Functoriality in Reversible Circuits
(Work in Progress)

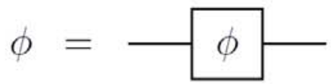
Tomoo Yokoyama
Aoyama Gakuin University

Tetsuo Yokoyama
Nagoya University

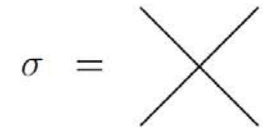
Objectives

- Characterize reversible combinatorial circuits.
  - To apply other theories, such as category theory, braid theory, and group theory.
  - To understand the differences among classical circuits, quantum circuits, etc.
- Using this experience, we want to characterize mathematical properties of reversible programming languages.

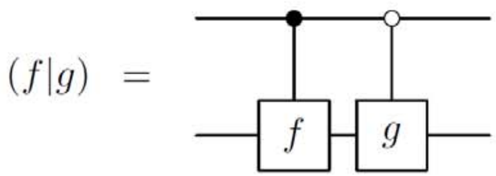
Reversible Circuits



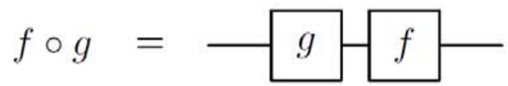
(a) Rotation (ϕ is $C(1,1)$ and invertible)



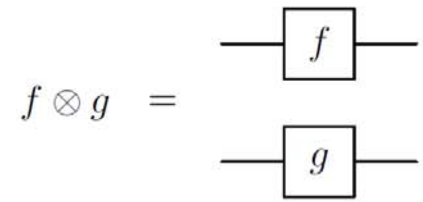
(b) Crossing



(c) Conditional composition



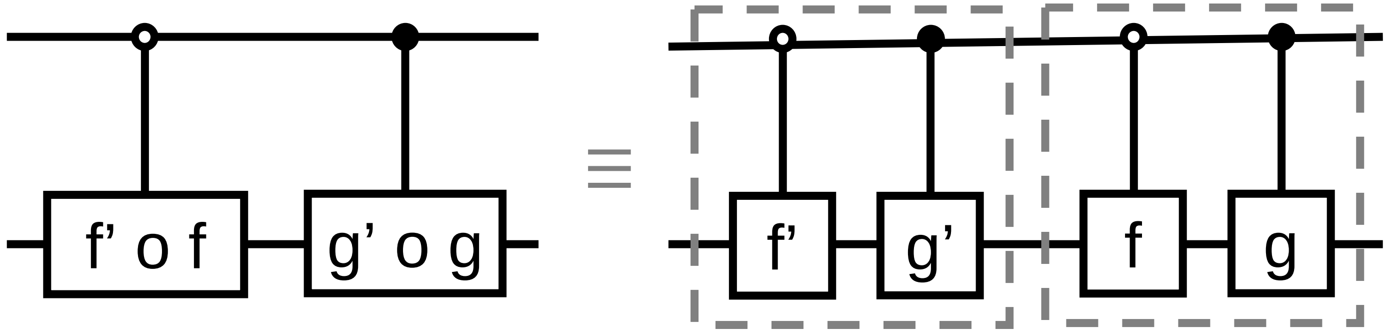
(d) Sequential composition



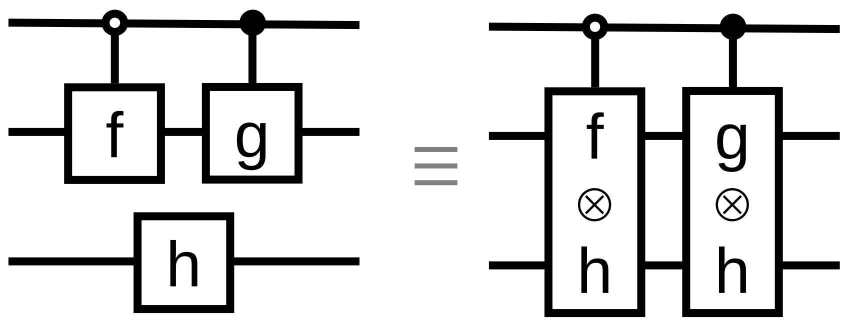
(e) Parallel composition

Fig. 1. Reversible circuits

Some Equivalence Relations of Reversible Circuits



(f' o f | g' o g) = (f' | g') o (f | g)



(f | g) ⊗ h = (f⊗h | g⊗h)

- How to model characteristics of circuits?
- What assumptions are required?

