Реверсивные конструктивные логики

Н. Н. Непейвода

Содержание

1 Реверсивная вычислимость и ее логика

Еще в 1961 г. Р. Ландауэр [1] указал важный род вычислений, не исследовавшийся ранее и мало исследуемый (хотя и не забытый) до сих пор.

Рассмотрим технический пример, подобный примеру Ландауэра. Пусть у нас есть компьютер, составленный из сверхпроводящих элементов. Для сохранения сверхпроводимости он должен охлаждаться, например, жидким водородом. Таким образом, выделение тепла может полностью разрушить его структуру и возникает вопрос: если нет «информационного трения» при обработке информации, можно ли организовать ее так, чтобы при вычислениях не выделялось тепло? Р. Ландауэр показал, что выделение тепла физически

неизбежно, если операции компьютера *необратимы*. Тем самым возник вопрос о вычислениях, в которых все операции обратимы. Совокупность вычислимых функций, замкнутую относительно композиции и взятия обратной функции, назовем *реверсивной*.

Базируясь на идее Ландауэра, С. Беннет [2] предложил в 1973 г. создать логически реверсивный булев компьютер. Т. Тоффоли и Э. Фредкин [3, 4] показали, что можно смоделировать полное множество булевых операций на сверхпроводящем компьютере без нарушения условий Ландауэра. Р. Меркле [5] предложил другой вариант булевых реверсивных вычислений.

Конечно же, задание исходных данных и чтение результатов по самой своей природе не реверсивные операции, так что полностью исключить выделение тепла никогда не удастся.

Но реверсивность вычислений является отнюдь не исключительным свойством сверхпроводников. Например, «квантовая вычислимость» также реверсивна по самой своей природе (задание исходных данных и чтение результатов и здесь являются неустранимыми исключениями). В редакторах было бы крайне желательно обеспечить возможность обратимости всех операций вплоть до явного подтверждения сделанных изменений. В бизнесе обратимыми являются заказы и счета вплоть до их утверждения. Более того, разные заказы и счета являются тут не просто обратимыми, а независимыми, и здесь мы имеем пример *коммутативных реверсивных* действий.

Таким образом, реверсивность не является частным свойством некоторых булевых операций. Она характеризует интересный и важный общий класс вычислений, и поэтому представляет интерес конструктивная логика такого класса вычислений.

Нет большой неожиданности в том, что данная логика весьма отлична от конструктивных логик других классов вычислений: функциональной (интуционистской)[1], линейной и нильпотентной логики. Эти логики также исключительно сильно различаются между собой.

Маленькое замечание о терминологии. Поскольку имеется постоянное недоразумение с порядком композиций, заметим, что у нас композиция функций $f \circ g$ означает $a \xrightarrow{f} b \xrightarrow{g} c$.

[1]Предлагаем называть ее именно так, поскольку она соответствует чистому типовому функциональному программированию, а термин «интуиционистская» крайне неудачен во всех отношениях, кроме исторического.

2 Группа как состояния и операторы. Язык и семантика.

Поскольку все действия в реверсивных вычислениях обратимы, естественно рассматривать пространство действий как *группу*. Сделаем еще один важный шаг[2]:

Пространство состояний та же самая группа, что и группа действий.

Тогда каждой пропозициональной букве сопоставляется подмножество группы[3], каждый элемент группы α представляет функцию $\lambda x.\, x \circ \alpha$.

Лексемами языка чистой реверсивной логики являются пропозициональные символы A, B, C, ..., пять логических связок классической логики ($\supset$, $\equiv, \wedge, \vee, \neg$), называемых *дескриптивными связками*, и три конструктивные логические связки $\Rightarrow, \&, \sim$. $\neg$ и $\sim$ — одноместные связки, все остальные двухместные. Сигнатура Σ — непустое множество пропозициональных символов

Классические связки читаются обычным образом, $\Rightarrow$ читается как «можно преобразовать», $A\&B$ как «последовательная конъюнкция» или «A, затем B»[4], $\sim A$ — превентивное отрицание, читаемое в разных контекстах как «отменить A», «воспрепятствовать A».

Как говорится в современной литературе по информатике, дескриптивные и конструктивные связки полностью интероперабельны, могут смешиваться произвольно. Формула называется *дескриптивной*, если все ее логические связки классические. Если в формуле нет ни одной классической связки, она называется *чисто конструктивной*. Таким образом, пропозициональные символы одновременно являются и дескриптивными, и чисто конструктивными формулами.

Основное семантическое понятие “элемент a *реализует* формулу A в интерпретации I” ($I \models a\textcircled{R}A$). В случае, если интерпретация фиксирована, упоминание о ней опускаем.

Определение 1 *Интерпретация сигнатуры Σ — пара из группы Gи функции $\zeta : \Sigma \to \mathbb{P}\, G$ из множества пропозициональных символов в множество подмножеств G. Подмножество, сопоставляемое A в интерпретации I, обозначим $\zeta_I(A)$. Если I фиксировано, индекс опускаем.*

[2]Впервые такая идея была предложена и успешно развита Ж.-И. Жираром в линейной логике

[3]Внимание! Не обязательно подгруппа: в этом коренное отличие от квантовых и им подобных логик!

