A Sound and Complete Calculus for Reversible Circuit Equivalence

Abstract

Many recent advances in quantum computing, low-power design, nanotechnology, optical information processing, and bioinformatics are based on *reversible circuits*. With the aim of designing a semantically well-founded approach for modeling and reasoning about reversible circuits, we propose viewing such circuits as proof terms witnessing equivalences between finite types. Proving that these type equivalences satisfy the commutative semiring axioms, we proceed with the categorification of type equivalences as *symmetric rig weak groupoids*. The coherence conditions of these categories then produce, for free, a sound and complete calculus for reasoning about reversible circuit equivalence. The paper consists of the "unformalization" of an Agda package formalizing the connections between reversible circuits, equivalences between finite types, permutations between finite sets, and symmetric rig weak groupoids.

1. Introduction

Because physical laws obey various conservation principles (including conservation of information) and because computation is fundamentally a physical process, every computation is, at the physical level, fundamentally an equivalence that preserves information. The idea that computation, at the logical and programming level, should also be based on "equivalences" (i.e., invertible processes) was originally motivated by such physical considerations (Feynman 1982; Landauer 1961; Peres 1985; Bennett 1973; Toffoli 1980; Fredkin and Toffoli 1982). More recently, the rising importance of energy conservation, the shrinking size of technology at which quantum effects become noticeable, and the potential for quantum computation and communication, are additional physical considerations adding momentum to such reversible computational models (Frank 1999; DeBenedictis 2005). From a more theoretical perspective, the recently proposed "univalent" foundation of mathematics (The Univalent Foundations Program 2013), based on Homotopy Type Theory (HoTT), greatly emphasizes computation based on *equivalences* that are satisfied up to equivalences that are themselves satisfied up to equivalence, etc.

To summarize, we are witnessing a convergence of ideas from several distinct research communities (physics, mathematics, and computer science) towards basing computations on equivalences (Baez and Stay 2011). A first step in that direction was the development of many *reversible programming languages* (e.g., (Yokoyama and Glück 2007; Mackie 2011; Di Pierro et al. 2006; Kluge 2000; Mu et al. 2004; Abramsky 2005).) Typically, programs in these languages correspond to some notion of equivalence. But reasoning *about* these programs abandons the notion of equivalence and uses conventional irreversible functions to specify evaluators and the derived notions of program equivalence. This unfortunately misses the beautiful combinatorial structure of programs and proofs that was first exposed in the historical paper by Hofmann and Streicher (1996) and that is currently the center of attention of HoTT and that requires keeping the focus on equivalences not only at the conventional level of programs but also at the higher levels of programs manipulating equivalences about other programs.

This paper addresses — and completely solves — a well-defined part of the general problem of programming with equivalences up to equivalences. Our approach, we argue, might also be suitable for the more general problem. The particular problem we focus on is that of programming with the finite types built from the empty type, the unit type, and closed under sums and products. Although limited in their expressive power, these types are rich enough to express all combinational (with no state or feedback) hardware circuits and as we show already exhibit substantial combinatorial structure at the "next level", i.e., at the level of equivalences about equivalences of types. What emerges from our study are the following results:

- a universal language for combinational reversible circuits that comes with a calculus for writing circuits and a calculus for manipulating that calculus;
- the language itself subsumes various representations for reversible circuits, e.g., truth tables, matrices, product of permutation cycles, etc. (Saeedi and Markov 2013);
- the first set of rules is sound and complete with respect to equivalences of types;
- the second set of rules is sound and complete with respect to equivalences of equivalences of types as specified by the first set of rules;

Outline. The next section reviews equivalences between finite types and relates them to various commutative semiring structures. The main message of that section is that, up to equivalence, the concept of equivalence of finite types is equivalent to permutations between finite sets. The latter is computationally well-behaved with existing reversible programming languages developed for programming with permutations and finite-type isomorphisms. This family of languages, called Π, is universal for describing combinational (without feedback or state) reversible circuits (see Sec. 3). The infrastructure of the HoTT-inspired type equivalences enriches these languages by viewing their original design as 1-paths and systematically producing 2-paths (equivalences between equivalences) manifesting themselves as syntactic rules for reasoning about equiva-

lences of programs representing reversible circuits. Sec. 4 starts the semantic investigation of the Π languages emphasizing the denotational approach that maps each Π program to a type equivalence or a permutation. The section also gives a small example showing how a few rules that are sound with respect to equivalence of permutations can be used to transform Π programs without reliance on any extensional reasoning. Sec. 5 then reveals that these rules are intimately related to the coherence conditions of the categorified analogues of type equivalences and permutations, namely, the so-called *symmetric rig weak groupoids*. Sec. 6 contains that "punchline": a sound and complete set of rules that can be used to reason about Π programs and their equivalences. Before concluding, we devote Sec. 7 to a detailed analysis of higher-order functions in the setting we describe suggesting a possible path towards a solution. We note that because the issues involved are quite subtle, the paper is the "unformalization" of an executable `Agda 2.4.2.3` package with the global `without-K` option enabled.

2. Equivalences and Commutative Semirings

Our starting point is the notion of equivalence of types. We then connect this notion to several semiring structures on finite types, on permutations, and on equivalences, with the goal of reducing the notion of equivalence for finite types to a notion of reversible computation.

2.1 Finite Types

The elementary building blocks of type theory are the empty type ($\bot$), the unit type ($\top$), and the sum ($\uplus$) and product ($\times$) types. These constructors can encode any *finite type*. Traditional type theory also includes several facilities for building infinite types, most notably function types. We will however not address infinite types in this paper except for a discussion in Sec. 7. We will instead focus on thoroughly understanding the computational structures related to finite types.

An essential property of a finite type A is its size $|A|$ which is defined as follows:

$$\begin{array}{rcl} |\bot| & = & 0 \\ |\top| & = & 1 \\ |A \uplus B| & = & |A| + |B| \\ |A \times B| & = & |A| * |B| \end{array}$$

A result by Fiore (2004); Fiore et al. (2006) completely characterizes the isomorphisms between finite types using the axioms of commutative semirings. (See Appendix A for the complete definition of commutative semirings.) Intuitively this result states that one can interpret each type by its size, and that this identification validates the familiar properties of the natural numbers, and is in fact isomorphic to the commutative semiring of the natural numbers.

Our work builds on this identification together with work by James and Sabry (2012a) which introduced the Π family of languages whose core computations are these isomorphisms between finite types. Taking into account the growing-in-importance idea that isomorphisms have interesting computational content and should not be silently or implicitly identified, we first recast Fiore et. al's result in the next section, making explicit that the commutative semiring structure can be defined up to the HoTT relation of *type equivalence* instead of strict equality $=$.

2.2 Commutative Semirings of Types

There are several equivalent definitions of the notion of equivalence of types (The Univalent Foundations Program 2013). For concreteness, we use the following definition as it appears to be the most intuitive in our setting.

Definition 1 (Quasi-inverse)**.** *For a function $f : A \to B$, a* quasi-inverse *of f is a triple (g, α, β), consisting of a function $g : B \to A$ and homotopies $\alpha : f \circ g = \mathrm{id}_B$ and $\beta : g \circ f = \mathrm{id}_A$.*

Definition 2 (Equivalence of types)**.** *Two types A and B are equivalent $A \simeq B$ if there exists a function $f : A \to B$ together with a quasi-inverse for f.*

As the definition of equivalence is parameterized by a function f, we are concerned with, not just the fact that two types are equivalent, but with the precise way in which they are equivalent. For example, there are two equivalences between the type Bool and itself: one that uses the identity for f (and hence for the quasi-inverse) and one that uses boolean negation for f (and hence for the quasi-inverse). These two equivalences are themselves *not* equivalent: each of them can be used to "transport" properties of Bool in a different way.

It is straightforward to prove that the universe of types (Set in Agda terminology) is a commutative semiring up to equivalence of types $\simeq$.

Theorem 1. *The collection of all types (Set) forms a commutative semiring (up to $\simeq$).*

Proof. As expected, the additive unit is $\bot$, the multiplicative unit is $\top$, and the two binary operations are $\uplus$ and $\times$. □

For example, we have equivalences such as:

$$\begin{array}{rcl} \bot \uplus A & \simeq & A \\ \top \times A & \simeq & A \\ A \times (B \times C) & \simeq & (A \times B) \times C \\ A \times \bot & \simeq & \bot \\ A \times (B \uplus C) & \simeq & (A \times B) \uplus (A \times C) \end{array}$$

One of the advantages of using equivalence $\simeq$ instead of strict equality $=$ is that we can reason one level up about the type of all equivalences $\mathrm{EQ}_{A,B}$. For a given A and B, the elements of $\mathrm{EQ}_{A,B}$ are all the ways in which we can prove $A \simeq B$. For example, $\mathrm{EQ}_{\mathsf{Bool},\mathsf{Bool}}$ has two elements corresponding to the id-equivalence and to the negation-equivalence that were mentioned before. More generally, for finite types A and B, the type $\mathrm{EQ}_{A,B}$ is only inhabited if A and B have the same size in which case the type has $|A|\,!$ (factorial of the size of A) elements witnessing the various possible identifications of A and B. The type of all equivalences has some non-trivial structure: in particular, it is itself a commutative semiring.

Theorem 2. *The type of all equivalences $\mathrm{EQ}_{A,B}$ for finite types A and B forms a commutative semiring up to extensional equivalence of equivalences.*

Proof. The most important insight is the definition of equivalence of equivalences. Two equivalences $e_1, e_2 : \mathrm{EQ}_{A,B}$ with underlying functions f_1 and f_2 and underlying quasi-inverses g_1 and g_2 are themselves equivalent if we have that both $f_1 = f_2$ and $g_1 = g_2$ extensionally. Given this notion of equivalence of equivalences, the proof proceeds smoothly with the additive unit being the vacuous equivalence $\bot \simeq \bot$, the multiplicative unit being the trivial equivalence $\top \simeq \top$, and the two binary operations being essentially a mapping of $\uplus$ and $\times$ over equivalences. □

We reiterate that the commutative semiring axioms in this case are satisfied up to extensional equality of the functions underlying the equivalences. We could, in principle, consider a weaker notion of equivalence of equivalences and attempt to iterate the construction but for the purposes of modeling circuits and optimizations, it is sufficient to consider just one additional level.

2.3 Commutative Semirings of Permutations

Type equivalences are fundamentally based on function extensionality (Def. 1 explicitly compares functions for extensional equality.) It is folklore that, even when restricted to finite types, function extensionality needs to be assumed for effective reasoning about about type equivalences. The situation gets worse when considering equivalences of equivalences. In the HoTT context, this is the open problem of finding a computational interpretation for *univalence*. In the case of finite types however, there is a computationally-friendly alternative characterization of type equivalences based on permutations of finite sets, which we prove to be formally equivalent.

