[Number in brackets refer to the transparencies]

[1] Stony Brook, 29 May 2003

STRUCTURAL VS FUNCTIONAL INVERTIBILITY IN COMPUTATION

Tommaso Toffoli (with P Pierini and P Mentrasti)

---

[2] Handbill manifesto:

== A new inversion scheme, or how to turn invertible second-order cellular automata into lattice gases.

== Mechanisms and pathways of \emph{causality} in distributed reversible systems. Specifically,

== Tradeoffs between simplicity of the primitives and coarsenes of the computational crystal's "pitch"---and thus range of the forces.

SECTION---

[3] To undo a reversible process, intuitively all one has to do is perform the inverse operations in the reverse order. This also applies to the case where the order of applicatiòn of the primitives is a _partial_ order, i.e., when we deal with distributed, concurrent computation.

SECTION---

-- Computation is a discipline of functional composition with using prespecified interaction and composition primitives.

A _transformation_ of a set X is a mapping from X to X itself.
An invertible transformation iis also called a _permutation_.

-- A main business of invertible computation is to express complicated invertible transformations of a set, thought of as a Cartesian product of component sets, as compositions of simple invertible transformations acting only on a few components at a time. Similarly, a main business of quantum computation is to express complicated unitary transformations as compositions of simple unitary transformations acting only on a few components at a time.

[4] -- Conditional permutations as convenient computational primitives.
Examples: The bicontinuous ("cranky") gate of Toffoli 1982 and the correponding digital gate. The Fredkin gate. The C-NOT gate.
Definition: 1. Consider two finite sets A, B. A _conditional permutation_ of A by B is a collection F={F_i} of permutations of B indexed by i in A.

[5] -- Decomposability of a permutation of AxB into a finite number of conditional permutations.
Lemma. Let f be a transformation of AxB. Iff f is invertible, then f can be written as a composition of a finite number of conditional permutations, F1 G1 F2 G2 ..., where permutations by A alternate with permutations by B

SECTION---

-- Composition schemes uniform in space and time: PDE, cellular automata, lattice gases.

[6] -- Numerical analysis' old-fashioned, anthropomorphic style to describe a computation. Local functional description.

[7] -- Gloabal functional description of a recurrence scheme.

[9] -- Possibly unnecessary sources of dissipation. Fan-ins are not one-to-one, and fan-outs are not onto. We have to pump free energy into the fanout nodes, and drain heat from the fanin nodes.

[10] -- Consider now the case of a globally invertible rule. This is functionally invertible; can it always be turned into a structurally invertible rule

-- Question: If the functional description is local, uniform, and globally _invertible_, can we turn this "numerical analyst's" description into a "physical engineer's" description, i.e, a similarly local and uniform _structural_ description given in terms of invertible primitives and composition rules? And at what cost?

SECTION---

[11] -- Light cone; verification of a proposed local inverse.
Lemma. Given a cellular automaton F with local rule f and a local rule g for a proposed inverse cellular automaton G, there is an effective procedure for telling whether G is indeed the inverse of F.
Example slide. Light cone of f and g.

SECTION---

[12] -- Question: Given the local rule f of a cellular automaton F, is this cellular automaton invertible?
Remark: Local rules can be effectively enumerated. Then we can try them one by one. When we get to a good one we will know.

-- In 1972, Amoroso and Patt proved that this question is decidable---for one dimension; conjectured its decidability in higher dimensions.

-- In 1990, Kari proved that this question is in general undecidable in more than one dimension.

-- Where is the problem? Kari's theorem shows that the light cone of the inverse rule may be of a different size than the direct rule, and in fact there is no effective upper bound. At no point in the enumeration we may ever be for sure that we are not longer going to find an inverse.

-- Example of different-size light cone between direct and inverse rule.

[15,16] -- To give the flavor of the difficulty: surjective rule with "infinite speed of propagation in the backward time direction.

SECTION---

[13] -- Second best kind of knowledge:
Conjecture (Toffoli+Margolus 1990): If a cellular automaton is invertible, then it admits of a structurally invertible implementation.
Theorem (Durand-Lose 2000): Above conjecture proved.

-- So we know that if it is globally invertible and is described by a local rule, it can be described by a uniform composition of finite invertible functions---in other words, it can be engineered.

-- A useful task is to find interesting classes of functionally invertible CA that can effectively be described in structurally invertible terms.

SECTION--

[17] -- We give an effective construction in the case of invertible CA having a special structure, ie, second-order (as defined in Toffoli+Margolus (1990).

-- Example: Pomeau 1984 paper on invariants for a class of cellular automata invented by Fredkin (examples Q2R, Vichniac 1984, which turned out to be a microcanonical Ising spin system implementation; a related one-dimensional system, SCARVES invented by Bennett ca 1986) [8].
Pomeau's used the traditional, "numerical analyst's" presentation of these CA, and had to spend two-and-a-half pages proving something that would have been almost obvious if presented in a structurally invertible format.

SECTION--

-- Conjugate-variable vs second-order schemes.
[17] Example: Second-order recurrence relation.
[18] Example: Lagrangian vs Hamiltonian formulation of dynamics.

q

SECTION--

[19] -- The simplest nontrivial case of asecond-order scheme..

[20,21,22] -- The promised effective construction.
Idea: why don't we have a SINGLE signal be seen (but not touched) by all the addresses (like in a circulation list).
Problem: Infinite regress.
Solution: Staggering the distribution [21], at the cost of making the regularity coarser [22; cf 13]

[24] -- Similarly in two dimensions. Since we have four neighbors, we'll have to make use of four "stages" or phases, labeled 0, 1, 2, 3.

(1)

STONY BROOK
29 May 2003

STRUCTURAL vs FUNCTIONAL INVERTIBILITY IN COMPUTATION

TOM TOFFOLI
BOSTON UNIVERSITY
tt@bu.edu

with

P. MENTRASTI
S. CAPOBIANCO
University of Rome (I)

(2) # HANDBILL

♠ A NEW INVERSION SCHEME

OR HOW TO TURN INVERTIBLE 2ND ORDER CELLULAR AUTOMATA INTO LATTICE GASES

♦ MECHANISMS & PATHWAYS OF CAUSALITY

IN DISTRIBUTED, REVERSIBLE COMPUTER SYSTEMS

♣ TRADEOFFS between

SIMPLICITY OF THE PRIMITIVES AND COARSENESS OF THE COMPUTATIONAL CRYSTAL'S PITCH (AND THUS RANGE OF THE FORCES)

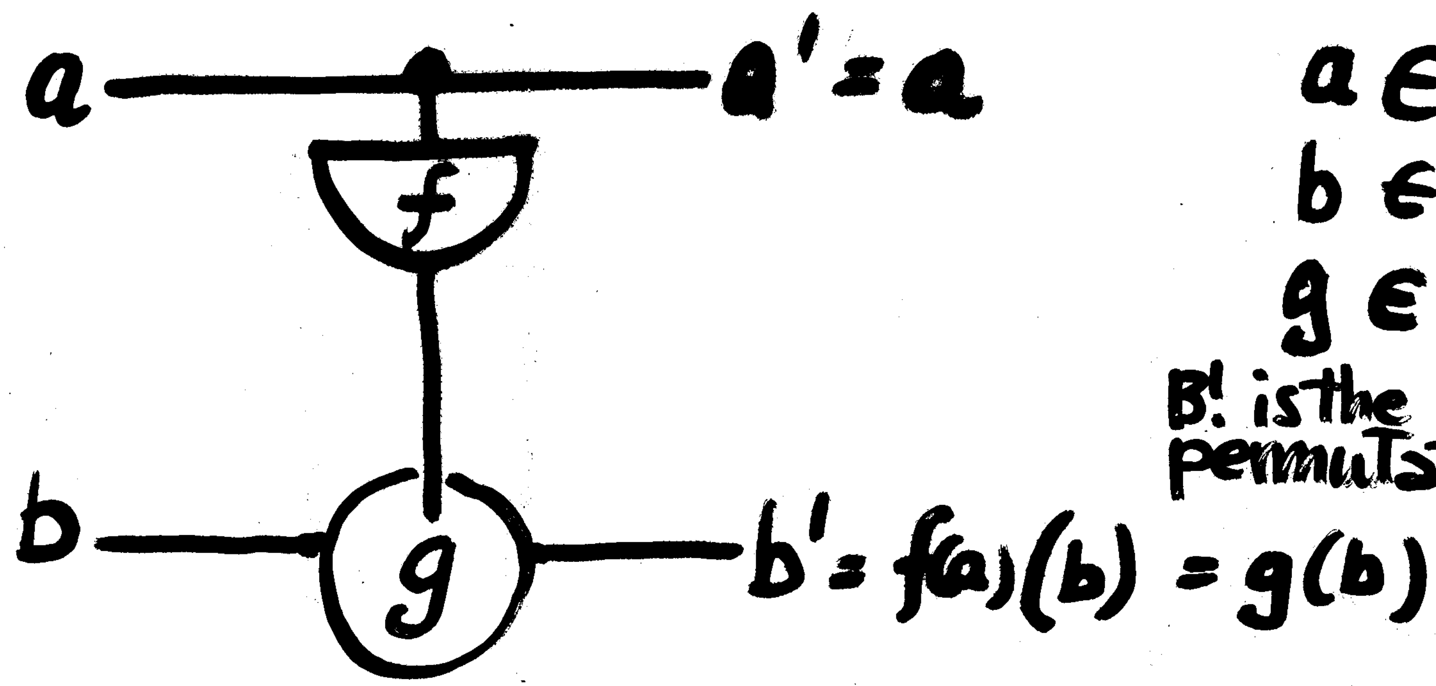
TODAY ONLY!!!