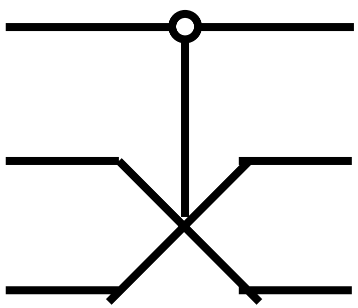
Our approach

- How to model characteristics of circuits?
  - To model them, we use categorical structure, i.e., the functoriality of a tensor $\otimes$ and a bifunctor $(. \mid .)$
- What assumptions are required?
  - Explicitly, we describe the assumptions for the family of all circuits

Group Structure in Reversible Circuits
[StormeDeVosJacobs99,GreenAltenkirch08]

- A function (or morphism) realized by circuits is an isomorphism.
  - One-to-one. The domain and the target are the same size.
- Any morphism is invertible.

E.g., Fredkin gate



Input	Output
000	000
001	001
010	010
011	011
100	100
101	110
110	101
111	111

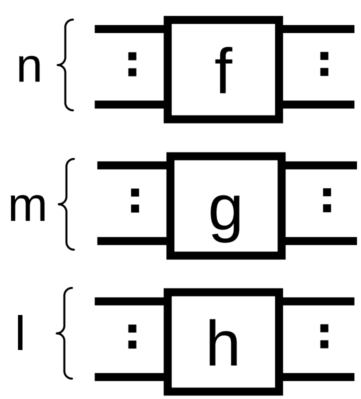
Morphisms comprise group structure.

⇒ Characterize a reversible circuit as a *groupoid C*:
a category in which any morphism is invertible.

Monoidal Structure in Reversible Circuits
[GreenAltenkirch08]

- $(C,\otimes,0)$: a strict symmetric monoidal category
  - C: a groupoid
  - $\otimes$: a tensor product
    - $n \otimes m := n + m$ for any $n,m \in C$
    - $(\otimes,0)$ and $(\otimes,id)$ are monoids.
      - $(n \otimes m) \otimes l = n \otimes (m \otimes l)$, $0 \otimes n = n \otimes 0 = n$
      - $(f \otimes g) \otimes h = f \otimes (g \otimes h)$, $id \otimes f = f \otimes id = f$

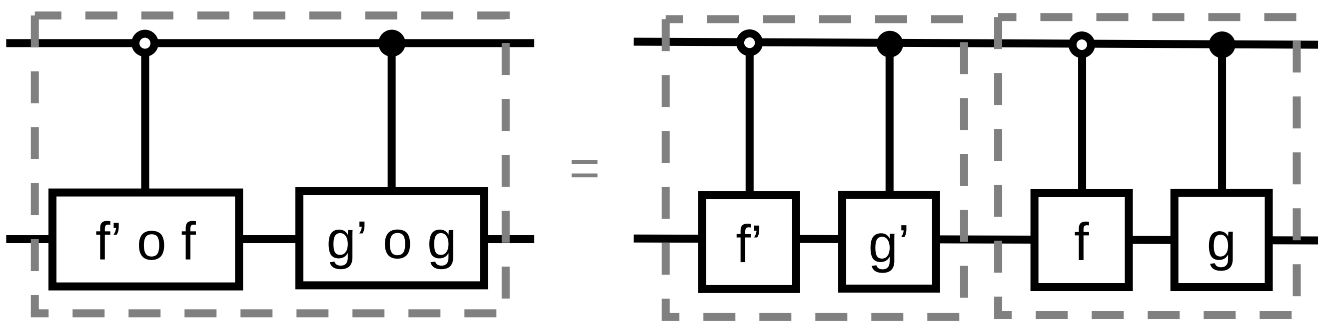
Example



- $f \otimes (g \otimes h) = (f \otimes g) \otimes h$
- $n \otimes (m \otimes l) = (n \otimes m) \otimes l$
  $= n + m + l$

Functoriarity in Reversible Circuits

- Functor F: C → D
  - $F(id_C) = id_D$, $F(f \circ g) = F(f) \circ F(g)$
- Bifunctor G
  - $G(id_C,id_C) = (id_D,id_D)$, $G(f' \circ f, g' \circ g) = G(f', g') \circ G(f,g)$
- We characterize a conditional composition (. | .) as a bifunctor.