The idea is that, *up to equivalence*, the only interesting property of a finite type is its size, so that type equivalences must be size-preserving maps and hence correspond to permutations. For example, given two equivalent types A and B of completely different structure, e.g., $A = (\top \uplus \top) \times (\top \uplus (\top \uplus \top))$ and $B = \top \uplus (\top \uplus (\top \uplus (\top \uplus (\top \uplus (\top \uplus \bot)))))$, we can find equivalences from either type to the finite set $\mathsf{Fin}\ 6$ and reduce all type equivalences between sets of size 6 to permutations.

We begin with the following theorem which precisely characterizes the relationship between finite types and finite sets.

Theorem 3. *If $A \simeq \mathsf{Fin}\ m$, $B \simeq \mathsf{Fin}\ n$ and $A \simeq B$ then $m = n$.*

Proof. We proceed by cases on the possible values for m and n. If they are different, we quickly get a contradiction. If they are both 0 we are done. The interesting situation is when $m = suc\ m'$ and $n = suc\ n'$. The result follows in this case by induction assuming we can establish that the equivalence between A and B, i.e., the equivalence between $\mathsf{Fin}\ (suc\ m')$ and $\mathsf{Fin}\ (suc\ n')$, implies an equivalence between $\mathsf{Fin}\ m'$ and $\mathsf{Fin}\ n'$. In a constructive setting, we actually need to construct a particular equivalence between the smaller sets given the equivalence of the larger sets with one additional element. This lemma is quite tedious as it requires us to isolate one element of $\mathsf{Fin}\ (suc\ m')$ and analyze every class of positions this element could be mapped to by the larger equivalence and in each case construct an equivalence that excludes this element. □

Given the correspondence between finite types and finite sets, we now prove that equivalences on finite types are equivalent to permutations on finite sets. We proceed in steps: first by proving that finite sets for a commutative semiring up to $\simeq$ (Thm. 4); second by proving that, at the next level, the type of permutations between finite sets is also a commutative semiring up to strict equality of the representations of permutations (Thm. 5); third by proving that the type of type equivalences is equivalent to the type of permutations (Thm. 6); and finally by proving that the commutative semiring of type equivalences is isomorphic to the commutative semiring of permutations (Thm. 7). This series of theorems will therefore justify our focus in the next section of develop a term language for permutations as a way to compute with type equivalences.

Theorem 4. *The collection of all finite types ($\mathsf{Fin}\ m$ for natural number m) forms a commutative semiring (up to $\simeq$).*

Proof. The additive unit is $\mathsf{Fin}\ 0$ and the multiplicative unit is $\mathsf{Fin}\ 1$. For the two binary operations, the proof crucially relies on the following equivalences:

$$\begin{array}{ll} \mathsf{iso\text{-}plus} & : \{m\ n : \mathbb{N}\} \to (\mathsf{Fin}\ m \uplus \mathsf{Fin}\ n) \simeq \mathsf{Fin}\ (m + n) \\ \mathsf{iso\text{-}times} & : \{m\ n : \mathbb{N}\} \to (\mathsf{Fin}\ m \times \mathsf{Fin}\ n) \simeq \mathsf{Fin}\ (m * n) \end{array}$$

□

Theorem 5. *The collection of all permutations $\mathrm{PERM}_{m,n}$ between finite sets $\mathsf{Fin}\ m$ and $\mathsf{Fin}\ n$ forms a commutative semiring up to strict equality of the representations of the permutations.*

Proof. The proof requires delicate attention to the representation of permutations as straightforward attempts turn out not to capture enough of the properties of permutations. A permutation of one set to another is represented using two sizes: n for the size of the input finite set and m for the size of the resulting finite set. Naturally in any well-formed permutations, these two sizes are equal but the presence of both types allows us to conveniently define a permutation $\mathsf{CPerm}\ m\ n$ using four components. The first two components are (i) a vector of size n containing elements drawn from the finite set $\mathsf{Fin}\ m$, and (ii) a dual vector of size m containing elements drawn from the finite set $\mathsf{Fin}\ n$. Each of these vectors can be interpreted as a map f that acts on the incoming finite set sending the element at index i to position $f!!i$ in the resulting finite set. To guarantee that these maps define an actual permutation, the last two components are proofs that the sequential composition of the maps in both directions produce the identity. Given this representation, we can prove that two permutations are equal if the underlying vectors are strictly equal. The proof proceeds using the vacuous permutation $\mathsf{CPerm}\ 0\ 0$ for the additive unit and the trivial permutation $\mathsf{CPerm}\ 1\ 1$ for the multiplicative unit. The binary operations on permutations map $\mathsf{CPerm}\ m_1\ m_2$ and $\mathsf{CPerm}\ n_1\ n_2$ to $\mathsf{CPerm}\ (m_1 + n_1)\ (m_2 + n_2)$ and $\mathsf{CPerm}\ (m_1 * n_1)\ (m_2 * n_2)$ respectively. Their definition relies on the important property that the union or product of vectors denoting permutations distributes over the sequential composition of permutations. □

Theorem 6. *If $A \simeq \mathsf{Fin}\ m$ and $B \simeq \mathsf{Fin}\ n$, then the type of all equivalences $\mathrm{EQ}_{A,B}$ is equivalent to the type of all permutations $\mathrm{PERM}\ m\ n$.*

Proof. The main difficulty in this proof was to generalize from sets to setoids to make the equivalence relations explicit. The proof is straightforward but long and tedious. □

Theorem 7. *The equivalence of Theorem 6 is an* isomorphism *between the commutative semiring of equivalences of finite types and the commutative semiring of permutations.*

Proof. In the process of this proof, we show that every axiom of semirings of types is an equivalence, and thus corresponds to a permutation. Some of the axioms like the associativity of sums gets mapped to the trivial identity permutation. However, some are axioms reveal interesting structure as permutations; the most notable is that the commutativity of products maps to a permutation solving the classical problem of in-place matrix transposition. □

Before concluding, we briefly mention that, with the proper Agda definitions, Thm. 6 can be rephrased in a more evocative way as follows.

Theorem 8.

$$(A \simeq B) \simeq \mathsf{Perm}|A||B|$$

This formulation shows that the univalence *postulate* can be proved and given a computational interpretation for finite types.

3. Programming with Permutations

In the previous section, we argued that, up to equivalence, the equivalence of types reduces to permutations on finite sets. We recall background work which proposed a term language for permutations and adapt it in later sections to be used to express, compute with, and reason about type equivalences between finite types.

$$
\begin{array}{rrcll}
identl_+ : & 0 + \tau & \leftrightarrow & \tau & : identr_+ \\
swap_+ : & \tau_1 + \tau_2 & \leftrightarrow & \tau_2 + \tau_1 & : swap_+ \\
assocl_+ : & \tau_1 + (\tau_2 + \tau_3) & \leftrightarrow & (\tau_1 + \tau_2) + \tau_3 & : assocr_+ \\
\\
identl_* : & 1 * \tau & \leftrightarrow & \tau & : identr_* \\
swap_* : & \tau_1 * \tau_2 & \leftrightarrow & \tau_2 * \tau_1 & : swap_* \\
assocl_* : & \tau_1 * (\tau_2 * \tau_3) & \leftrightarrow & (\tau_1 * \tau_2) * \tau_3 & : assocr_* \\
\\
dist_0 : & 0 * \tau & \leftrightarrow & 0 & : factorl_0 \\
dist : & (\tau_1 + \tau_2) * \tau_3 & \leftrightarrow & (\tau_1 * \tau_3) + (\tau_2 * \tau_3) & : factor
\end{array}
$$

$$
\frac{}{\vdash id : \tau \leftrightarrow \tau} \qquad \frac{\vdash c_1 : \tau_1 \leftrightarrow \tau_2 \quad \vdash c_2 : \tau_2 \leftrightarrow \tau_3}{\vdash c_1 \fatsemi c_2 : \tau_1 \leftrightarrow \tau_3}
$$

$$
\frac{\vdash c_1 : \tau_1 \leftrightarrow \tau_2 \quad \vdash c_2 : \tau_3 \leftrightarrow \tau_4}{\vdash c_1 \oplus c_2 : \tau_1 + \tau_3 \leftrightarrow \tau_2 + \tau_4}
$$

$$
\frac{\vdash c_1 : \tau_1 \leftrightarrow \tau_2 \quad \vdash c_2 : \tau_3 \leftrightarrow \tau_4}{\vdash c_1 \otimes c_2 : \tau_1 * \tau_3 \leftrightarrow \tau_2 * \tau_4}
$$

Figure 1. Π-combinators (Bowman et al. 2011; James and Sabry 2012a)

3.1 The Π-Languages

Bowman et al. (2011); James and Sabry (2012a) introduced the Π family of languages whose only computations are permutations (isomorphisms) between finite types and which is complete for all reversible combinational circuits. We propose that this family of languages is exactly the right programmatic interface for manipulating and reasoning about type equivalences.

The syntax of the previously-developed Π language consists of types τ including the empty type 0, the unit type 1, and conventional sum and product types. The values classified by these types are the conventional ones: $()$ of type 1, $\mathsf{inl}\ v$ and $\mathsf{inr}\ v$ for injections into sum types, and (v_1, v_2) for product types:

$$
\begin{array}{lrcl}
(\textit{Types}) & \tau & ::= & 0 \mid 1 \mid \tau_1 + \tau_2 \mid \tau_1 * \tau_2 \\
(\textit{Values}) & v & ::= & () \mid \mathsf{inl}\ v \mid \mathsf{inr}\ v \mid (v_1, v_2) \\
(\textit{Combinator types}) & & & \tau_1 \leftrightarrow \tau_2 \\
(\textit{Combinators}) & c & ::= & [\textit{see Fig. 1}]
\end{array}
$$

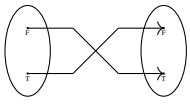
The interesting syntactic category of Π is that of *combinators* which are witnesses for type isomorphisms $\tau_1 \leftrightarrow \tau_2$. They consist of base combinators (on the left side of Fig. 1) and compositions (on the right side of the same figure). Each line of the figure on the left introduces a pair of dual constants[1] that witness the type isomorphism in the middle. Every combinator c has an inverse $!c$ according to the figure. The inverse is homomorphic on sums and products and flips the order of the combinator in sequential composition.

3.2 Example Circuits

The language Π is universal for reversible combinational circuits (James and Sabry 2012a).[2] We illustrate the expressiveness of the language with a few short examples.

