LABORATORY FOR
COMPUTER SCIENCE

MASSACHUSETTS
INSTITUTE OF
TECHNOLOGY

MIT/LCS/TM-124

BICONTINUOUS EXTENSIONS OF INVERTIBLE COMBINATORIAL FUNCTIONS

Tommaso Toffoli

January 1979

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

MIT/LCS/TM-124

BICONTINUOUS EXTENSIONS OF INVERTIBLE COMBINATORIAL FUNCTIONS

by

Tommaso Toffoli

December 1978

This research was supported by the Advanced Research Projects Agency of the Department of Defense and was monitored by the Office of Naval Research under Contract No. N00014-75-C-0661.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LABORATORY FOR COMPUTER SCIENCE
CAMBRIDGE MASSACHUSETTS 02139

BICONTINUOUS EXTENSIONS OF INVERTIBLE COMBINATORIAL FUNCTIONS

Tommaso Toffoli

MIT Laboratory for Computer Science, 545 Technology Sq., Cambridge, MA 02139

Abstract. We discuss and solve the problem of constructing a diffeomorphic componentwise extension for an arbitrary invertible combinatorial function. Interpreted in physical terms, our solution constitutes a proof of the physical realizability of general computing mechanisms based on *reversible* primitives.

Keywords. Invertible combinatorial functions, continuous extensions, reversibility, Boolean functions.

1. Motivations

In an ordinary digital computer, the two logic states associated with a binary signal are realized as distinguished values of a continuous variable which represents the range of a physical quantity; correspondingly, the logic function associated with a given combinatorial network is realized as the appropriate restriction of a suitable continuous function which characterizes a physical system involving a number of such quantities. If the logic function is not invertible (note that a computation may yield the same output for different inputs), its continuous extension cannot be invertible. On the other hand, the microscopic physical laws which underly the operation of a computer are presumed to be *strictly reversible*, i.e., they uniquely specify a trajectory both forward and backward in time. Thus, it is clear that a noninvertible continuous function such as the above characterizes a physical system only in terms of *statistical* mechanics, rather than of *microscopic* mechanics. In other words, such a function is necessarily an *incomplete* specification of a mechanical system[1]; in particular, it does not give one the means to deal in any detail with the information that is "discarded" during a computation, besides accounting for it in terms of the

(*a*) When all input levers occupy distinguished positions, so do all the output ones. In this way, the box "computes" a combinatorial function from binary n-tuples to binary n-tuples.

(*b*) The collective configuration of the output levers is a continuous function of the input configuration. Continuity should extend to the higher derivatives (velocity, acceleration, etc.).

(*c*) The box is *reversible*, i.e., condition (*b*) holds when input and output levers are exchanged.

Clearly, (*c*) implies that (a) too holds when input and output levers are exchanged. Thus, the combinatorial function "computed" by the box must be invertible. We want design principles to construct a box with the above properties for *any* invertible combinatorial function $f^{(n)}$. The specifications for such a box will be represented by a diffeomorphism $F^{(n)}$ from M^n to M^n. (When one is dealing with manifolds instead of intervals of the real line, a *diffeomorphism* is the appropriate generalization of a bicontinuous function).

It must be stressed that Goal 2.1 does not just ask for an arbitrary diffeomorphic extension of the given function $f^{(n)}$ to an arbitrary manifold. Rather, the extension must be *componentwise*. In other words, besides being a *superset* of B^n, the manifold must also be of the form M^n, i.e., possess the same *Cartesian product structure* as B^n; moreover, the extension itself must maintain the variables *separated*, i.e., each component of the extension must be an extension of the corresponding component of the given function. In physical terms, each binary variable must be encoded in a separate "channel," so that in interconnecting several boxes of this kind each variable may be routed independently of the others. Figure 2.2 illustrates the case of an extension that is not componentwise. This box too "computes" a combinatorial function, but it is hard to see how the components of the input n-tuple could be made to come from different boxes, and those of the output n-tuple go to different boxes, without using complex encoders and decoders for which the problem of physical realizability would arise afresh.