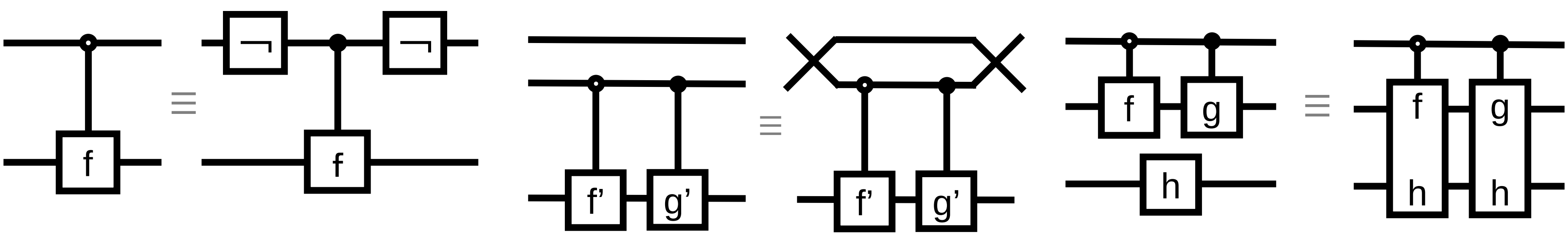


(f' o f | g' o g) = (f' | g') o (f | g)

It should be noted that we do not have semantics of ○ and ●.

Wired Category [Informal definition]

- (C,⊗,(. | .)) is called wired if
  - Negations $\boxed{\neg}$ and wire crossings $\sigma = \times$ are well-defined, and all the circuits can be appropriately generated.
  - Wirings are well-defined.
  - The following holds:



$$(f| = \underline{\neg}_{n-1} \circ |f) \circ \underline{\neg}_{n-1} \qquad \overline{(f|g)} = \underline{\sigma}_n \circ (\overline{f}|\overline{g}) \circ \underline{\sigma}_n \qquad (f \mid g) \otimes h = (f \otimes h \mid g \otimes h)$$

where $\overline{f} := id_1 \otimes f$, $\underline{f} := f \otimes id_1$, and $\underline{f}_m := f \otimes id_m$

Wired Category [Formal Definition] (1/3)

For a category C, define a subcategory $\mathrm{Diag}(C)$ of a category $C \times C$ as follows:

$$\begin{aligned} \mathrm{ob}(\mathrm{Diag}(C)) &:= \{(c, c) \mid c \in \mathrm{ob}(C)\}\,, \\ \mathrm{Diag}(C)((c, c), (d, d)) &:= \{(f, g) \mid f, g \in C(c, d)\}\,. \end{aligned}$$

Wired Category [Formal Definition] (2/3)

Let $(\cdot \mid \cdot) : \mathrm{Diag}(C) \to C$ be a functor with $(\cdot \mid \cdot)(n,n) = n+1$ for any object n. The tuple $(C, \otimes, (\cdot \mid \cdot))$ is called *wired* if

(i) $C(n,m) := \{\}$ if $n \neq m$, $C(0,0) := \{id_0\}$, $C(1,1) := \{id_1, \phi_1, \phi_2, \ldots\}$, and there are a negation $\neg \in C(1,1)$ and a wire crossing $\sigma \in C(2,2)$ such that $\boxed{\neg \circ \neg = id_1 \neq \neg \text{ and } \sigma \circ \sigma = id_2 \neq \sigma,}$ respectively. For each $n \geq 2$, each hom-set $C(n,n)$ is generated by taking $\circ$, $\otimes$ and $(\cdot \mid \cdot)$ of $C(m,m)$ and σ where $1 \leq m < n$.