The first example is simply boolean encoding and negation which can defined as shown on the left and visualized as a permutation on the right:

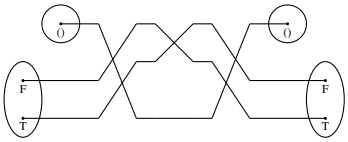
```
BOOL : U
BOOL = PLUS ONE ONE

NOT₁ : BOOL ↔ BOOL
NOT₁ = swap₊
```



Naturally there are many ways of encoding boolean negation. The following example implements a more convoluted circuit that computes the same function:

```
NOT₂ : BOOL ↔ BOOL
NOT₂ =   uniti⋆ ⊙
         swap⋆ ⊙
         (swap₊ ⊗ id↔) ⊙
         swap⋆ ⊙
         unite⋆
```

Viewing this combinator as a permutation on finite sets, we might visualize it as follows:



Writing circuits using the raw syntax for combinators is clearly tedious. In other work, one can find a compiler from a conventional functional language to generate the circuits (James and Sabry 2012a), a systematic technique to translate abstract machines to Π (James and Sabry 2012b), and a Haskell-like surface language (James and Sabry 2014) which can be of help in writing circuits. These essential tools are however a distraction in the current setting and we content ourselves with some Agda syntactic sugar illustrated below and used again in the next section:

```
BOOL² : U
BOOL² = TIMES BOOL BOOL

CNOT : BOOL² ↔ BOOL²
CNOT = TIMES BOOL BOOL
       ↔⟨ id↔ ⟩
     TIMES (PLUS x y) BOOL
       ↔⟨ dist ⟩
     PLUS (TIMES x BOOL) (TIMES y BOOL)
       ↔⟨ id↔ ⊕ (id↔ ⊗ NOT₁) ⟩
     PLUS (TIMES x BOOL) (TIMES y BOOL)
       ↔⟨ factor ⟩
     TIMES (PLUS x y) BOOL
       ↔⟨ id↔ ⟩
     TIMES BOOL BOOL □
     where x = ONE; y = ONE

TOFFOLI : TIMES BOOL BOOL² ↔ TIMES BOOL BOOL²
TOFFOLI = TIMES BOOL BOOL²
       ↔⟨ id↔ ⟩
     TIMES (PLUS x y) BOOL²
       ↔⟨ dist ⟩
     PLUS (TIMES x BOOL²) (TIMES y BOOL²)
       ↔⟨ id↔ ⊕ (id↔ ⊗ CNOT) ⟩
     PLUS (TIMES x BOOL²) (TIMES y BOOL²)
       ↔⟨ factor ⟩
     TIMES (PLUS x y) BOOL²
```

[1] where $swap_+$ and $swap_*$ are self-dual.

[2] With the addition of recursive types and trace operators (Hasegawa 1997), Π become a Turing complete reversible language (James and Sabry 2012a; Bowman et al. 2011).

```
    ↔⟨ id↔ ⟩
    TIMES BOOL BOOL² □
  where x = ONE; y = ONE
```

This style makes the intermediate steps explicit showing how the types are transformed in each step by the combinators. The example incidentally confirms that Π is universal for reversible circuits since the Toffoli gate is universal for such circuits (Toffoli 1980).

4. Semantics

In the previous sections, we established that type equivalences on finite types can be, up to equivalence, expressed as permutations and proposed a term language for expressing permutations on finite types that is complete for reversible combinational circuits. We are now ready for the main technical contribution of the paper: an effective computational framework for reasoning *about* type equivalences. From a programming perspective, this framework manifests itself as a collection of rewrite rules for optimizing circuit descriptions in Π. Naturally we are not concerned with just any collection of rewrite rules but with a sound and complete collection. The current section will set up the framework and illustrate its use on one example and the next sections will introduce the categorical framework in which soundness and completeness can be proved.

4.1 Operational and Denotational Semantics

In conventional programming language research, valid optimizations are specified with reference to the *observational equivalence* relation which itself is defined with reference to an *evaluator*. As the language is reversible, a reasonable starting point would then be to define forward and backward evaluators with the following signatures:

```
eval  : {t₁ t₂ : U} → (t₁ ↔ t₂) → ⟦ t₁ ⟧ → ⟦ t₂ ⟧
evalB : {t₁ t₂ : U} → (t₁ ↔ t₂) → ⟦ t₂ ⟧ → ⟦ t₁ ⟧
```

In the definition, the function $[\![\cdot]\!]$ maps each type constructor to its Agda denotation, e.g., it maps the type 0 to $\bot$, the type 1 to $\top$, etc. The complete definitions for these evaluators can be found in the papers by Bowman et al. (2011); James and Sabry (2012b,a) (and in the accompanying Agda code) and will not be repeated here. The reason is that, although these evaluators adequately serve as semantic specifications, they drive the development towards extensional reasoning as evident from the signatures which map a permutation to a function. We will instead pursue a denotational approach mapping the combinators to type equivalences or equivalently to permutations:

```
c2equiv : {t₁ t₂ : U} → (c : t₁ ↔ t₂) → ⟦ t₁ ⟧ ≃ ⟦ t₂ ⟧
c2perm  : {t₁ t₂ : U} → (c : t₁ ↔ t₂) →
          CPerm (size t₂) (size t₁)
```

The advantage is that permutations have a concrete representation which can be effectively compared for equality as explained in the proof of Thm. 5.

4.2 Rewriting Approach

Having mapped each combinator to a permutation, we can reason about valid optimizations mapping a combinator to another by studying the equivalence of permutations on finite sets. The traditional definition of equivalence might equate two permutations if their actions on every input produce the same output but we again resist that extensional reasoning. Instead we are interested in a calculus, a set of rules, that can be used to rewrite combinators preserving their meaning. It is trivial to come up with a few rules such as:

```
id⇔    : {t₁ t₂ : U} {c : t₁ ↔ t₂} → c ⇔' c

trans⇔ : {t₁ t₂ : U} {c₁ c₂ c₃ : t₁ ↔ t₂} →
         (c₁ ⇔' c₂) → (c₂ ⇔' c₃) → (c₁ ⇔' c₃)

assoc⇔ : {t₁ t₂ t₃ t₄ : U}
         {c₁ : t₁ ↔ t₂} {c₂ : t₂ ↔ t₃} {c₃ : t₃ ↔ t₄} →
         (c₁ ⊙ (c₂ ⊙ c₃)) ⇔' ((c₁ ⊙ c₂) ⊙ c₃)

id⊙⇔   : {t₁ t₂ : U} {c : t₁ ↔ t₂} →
         (id↔ ⊙ c) ⇔' c

swap₊⇔ : {t₁ t₂ t₃ t₄ : U}
         {c₁ : t₁ ↔ t₂} {c₂ : t₃ ↔ t₄} →
         (swap₊ ⊙ (c₁ ⊕ c₂)) ⇔' ((c₂ ⊕ c₁) ⊙ swap₊)
```

which are evidently sound. The challenge of course is to come up with a sound and complete set of such rules.

Before we embark on the categorification program in the next section, we show that, with some ingenuity, one can develop a reasonable set of rewrite rules that would allow us to prove that the two negation circuits from the previous section are actually equivalent:

```
negEx : NOT₂ ⇔ NOT₁
negEx =
  uniti⋆ ⊙ (swap⋆ ⊙ ((swap₊ ⊗ id↔) ⊙ (swap⋆ ⊙ unite⋆)))
    ⇔⟨ id⇔ ◫ assoc⊙l ⟩
  uniti⋆ ⊙ ((swap⋆ ⊙ (swap₊ ⊗ id↔)) ⊙ (swap⋆ ⊙ unite⋆))
    ⇔⟨ id⇔ ◫ (swapl⋆⇔ ◫ id⇔) ⟩
  uniti⋆ ⊙ (((id↔ ⊗ swap₊) ⊙ swap⋆) ⊙ (swap⋆ ⊙ unite⋆))
    ⇔⟨ id⇔ ◫ assoc⊙r ⟩
  uniti⋆ ⊙ ((id↔ ⊗ swap₊) ⊙ (swap⋆ ⊙ (swap⋆ ⊙ unite⋆)))
    ⇔⟨ id⇔ ◫ (id⇔ ◫ assoc⊙l) ⟩
  uniti⋆ ⊙ ((id↔ ⊗ swap₊) ⊙ ((swap⋆ ⊙ swap⋆) ⊙ unite⋆))
    ⇔⟨ id⇔ ◫ (id⇔ ◫ (linv⊙l ◫ id⇔)) ⟩
  uniti⋆ ⊙ ((id↔ ⊗ swap₊) ⊙ (id↔ ⊙ unite⋆))
    ⇔⟨ id⇔ ◫ (id⇔ ◫ idl⊙l) ⟩
  uniti⋆ ⊙ ((id↔ ⊗ swap₊) ⊙ unite⋆)
    ⇔⟨ assoc⊙l ⟩
  (uniti⋆ ⊙ (id↔ ⊗ swap₊)) ⊙ unite⋆
    ⇔⟨ unitil⋆⇔ ◫ id⇔ ⟩
  (swap₊ ⊙ uniti⋆) ⊙ unite⋆
    ⇔⟨ assoc⊙r ⟩
  swap₊ ⊙ (uniti⋆ ⊙ unite⋆)
    ⇔⟨ id⇔ ◫ linv⊙l ⟩
  swap₊ ⊙ id↔
    ⇔⟨ idr⊙l ⟩
  swap₊ □
```

The sequence of rewrites can be visualized in Appendix B.

5. Categorification

Amr says: Laplaza only considers Rig Categories to have 'natural monomorphisms' for distributivity, unlike the definition on nLab. I've tried to read [Kelly 74], but found it to be completely unreadeable. If distributivity is made an iso, then the coherence conditions "double up", with every one also holding for 'factor'. Which is true [proofs already done], and goes to the heart of my comment that we have 2 commuting involutions on level-2 combinators.
However, it did let me observe one thing: we have 2! which says that given (c <-> d), we can get (d <-> c). What we don't have, and SHOULD, is 2flip which would say that given (c <-> d), we can get (! c <-> ! d). This is "obviously true". More, we also ought to be able to prove (easily!) that all (e : c <-> d) 2! (2flip e) == 2flip (2! e) where I really mean == there.

Amr says: show some of the definitions (signatures only) of the coherences (from Data.SumProd.Properties) that correspond to the laplazaYYY lines.
One of the interesting conclusions of the coherence laws (see the comments in the file above) is that it forces all (putative) elements of bot to be equal. This comes from the coherence law for the two ways of proving that 0 * 0 = 0.

Amr says: Note that a few of those "id" in there are actually "id<-> ZERO ZERO", that is very important. Most of the laws having to do with absorb0 have some occurrences of both kinds of id in their signature, which made figuring them out very challenging! Same with laws involving factor0
Similarly, the c1 in the identl* exchange law MUST map between ONE (same with identr*). In the same vein, c1 in the identl+ and identr+ laws must involve ZERO.

The problem of finding a sound and complete set of rules for reasoning about equivalence of permutations is solved by appealing to various results about specialized monoidal categories (Selinger 2011). The main technical vehicle is that of *categorification* (Baez and Dolan 1998) which is a process, intimately related to homotopy theory, for finding category-theoretic analogs of set-theoretic concepts. From an intuitive perspective, the algebraic structure of a commutative semiring only captures a "static" relationship between types; it says nothing about how these relationships behave under *composition* which is after all the essence of computation (cf. Moggi (1989)'s original paper on monads). Thus from a programmer's perspective, this categorification process is about understanding how type equivalences evolve under compositions, e.g., how two different paths of type equivalences sharing the same source and target relate two each other.