TO UNDO A REVERSIBLE PROCESS, PERFORM THE <u>INVERSE</u> OPERATIONS IN THE REVERSE ORDER

(This also works when this "order" is a <u>partial</u> order, as in distributed concurrent computation)

BUT WHAT IF THE <u>DIRECT</u> OPERATIONS DON'T LOOK INVERTIBLE?

CONDITIONAL PERMUTER ④
OF B BY A



$a \in A$

$b \in B$

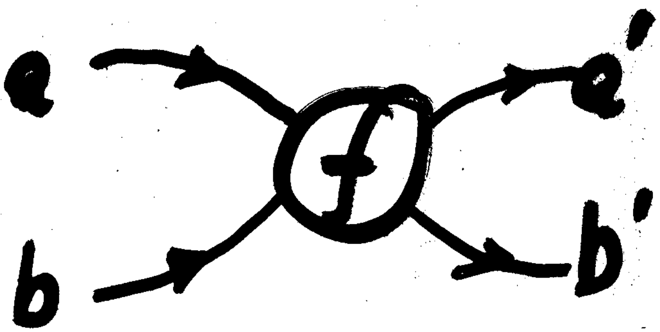
$g \in B!$

$B!$ is the group of permutations of B

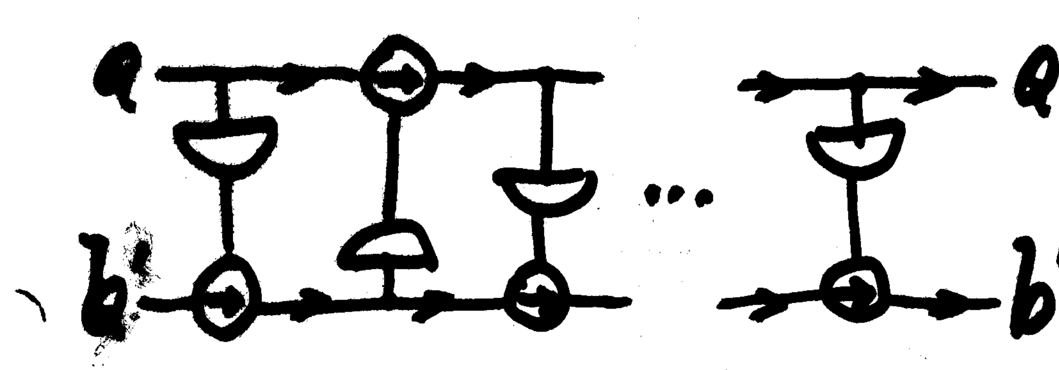
$$f : A \to B!$$

THEOREM

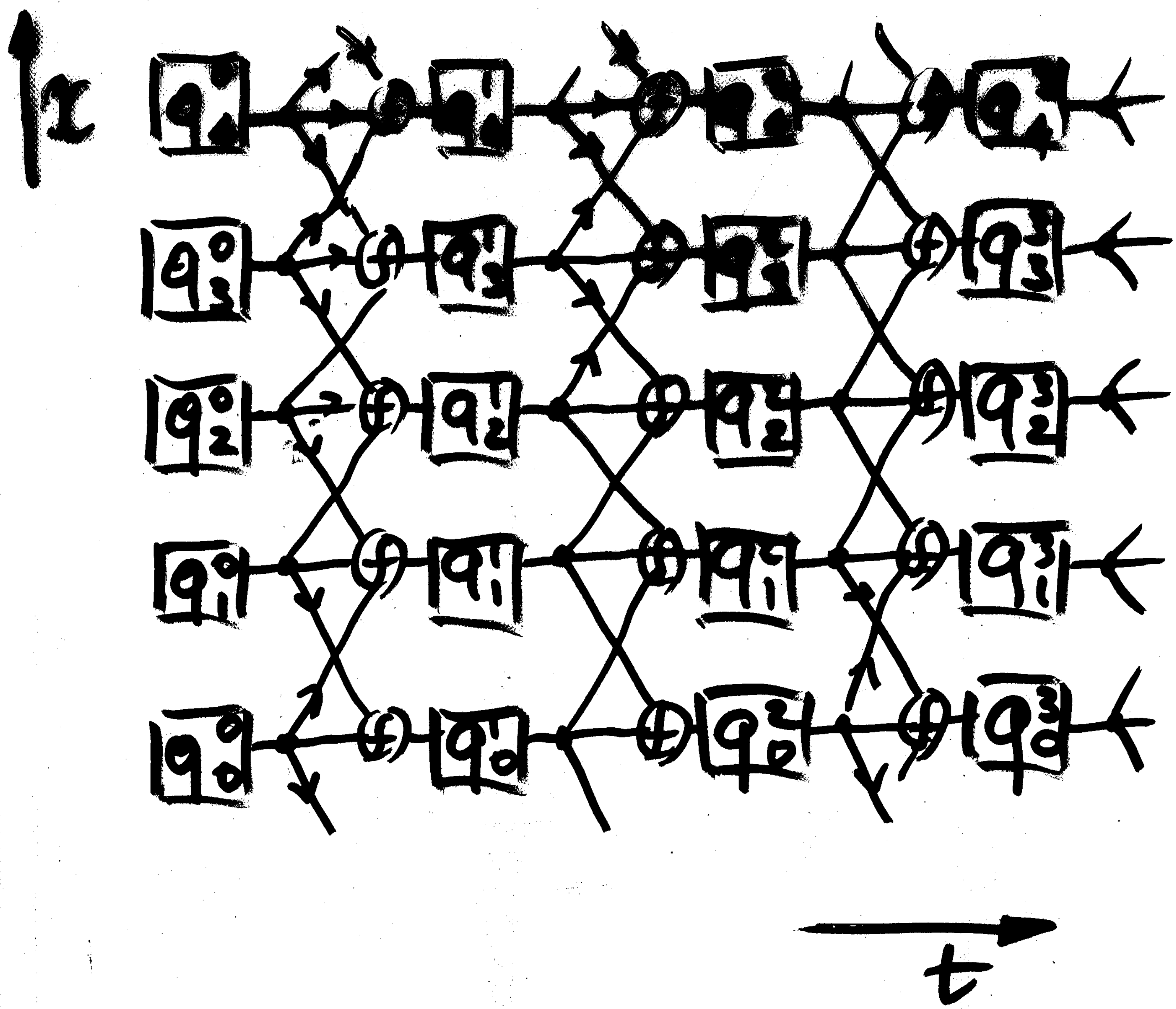
A transformation of the set $A \times B$