[4]Впрочем, можно читать и как «и» в смысле знаменитых клиниевских примеров: «Маша вышла замуж и родила ребенка»,«Маша родила ребенка и вышла замуж.»

Определение 2 . *Реализация формулы в интерпретации* I.

1. $a\circledR A \triangleq a \in \zeta(A)$ *если* A *— пропозициональный символ и* $A \in \Sigma$.
2. $a\circledR A \wedge B \triangleq a\circledR A$ *и* $a\circledR B$.
3. *Для других классических связок определения также стандартны*.
4. $a\circledR A \Rightarrow B \triangleq \forall b \in G(b\circledR A \supset b \circ a\circledR B)$. *Итак,* a *преобразует решения* A *в решения* B.
5. $a \circ b\circledR A\&B \triangleq a\circledR A \wedge b\circledR B$. *Решение* B *применяется к решению* A.
6. $a\circledR \sim A \triangleq a^{-1}\circledR A$. a *аннулирует решение* A *либо препятствует ему.*

Множество реализаций A *обозначим* $\circledR A$.

Определение 3 . A *истинно в интерпретации* I, *если* $\{a|a\circledR A\} = G$. A *общезначимо, если* A *истинно в любой интерпретации ее сигнатуры. Общезначимость формулы* A *обозначается* $\models A$.
A *реализуемо в интерпретации* I, *если* $\{a|a\circledR A\} \neq \emptyset$. A *тождественно реализуемо, если* A *реализуемо любой интерпретации ее сигнатуры.*

Примечание для невежественных рецензентов. То, что пространство состояний — группа, а не полугруппа, и наличие $\&$ принципиально отличает нашу логику от линейной логики Ж.-И. Жирара (идейное влияние которой, конечно же, есть). То, что у нас есть $\sim$ и $\&$, принципиально отличает ее от «исчислений областей». И, наконец, еще одно коренное отличие от указанных выше двух аналогов: неуклонное следование принципу, давно осознанному в нашей научной школе и упорно игнорируемому большинством прикладных математиков и информатиков: худший враг хороших систем — лишние возможности. Мы стремились включить в логическую систему лишь самое необходимое, чтобы иметь надежду не просто на разрешимость, а на достаточно эффективные алгоритмы разрешения и поиска вывода.

3 Некоторые результаты

Первые две теоремы дают минимальные условия того, чтобы реверсивная логика могла претендовать на звание логического исчисления.

Теорема 1 *Множества общезначимых и тождественно реализуемых формул перечислимы.*

Доказательство. Пусть $\mathbf{G}_\Sigma$ — элементарная теория групп с дополнительными одноместными предикатами для всех символов Σ. Для новых предикатов аксиом нет. Определим перевод $\mathbf{T}(A, x)$ формул реверсивной логики в формулы $\mathbf{G}_\Sigma$ с единственной свободной переменной x.

1. $\mathbf{T}(A, x) \triangleq A(x)$ для пропозиционального символа A.
2. $\mathbf{T}(A \wedge B, x) \triangleq \mathbf{T}(A, x) \wedge \mathbf{T}(B, x)$.
3. $\mathbf{T}(A \vee B, x) \triangleq \mathbf{T}(A, x) \vee \mathbf{T}(B, x)$.
4. $\mathbf{T}(A \supset B, x) \triangleq \mathbf{T}(A, x) \supset \mathbf{T}(B, x)$.
5. $\mathbf{T}(\neg A, x) \triangleq \neg\mathbf{T}(A, x)$.
6. $\mathbf{T}(A \Rightarrow B, x) \triangleq \forall y(\mathbf{T}(A, y) \supset \mathsf{Subst}[\mathbf{T}(B, x), y \circ x])$.
7. $\mathbf{T}(A\&B, x) \triangleq \exists y \exists z(\mathbf{T}(A, y) \wedge \mathbf{T}(B, z) \wedge x = y \circ z)$.
8. $\mathbf{T}(\sim A, x) \triangleq \exists y(\mathbf{T}(A, y) \wedge x = y^{-1})$.

Формула A общезначима тогда и только тогда, когда $\forall x\mathbf{T}(A, x)$ истинно во всех моделях $\mathbf{G}_\Sigma$, и, значит, тогда и только тогда, когда $\forall x\mathbf{T}(A, x)$ доказуемо в $\mathbf{G}_\Sigma$.

Соответственно, формула A тождественно реализуема тогда и только тогда, когда $\exists x\mathbf{T}(A, x)$ $\exists x\mathbf{T}(A, x)$ доказуемо в $\mathbf{G}_\Sigma$.