(ii) (a) Let $\sigma_l := id_{i+j-1-l} \otimes \sigma \otimes id_{l-1}$, $\sigma_{i,l} := \sigma_l \circ \cdots \circ \sigma_{i-1} \circ \sigma_i$, and $\Sigma_{j,i} := \sigma_{i+j-1,j} \circ \cdots \circ \sigma_{i+1,2} \circ \sigma_{i,1} \in C(i+j, i+j)$ for any $l = 1, 2, \ldots, i+j-1$. For $f \in C(j,j)$ and $g \in C(i,i)$,

$$f \otimes g = (\Sigma_{j,i})^{-1} \circ (g \otimes f) \circ \Sigma_{j,i}\,. \tag{3}$$

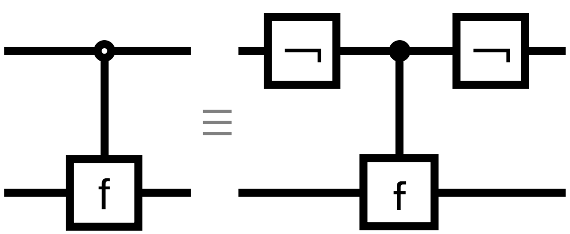
(b) $\overline{\sigma} \circ \underline{\sigma} \circ \overline{\sigma} = \underline{\sigma} \circ \overline{\sigma} \circ \underline{\sigma}$.

Wired Category [Formal Definition] (3/3)

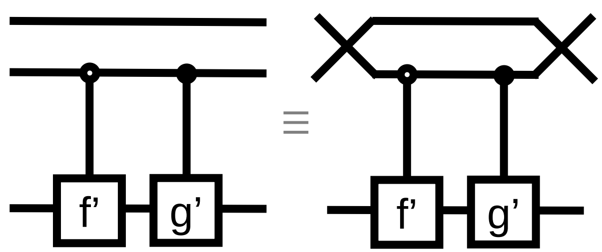
(iii) $(\cdot \mid \cdot)$ satisfies the following: For $f, g \in C(n,n)$ and $h \in C(m,m)$,

$$(f| = \underline{\neg}_{n-1} \circ |f) \circ \underline{\neg}_{n-1} \tag{4}$$
$$\overline{(f|g)} = \underline{\sigma}_n \circ (\overline{f}|\overline{g}) \circ \underline{\sigma}_n \tag{5}$$
$$(f \mid g) \otimes h = (f \otimes h \mid g \otimes h) \tag{6}$$

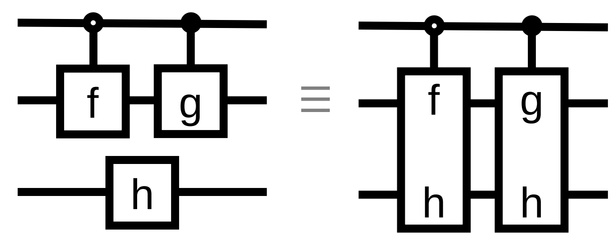
where $(f| := (f \mid id_n)$ and $|f) := (id_n \mid f)$.



$(f| = \underline{\neg}_{n-1} \circ |f) \circ \underline{\neg}_{n-1}$



$\overline{(f|g)} = \underline{\sigma}_n \circ (\overline{f}|\overline{g}) \circ \underline{\sigma}_n$



$(f \mid g) \otimes h = (f \otimes h \mid g \otimes h)$

Properties of Circuits

Lemma 2.1 *Let C be a wired category. For* $f_n, g_n, h_n, k_n, t_n, s_n \in C(n, n)$,

$$\overline{\neg} \circ \sigma = \sigma \circ \underline{\neg} \tag{7}$$

$$(id_n | id_n) = (id_n| = |id_n) = id_{n+1} \tag{8}$$

$$\overline{h_n} = (h_n | h_n) \tag{9}$$

$$\boxed{(f_n | g_n) \circ (h_n | k_n) = (f_n \circ h_n | g_n \circ k_n)} \tag{10}$$

$$\text{In particular, } (f_n | g_n) \circ \overline{h_n} = (f_n \circ \overline{h_{n-1}} | g_n \circ \overline{h_{n-1}}) \tag{11}$$

$$t_l \otimes s_m \otimes (f_n | g_n) = \Sigma^{-1} \circ t_l \otimes (f_n | g_n) \otimes s_m \circ \Sigma \tag{12}$$

$$\boxed{(f_n \mid g_n) = |g_n) \circ (f_n|} \tag{13}$$

$$\boxed{(f_n \otimes g_m) \circ (h_n \otimes k_m) = (f_n \circ h_n) \otimes (g_m \circ k_m)} \tag{14}$$

$$\text{In particular, } \overline{\psi} \circ \underline{\phi} = \phi \otimes \psi = \underline{\phi} \circ \overline{\psi} \tag{15}$$

where $\Sigma = id_l \otimes \Sigma_{m,n+1}$.