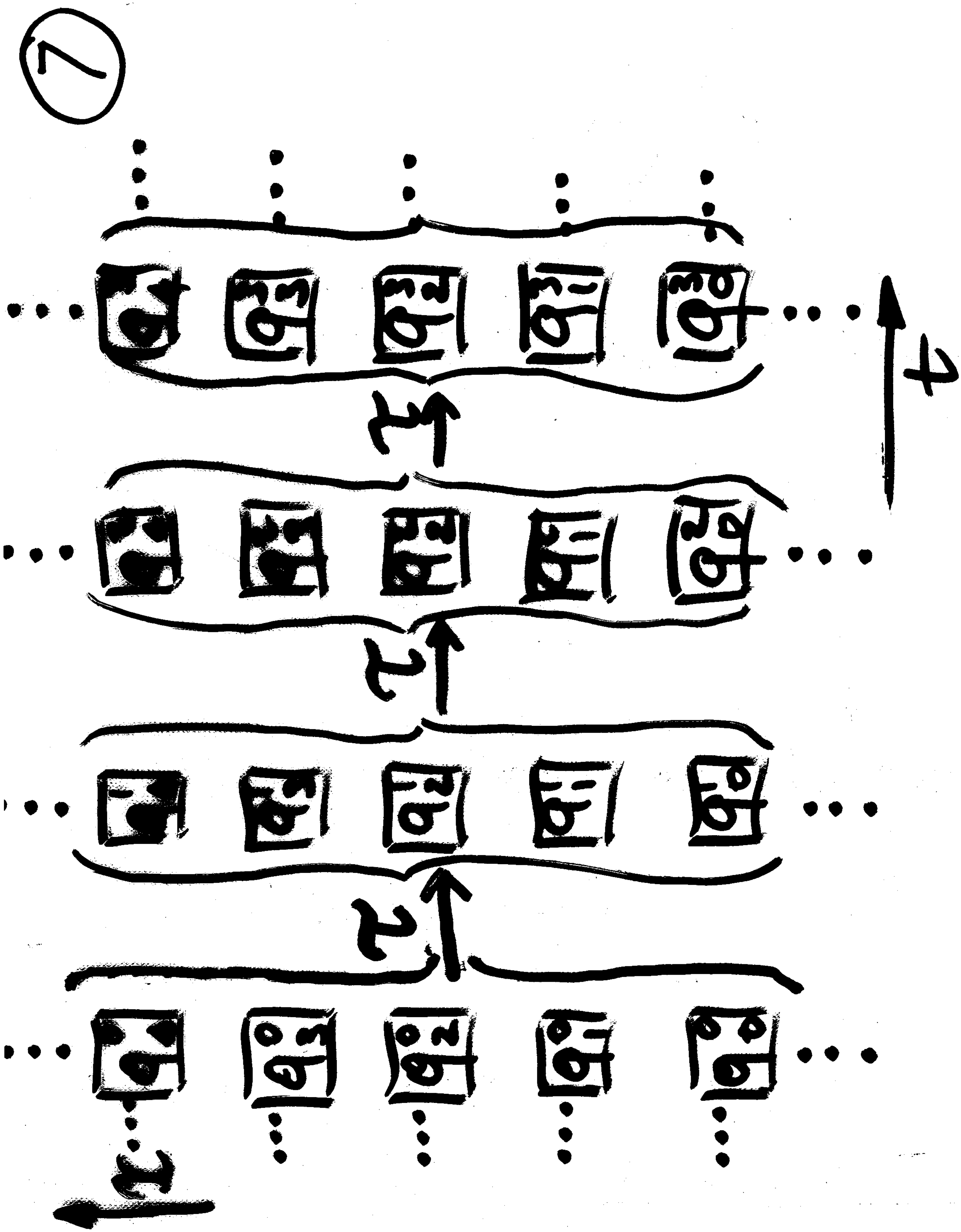


can be decomposed into a sequence of conditional perm.



IFF IT IS INVERTIBLE


x
t



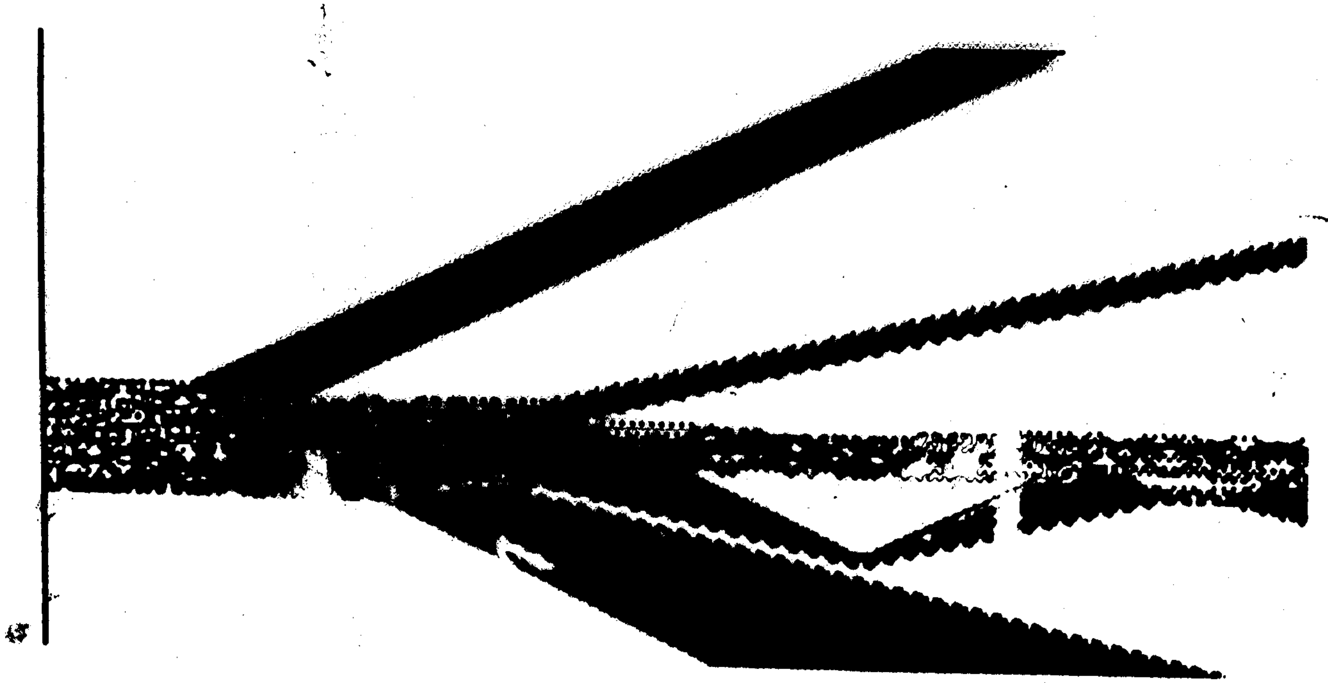
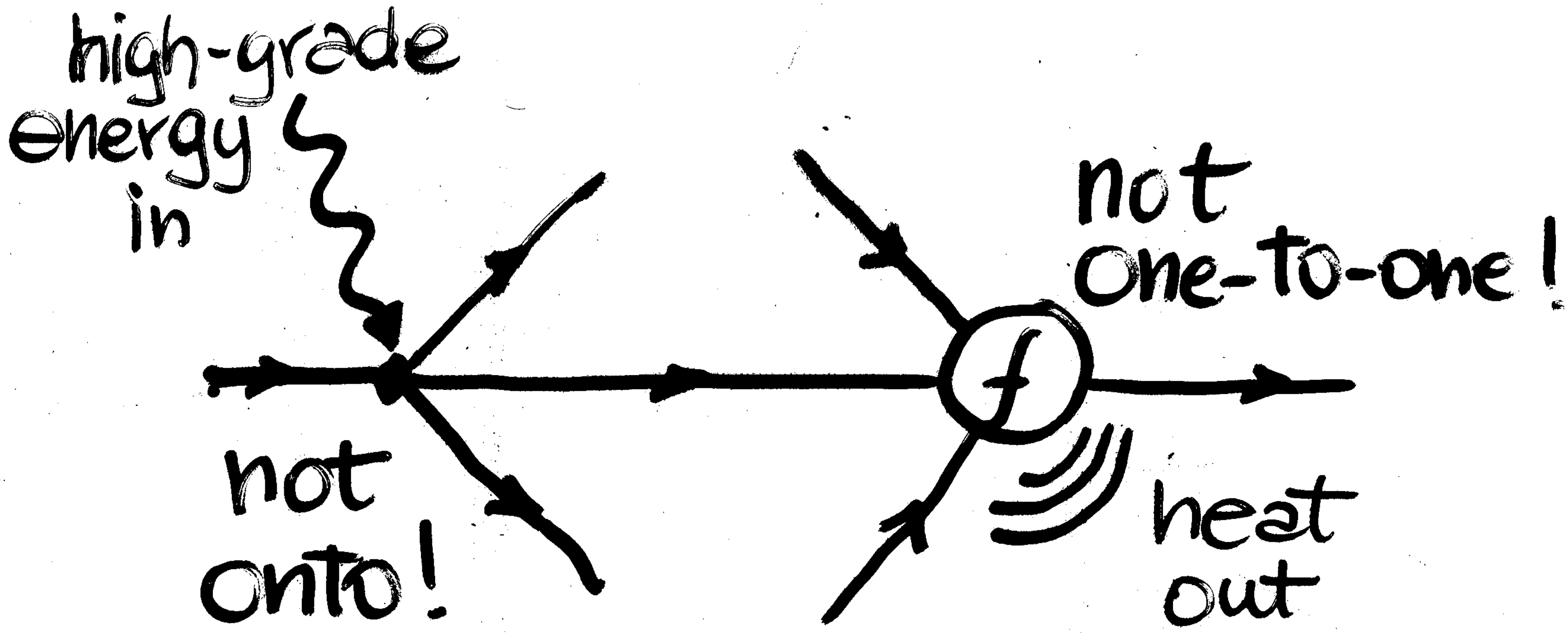
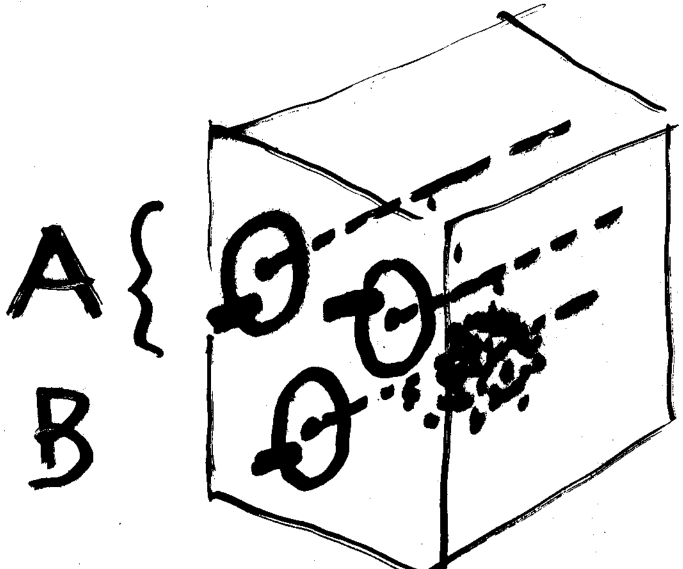


