEMENTS

A special acknowledgement to Ugo Dal Lago, to whom we owe the intuition that using labels may lead to a local and efficient implementation of useful sharing. We are also grateful to François Pottier, whose comments on a draft helped to improve the terminology and the presentation.

REFERENCES