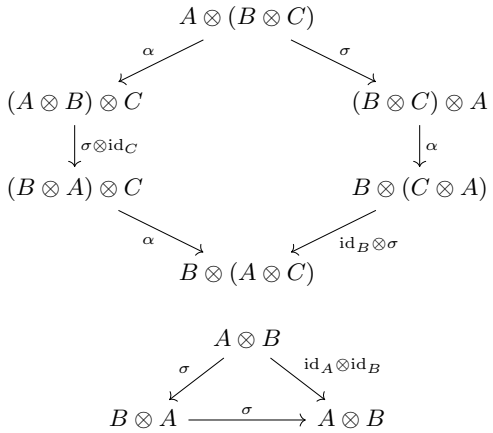
5.1 Monoidal Categories

We begin with the conventional definitions for monoidal and symmetric monoidal categories.

Definition 3 (Monoidal Category)**.** *A* monoidal category *(Mac Lane 1971) is a category with the following additional structure:*

- *a bifunctor* $\otimes$ *called the monoidal or tensor product,*
- *an object* I *called the unit object, and*
- *natural isomorphisms* $\alpha_{A,B,C} : (A \otimes B) \otimes C \xrightarrow{\sim} A \otimes (B \otimes C)$, $\lambda_A : I \otimes A \xrightarrow{\sim} A$, *and* $\rho_A : A \otimes I \xrightarrow{\sim} A$, *such that the two diagrams (known as the* associativity pentagon *and the* triangle for unit*) in Fig. 2 commute.*

Definition 4 (Symmetric Monoidal Category)**.** *A monoidal category is* symmetric *if it has an isomorphism* $\sigma_{A,B} : A \otimes B \xrightarrow{\sim} B \otimes A$ *where* σ *is a natural transformation which satisfies the following two coherence conditions (called* bilinearity *and* symmetry*):*



According to Mac Lane's coherence theorem, the coherence laws for monoidal categories are justified by the desire to equate any two isomorphisms built using σ, λ, and ρ and having the same source and target. Similar considerations justify the coherence laws for symmetric monoidal categories. It is important to note that the coherence conditions do *not* imply that every pair of parallel morphisms with the same source and target are equal. Indeed, as Dosen and Petric explain:

> In Mac Lane's second coherence result of [...], which has to do with symmetric monoidal categories, it is not intended that all equations between arrows of the same type should hold. What Mac Lane does can be described in logical terms in the following manner. On the one hand, he has an axiomatization, and, on the other hand, he has a model category where arrows are permutations; then he shows that his axiomatization is complete with respect to this model. It is no wonder that his coherence problem reduces to the completeness problem for the usual axiomatization of symmetric groups (Dosen and Petric 2004).

From a different perspective, Baez and Dolan (1998) explain the source of these coherence laws as arising from homotopy theory. In this theory, laws are only imposed up to homotopy with these homotopies satisfying certain laws, up again only up to homotopy, with these higher homotopies satisfying their own higher coherence laws, and so on. Remarkably, they report, among other results, that the pentagon identity of Fig. 2 arises when studying the algebraic structure possessed by a space that is homotopy equivalent to a loop space and that the hexagon identity arises in the context of spaces homotopy equivalent to double loop spaces.

In our context, we will build monoidal categories where the objects are finite types and the morphisms are reversible circuits represented as Π-combinators. Clearly not all reversible circuits mapping Bool to Bool are equal. There are at least two distinct such circuits: the identity and boolean negation. The coherence laws should not equate these two morphisms and they do not. We might also hope that the two versions of boolean negation in Sec. 3.2 and Sec. 4.2 could be identified using the coherence conditions of monoidal categories. This will be the case but, for that, we need categories that are much richer than just the symmetric monoidal categories which are only categorifications of commutative monoids. We will need to consider the categorification of commutative semirings.

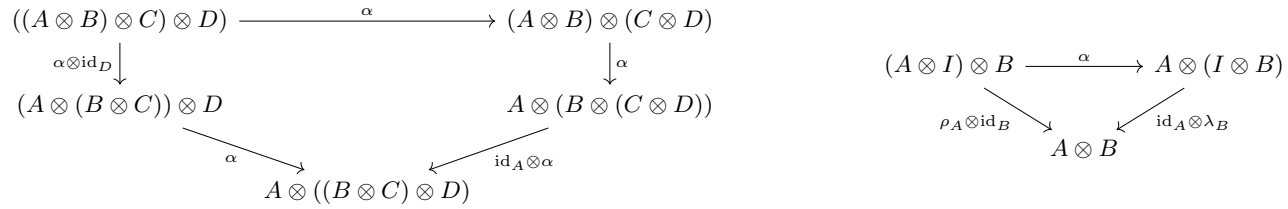


Figure 2. Pengaton and Triangle Diagrams

5.2 Symmetric Rig Weak Groupoids

The categorification of a commutative semiring is called a *symmetric rig category*. It is build from a *symmetric bimonoidal category* to which distributivity natural isomorphisms are added, and accompanying coherence laws added. Since we can easily set things up so that every morphism is a isomorphism, the category will also be a groupoid. Since the laws of the category only hold up to a higher equivalence, the entire setting is that of weak categories.

There are several equivalent definitions of rig categories. We use the following definition from the ncatlab pages (`http://ncatlab.org/nlab/show/rig+category`).

Definition 5 (Rig Category)**.** *A* rig category C *is a category with a symmetric monoidal structure* $(C, \oplus, 0)$ *for addition and a monoidal structure* $(C, \otimes, 1)$ *for multiplication together with left and right distributivity natural isomorphisms:*

$$\begin{array}{rcl} d_\ell : x \otimes (y \oplus z) & \tilde{\to} & (x \otimes y) \oplus (x \otimes z) \\ d_r : (x \oplus y) \otimes z & \tilde{\to} & (x \otimes z) \oplus (y \otimes z) \end{array}$$

and absorption/annihilation isomorphisms:

$$\begin{array}{rcl} a_\ell : x \otimes 0 & \tilde{\to} & 0 \\ a_r : 0 \otimes x & \tilde{\to} & 0 \end{array}$$

satisfying coherence conditions worked out by Laplaza (1972) and discussed below.

Definition 6 (Symmetric Rig Category)**.** *A* symmetric rig category *is a rig category in which the multiplicative structure is symmetric.*

Definition 7 (Symmetric Rig Groupoid)**.** *A* symmetric rig groupoid *is a symmetric rig category in which every morphism is invertible.*

The coherence conditions for rig categories were first worked out by Laplaza (1972). Pages 31-35 of his paper report 24 coherence conditions that vary from simple diagrams to one that includes 9 nodes showing that two distinct ways of simplifying $(A \oplus B) \otimes (C \oplus D)$ to $(((A \otimes C) \oplus (B \otimes C)) \oplus (A \otimes D)) \oplus (B \otimes D)$ commute. The 24 coherence conditions are not independent which somewhat simplifies the situation and allows us to prove that our structures satisfy the coherence conditions in a more economic way.

5.3 Instances of Symmetric Rig Categories

Most of the structures we have discussed so far are instances of symmetric rig weak groupoids.

Theorem 9. *The collection of all types and type equivalences is a symmetric rig groupoid.*

Proof. The objects of the category are Agda types and the morphisms are type equivalences. These morphisms directly satisfy the axioms stated in the definitions of the various categories. The bulk of the work is in ensuring that the coherence conditions are satisfied up to extensional equality. □

More relevant for our purposes, is the next theorem which applies to reversible circuits (represented as Π-combinators).

Theorem 10. *The collection of finite types and* Π*-combinators is a symmetric rig groupoid.*

Proof. The objects of the category are finite types and the morphisms are the Π-combinators. Short proofs establish that these morphisms satisfy the axioms stated in the definitions of the various categories. The bulk of the work is in ensuring that the coherence conditions are satisfied. This required us to add a few Π combinators (see Fig. 3) and then to add a whole new layer of 2-combinators (discussed in the next section) witnessing enough equivalences of Π combinators to prove the coherence laws. The new Π combinators, also discussed in more detain in the next section, are redundant (from an operational perspective) exactly because of the coherence conditions; they are however important as they have rather nontrivial relations to each other that are captured in the more involved coherence laws. □

Putting the result above together with Laplaza's coherence result about rig categories, we conclude with our main result.

Theorem 11. *We have two levels of* Π*-combinators such that:*

- *The first level of* Π*-combinators is complete for representing reversible combinational circuits.*
- *The second level of* Π*-combinators is sound and complete for the equivalence of circuits represented by the first level.*

6. Revised Π and its Optimizer

Collecting the previous results we arrive at a universal language for expressing reversible combinational circuits *together with* a sound and complete metalanguage for reasoning about equivalences of programs written in the lower level language.

6.1 Example

[This is weak; I could get away with it in a short talk, but this should be made more precise. It is essentially what the code says, and what is encoded by the natural transformations, but there has to be a better way to say this. —JC] The general structure explaining the nature of the second level metalanguage and how the two languages fit together from a categorical perspective is the following:

- type equivalences for example between $A \oplus B$ and $B \oplus A$ are *functors*;
- equivalences between such functors are *natural isomorphisms*;
- at the value level, these equivalences induce 2-morphisms.

For example, assuming we are given two Π-combinators:

$c_1 : \{B\ C : \mathsf{U}\} \to \quad B \leftrightarrow C$
$c_2 : \{A\ D : \mathsf{U}\} \to \quad A \leftrightarrow D$

from which we build two larger combinators p_1 and p_2 below:

$p_1\ p_2 : \{A\ B\ C\ D : \mathsf{U}\} \to \mathsf{PLUS}\ A\ B \leftrightarrow \mathsf{PLUS}\ C\ D$
$p_1 = \mathsf{swap}_+ \odot (c_1 \oplus c_2)$
$p_2 = (c_2 \oplus c_1) \odot \mathsf{swap}_+$

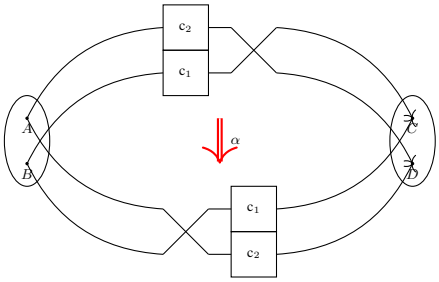
$$
\begin{array}{rrcll}
identls_+ : & \tau + 0 & \leftrightarrow & \tau & : identrs_+ \\
identls_* : & \tau * 1 & \leftrightarrow & \tau & : identrs_* \\
absorbr_0 : & 0 * \tau & \leftrightarrow & 0 & : factorl_0 \\
absorbl_0 : & \tau * 0 & \leftrightarrow & 0 & : factorr_0 \\
distl : & \tau_1 * (\tau_2 + \tau_3) & \leftrightarrow & (\tau_1 * \tau_2) + (\tau_1 * \tau_3) & : factorl
\end{array}
$$

Figure 3. Additional Π-combinators

As reversible circuits, p_1 and p_2 evaluate as follows. If p_1 is given the value inl a, it first transforms it to inr a, and then passes it to c_2. If p_2 is given the value inl a, it first passes it to c_2 and then flips the tag of the result. Since c_2 is functorial, it must act polymorphically on its input and hence, it must be the case that the two evaluations produce the same result. The situation for the other possible input value is symmetric. This extensional reasoning is embedded once and for all in the proofs of coherence and distilled in a 2-level combinator:

$$
\begin{array}{rl}
\mathsf{swapl}_+\Leftrightarrow : & \{t_1\ t_2\ t_3\ t_4 : \mathsf{U}\}\ \{c_1 : t_1 \leftrightarrow t_2\}\ \{c_2 : t_3 \leftrightarrow t_4\} \rightarrow \\
& (\mathsf{swap}_+ \odot (c_1 \oplus c_2)) \Leftrightarrow' ((c_2 \oplus c_1) \odot \mathsf{swap}_+)
\end{array}
$$

Pictorially, this 2-level combinator is a 2-path showing how the two paths can be transformed to one another. The proof of equivalence can be visualized by simply imagining the connections as wires whose endpoints are fixed: holding the wires on the right side of the top path and flipping them produces the connection in the bottom path:



6.2 Revised Syntax

[The second sentence below is a repeat; where does it belong? —JC] [You're missing 4 combinators from that picture! Plus the ones you added are the ones for absorption and distributivity, NOT the ones which are redundant, they are really needed for a proper semiring. —JC]

The inspiration of symmetric rig groupoids suggested a refactoring of Π with additional level-1 combinators. The added combinators 3 are redundant (from an operational perspective) exactly because of the coherence conditions. In addition to being critical to the proofs, they are useful when representing circuits leading to smaller programs with fewer redexes.