Следствие 1 *Можно построить исчисления для общезначимых и для реализуемых формул реверсивной логики.*

Задача 1 *Явно построить исчисления для реверсивной логики.*

Теорема 2 *Множества всех общезначимых и тождественно реализуемых формул реверсивной логики замкнуты относительно операции подстановки произвольной формулы вместо пропозиционального символа.*

Доказательство. Теорема следует из следующей леммы, доказываемой непосредственной индукцией по определению реализуемости.
Лемма 2.1. Если $A[B]$ — формула с выделенной подформулой B, p — пропозициональный символ, в нее не входящий, и $\zeta(p) = \{a \mid a®B\}$, то

$$\{a \mid a®A[B]\} = \{a \mid a®A[p]\}\,.$$

4 Некоторые свойства реверсивной логики

Рассмотрим теперь некоторые особенности и выразительные свойства реверсивной логики.

Предложение 2 *A реализуемо (истинно, тождественно реализуемо, тождественно истинно) тогда и только тогда, когда соответственное свойство выполнено для $\sim A$.*

Доказательство. Множество X непусто тогда и только тогда, когда множество $\{x \mid x^{-1} \in X\}$ непусто. Если же X совпадает со всей группой, то $\{x \mid x^{-1} \in X\}$ также совпадает со всей группой.

Таком образом, внешне наша логика выглядит несколько необычной: она предельно противоречива в том смысле, что любое утверждение имеет тот же статус, что и его превентивное отрицание. Но это не означает конструктивной эквивалентности утверждения и его превентивного отрицания.

Пример 1 *Рассмотрим мультипликативную группу рациональных чисел. Пусть значение p есть $\{1, 2, 3\}$. Тогда множество реализаций $\sim p$ есть $\{1, \frac{1}{2}, \frac{1}{3}\}$. Нет такого рационального числа, при умножении которого на элементы первого множества получались бы элементы второго.*
Таким образом,$A \Rightarrow \sim A$ не всегда реализуемо.

Предложение 3 *Дескриптивная формула общезначима тогда и только тогда, когда она тождественно реализуема, и тогда и только тогда, когда она классически общезначима.*

Доказательство. Вторая эквивалентность следует из того, что для проверки общезначимости достаточно рассмотреть формулу на единичной группе и задать всевозможные присваивания значений пропозициональным буквам. Первая из того, что если формула не является общезначимой, то есть интерпретация, где она тождественно ложна (также на единичной группе).

Теорема 3 *Ни одна чисто конструктивная формула не является общезначимой. Ни для одной чисто конструктивной формулы не является общезначимым ее классическое отрицание.*

Доказательство. Достаточно заметить, что, если придать всем пропозициональным буквам множество реализуемости $\{e\}$, то множество реализуемости всей формулы также будет e.

Общезначимые формулы.

$$\sim\sim A \equiv A \tag{1}$$

Закон двойного превентивного отрицания.

$$((A\&B)\&C) \equiv (A\&(B\&C)). \tag{2}$$

Ассоциативность последовательной конъюнкции.

$$\begin{array}{c} A\&(A \Rightarrow B) \supset B; \\ A \supset B\& \sim (A \Rightarrow B). \end{array} \tag{3}$$

Таким образом, $\sim (B \Rightarrow A)$ может рассматриваться как другой вид конструктивной импликации. Обычную импликацию можно называть инъективной, поскольку функция $\lambda x.\, x \circ a$ является инъекцией A в B. Вторая импликация сюръективна, поскольку $\sim (B \Rightarrow A)$ отображает A на все B (и, возможно, куда-либо еще). Сюръективную импликацию обозначим $\sqsupset$.

$$A \supset (B \Rightarrow A\&B) \tag{4}$$

Ни одну из импликаций в данной формуле нельзя заменить на другую.

$$\sim (A\&B) \equiv\sim B\& \sim A \tag{5}$$

Соответствует известному тождеству в группах $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Тождественно реализуемые формулы.

$$A \Rightarrow A \tag{6}$$

Эта формула представляет пример тождественно реализуемой, но не общезначимой, формулы. В самом деле, возьмем аддитивную группу целых чисел и $\{0\}$ в качестве интерпретации A. Тогда $®A \Rightarrow A = \{0\}$. Реализация этой формулы обязательно включает в себя единицу группы e, но не обязательно сводится к ней.

Предложение 4 *$A \Rightarrow A$ истинна тогда и только тогда, когда либо истинна A, либо истинна $\neg A$.*

Доказательство. Часть «тогда» очевидна. «Только тогда» докажем от противного. Пусть есть элементы a, b, такие, что $a \in ®A$, $b \notin ®A$. Тогда $a^{-1} \circ b \notin ®A$. В самом деле

$$a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = b.$$

$$B \Rightarrow (A \Rightarrow A\&B). \tag{7}$$

Реализацией этой формулы является, в частности, e. Перестановка посылок невозможна.

Формулы, характеризующие некоторые важные свойства.