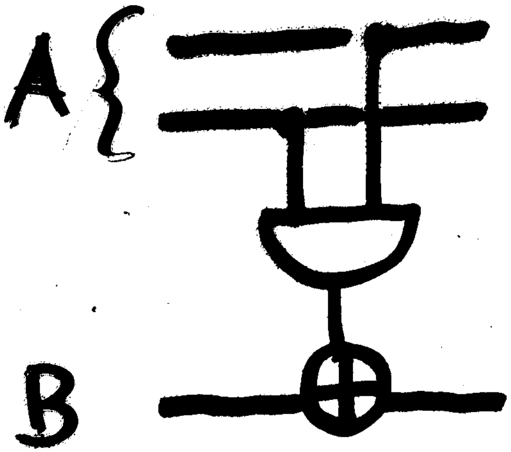
Figure 2: A spacetime history from the SCARVES rule. Time progresses righwards.

9

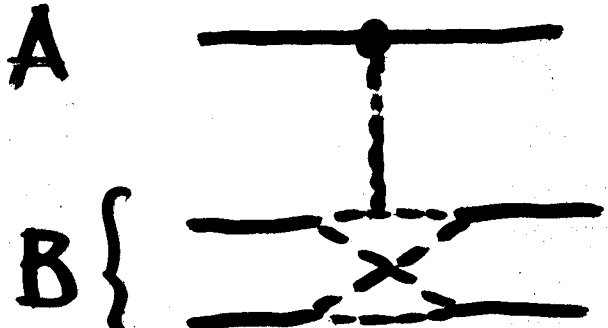




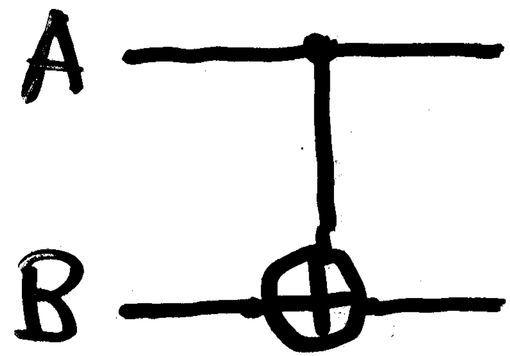
ORIGINAL "TOFFOLI" GATE
(CRANKS)



STYLIZED VERSION (DIGITAL OR ANALOG)

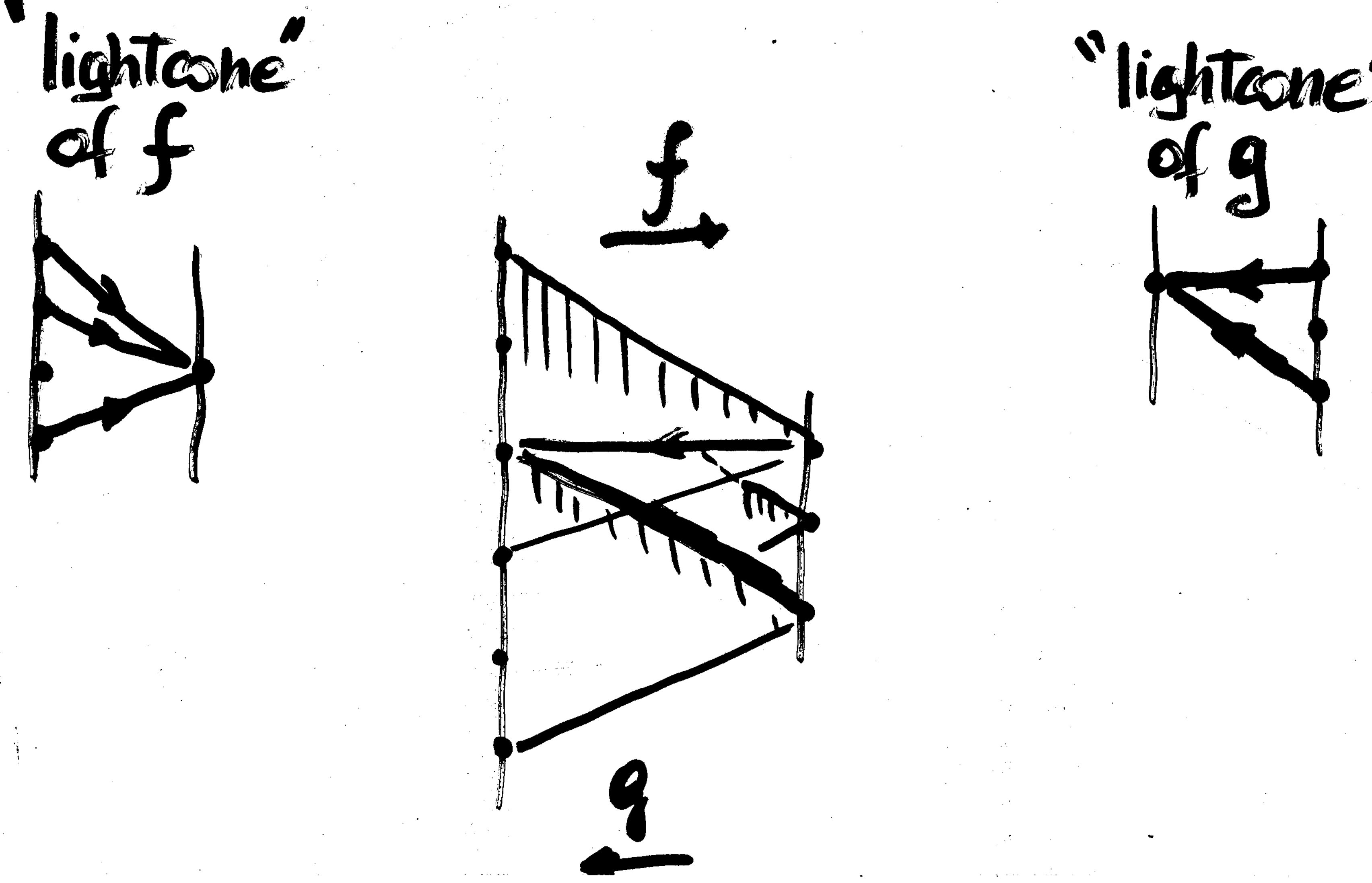


FREDKIN GATE



C-NOT GATE

LEMMA: We know how to tell whether global maps F, G generated by local maps f, g are inverses of one another



– Given the local rule f of a CA F, is this CA invertible?

(Remark: Local rules can be effectively enumerated. Then we can try them one by one. When we get a good one we will know the answer!?) →

- In 1972, Amoroso & Patt proved that this question is decidable — for one dimension. Conjectured its decidability in more dimensions
- In 1990, Kari proved that this question is in general undecidable in more than one dimension.

(13) Second-best kind of knowledge:

- In 1990, Toffoli + Margolus conjectured "If a CA is invertible, then it admits of a <u>structurally invertible</u> implement.