speak of *output variables* (or *output components*) of the function. In ordinary function composition, an output variable of one function may be substituted for *any number* of input variables of other functions, i.e., "fan-out" is allowed, as indicated in Figure 3.1a. In what follows, we shall use a more restricted form of composition, called *one-to-one* composition, where any substitution of output variables for input variables must be one-to-one, as indicated in Figure 3.1*b*. If the output variable and the input variable involved in every such substitution range over identical sets, then one-to-one composition always yields invertible functions when applied to invertible functions.

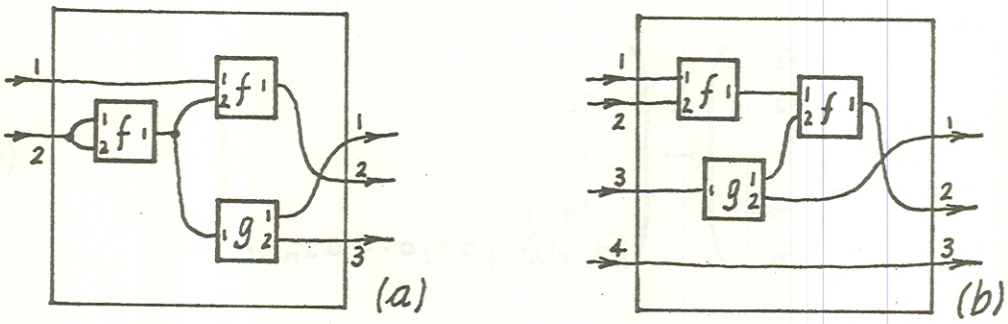

FIG. 3.1 *(a) Examples of ordinary composition and (b) one-to-one composition of functions.*

A re-indexing of input or output variables is a special case of one-to-one composition. One-to-one composition is conveniently handled by means of an algebraic notation formally analogous to that of tensor calculus[4]. From a physical viewpoint, the one-to-one constraint reflects the fact that signal fan-out requires a source of energy other than that carried by the signal itself.

Let ϕ be a binary relation from $S \times U_1 \times \cdots \times U_n$ to $S' \times U'_1 \cdots \times U'_{n'}$, where the sets $U_1, \ldots, U_n, U'_1, \ldots, U'_{n'}$ are *singletons*. For convenience, the one element of any of these singletons will be denoted by o. The variables associated with these singletons will be called *dummy*. A relation $\overline{\phi}$ from $S \times U_{i_1} \times \cdots \times U_{i_p}$ to $S' \times U'_{j_1} \times \cdots \times U'_{j_{p'}}$, where $1 \leq i_1 < \cdots < i_p \leq n$ and $1 < j_1 \leq \cdots < j_{p'} \leq n'$, is said to be *obtained from* ϕ *by deletion of dummy variables* if

$$\langle s, \overbrace{o, \ldots, o}^{n} \rangle \phi \langle s', \overbrace{o, \ldots, o}^{n'} \rangle \Leftrightarrow \langle s, \overbrace{o, \ldots, o}^{p} \rangle \overline{\phi} \langle s', \overbrace{o, \ldots, o}^{p'} \rangle,$$

that is, if the two relations coincide when the trailing o's which accompany each tuple are disregarded.

atomic permutations, i.e., of permutations that exchange two n-tuples which differ in only one component. Observe that $\theta^{(n)}$ is the atomic permutation which exchanges $\langle 1, 1, \ldots, 1, 0\rangle$ with $\langle 1, 1, \ldots, 1, 1\rangle$. By reordering the components of $\theta^{(n)}$ and applying $\theta^{(1)}$ to selected components one obtains the family of all *atomic* permutations. Note that all the operations used above are forms of one-to-one composition. It remains to prove (*b*); this is done in the following way.