Формула

$$A\&B \equiv B\&A, \tag{8}$$

выполненная как логический закон, характеризует коммутативные группы. Их же характеризует и приведенный ниже конструктивный закон контрапозиции.

$$(A \Rightarrow B) \equiv (\sim B \sqsupset \sim A). \qquad \text{(Contraposition)} \tag{9}$$

Задача 2 *Доказать либо опровергнуть следующее. RL+Contraposition является реверсивной логикой коммутативных групп.*

Истинность формулы

$$A\&(A \vee \neg A) \tag{10}$$

означает непустоту A. В самом деле, если в A есть хотя бы один элемент, он дает в данном произведении все элементы группы. Формулу (10) обозначим $\exists A$.

Задача 3 *Из наличия предыдущей формулы следует, что из разрешимости множества общезначимых формул следует разрешимость множества тождественно реализуемых. Разрешимы ли множества общезначимых и (или) тождественно реализуемых формул?*

Задача 4 *Можно ли выразить непустоту, не используя связки $\&$?*

Установим несколько общезначимых формул.

$$\exists(A\&B) \equiv (\exists A \wedge \exists B). \tag{11}$$

$$\exists A \equiv \exists \sim A. \tag{12}$$

$$(\exists A \wedge \exists \neg B) \equiv \exists \neg (A \Rightarrow B). \tag{13}$$

$$(\neg \exists A \vee \neg \exists \neg A) \equiv \neg \exists \neg (A \Rightarrow A). \tag{14}$$

Докажем важную формулу.

$$(\exists(A \Rightarrow B) \equiv \exists(B \Rightarrow A)) \equiv ((A \Rightarrow B) \equiv\sim (B \Rightarrow A)). \tag{15}$$

Доказательство. В случае, когда обе формулы $\exists(A \Rightarrow B)$ и $\exists(B \Rightarrow A)$ложны, оба множества реализуемости из заключения пусты.

В случае, если оба они непусты, и $a®(A \Rightarrow B)$, $b®(B \Rightarrow A)$, то $(b^{-1} \circ b) \circ a = b^{-1} \circ (b \circ a)$, и, значит, $b^{-1}®(A \Rightarrow B)$. Обратная импликация доказывается аналогично.

Если одно из этих множеств пусто, а второе нет, то ложность тождества в заключении очевидна.

□

Истинность формулы

$$(A\&A \equiv A) \wedge (A \equiv\sim A) \wedge \exists A \tag{16}$$

означает, что $®A$ есть подгруппа.

5 Расширенная реверсивная логика

Добавим к RL пропозициональную константу E, интерпретацией которой является множество $\{e\}$.

Предложение 5 *E невыразима в RL.*

Доказательство. Рассмотрим произвольную формулу RL и произвольную пару групп G_1, G_2, где G_1 является нетривиальной фактор-группой G_2. Возьмем некоторую интерпретацию I_1 пропозициональных букв на G_1. Определим $I_2(P, x)$ как $I_1(P, \hat{x})$. Тогда $®_{I_2}A = \{x \mid \hat{x}®_{I_1}A\}$. Таким образом, если $®_{I_1}A = \{e\}$, $®_{I_2}A = \{x|\hat{x} = e\}$.

Расширенный вариант RL обозначим ERL. Теоремы 1–3 переносятся на ERL. В ERL выразимы некоторые свойства, невыразимые в RL. Одно из них — A истинно на единственном элементе. Определим $\exists_1 A$ как

$$\exists(A \Rightarrow E) \wedge \exists A \tag{17}$$

Доказательство того, что $\exists_1 A$ невыразимо в RL, совершенно аналогично предложению 4.

Контекст $A \Rightarrow E$ — единственный контекст, где E меняет значение конструктивных связок.

$$(E \Rightarrow A) \equiv A \qquad (E\&A) \equiv A \qquad (A\&E) \equiv A \qquad \sim E \equiv E \tag{18}$$

6 Логическая теория групп

Рассмотрение реверсивной логики подводит к следующей математической теории, лежащей на грани между алгеброй и логикой, которая, насколько известно автору, не изучалась, поскольку алгебраисты «зациклилились» на том, что основным и необходимым предикатом является равенство.

Рассмотрим некоторую пропозициональную сигнатуру Σ. Все пропозициональные буквы превратим в одноместные предикаты. Равенства нет. Имеются двухместная операция $\circ$ и одноместная операция $^{-1}$.

$\tilde{\forall}$ означает совокупность кванторов всеобщности по всем свободным переменным последующей формулы. Пусть $t[u]$ — терм с выделенным вхождением переменной u, а $t[r]$, соответственно, результат замены этого выделенного вхождения на терм r. Теория $\mathbf{G}^0_\Sigma$ состоит из всех аксиом вида

$$\begin{array}{c} \tilde{\forall}\forall x,y,z(P(t[x\circ(y\circ z)])\equiv P(t[(x\circ y)\circ z)]) \\ \tilde{\forall}\forall x,y(P(t[x\circ(y\circ y^{-1})])\equiv P(t[x])) \\ \tilde{\forall}\forall x,y(P(t[(y\circ y^{-1})\circ x])\equiv P(t[x])) \\ \tilde{\forall}\forall x,y(P(t[y\circ y^{-1}])\equiv P(t[x\circ x^{-1}])) \end{array} \tag{19}$$

для всех P из Σ.