- Above conjecture proved (2000) by Durand-Lose

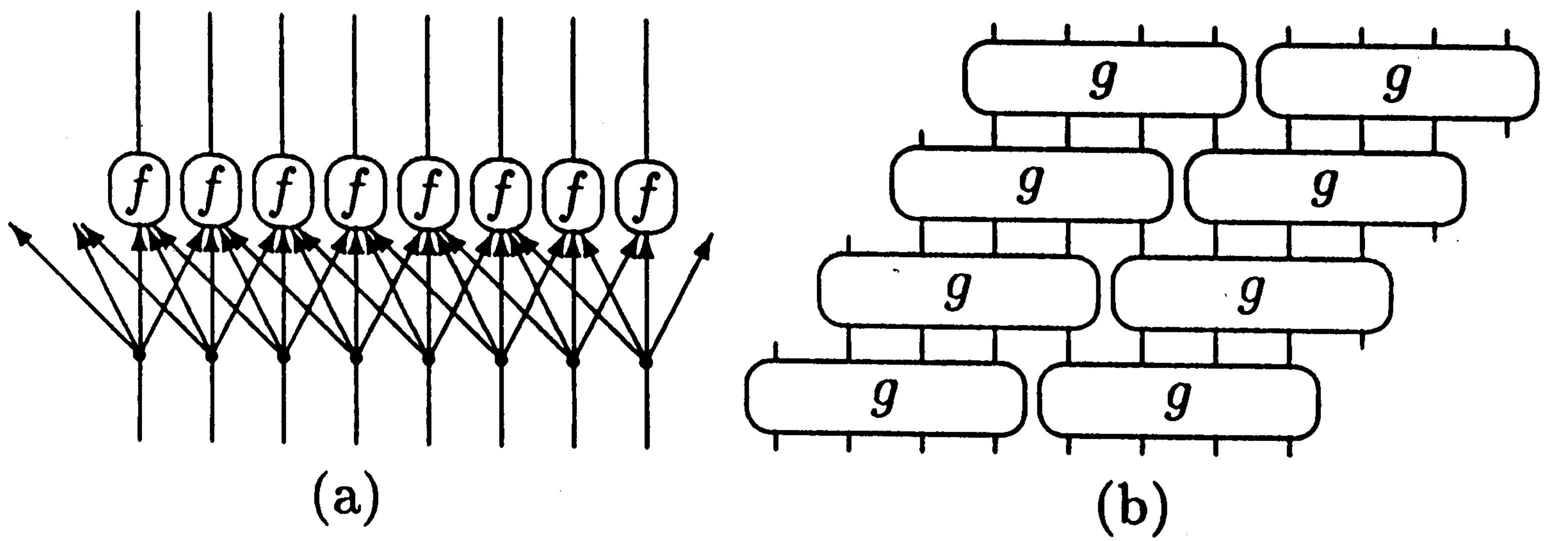
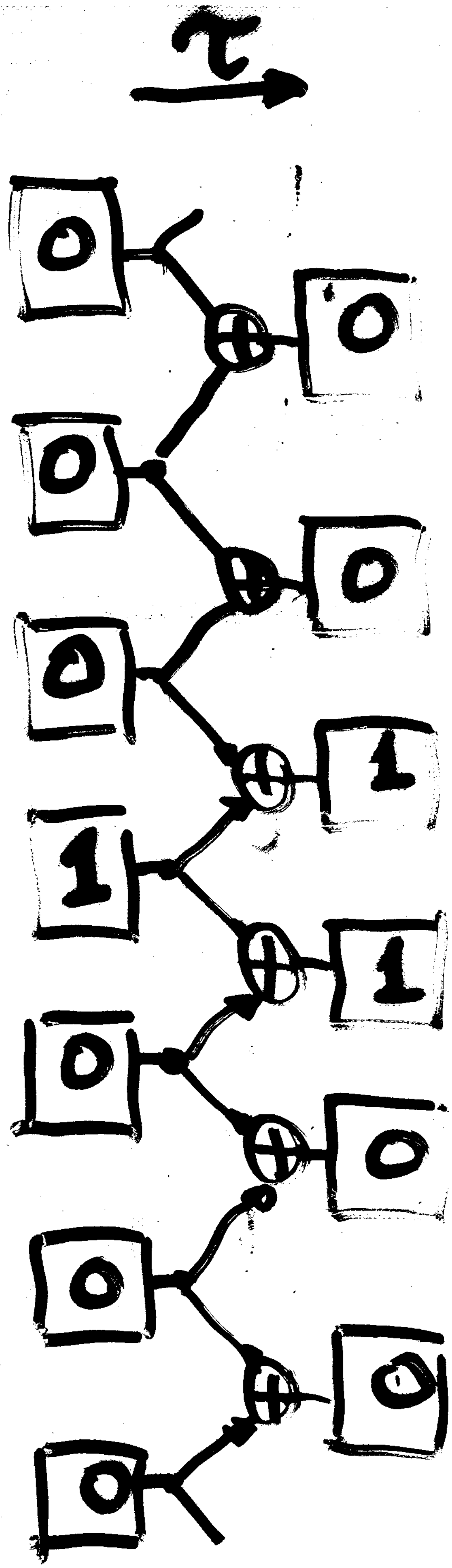
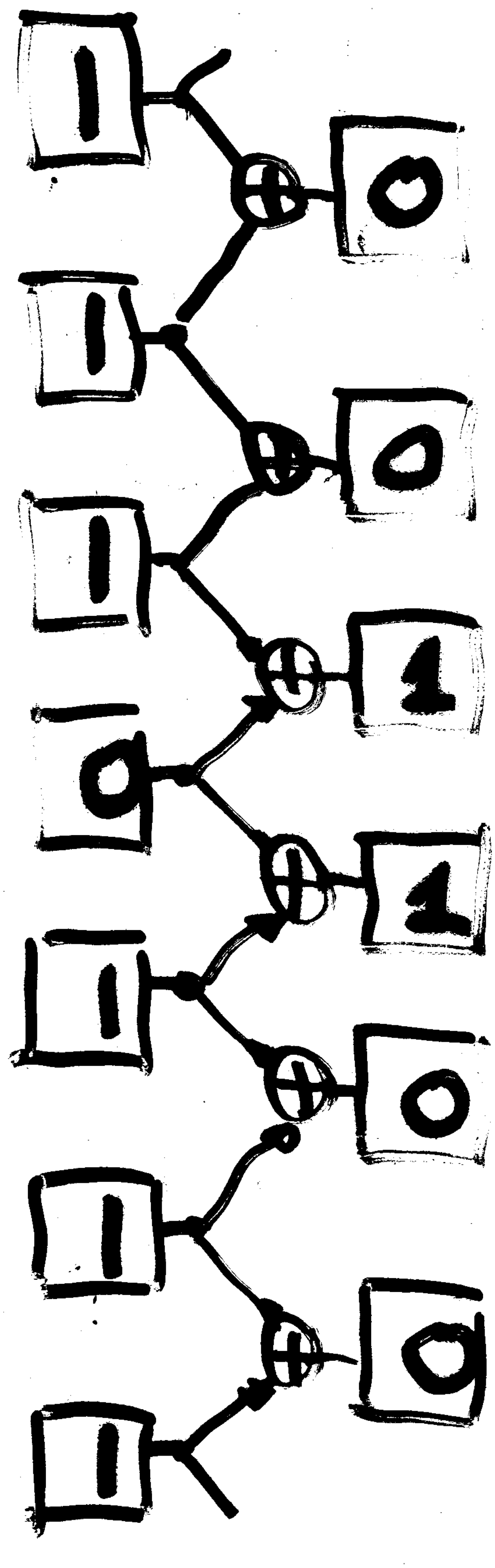


Figure 15: (a) Combinational network representation of the ICA defined by table (9). (b) The same ICA, in a version that exhibits structural invertibility. The g nodes are all invertible Boolean functions; one of the four outputs yields the same value of f, while the other three just pass through the corresponding inputs.