The big addition of course is the level-2 combinators which are collected in Fig. 4. To avoid clutter we omit the names of the combinators and only show the signatures.

[I suggest adding the following laplaza combinators to that table: I, IV, IX (sorry), X ans XVII. Also a short paragraph explaining what they do. For some of them, I suggest digging into Data.SumProd.Properties and showing some of these too (just as signatures). The later ones are much better. Anything with a proj in the statement is "wrong" (it builds in some premature beta-redexes in the statement), so don't pick those. But they are theorems which are not in Agda's standard library. Most of the properties of sums and products (aka coherences) were already there, but not these, which are interesting interactions between them. —JC]

As Fig. 4 illustrates, we have rules to manipulate code fragments rewriting them in a small-step fashion. The rules apply only when both sides are well-typed. The small-step nature of the rules should allow us to make efficient optimizers following the experience in functional languages (Peyton Jones and Santos 1998). In contrast the coherence conditions are much smaller in number and many them express invariants about much bigger "chunks." From our small experiments, an effective way to use the rules is to fix a canonical representation of circuits that has the "right" properties and use the rules in a directed fashion to produce that canonical representation. For example, Saeedi and Markov (2013) survey several possible canonical representations that trade-off various desired properties. Of course, finding a rewriting procedure that makes progress towards the canonical representation is far from trivial.

7. The Problem with Higher-Order Functions

In the context of monoidal categories, it is known that a notion of higher-order functions emerges from having an additional degree of *symmetry*. In particular, both the **Int** construction of Joyal et al. (1996) and the closely related $\mathcal{G}$ construction of linear logic (Abramsky 1996) construct higher-order *linear* functions by considering a new category built on top of a given base traced monoidal category (Hasegawa 2009). The objects of the new category are of the form $\boxed{\tau_1}\boxed{\tau_2}$ where τ_1 and τ_2 are objects in the base category. Intuitively, this object represents the *difference* $\tau_1 - \tau_2$ with the component τ_1 viewed as conventional type whose elements represent values flowing, as usual, from producers to consumers, and the component τ_2 viewed as a *negative type* whose elements represent demands for values or equivalently values flowing backwards. Under this interpretation, a function is nothing but an object that converts a demand for an argument into the production of a result. We will explain in this section that the naïve generalization of the construction from monoidal to bimonoidal (aka rig) categories fails but that a recent result by Baas et al. (2012) might provide a path towards a solution.

7.1 The Int Construction

For this construction, we assume that we have extended Π with a trace operator to implement recursion or feedback, as done in some of the work on Π (Bowman et al. 2011; James and Sabry 2012a). The trace operator has the following type rule:

$$
\frac{\vdash c : a + b \leftrightarrow a + c}{\vdash trace\ c : b \leftrightarrow c}
$$

Under "normal" operation, a b input is expected which is injected into the sum and fed to the traced computation. The evaluation continues until a c value is produced, possibly after feeding several intermediate a results back to the input.

We then extend Π with a new universe of types $\mathbb{T}$ that consists of composite types $\boxed{\tau_1}\boxed{\tau_2}$:

$$
(1d\ types) \quad \mathbb{T} \quad ::= \quad \boxed{\tau_1}\boxed{\tau_2}
$$

We will refer to the original types τ as 0-dimensional (0d) types and to the new types $\mathbb{T}$ as 1-dimensional (1d) types. The 1d level is a "lifted" instance of Π with its own notions of empty, unit, sum,

$$
\begin{array}{rcl}
id \fatsemi c & \Leftrightarrow & c \\
c \fatsemi id & \Leftrightarrow & c \\
c \fatsemi (!\ c) & \Leftrightarrow & id \\
(!\ c) \fatsemi c & \Leftrightarrow & id \\
id \oplus id & \Leftrightarrow & id \\
id \otimes id & \Leftrightarrow & id \\
c_1 \fatsemi (c_2 \fatsemi c_3) & \Leftrightarrow & (c_1 \fatsemi c_2) \fatsemi c_3 \\
(c_1 \fatsemi c_3) \oplus (c_2 \fatsemi c_4) & \Leftrightarrow & (c_1 \oplus c_2) \fatsemi (c_3 \oplus c_4) \\
(c_1 \fatsemi c_3) \otimes (c_2 \fatsemi c_4) & \Leftrightarrow & (c_1 \otimes c_2) \fatsemi (c_3 \otimes c_4)
\end{array}
$$

$$
\begin{array}{rcl}
identl_+ \fatsemi c_2 & \Leftrightarrow & (c_1 \oplus c_2) \fatsemi identl_+ \\
identr_+ \fatsemi (c_1 \oplus c_2) & \Leftrightarrow & c_2 \fatsemi identr_+ \\
identls_+ \fatsemi c_2 & \Leftrightarrow & (c_2 \oplus c_1) \fatsemi identls_+ \\
identrs_+ \fatsemi (c_2 \oplus c_1) & \Leftrightarrow & c_2 \fatsemi identrs_+ \\
identls_+ \oplus id & \Leftrightarrow & assocr_+ \fatsemi (id \oplus identl_+)
\end{array}
$$

$$
\begin{array}{rcl}
(c_1 \oplus (c_2 \oplus c_3)) \fatsemi assocl_+ & \Leftrightarrow & assocl_+ \fatsemi ((c_1 \oplus c_2) \oplus c_3) \\
((c_1 \oplus c_2) \oplus c_3) \fatsemi assocr_+ & \Leftrightarrow & assocr_+ \fatsemi (c_1 \oplus (c_2 \oplus c_3)) \\
(c_1 \otimes (c_2 \otimes c_3)) \fatsemi assocl_* & \Leftrightarrow & assocl_* \fatsemi ((c_1 \otimes c_2) \otimes c_3) \\
((c_1 \otimes c_2) \otimes c_3) \fatsemi assocr_* & \Leftrightarrow & assocr_* \fatsemi (c_1 \otimes (c_2 \otimes c_3)) \\
((a \oplus b) \otimes c) \fatsemi dist & \Leftrightarrow & dist \fatsemi ((a \otimes c) \oplus (b \otimes c)) \\
((a \otimes c) \oplus (b \otimes c)) \fatsemi factor & \Leftrightarrow & factor \fatsemi ((a \oplus b) \otimes c) \\
(a \otimes (b \oplus c)) \fatsemi distl & \Leftrightarrow & distl \fatsemi ((a \otimes b) \oplus (a \otimes c)) \\
((a \otimes b) \oplus (a \otimes c)) \fatsemi factorl & \Leftrightarrow & factorl \fatsemi (a \otimes (b \oplus c))
\end{array}
$$

$$
\begin{array}{rcl}
identl_* \fatsemi c_2 & \Leftrightarrow & (c_1 \otimes c_2) \fatsemi identl_* \\
identr_* \fatsemi (c_1 \otimes c_2) & \Leftrightarrow & c_2 \fatsemi identr_* \\
identls_* \fatsemi c_2 & \Leftrightarrow & (c_2 \otimes c_1) \fatsemi identls_* \\
identrs_* \fatsemi (c_2 \otimes c_1) & \Leftrightarrow & c_2 \fatsemi identrs_* \\
identls_* \otimes id & \Leftrightarrow & assocr_* \fatsemi (id \oplus identl_*)
\end{array}
$$

$$
\begin{array}{rcl}
absorbr_0 & \Leftrightarrow & identl_* \\
absorbr_0 & \Leftrightarrow & absorbl_0 \\
absorbr_0 & \Leftrightarrow & (assocl_* \fatsemi (absorbr_0 \otimes id)) \fatsemi absorbr_0 \\
absorbr_0 & \Leftrightarrow & (distl \fatsemi (absorbr_0 \oplus absorbr_0)) \fatsemi identl_+ \\
absorbl_0 & \Leftrightarrow & swap_* \fatsemi absorbr_0 \\
(c \otimes id) \fatsemi absorbl_0 & \Leftrightarrow & absorbl_0 \fatsemi id \\
(id \otimes c) \fatsemi absorbr_0 & \Leftrightarrow & absorbr_0 \fatsemi id \\
(id \otimes absorbr_0) \fatsemi absorbl_0 & \Leftrightarrow & (assocl_* \fatsemi (absorbl_0 \otimes id) \fatsemi absorbr_0 \\
(id \otimes identl_+) & \Leftrightarrow & (distl \fatsemi (absorbl_0 \oplus id)) \fatsemi identl_+
\end{array}
$$

$$
\begin{array}{rcl}
swap_+ \fatsemi (c_1 \oplus c_2) & \Leftrightarrow & (c_2 \oplus c_1) \fatsemi swap_+ \\
swap_* \fatsemi (c_1 \otimes c_2) & \Leftrightarrow & (c_2 \otimes c_1) \fatsemi swap_* \\
swap_+ \fatsemi factor & \Leftrightarrow & factor \fatsemi (swap_+ \otimes id)
\end{array}
$$

$$
\begin{array}{rcl}
identl_+ & \Leftrightarrow & distl \fatsemi (identl_+ \oplus identl_+) \\
(id \otimes swap_+) \fatsemi distl & \Leftrightarrow & distl \fatsemi swap_+ \\
dist \fatsemi (swap_* \oplus swap_*) & \Leftrightarrow & swap_* \fatsemi distl \\
id \fatsemi factorl_0 & \Leftrightarrow & factorl_0 \fatsemi (id \otimes c) \\
id \fatsemi factorr_0 & \Leftrightarrow & factorr_0 \fatsemi (c \otimes id)
\end{array}
$$