Не любая модель данной теории является группой, но фактор-модель любой модели по отношению эквивалентности

$$\left\{< a,b >|\ \forall t\in \mathrm{Term}, P\in\Sigma\ \models \tilde{\forall}(P(t[a])\equiv P(t[b]))\right\}$$

является группой. Здесь Term — множество всех термов, FV — множество свободных переменных терма. Таким образом, данная теория является полной логической теорией одноместных предикатов на группах. Понятие реализуемости формул реверсивной логики формулируется в данной теории.

Задача 5 *Верно ли, что по выразительным способностям $\mathbf{G}^0_\Sigma$ и RL совпадают в следующем смысле:*
Для каждой замкнутой формулы $\mathbf{G}^0_\Sigma$ можно построить формулу RL, истинную тогда и только тогда, когда истинна исходная формула?

Задача 6 *Верно ли, что по выразительным способностям реализуемости $\mathbf{G}^0_\Sigma$ и RL совпадают в следующем смысле:*
Для каждой формулы $A(x)$ теории $\mathbf{G}^0_\Sigma$ с одной свободной переменной x можно построить формулу RL A, такую, что в любой интерпретации на группе

$$\{x\mid x\circledR A\}=\{x\mid\!\models A(x)\}?$$

Расширение логической теории групп для E включает следующее множество аксиом для всех $P\in\Sigma$.

$$\forall x\, E(x\circ x^{-1}) \qquad \forall x\,(\exists x(E(x)\wedge A(x))\equiv A(x\circ x^{-1}))$$

Для этого расширения можно поставить задачи, аналогичные задачам 5 и 6.

7 Набросок альтернативного подхода: типизированная реверсивная логика

Десять лет назад автором была предложена первая система реверсивной логики, но она оказалась неудовлетворительной по многим критериям: как по практической приемлемости для задач анализа проблем информатики, так и по эстетическим и внутрилогическим критериям. Бестиповая реверсивная логика кажется намного лучше, но необходимо показать и возможность типового подхода.

Самым сильным предположением нашей реверсивной логики является то, что пространство состояний и действий — практически одно и тоже: группа G и ее автоморфизмы вида $\lambda x.\, a \circ x$. Но у группы G могут быть и другие автоморфизмы, и даже вычислимые.

Второе предположение нашей логики — замена традиционной конъюнкции на последовательную конъюнкцию. Традиционная конъюнкция также прекрасно представима в теории групп, но в этом случае реализацией ее является уже другая группа: прямое произведение групп, реализующих ее члены.

А вот почему нет дизъюнкции, при таком подходе становится полностью понятно: в категории групп нет прямой суммы. В категории коммутативных групп она есть, но там она совпадает с прямым произведением. Так что отсутствие конструктивной дизъюнкции — фундаментальный феномен реверсивности.

Есть некоторой непустой подкласс групп, которые естественно назвать *логическими группами*: группы, изоморфные собственной группе автоморфизмов и прямому произведению самих на себя. *Слабо логическая группа* — группа G, изоморфная $G \times G$, и такая, что есть изоморфизм $\phi : G \leftrightarrow G \times G$, такой, что для всякой пары $\langle a, b \rangle$ имеется такое c, что

$$\phi \circ (\lambda x.\, x \circ \langle a, b \rangle) \circ \phi^{-1} = \lambda x.\, c \circ x.$$

На логических и слабо логических группах можно интерпретировать бестиповую реверсивную логику с двумя конъюнкциями: последовательной и почти традиционной.

Но классы логических и слабо логических групп не являются многообразиями, они очень узки и поэтому непонятно, будет ли соответствующая логика формализуемой.

Рассмотрим другую конструкцию.

Определение 4 *Реверсивные типы и их изоморфность задаются следующим одновременным индуктивным определением.*

1. 0 — *тип.*

2. $\tau \simeq \tau$, *где* τ *— произвольный реверсивный тип.*

3. *Если* $\tau \simeq \pi$, *то* $\pi \simeq \tau$.

4. *Если* $\tau \simeq \pi$ *и* $\pi \simeq \rho$, *то* $\tau \simeq \rho$.

5. *Если* τ *и* π *— типы, то* $(\tau \to \pi)$ *— тип.*

6. *Если* $\tau \simeq \rho$, *то* $(\tau \to \pi) \simeq (\rho \to \pi)$ *и* $(\pi \to \tau) \simeq (\pi \to \rho)$.

7. *Если* $\tau_1, \ \ldots, \tau_n$ *— типы,* $a_1, \ \ldots, a_n$ *— различные слова, то* $(a_1 : \tau_1 \times \cdots \times a_n : \tau_n)$ *— тип.*

8. $(a_1 : \tau_1 \times \cdots \times a_i : \tau_i \times a_{i+1} : \tau_{i+1} \times \cdots \times a_n : \tau_n) \simeq$ $(a_1 : \tau_1 \times \cdots \times a_{i+1} : \tau_{i+1} \times a_i : \tau_i \times \cdots \times a_n : \tau_n)$, *где* $1 \leqslant i < n$.