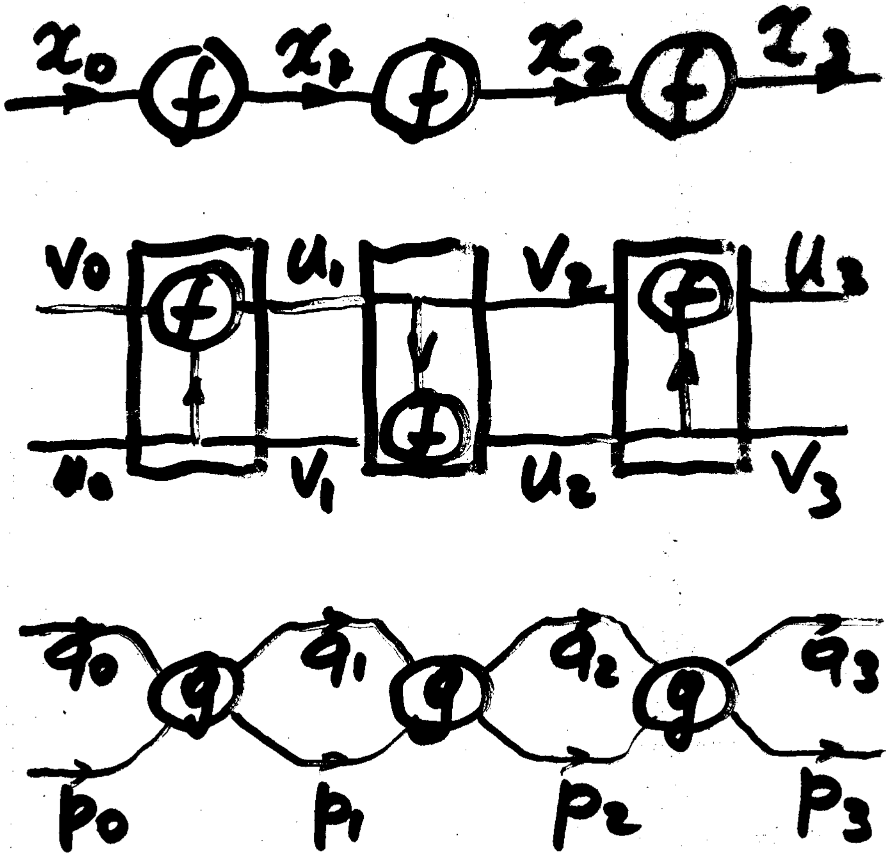

τ

τ →

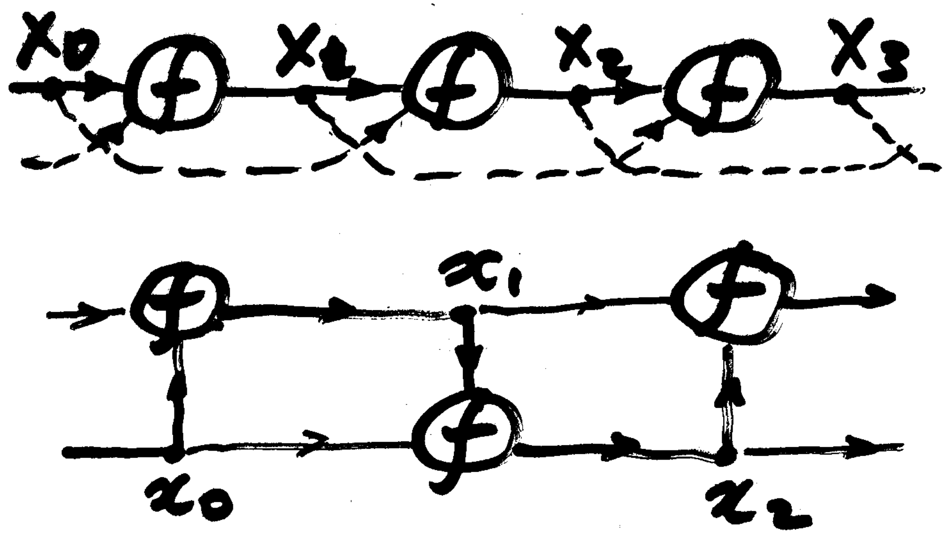


DYNAMICS: FIRST-ORDER vs SECOND-ORDER

$$x_{t+1} = f(x_t)$$



$$x_{t+1} = f(x_t, x_{t-1})$$



DYNAMICS

LAGRANGIAN VS HAMILTONIAN

$$\frac{\partial L(q,\dot{q})}{\partial q} = \frac{d}{dt}\frac{\partial L(q,\dot{q})}{\partial \dot{q}}$$

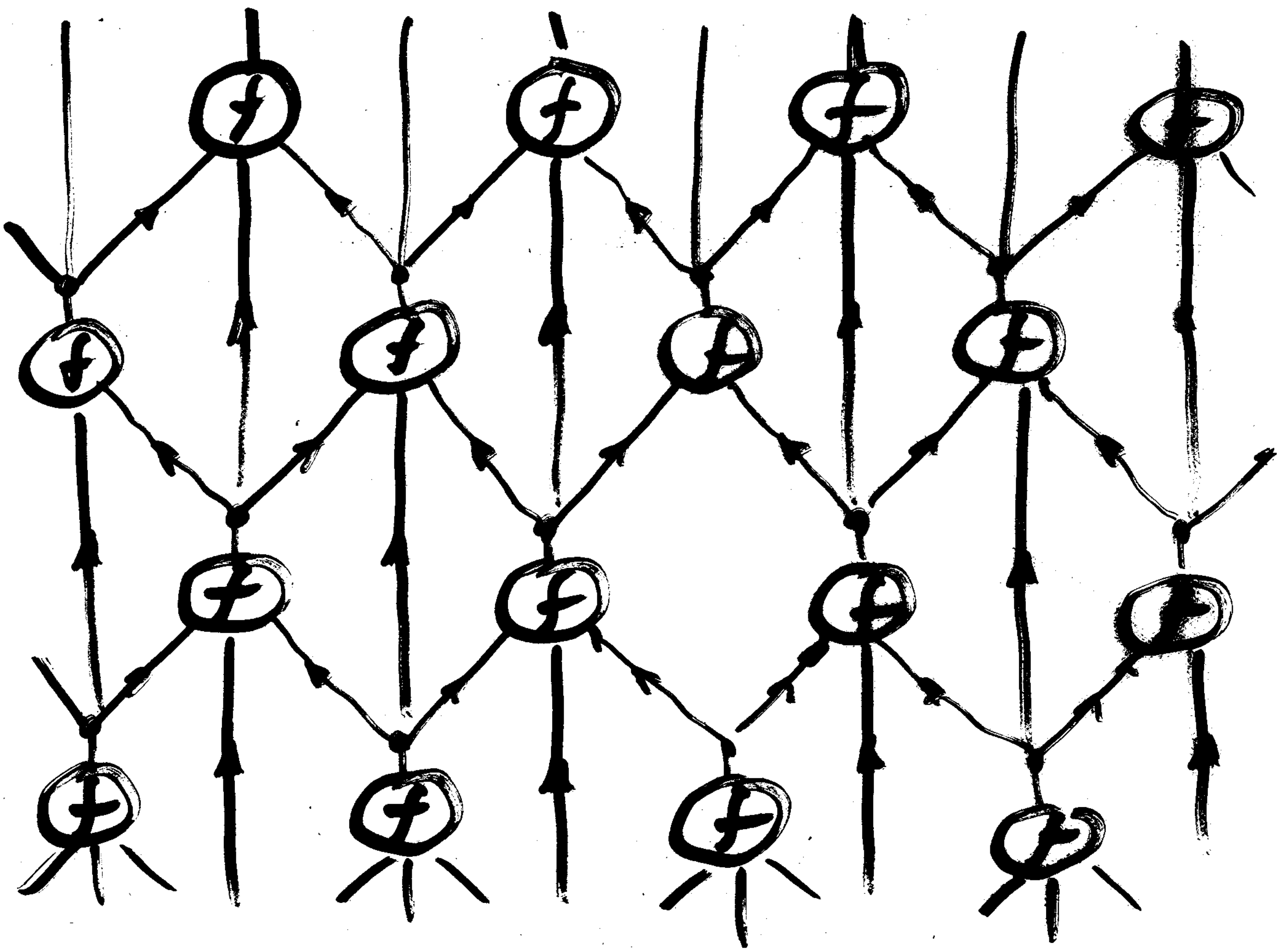
$$\ddot{q} = \mathcal{F}(q,\dot{q})$$

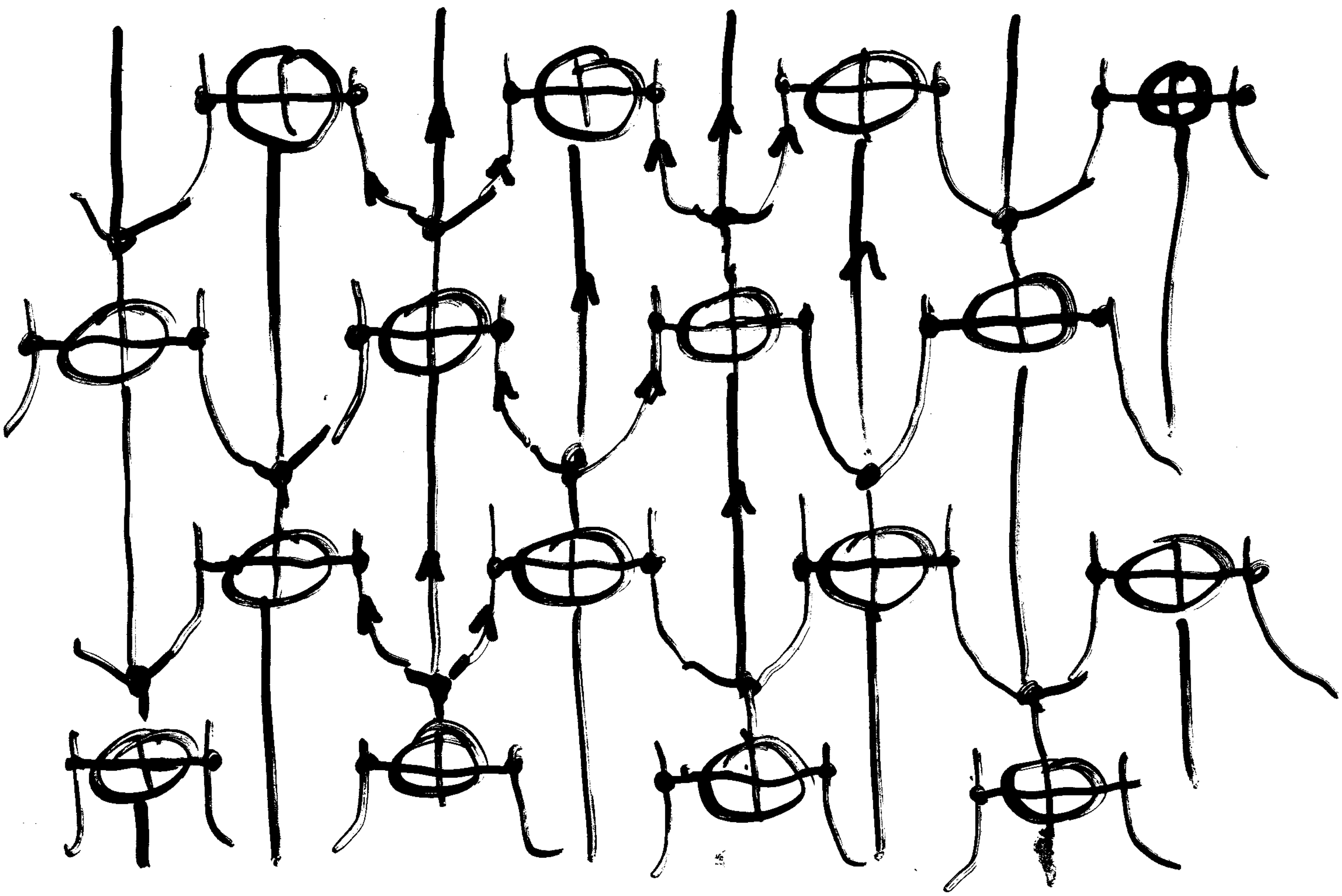
$$\begin{cases} \frac{dq}{dt} = \dot{q} \\ \frac{d\dot{q}}{dt} = \mathcal{F}(q,\dot{q}) \end{cases}$$