The n-tuples $a_1, a_2, \ldots, a_i$ are said to form a *Gray-code path* if two adjacent n-tuples differ by an atomic permutation. It is easy to verify that by means of sequence of atomic permutations the element at the beginning of the path can be moved to the end position, leaving the remainder of the path unchanged. By repeating such a move the first and last elements can be exchanged. The proof is completed by observing that any two n-tuples can be joined by a Gray-code path.∎

LEMMA 4.2 *Consider the 1-manifold* $\mathring{\mathbf{R}}$ *obtained by identifying all points of the real line* $\mathbf{R}$ *that differ by a multiple of* 2π ($\mathring{\mathbf{R}}$ *can be thought of as the real circle), and let the points* $\mathbf{0}$ *and* $\mathbf{1}$ *of* $\mathbf{B}$ *coincide with, respectively,* 0 *and* π *of* $\mathring{\mathbf{R}}$. *Then there exists a diffeomorphism from* $\mathring{\mathbf{R}}^n$ *to* $\mathring{\mathbf{R}}^n$ *whose restriction to* $\langle \mathbf{B}^n, \mathbf{B}^n\rangle$ *coincides with* $\theta^{(n)}$.

Proof. Consider $\mathring{\mathbf{R}}$ with addition ("$\oplus$") and additive inverse ("$\ominus$") induced from those on $\mathbf{R}$, and multiplication ("$\circ$") defined as follows

$$x \circ y = \pi \frac{1 - \cos x}{2} \cdot \frac{1 - \cos y}{2}.$$

$\mathring{\mathbf{R}}$ satisfies all the axioms for a ring except distributivity. Let $\Theta^{(n)}: \mathring{\mathbf{R}}^n \to \mathring{\mathbf{R}}^n$ be defined by

$$\Theta^{(n)}: \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ \ominus x_n \oplus x_1 \circ x_2 \circ \cdots \circ x_{n-1} \end{pmatrix}. \tag{4.2}$$

Observe that when the operators defined on $\mathring{\mathbf{R}}$ are restricted to $\mathbf{B} \subseteq \mathring{\mathbf{R}}$ the Boolean-ring structure for $\mathbf{B}$ is recovered; thus, the restriction of $\Theta^{(n)}$ to $\langle \mathbf{B}^n, \mathbf{B}^n\rangle$ coincides with $\theta^{(n)}$. Moreover, $\Theta^{(n)}$ is infinitely differentiable by construction and coincides with its inverse; thus, $\Theta^{(n)}$ is a diffeomorphism.∎

As an immediate consequence of Lemmas 4.1 and 4.2, one obtains the following theorem (cf. GOAL 2.1).

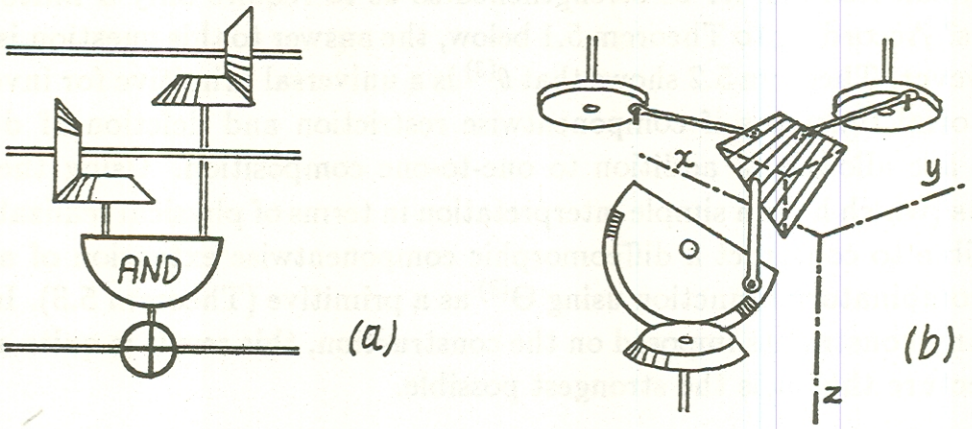

FIG. 5.2 *(a) Realization of* $\Theta^{(3)}$. *(b) Details of the* AND *mechanism.*