9. *Если* $\tau \simeq \rho$, *то*

$$(a : \tau \times a_1 : \tau_1 \times \cdots a_n : \tau_n) \simeq (a : \rho \times a_1 : \tau_1 \times \cdots a_n : \tau_n).$$

Из этого определения очевидно следуют простейшие свойства $\simeq$.

$$((\tau \to \pi) \simeq (\tau_1 \to \pi_1)) \iff (\tau \simeq \tau_1) \wedge (\pi \simeq \pi_1);$$
$$((a : \tau \times b : \pi) \simeq (a : \tau_1 \times b : \pi_1)) \iff (\tau \simeq \tau_1) \wedge (\pi \simeq \pi_1);$$
$$((a : \tau \times b : \pi) \simeq (b : \pi_1 \times a : \tau_1)) \iff ((\tau \simeq \pi_1) \wedge (\pi \simeq \tau_1)).$$

Теперь определим естественный изоморфизм над любой парой изоморфных типов, предполагая, что функции и прямые произведения интерпретируются естественно. При этом не предполагается, что интерпретация функционального типа включает в себя *все* функции; но множество всех интерпретаций обязательно замкнуто относительно композиции.

Определение 5 *Естественный изоморфизм* $e_{(\tau \to \pi)}$ *изоморфных типов.*

1. $e_{(\tau \to \tau)} = \lambda x.\, x$.

2. $e_{((a_1:\tau_1 \times \cdots \times a_n:\tau_n) \to (a_1:\rho_1 \times \cdots \times a_n:\rho_n))} = (e_{(\tau_1 \to \rho_1)} \times \cdots \times e_{(\tau_n \to \rho_n)})$.

3. *Для произведений* $\tau = (\tau_1 \times \cdots \times a_n : \tau_n)$ *и* $\rho = (a_{\vartheta(1)} : \rho_{\vartheta(1)} \times \cdots \times a_{\vartheta(n)} : \tau_{\vartheta(n)})$, *где* ϑ *— перестановка чисел* $[1, \ldots, n]$, $e_{(\tau \to \rho)} = (e_{(\tau \to \tau_1)} \times e_{(\rho \to \rho_1)}) \circ \lambda x.\, \langle \mathrm{pr}_{\vartheta(1)}\ x, \ \ldots, \ \mathrm{pr}_{\vartheta(n)}\ x \rangle$.

4. $e_{((\tau \to \rho) \to (\tau_1 \to \rho_1))} = (e_{(\tau_1 \to \tau)} \circ e_{(\tau \to \rho)} \circ e_{(\rho \to \rho_1)})$.

Это определение корректно и удовлетворяет необходимому свойству стандартных изоморфизмов:

$$e_{(\tau\to\pi)} \circ e_{(\pi\to\rho)} = e_{(\tau\to\rho)}.$$

Оно же мотивирует введение меток членов прямого произведения: без меток невозможно однозначно определить стандартные изоморфизмы.

Пусть дан некоторый универс состояний — группа S. Построим над ним башню групп. Интерпретации типов $\tau \to \tau$ в этой башне являются группами, остальные — просто множествами биекций.

Определение 6 *Интерпретация типов.*

1. $\mathfrak{I}\lfloor 0\rfloor = S$.

2. *Для каждого класса эквивалентности типов, имеющих вид $\tau \to \tau$, где τ имеет такую же форму, выберем некоторый представитель класса τ и для него определим $\mathfrak{I}\lfloor(\tau\to\tau)\rfloor$ как некоторую подгруппу* $\mathrm{Aut}\ \mathfrak{I}\lfloor\tau\rfloor$.

3. *Для остальных типов, имеющих вид $\tau_1 \to \tau_2$, где τ_i имеют такую же форму (и по нашему определению должны быть эквивалентны), и ρ является представителем их класса эквивалентности, положим*
   $\mathfrak{I}\lfloor(\tau_1\to\tau_2)\rfloor = \left\{\varphi \mid \exists\psi\,(\psi \in \mathfrak{I}\lfloor(\rho\to\rho)\rfloor \wedge \varphi = e_{(\tau_1\to\rho)} \circ \psi \circ e_{(\rho\to\tau_2)}\right\}$.

4. *Для произведений*
   $\mathfrak{I}\lfloor(a_1 : \tau_1 \times \cdots \times a_n : \tau_n)\rfloor = \mathfrak{I}\lfloor a_1 : \tau_1\rfloor \times \cdots \times \mathfrak{I}\lfloor a_n : \tau_n\rfloor$.
   Если все эти типы являются группами, то $times$ понимается как прямое произведение групп преобразований.