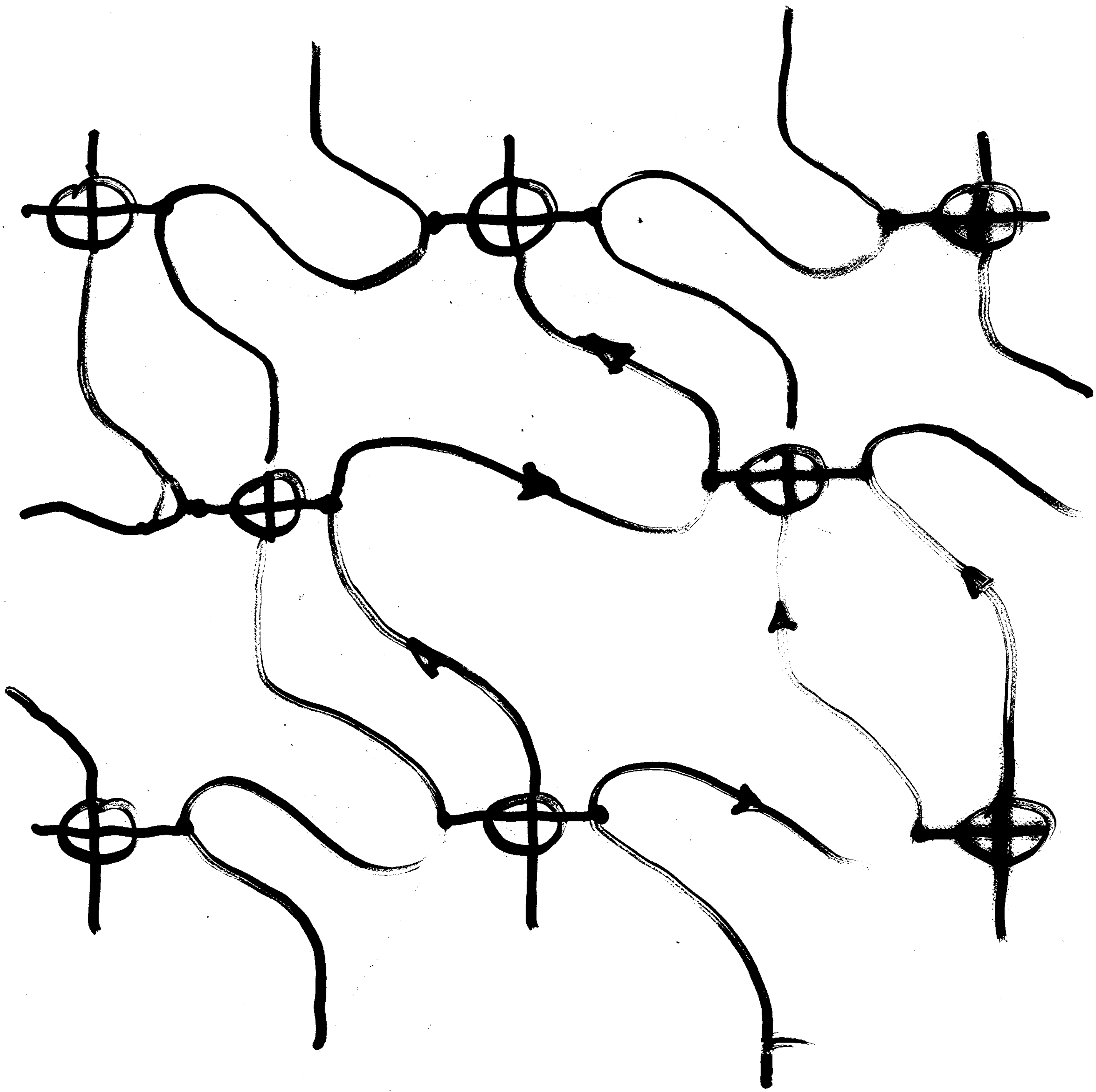
$L \rightarrow H$

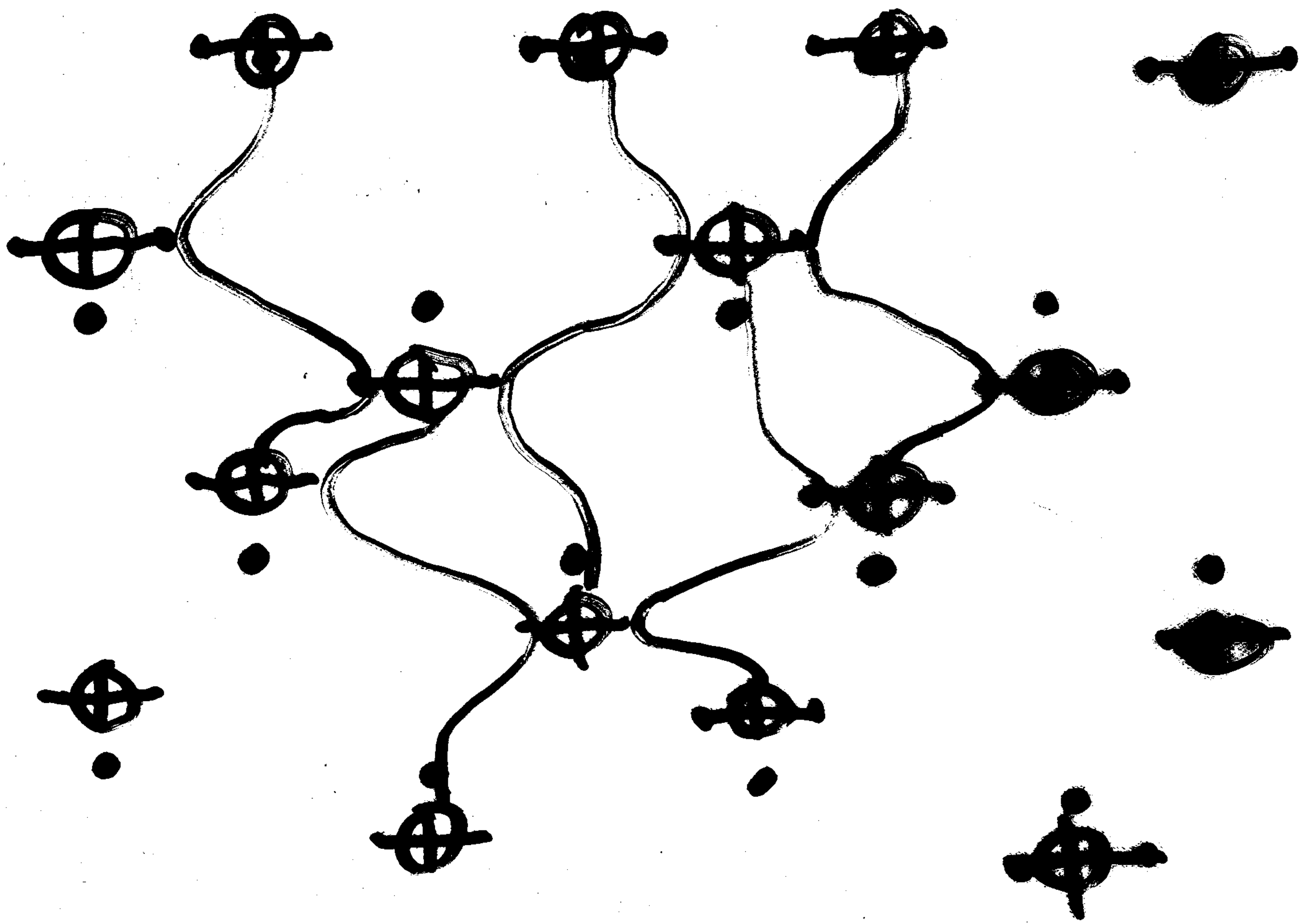
via Legendre transform

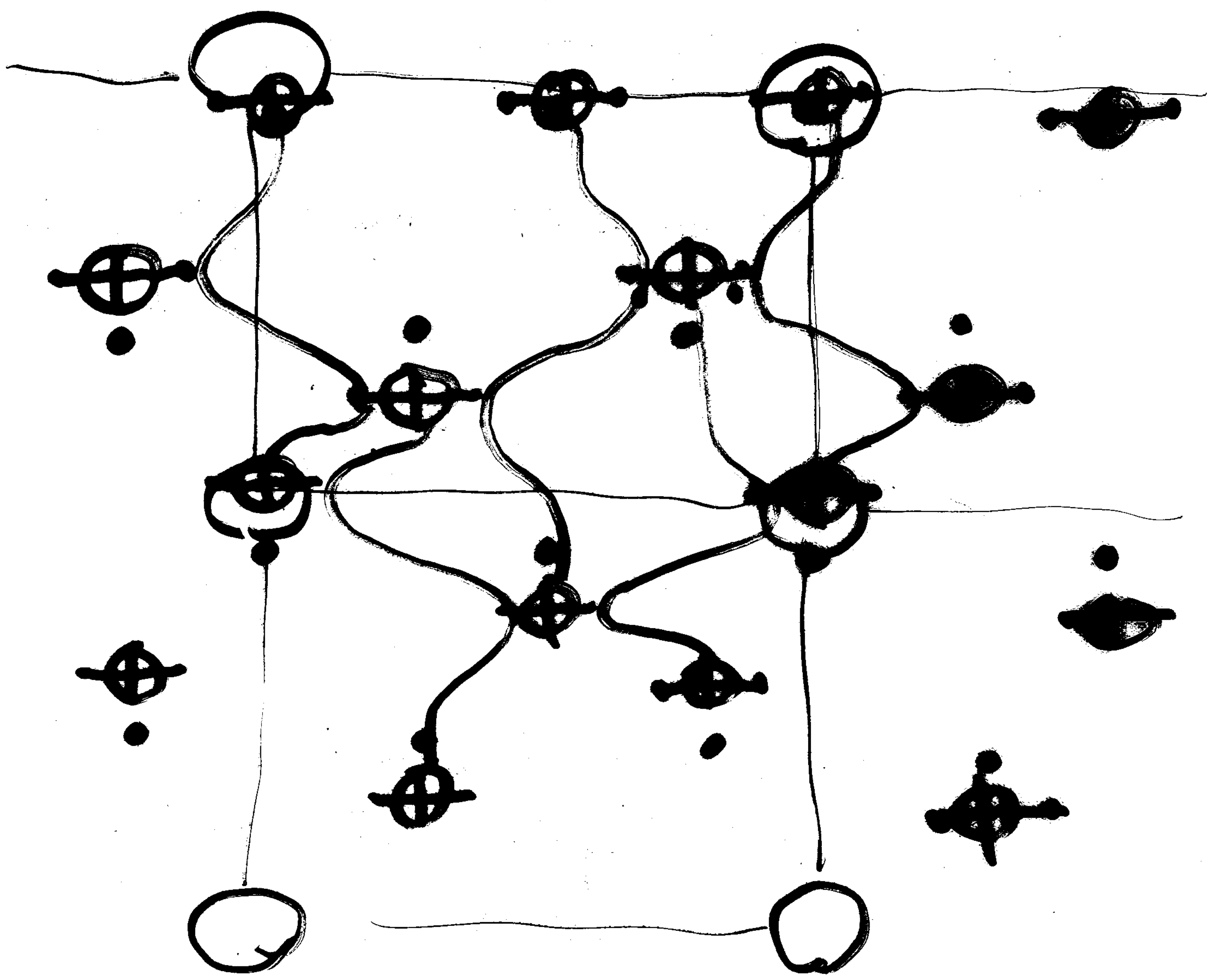