It should be noted that we do not use truth values.
Therefore, this holds for any circuits that satisfy wired properties.

Classical case

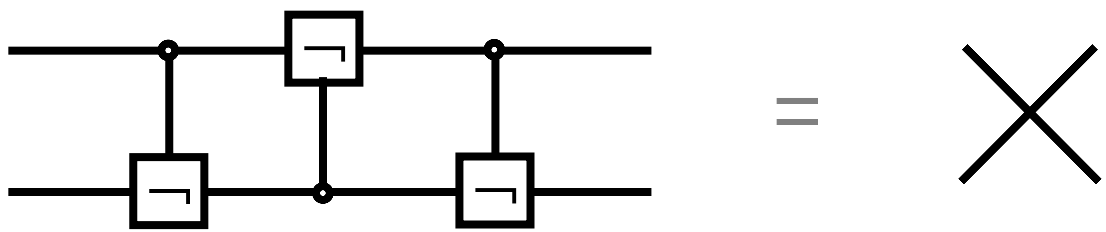
- A wired category C is called *classical* if C(1,1) has exactly two morphisms.

- **Remark** Since C is a groupoid, $id_1 \in C(1,1)$ and there is $\psi \neq id_1$ s.t. $\psi \circ \psi = id_1$. ψ is a negation and hereafter we denote it by $\neg$.

Proposition

C: a classically wired category

Suppose that $(\neg| \circ \sigma \circ (\neg| \circ \sigma \circ (\neg| = \sigma$:



XOR swap

C(2,2) can be transformed into the following 24 elements:

$$\begin{gathered}
id_2,\ \overline{\neg},\ \underline{\neg},\ \neg \otimes \neg,\ \sigma,\ \overline{\neg} \circ \sigma,\ \underline{\neg} \circ \sigma,\ (\neg \otimes \neg) \circ \sigma,\ (\neg|,\ |\neg),\ \underline{\neg} \circ (\neg|,\ \underline{\neg} \circ |\neg), \\
\sigma \circ (\neg|,\ \sigma \circ |\neg),\ \overline{\neg} \circ \sigma \circ (\neg|,\ \overline{\neg} \circ \sigma \circ |\neg), \\
(\neg| \circ \sigma \circ (\neg|,\ (\neg| \circ \sigma \circ |\neg),\ |\neg) \circ \sigma \circ |\neg),\ |\neg) \circ \sigma \circ (\neg|, \\
\sigma \circ (\neg| \circ \sigma \circ (\neg|,\ \sigma \circ |\neg) \circ \sigma \circ |\neg),\ \underline{\neg} \circ \sigma \circ |\neg) \circ \sigma \circ |\neg),\ \underline{\neg} \circ \sigma \circ (\neg| \circ \sigma \circ (\neg|.
\end{gathered}$$

The number corresponds to the number of all circuits: 4!

Proof (Sketch)

1. f can be transformed into a sequence of functional compositions of id_2, $\overline{\neg}$, $\underline{\neg}$, $|\neg)$, $(\neg|$, and σ.

2. Any subcircuit of a form $(B_3 \circ \sigma) \circ (B_2 \circ \sigma) \circ (B_1 \circ \sigma)$ in f' can be replaced with $id_2, \overline{\neg}, \underline{\neg}$, or $\neg \otimes \neg$.

3. Using an XOR swap, we can move $(\neg|$ or $|\neg)$ to the rightmost if it exists.

4. Many repeats of this step can reduce f to one of the 24 elements.

Concluding Remark

- Using functoriarity of $(. | .)$ and $\otimes$ models characteristic of circuits, effectively.

- None of the proofs of the properties of circuits requires the truth tables.

- Our results in the general case hold for non 0/1 circuits.