5. *Для функций из произведение в произведение с одинаковыми метками и типами*
   $\mathfrak{I}\lfloor((a_1 : \tau_1 \times \cdots \times a_n : \tau_n) \to (a_1 : \tau_1 \times \cdots \times a_n : \tau_n))\rfloor =$
   $\mathfrak{I}\lfloor(a_1 : \tau_1 \to a_1 : \tau_1)\rfloor \times \cdots \times \mathfrak{I}\lfloor(a_n : \tau_n \to a_n : \tau_n)\rfloor$,
   где $\times$ понимается как прямое произведение групп преобразований.

6. *Для остальных функций из произведения $\tau = (\tau_1 \times \cdots \times a_n : \tau_n)$ в произведение $\rho = (a_{\vartheta(1)} : \rho_{\vartheta(1)} \times \cdots \times a_{\vartheta(n)} : \tau_{\vartheta(n)})$, где ϑ — перестановка чисел $[1, \ldots, n]$, положим*
   $\mathfrak{I}\lfloor(\tau\to\rho)\rfloor = \left\{\varphi \mid \exists\psi\,(\psi \in \mathfrak{I}\lfloor(\tau\to\tau)\rfloor) \wedge \varphi = \psi \circ e_{(\tau\to\rho)})\right\}$.

Предложение 6 *Для каждого типа $\tau \to \rho$ можно найти такой тип $\pi \to \pi$, что*

$$\mathfrak{I}\lfloor(\tau\to\rho)\rfloor = \left\{\varphi \mid \exists\psi\,(\psi \in \mathfrak{I}\lfloor(\pi\to\pi)\rfloor \wedge \varphi = e_{(\tau\to\pi)} \circ \psi \circ e_{(\pi\to\rho)})\right\}.$$

Легко доказывается индукцией по определению интерпретации. Рассмотрим пропозициональную логику с конструктивными связками $\Rightarrow, \&, \&\&, \sim$ и обычными классическими связками. Связка $\&\&$ называется *параллельной конъюнкцией* и имеет неопределенную местность. Таким образом, $(A_1\&\& \cdots \&\& A_n)$ не является сокращением.

Определение 7 *Типы формул.*
Определим отношение $\mathrm{Type}(A, \tau)$*, читаемое «формула* A *имеет тип* tau*». Это отношение не является функцией.*

1. *Если* A *— элементарная формула, то* $\mathrm{Type}(A, 0)$.
2. *Если* $\mathrm{Type}(A, \tau)$ *и* $\mathrm{Type}(B, \pi)$*, то* $\mathrm{Type}((A \Rightarrow B), (\tau \to \pi)$.
3. *Если* $\mathrm{Type}(A, 0)$, $\mathrm{Type}(B, 0)$*, то* $\mathrm{Type}((A\&B), 0)$.
4. *Если* $\mathrm{Type}(A, \tau)$*, то* $\mathrm{Type}(\sim A, \tau)$.
5. *Если* $\mathrm{Type}(A, \tau)$, $\mathrm{Type}(B, \rho))$*, то* $\mathrm{Type}((A \Rightarrow B), (\tau \to \rho))$.
6. *Если* $\mathrm{Type}(A, (\tau \to \pi))$, $\mathrm{Type}(B, (\pi \to \rho))$*, то* $\mathrm{Type}((A\&B), (\tau \to \rho))$.
7. *Если* $\mathrm{Type}(A_1, \tau_1)$, $\ldots$, $\mathrm{Type}(A_n, \tau_n))$, $a_1, \ \ldots, \ a_n$ *— различные слова, то то* $\mathrm{Type}((A_1\&\& \cdots \&\& A_n), (a_1 : \tau_1 \times \cdots \times a_n : \tau_n))$.
8. *Классические связки типа не меняют*.

Определение 8 *Приписывание типов* $\mathrm{TheType}(A[B])$ *вхождениям подформулы* B *в формулу* A*. Это приписывание является функцией, причем, возможно, не всюду определенной. Эта функция определена неоднозначно.*

1. *Всем экземплярам одной и той же пропозициональной буквы* L *приписывается один и тот же тип.*
2. *Если в подформуле* $B \Rightarrow C$ B *и* C *приписаны изоморфные типы, то* $\mathrm{TheType}(A[(B \Rightarrow C)])$ *может быть либо типом* B*, либо типом* C.
3. *Точно так же для связок* $\supset$, $\vee$, $wedge$, $\equiv$.
4. *Если выделена подформула* $\sim B$*, то* $\mathrm{TheType}(A[\sim B]) = \mathrm{TheType}(A[B])$.
5. *Если выделена подформула* $\neg B$*, то* $\mathrm{TheType}(A[\neg B]) = \mathrm{TheType}(A[B])$.
6. *Если выделена подформула* $B\&C$*, и* $\mathrm{TheType}(A[B]) = (\tau \to \rho)$, $\mathrm{TheType}(A[C]) = (\rho \to \pi)$*, то* $\mathrm{TheType}(A[B\&C]) = (\tau \to \pi)$.