$$\begin{cases} \frac{dq}{dt} = \frac{\partial H(q,p)}{\partial p} \\ \frac{dp}{dt} = -\frac{\partial H(q,p)}{\partial q} \end{cases}$$

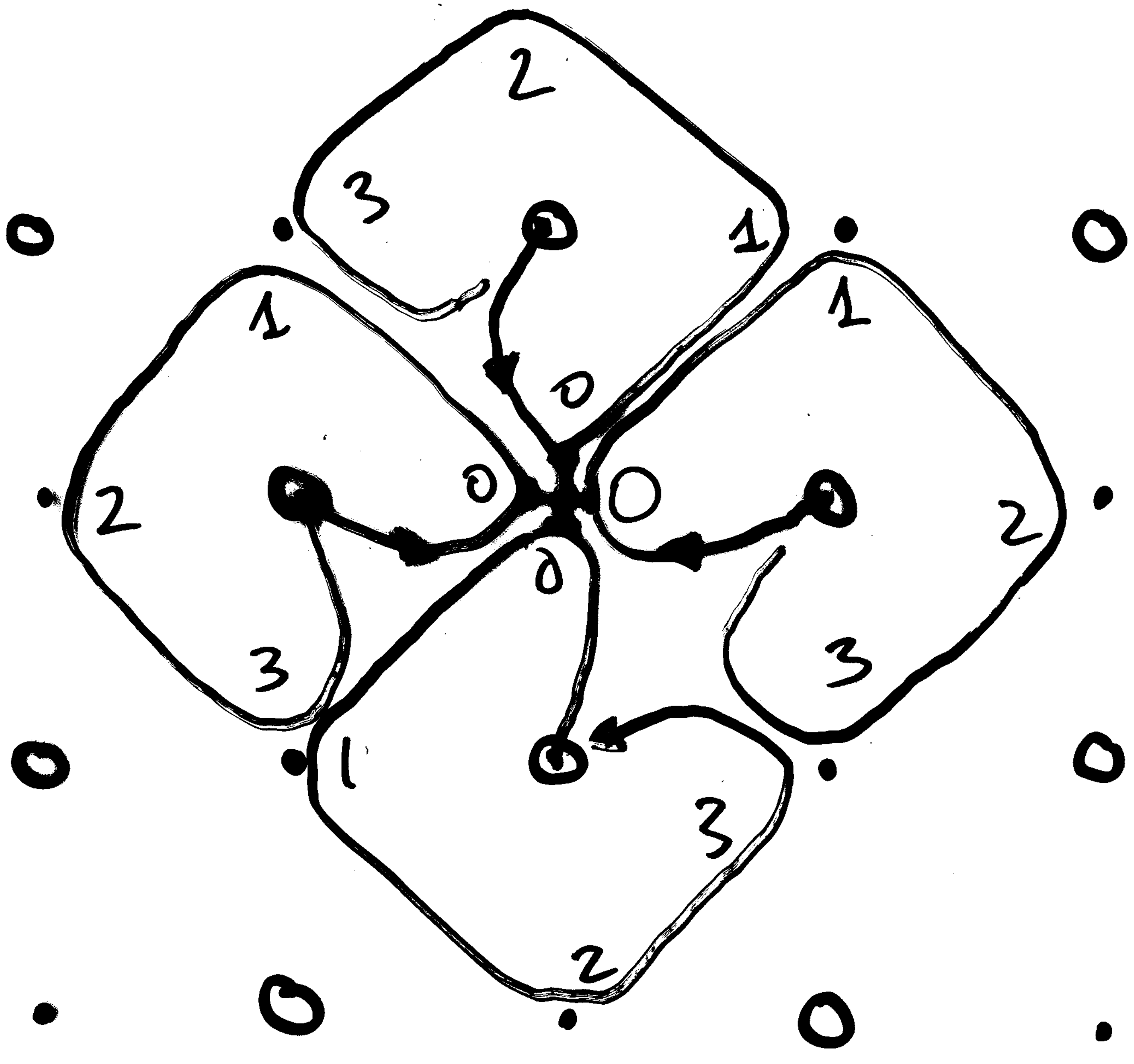

f










2
3
1
0
1
0
1
2
0
2
0
3
3
1
3
2