In general, $\Theta^{(n)}$ will be realized according to the scheme of Figure 5.3, which is convenient also for representing the corresponding discrete function $\theta^{(n)}$. The $(n-1)$-dimensional cam required for the $(n-1)$-input AND mechanism can be realized by cascading a suitable number of two-dimensional cams. Note that, although our construction makes use of rotary-to-linear conversion, which by itself is not an invertible operation and in general may introduce "dead points" in a mechanism, the resulting overall mechanism is indeed reversible.

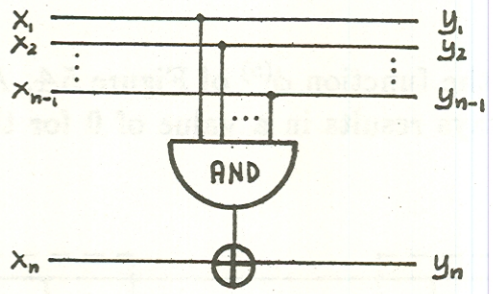

FIG. 5.3 *Schematic representation of* $\Theta^{(n)}$ *or* $\theta^{(n)}$

Returning to our mathematical exposition, let us observe that Lemma 4.1 supplies a set of invertible primitives for constructing—via one-to-one composition—any invertible combinatorial function. However, this set is unbounded, in the sense that θ's of ever larger order may be needed as the order of the given invertible function increases. It is well known that any combinatorial function can be synthesized by ordinary function composition starting from a single computing primitive such as the two-input NAND function. In analogy

From the restriction of $\phi^{(5)}$ to $\langle B^3 \times \{0\}, B^3 \times \{0\}\rangle$ one obtains $\theta^{(4)}$ by deletion of the dummy variables x_5 and y_5. In a similar way, all $\theta^{(n)}$ $(n > 3)$ can be obtained. $\theta^{(2)}$ and $\theta^{(1)}$ are obtained directly from $\theta^{(3)}$ when the first and, respectively, the first two components are restricted to the value 1 and the resulting dummy variables are deleted. If one-to-one composition is applied before deletion, it is easy to verify that the number of deletions (i.e., the number of constant inputs) required for the construction of any invertible combinatorial function of order n does not exceed $2n - 3$.□

THEOREM 5.3 *For any invertible combinatorial function $f^{(n)}$, a diffeomorphic componentwise extension $F^{(n)}$ can be obtained by one-to-one composition, componentwise restriction, and deletion of dummy variables from $\Theta^{(3)}$.*

Proof. The proof parallels that of Theorem 5.2.□

6. Conclusions

Computing is based on the evaluation of functions that are *discrete* and *many-to-one*. On the other hand, the mechanisms offered by a schematization of physics such as classical mechanics are based on functions that are *continuous* and *one-to-one*. We have explicitly bridged the gap between these two conceptions.

Appendix

The question of whether there exist *reversible* systems (i.e., systems characterized by an invertible transition function) which possess universal computing capabilities has been considered by many authors (see [5] for references). The answer to this question is positive. For our purposes, it will be sufficient to recall the following basic proposition[3]:

For every combinatorial function $\phi: B^m \to B^n$ there exists an invertible combinatorial function $f^{(m+r)}: B^{m+r} \to B^{m+r}$ (with $r \leq n$) such that

$$\bigwedge_{1 \leq i \leq n} f_i^{(m+r)}\langle x_1, \ldots, x_m, \overbrace{0, \ldots, 0}^{r}\rangle = \phi_i\langle x_1, \ldots, x_m\rangle.$$

Informally, the required function ϕ is obtained from $f^{(m+r)}$ by assigning constant values to the r additional input components and ignoring the "random" values