7. *Если выделена подформула* $B\&C$, *и* $\mathrm{TheType}(A[B]) = 0$, $\mathrm{TheType}(A[C]) = 0$, *то* $\mathrm{TheType}(A[B\&C]) = 0$.

8. *Если выделена подформула* $B_1\&\&\cdots\&\&B_n$, *и* $\mathrm{TheType}(A[B_1]) = \tau_1$, *...,* $\mathrm{TheType}(A[B_n]) = \tau_n$, *и* $a_1,\ \ldots,\ a_n$ *— различные слова, то* $\mathrm{TheType}(A[B_1\&\&\cdots\&\&B_n]) = (a_1 : \tau_1 \times \cdots \times a_n : \tau_n)$.

9. $\mathrm{TheType}(A[A])$ *называется типом самой формулы при данном приписывании.*

Формула корректна, если хотя бы при одном приписывании она имеет тип.

Это определение накладывает следующие синтаксические ограничения: две формулы могут связываться связкой, отличной от $\&\&$ или $\&$ лишь в том случае, если у них имеются изоморфные типы. Две формулы A, B могут связываться связкой $\&$ лишь в том случае, если они обе имеют тип 0 одновременно или же для некоторых типов τ, π, ρ выполнено $\mathrm{Type}(A, (\tau \to \pi))$, $\mathrm{Type}(B, (\pi \to \rho))$.

Таким образом, лишь параллельная конъюнкция может связывать произвольные формулы. Во всех остальных случаях мы потрудились, чтобы при преобразованиях информация не появлялась и не терялась.

Заметим, что параллельная конъюнкция не идемпотентна и не ассоциативна. Отсутствие каких-то импликаций между A и $A\&\&A$ неизбежно, поскольку при переходе от одной формулы к другой либо дублируется, либо теряется информация. Неассоциативность является скорее интуитивным решением, навеянным аналогией между конъюнкцией и структурами данных. Ни один информатик не скажет, что три списка

$$(a, b, c), ((a, b), c), (a, (b, c))$$

эквивалентны по информации. А формулы типа

$$(A\&\&B\&\&C) \Rightarrow ((A\&\&B)\&\&C)$$

просто синтаксически некорректны.

Истинность и реализуемость корректной формулы на башне групп определяется естественно, так же, как для RL.

Коммутативность параллельной конъюнкции выполняется. Формула

$$((A\&\&B) \Rightarrow (B\&\&A))\&\&((B\&\&A) \Rightarrow (A\&\&B))$$

тождественно реализуема.

8 Некоторые выводы для информатики и электроники

Внимательно рассматривая т. н. «Toffoli Gate» [3], рекламируемый как реализация условного оператора для реверсивных вычислений, видим, что он отнюдь не противоречит нашим выводам о нереверсивности дизъюнкции: информация удваивается! Таким образом, каждый условный оператор либо цикл вызывает еще одно дублирование информации, обрабатываемой в нем.

Это показывает, почему сорвались проекты сверхпроводящего суперкомпьютера. Такой суперкомпьютер может быть лишь вычислительной мельницей для практически прямых вычислений. Все управление (не говоря уже о вводе и выводе информации) должно осуществляться внешним традиционным компьютером.

Но ситуация с экономической реверсивностью не выглядит столь безнадежно. Поскольку дублироваться должна лишь та информация, которая меняется непосредственно при выборе, а базы данных все равно громадные, реверсивность может быть здесь вполне приемлемым решением.

Заметим теперь, что формально допустимая с точки зрения групповой интерпретации реверсивности параллельная конъюнкция сразу же приводит к колоссальному утяжелению концепций. Так что общий вывод о том, что лишние возможности — самый страшный враг, тем более в нынешней ситуации, когда упоминание «новых возможностей» влечет приступ слюнявого телячьего восторга, получает еще более жестокое подтверждение. Даже теоретически полностью обоснованная возможность может на практике оказаться врагом, поскольку хорошая теория всегда односторонняя.

А в общем, видно, что реверсивные вычисления — прежде всего еще один стиль программирования со своей исключительно своеобразной логикой, и главное препятствие здесь — невозможность подходить к ним с традиционными мерками.

Список литературы

[1] R. Landauer, *Irreversibility and heat generation in the computing process*, IBM Journal of Research and Development, vol. 5, pp. 183-191, 1961.

[2] C. H. Bennett, Logical reversibility of computation, IBM Journal of Research and Development, vol. 17, no. 6, pp. 525-532, 1973.

[3] T. Toffoli, Reversible Computing, *MIT Technical Report* MIT/LCS/TM-151 (1980).

[4] E. Fredkin and T. Toffoli. *Conservative logic*. International Journal of Theoretical Physics, 21:219Ц253, 1982.

[5] Ralph C. Merkle. *Towards Practical Reversible Logic*, in Workshop on Physics and Computation, PhysComp '92, October, Dallas Texas; IEEE press 1992.

[6] Н. Н. Непейвода, И. Н. Скопин. *Основания программирования*. Москва–Ижевск, РХД, 2004, 686 р.