$$
\begin{array}{rcl}
((assocl_+ \otimes id) \fatsemi dist) \fatsemi (dist \oplus id) & \Leftrightarrow & (dist \fatsemi (id \oplus dist)) \fatsemi assocl_+ \\
(distl \fatsemi (dist \oplus dist)) \fatsemi assocl_+ & \Leftrightarrow & ((((dist \fatsemi (distl \oplus distl)) \fatsemi assocl_+) \fatsemi (assocr_+ \oplus id)) \fatsemi (id \oplus swap_+) \oplus id)) \fatsemi (assocl_+ \oplus id) \\
assocl_* \fatsemi distl & \Leftrightarrow & ((id \otimes distl) \fatsemi distl) \fatsemi (assocl_* \oplus assocl_*) \\
assocr_+ \fatsemi assocr_+ & \Leftrightarrow & ((assocr_+ \oplus id) \fatsemi assocr_+) \fatsemi (id \oplus assocr_+) \\
assocr_* \fatsemi assocr_* & \Leftrightarrow & ((assocr_* \otimes id) \fatsemi assocr_*) \fatsemi (id \otimes assocr_*) \\
(assocr_+ \fatsemi swap_+) \fatsemi assocr_+ & \Leftrightarrow & ((swap_+ \oplus id) \fatsemi assocr_+) \fatsemi (id \oplus swap_+) \\
(assocl_+ \fatsemi swap_+) \fatsemi assocl_+ & \Leftrightarrow & ((id \oplus swap_+) \fatsemi assocl_+) \fatsemi (swap_+ \oplus id) \\
(assocr_* \fatsemi swap_*) \fatsemi assocr_* & \Leftrightarrow & ((swap_* \oplus id) \fatsemi assocr_*) \fatsemi (id \otimes swap_*) \\
(assocl_* \fatsemi swap_*) \fatsemi assocl_* & \Leftrightarrow & ((id \otimes swap_*) \fatsemi assocl_*) \fatsemi (swap_* \otimes id)
\end{array}
$$

$$
\frac{}{\vdash c \Leftrightarrow c} \qquad \frac{\vdash c_1 \Leftrightarrow c_2 \quad \vdash c_2 \Leftrightarrow c_3}{\vdash c_1 \Leftrightarrow c_3} \qquad \frac{\vdash c_1 \Leftrightarrow c_3 \quad \vdash c_2 \Leftrightarrow c_4}{\vdash (c_1 \fatsemi c_2) \Leftrightarrow (c_3 \fatsemi c_4)} \qquad \frac{\vdash c_1 \Leftrightarrow c_3 \quad \vdash c_2 \Leftrightarrow c_4}{\vdash (c_1 \oplus c_2) \Leftrightarrow (c_3 \oplus c_4)}
$$

$$
\frac{\vdash c_1 \Leftrightarrow c_3 \quad \vdash c_2 \Leftrightarrow c_4}{\vdash (c_1 \otimes c_2) \Leftrightarrow (c_3 \otimes c_4)}
$$

Figure 4. Signatures of level-2 Π-combinators

and product types, and its corresponding notions of isomorphisms and composition on these 1d types.

Our next step is to define lifted versions of the 0d types:

$$
\begin{array}{rcl}
\mathbb{0} & \triangleq & \boxed{0 \mid 0} \\
\mathbb{1} & \triangleq & \boxed{1 \mid 0} \\
\boxed{\tau_1 \mid \tau_2} \boxplus \boxed{\tau_3 \mid \tau_4} & \triangleq & \boxed{\tau_1 + \tau_3 \mid \tau_2 + \tau_4} \\
\boxed{\tau_1 \mid \tau_2} \boxtimes \boxed{\tau_3 \mid \tau_4} & \triangleq & \boxed{(\tau_1 * \tau_3) + (\tau_2 * \tau_4) \mid (\tau_1 * \tau_4) + (\tau_2 * \tau_3)}
\end{array}
$$

Building on the idea that Π is a categorification of the natural numbers and following a long tradition that relates type isomorphisms and arithmetic identities (Di Cosmo 2005), one is tempted to think that the **Int** construction (as its name suggests) produces a categorification of the integers. Based on this hypothesis, the definitions above can be intuitively understood as arithmetic identities. The same arithmetic intuition explains the lifting of isomorphisms to 1d types:

$$
\boxed{\tau_1 \mid \tau_2} \Leftrightarrow \boxed{\tau_3 \mid \tau_4} \quad \triangleq \quad (\tau_1 + \tau_4) \leftrightarrow (\tau_2 + \tau_3)
$$

In other words, an isomorphism between 1d types is really an isomorphism between "re-arranged" 0d types where the negative input τ_2 is viewed as an output and the negative output τ_4 is viewed as an input. Using these ideas, it is now a fairly standard exercise to define the lifted versions of most of the combinators in Table 1.[3] We discuss a few cases in detail.

[3] See Krishnaswami (2012)'s excellent blog post implementing this construction in OCaml.

Trivial cases. Many of the 0d combinators lift easily to the 1d level. For example:

$$\begin{array}{rcl} id & : & \mathbb{T} \Leftrightarrow \mathbb{T} \\ & : & \boxed{\tau_1}\boxed{\tau_2} \Leftrightarrow \boxed{\tau_1}\boxed{\tau_2} \\ & \triangleq & (\tau_1 + \tau_2) \leftrightarrow (\tau_2 + \tau_1) \\ id & = & swap_+ \end{array}$$

$$\begin{array}{rcl} identl_+ & : & \mathbb{0} \boxplus \mathbb{T} \Leftrightarrow \mathbb{T} \\ & \triangleq & \boxed{0 + \tau_1}\boxed{0 + \tau_2} \Leftrightarrow \boxed{\tau_1}\boxed{\tau_2} \\ & \triangleq & ((0 + \tau_1) + \tau_2) \leftrightarrow ((0 + \tau_2) + \tau_1) \\ & = & assocr_+ \fatsemi (id \oplus swap_+) \fatsemi assocl_+ \end{array}$$

Composition using *trace.* Let $assoc_1$, $assoc_2$, and $assoc_3$ be the very simple Π combinators with the following signatures:

$$\begin{array}{ll} assoc_1 : & \tau_1 + (\tau_2 + \tau_3) \leftrightarrow (\tau_2 + \tau_1) + \tau_3 \\ assoc_2 : & (\tau_1 + \tau_2) + \tau_3 \leftrightarrow (\tau_2 + \tau_3) + \tau_1 \\ assoc_3 : & (\tau_1 + \tau_2) + \tau_3 \leftrightarrow \tau_1 + (\tau_3 + \tau_2) \end{array}$$

Composition is then defined as follows:

$$\begin{array}{rcl} (\fatsemi) : & (\mathbb{T}_1 \Leftrightarrow \mathbb{T}_2) \to (\mathbb{T}_2 \Leftrightarrow \mathbb{T}_3) \to (\mathbb{T}_1 \Leftrightarrow \mathbb{T}_3) \\ seq : & (\boxed{\tau_1}\boxed{\tau_2} \Leftrightarrow \boxed{\tau_3}\boxed{\tau_4}) \to (\boxed{\tau_3}\boxed{\tau_4} \Leftrightarrow \boxed{\tau_5}\boxed{\tau_6}) \\ & \quad \to (\boxed{\tau_1}\boxed{\tau_2} \Leftrightarrow \boxed{\tau_5}\boxed{\tau_6}) \\ & \triangleq & ((\tau_1 + \tau_4) \leftrightarrow (\tau_2 + \tau_3)) \to ((\tau_3 + \tau_6) \leftrightarrow (\tau_4 + \tau_5)) \\ & \quad \to ((\tau_1 + \tau_6) \leftrightarrow (\tau_2 + \tau_5)) \\ f \fatsemi g = & trace\ (assoc_1 \fatsemi (f \oplus id) \fatsemi assoc_2 \fatsemi (g \oplus id) \fatsemi assoc_3) \end{array}$$

At the level of 1d-types, the first computation produces $\boxed{\tau_3}\boxed{\tau_4}$ which is consumed by the second computation. Expanding these types, we realize that the τ_4 produced from the first computation is actually a demand for a value of that type and that the τ_4 consumed by the second computation can satisfy a demand by an earlier computation. This explains the need for a feedback mechanism to send future values back to earlier computations.

Higher-order functions. Given values that flow in both directions, it is fairly straightforward to encode functions. At the type level, we have:

$$\begin{array}{rcl} \boxminus(\boxed{\tau_1}\boxed{\tau_2}) & \triangleq & \boxed{\tau_2}\boxed{\tau_1} \\ \boxed{\tau_1}\boxed{\tau_2} \multimap \boxed{\tau_3}\boxed{\tau_4} & \triangleq & \boxminus(\boxed{\tau_1}\boxed{\tau_2}) \boxplus \boxed{\tau_3}\boxed{\tau_4} \\ & \triangleq & \boxed{\tau_2 + \tau_3}\boxed{\tau_1 + \tau_4} \end{array}$$

The $\boxminus$ flips producers and consumers and the $\multimap$ states that a function is just a transformer demanding values of the input type and producing values of the output type. As shown below, it now becomes possible to manipulate functions as values by currying and uncurrying:

$$\begin{array}{rcl} flip & : & (\mathbb{T}_1 \Leftrightarrow \mathbb{T}_2) \to (\boxminus\mathbb{T}_2 \Leftrightarrow \boxminus\mathbb{T}_1) \\ flip\ f & = & swap_+ \fatsemi f \fatsemi swap_+ \end{array}$$

$$\begin{array}{rcl} curry & : & ((\mathbb{T}_1 \boxplus \mathbb{T}_2) \Leftrightarrow \mathbb{T}_3) \to (\mathbb{T}_1 \Leftrightarrow (\mathbb{T}_2 \multimap \mathbb{T}_3)) \\ curry\ f & = & assocl_+ \fatsemi f \fatsemi assocr_+ \end{array}$$

$$\begin{array}{rcl} uncurry & : & (\mathbb{T}_1 \Leftrightarrow (\mathbb{T}_2 \multimap \mathbb{T}_3)) \to ((\mathbb{T}_1 \boxplus \mathbb{T}_2) \Leftrightarrow \mathbb{T}_3) \\ uncurry\ f & = & assocr_+ \fatsemi f \fatsemi assocl_+ \end{array}$$

Products. The **Int** construction works perfectly well as a technique to define higher-order functions if we just have *one* monoidal structure: the additive one as we have assumed so far. We will now try to extend the construction to encompass the other (multiplicative) monoidal structure. Recall that natural definition for the product of 1d types used above was:

$$\boxed{\tau_1}\boxed{\tau_2} \boxtimes \boxed{\tau_3}\boxed{\tau_4} \triangleq \boxed{(\tau_1 * \tau_3) + (\tau_2 * \tau_4)}\boxed{(\tau_1 * \tau_4) + (\tau_2 * \tau_3)}$$

That definition is "obvious" in some sense as it matches the usual understanding of types as modeling arithmetic identities. Using this definition, it is possible to lift all the 0d combinators involving products *except* the functor:

$$(\otimes) : (\mathbb{T}_1 \Leftrightarrow \mathbb{T}_2) \to (\mathbb{T}_3 \Leftrightarrow \mathbb{T}_4) \to ((\mathbb{T}_1 \boxtimes \mathbb{T}_3) \Leftrightarrow (\mathbb{T}_2 \boxtimes \mathbb{T}_4))$$

After a few failed attempts, we suspected that this definition of multiplication is not functorial which would mean that the **Int** construction only provides a limited notion of higher-order functions at the cost of losing the multiplicative structure at higher-levels. Further investigation reveals that this observation is intimately related to a well-known problem in algebraic topology and homotopy theory that was identified thirty years ago as the **"phony" multiplication** (Thomason 1980) in a special class categories related to ours. This observation, that the **Int** construction on the additive monoidal structure does *not* allow one to lift multiplication in a straightforward manner is less well-known than it should be. This problem was however recently solved (Baas et al. 2012) using a technique whose fundamental ingredients are to add more dimensions and then take homotopy colimits.

The process of adding more dimensions is relatively straightforward: if the original intuition was that 1d types like $\boxed{\tau_1}\boxed{\tau_2}$ represent $\tau_1 - \tau_2$, i.e., two types one in the + direction and one in the − direction, then multiplication of two such 1d types ought to produce components in the $++$, $+-$, $-+$, and $--$ directions and so on. The idea is illustrated with a simple example in Fig. 5. It remains to investigate whether this idea could lead to a generalization of our results to incorporate higher-order functions while retaining the multiplicative structure. Another intriguing point to consider is the connection between this idea and the recently proposed cubical models of type theory that also aim at producing computational interpretations of univalence (Bezem et al. 2014).

8. Conclusion

We have developed a tight integration between *reversible circuits* with *symmetric rig weak groupoids* based on the following elements:

- reversible circuits are represented as terms witnessing morphisms between finite types in a symmetric rig groupoid;
- the term language for reversible circuits is universal; it could be used as a standalone point-free programming language or as a target for a higher-level language with a more conventional syntax;
- the symmetric rig groupoid structure ensures that programs can be combined using sums and products satisfying the familiar laws of these operations;
- the *weak* versions of the categories give us a second level of morphisms that relate programs to equivalent programs and is exactly captured in the coherence conditions of the categories; this level of morphisms also comes equipped with sums and products with the familiar laws and the coherence conditions capture how these operations interact with sequential composition;
- a sound and complete optimizer for reversible circuits can be represented as terms that rewrite programs in small steps witnessing this second level of morphisms.

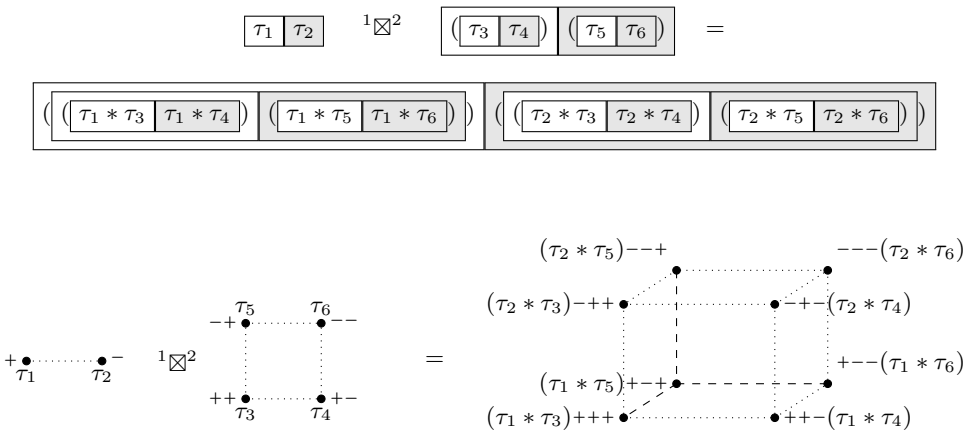


Figure 5. Example of multiplication of two cartesian types.

Our calculus provides a semantically well-founded approach to representation, manipulation, and optimization of reversible circuits. In principle, subsets of the optimization rules can be selected to rewrite programs to several possible canonical forms as desired. We aim to investigate such frameworks in the future.

From a much more general perspective, our result can be viewed as part of a larger programme aiming at a better integration of several disciplines most notably computation, topology, and physics. Computer science has traditionally been founded on models such as the λ-calculus which are at odds with the increasingly relevant physical principle of conservation of information as well as the recent foundational proposal of HoTT that identifies equivalences (i.e., reversible, information-preserving, functions) as a primary notion of interest.[4] Currently, these reversible functions are a secondary notion defined with reference to the full λ-calculus in what appears to be a detour. In more detail, current constructions start with the class of all functions $A \to B$, then introduce constraints to filter those functions which correspond to type equivalences $A \simeq B$, and then attempt to look for a convenient computational framework for effective programming with type equivalences. As we have shown, in the case of finite types, this is just convoluted since the collection of functions corresponding to type equivalences is the collection of isomorphisms between finite types and these isomorphisms can be inductively defined, giving rise to a well-behaved programming language and its optimizer.

More generally, reversible computational models — in which all functions have inverses — are known to be universal computational models (Bennett 1973) and more importantly they can be defined without any reference to irreversible functions, which ironically become the derived notion (Green and Altenkirch 2008). It is therefore, at least plausible, that a variant of HoTT based exclusively on reversible functions would have better computational properties. Our current result is a step, albeit preliminary in that direction as it only applies to finite types. However, it is plausible that this approach can be generalized to accommodate higher-order functions. The intuitive idea is that our current development based on the commutative semiring of the natural numbers might be generalizable to the ring of integers or even to the field of rational numbers. The generalization to rings would introduce *negative types* and the generalization to fields would further introduce *fractional types*. As Sec. 7 suggests, there is good evidence that these generalizations would introduce some notion of higher-order functions. It is even possible to conceive of more exotic types such as types with square roots and imaginary numbers by further generalizing the work to the field of *algebraic numbers*. These types have been shown to make sense in computations involving datatypes such as trees that can be viewed as solutions to polynomials over type variables (Blass 1995; Fiore 2004; Fiore and Leinster 2004).

[4] The λ-calculus is not even suitable for keeping track of computational resources; linear logic (Girard 1987) is a much better framework for that purpose but it does not go far enough as it only tracks "multiplicative resources." (Sparks and Sabry 2014)

A. Commutative Semirings

Given that the structure of commutative semirings is central to this paper, we recall the formal algebraic definition. Commutative rings are sometimes called *commutative rigs* as they are commutative rings without negative elements.

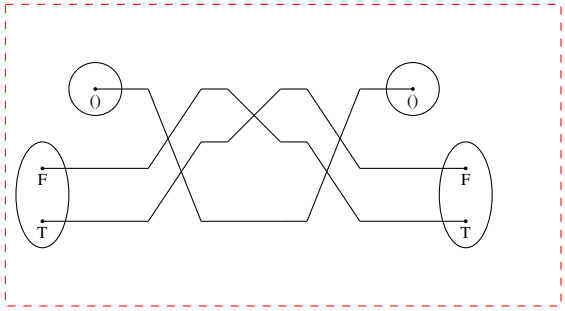
Definition 8. *A* commutative semiring *consists of a set R, two distinguished elements of R named 0 and 1, and two binary operations $+$ and $\cdot$, satisfying the following relations for any $a, b, c \in R$:*

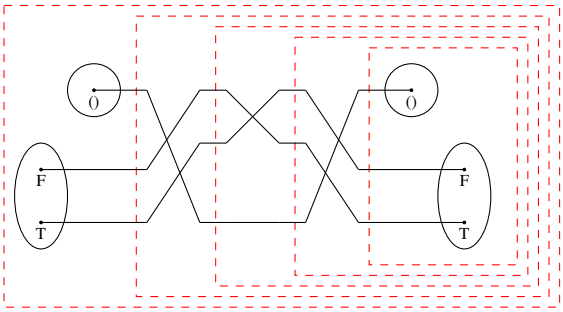
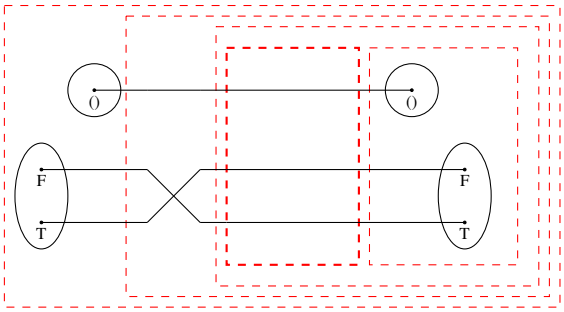
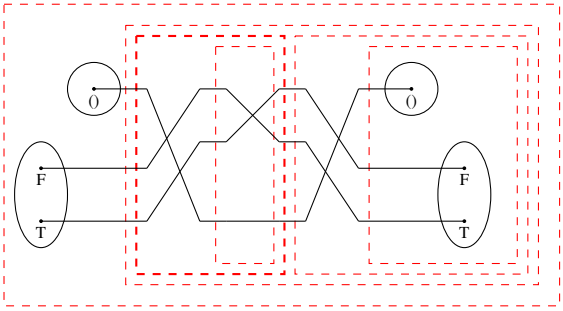
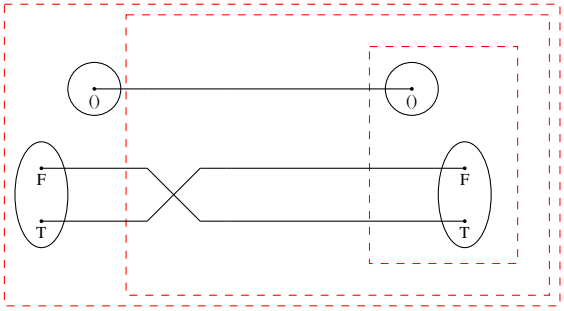
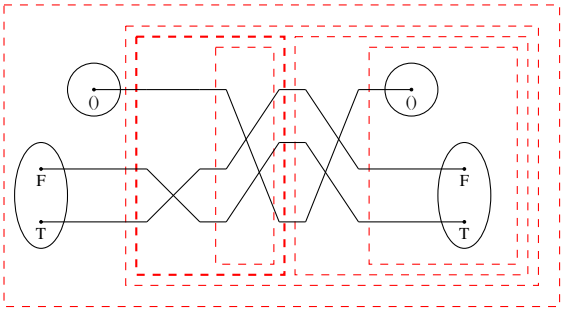
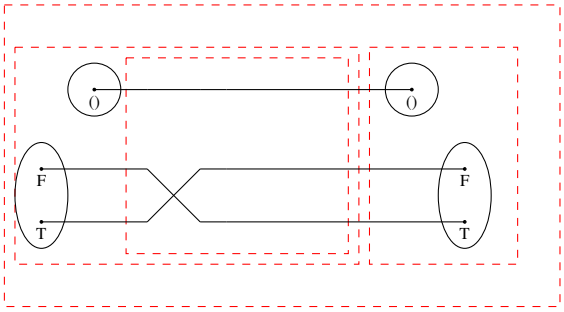
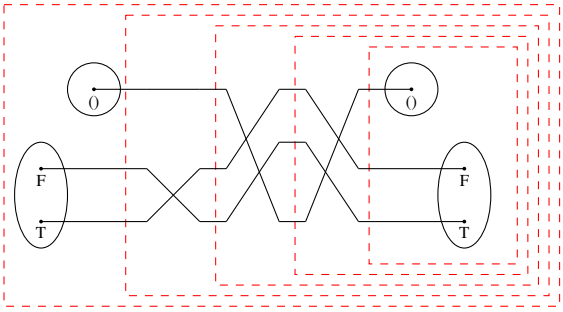
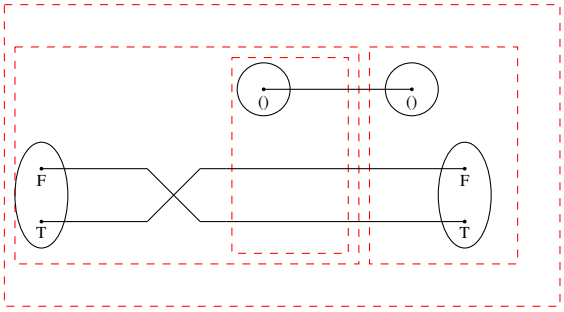
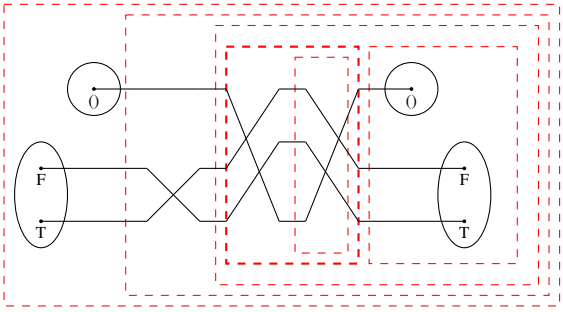
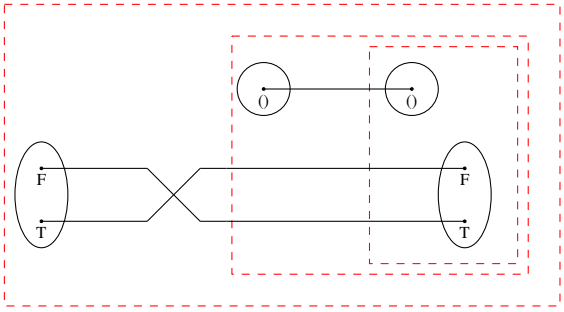
$$\begin{aligned} 0 + a &= a \\ a + b &= b + a \\ a + (b + c) &= (a + b) + c \end{aligned}$$

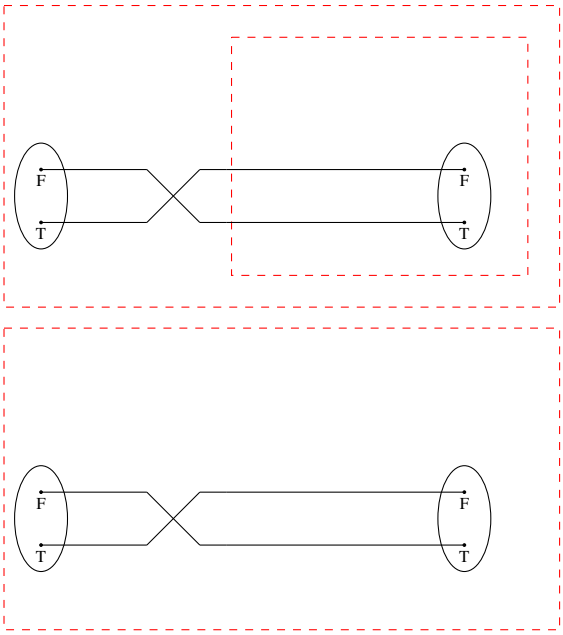
$$\begin{aligned} 1 \cdot a &= a \\ a \cdot b &= b \cdot a \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \end{aligned}$$

$$\begin{aligned} 0 \cdot a &= 0 \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \end{aligned}$$

B. Diagrammatic Optimization





References

S. Abramsky. Retracing some paths in process algebra. In *CONCUR '96: Concurrency Theory*, volume 1119 of *Lecture Notes in Computer Science*, pages 1–17. Springer Berlin Heidelberg, 1996.

S. Abramsky. A structural approach to reversible computation. *Theor. Comput. Sci.*, 347:441–464, December 2005.

N. Baas, B. Dundas, B. Richter, and J. Rognes. Ring completion of rig categories. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2013(674):43–80, Mar. 2012.

J. Baez and M. Stay. Physics, topology, logic and computation: a rosetta stone. *New Structures for Physics*, pages 95–172, 2011.

J. C. Baez and J. Dolan. Categorification. In Higher Category Theory, Contemp. Math. 230, 1998, pp. 1-36., 1998.

C. H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.*, 17: 525–532, November 1973.

M. Bezem, T. Coquand, and S. Huber. A model of type theory in cubical sets. In *LIPIcs. Leibniz Int. Proc. Inform.*, volume 26, pages 107–128, Dagstuhl, Germany, 2014. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

A. Blass. Seven trees in one. *Journal of Pure and Applied Algebra*, 103 (1-21), 1995.

W. J. Bowman, R. P. James, and A. Sabry. Dagger Traced Symmetric Monoidal Categories and Reversible Programming. In *RC*, 2011.

E. P. DeBenedictis. Reversible logic for supercomputing. In *Proceedings of the 2Nd Conference on Computing Frontiers*, CF '05, pages 391–402, New York, NY, USA, 2005. ACM. ISBN 1-59593-019-1. . URL `http://doi.acm.org/10.1145/1062261.1062325`.

R. Di Cosmo. A short survey of isomorphisms of types. *Mathematical. Structures in Comp. Sci.*, 15(5):825–838, Oct. 2005.

A. Di Pierro, C. Hankin, and H. Wiklicky. Reversible combinatory logic. *MSCS*, 16:621–637, August 2006.

K. Dosen and Z. Petric. *Proof-Theoretical Coherence*. KCL Publications (College Publications), London, 2004. (revised version available at: `http://www.mi.sanu.ac.yu/~kosta/coh.pdf`).

R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

M. Fiore. Isomorphisms of generic recursive polynomial types. In *POPL*, pages 77–88. ACM, 2004.

M. Fiore and T. Leinster. An objective representation of the gaussian integers. *Journal of Symbolic Computation*, 37(6):707 – 716, 2004. ISSN 0747-7171. . URL `http://www.sciencedirect.com/science/article/pii/S0747717104000094`.

M. P. Fiore, R. Di Cosmo, and V. Balat. Remarks on isomorphisms in typed calculi with empty and sum types. *Annals of Pure and Applied Logic*, 141(1-2):35–50, 2006.

M. P. Frank. *Reversibility for efficient computing*. PhD thesis, Massachusetts Institute of Technology, 1999.

E. Fredkin and T. Toffoli. Conservative logic. *International Journal of Theoretical Physics*, 21(3):219–253, 1982.

J.-Y. Girard. Linear logic. *Theor. Comput. Sci.*, 50:1–102, 1987.

A. S. Green and T. Altenkirch. From reversible to irreversible computations. *Electron. Notes Theor. Comput. Sci.*, 210:65–74, July 2008.

M. Hasegawa. Recursion from cyclic sharing: Traced monoidal categories and models of cyclic lambda calculi. In *TLCA*, pages 196–213, 1997.

M. Hasegawa. On traced monoidal closed categories. *MSCS*, 19:217–244, April 2009. ISSN 0960-1295. .

M. Hofmann and T. Streicher. The groupoid interpretation of type theory. In *Venice Festschrift*, pages 83–111, 1996.

R. James and A. Sabry. Theseus: A high-level language for reversible computation. In *Reversible Computation*, 2014. Booklet of work-in-progress and short reports.

R. P. James and A. Sabry. Information effects. In *POPL*, pages 73–84. ACM, 2012a.

R. P. James and A. Sabry. Isomorphic interpreters from logically reversible abstract machines. In *RC*, 2012b.

A. Joyal, R. Street, and D. Verity. Traced monoidal categories. In *Mathematical Proceedings of the Cambridge Philosophical Society*. Cambridge Univ Press, 1996.

W. E. Kluge. A reversible SE(M)CD machine. In *International Workshop on Implementation of Functional Languages*, pages 95–113. Springer-Verlag, 2000.

N. Krishnaswami. The geometry of interaction, as an OCaml program. `http://semantic-domain.blogspot.com/2012/11/in-this-post-ill-show-how-to-turn.html`, 2012.

R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183–191, July 1961.

M. Laplaza. Coherence for distributivity. In *Lecture Notes in Mathematics*, number 281, pages 29–72. Springer Verlag, Berlin, 1972.

S. Mac Lane. *Categories for the working mathematician*. Springer-Verlag, 1971.

I. Mackie. Reversible higher-order computations. In *Workshop on Reversible Computation*, 2011.

E. Moggi. Computational lambda-calculus and monads. In *Proceedings of the Fourth Annual Symposium on Logic in Computer Science*, pages 14–23, Piscataway, NJ, USA, 1989. IEEE Press. ISBN 0-8186-1954-6. URL `http://dl.acm.org/citation.cfm?id=77350.77353`.

S.-C. Mu, Z. Hu, and M. Takeichi. An injective language for reversible computation. In *MPC*, pages 289–313, 2004.

A. Peres. Reversible logic and quantum computers. *Phys. Rev. A*, 32(6), Dec 1985.

S. L. Peyton Jones and A. L. M. Santos. A transformation-based optimiser for haskell. *Sci. Comput. Program.*, 32(1-3):3–47, Sept. 1998. ISSN 0167-6423. . URL `http://dx.doi.org/10.1016/S0167-6423(97)00029-4`.

M. Saeedi and I. L. Markov. Synthesis and optimization of reversible circuits — a survey. *ACM Comput. Surv.*, 45(2):21:1–21:34, Mar. 2013. ISSN 0360-0300. . URL `http://doi.acm.org/10.1145/2431211.2431220`.

P. Selinger. A survey of graphical languages for monoidal categories. In B. Coecke, editor, *New Structures for Physics*, volume 813 of *Lecture Notes in Physics*, pages 289–355. Springer Berlin / Heidelberg, 2011.

Z. Sparks and A. Sabry. Superstructural reversible logic. In *3rd International Workshop on Linearity*, 2014.

The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. `http://homotopytypetheory.org/book`, Institute for Advanced Study, 2013.

R. Thomason. Beware the phony multiplication on Quillen's $\mathcal{A}^{-1}\mathcal{A}$. *Proc. Amer. Math. Soc.*, 80(4):569–573, 1980.

T. Toffoli. Reversible computing. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 632–644. Springer-Verlag, 1980.

T. Yokoyama and R. Glück. A reversible programming language and its invertible self-interpreter. In *PEPM*, pages 144–153. ACM, 2007.