Pancake Flipping Is Hard

Laurent Bulteau, Guillaume Fertin, Irena Rusu

Laboratoire d'Informatique de Nantes-Atlantique (LINA), UMR CNRS 6241
Université de Nantes, 2 rue de la Houssinière, 44322 Nantes Cedex 3 - France
{Laurent.Bulteau, Guillaume.Fertin, Irena.Rusu}@univ-nantes.fr

Abstract. Pancake Flipping is the problem of sorting a stack of pancakes of different sizes (that is, a permutation), when the only allowed operation is to insert a spatula anywhere in the stack and to flip the pancakes above it (that is, to perform a prefix reversal). In the burnt variant, one side of each pancake is marked as burnt, and it is required to finish with all pancakes having the burnt side down. Computing the optimal scenario for any stack of pancakes and determining the worst-case stack for any stack size have been challenges over more than three decades. Beyond being an intriguing combinatorial problem in itself, it also yields applications, e.g. in parallel computing and computational biology.
In this paper, we show that the Pancake Flipping problem, in its original (unburnt) variant, is NP-hard, thus answering the long-standing question of its computational complexity.

Keywords. Pancake problem, Permutations, Prefix reversals, Computational complexity.

1 Introduction

The pancake problem was stated in [7] as follows:

> The chef in our place is sloppy, and when he prepares a stack of pancakes they come out all different sizes. Therefore, when I deliver them to a customer, on the way to the table I rearrange them (so that the smallest winds up on top, and so on, down to the largest at the bottom) by grabbing several from the top and flipping them over, repeating this (varying the number I flip) as many times as necessary. If there are n pancakes, what is the maximum number of flips (as a function of n) that I will ever have to use to rearrange them?

Stacks of pancakes are represented by permutations, and a flip consists in reversing a prefix of any length. The previous puzzle yields two entangled problems:

- Designing an algorithm that sorts any permutation with a minimum number of flips (this optimization problem is called MIN-SBPR, for Sorting By Prefix Reversals).
- Computing $f(n)$, the maximum number of flips required to sort a permutation of size n (the diameter of the so-called *pancake network*).

Gates and Papadimitriou [9] introduced the *burnt* variant of the problem: the pancakes are two-sided, and an additional constraint requires the pancakes to end with the unburnt side up. The diameter of the corresponding *burnt pancake network* is denoted $g(n)$. A number of studies [4, 5, 6, 9, 11, 12, 13] have aimed at determining more precisely the values of $f(n)$ and $g(n)$, with the following results:

- $f(n)$ and $g(n)$ are known exactly for $n \leq 19$ and $n \leq 17$, respectively [5].
- $15n/14 \leq f(n) \leq 18n/11 + O(1)$ [12, 4].
- $\lfloor (3n+3)/2 \rfloor \leq g(n) \leq 2n - 6$ [5] (upper bound for $n \geq 16$).

Considering MIN-SBPR, 2-approximation algorithms have been designed, both for the burnt [6, 8] and unburnt [8] variants. Moreover, Labarre and Cibulka [13] have characterized a subclass of permutations, which they called *simple permutations*, and which can be sorted in polynomial time.

The pancake problems have various applications. For instance, the pancake network, having both a small degree and diameter, is of interest in parallel computing. The algorithmic aspect, i.e. the sorting problem, has applications in comparative genomics, since prefix reversals are possible elementary modifications that can affect a genome during evolution. A related problem is Sorting By Reversals [1] where any subsequence can be flipped at any step, not only prefixes. This problem is now well-known, with a polynomial-time exact algorithm [10] for the signed case, and a 1.375-approximation [2] for the APX-hard unsigned case [3].

In this paper, we prove that the MIN-SBPR problem is NP-hard (in its unburnt variant), thus answering an open question raised several decades ago. We in fact prove a stronger result: it is known that the number of breakpoints of a permutation (that is, the number of pairs of consecutive elements that are not consecutive in the identity permutation) is a lower bound on the number of flips necessary to sort a permutation. We show that deciding whether this bound is tight is already NP-hard.

2 Notations

We denote by $[\![a\,;\,b]\!]$ the interval $\{a, a+1, \ldots, b\}$ (for $b < a$, we have $[\![a\,;\,b]\!] = \emptyset$). Let n be an integer. Input sequences are permutations of $[\![1\,;\,n]\!]$, hence we consider only sequences where all elements are unsigned, and there cannot be duplicates. When there is no ambiguity, we use the same notation for a sequence and the set of elements it contains. We use upper case for sets and sequences, and lower case for elements.

Consider a sequence S of length n, $S = \langle x_1, x_2, \ldots, x_n \rangle$. Element x_1 is said to be the *head element* of S. Sequence S has a *breakpoint* at position r, $1 \leq r < n$ if $x_r \neq x_{r+1} - 1$ and $x_r \neq x_{r+1} + 1$. It has a *breakpoint* at position n if $x_n \neq n$. We write $d_b(S)$ the number of breakpoints of S. Note that having

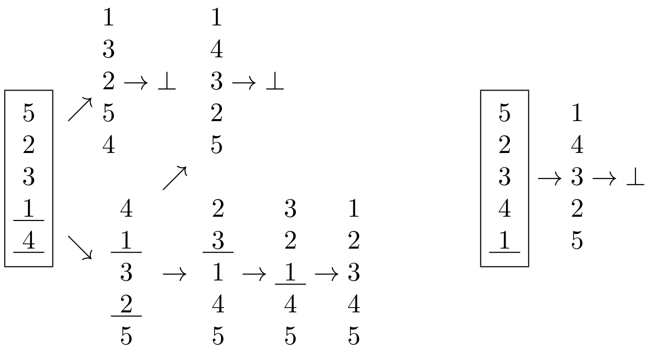


Figure 1: Examples of efficient flips. Sequence $\langle 5,\, 2,\, 3,\, 1,\, 4\rangle$ is efficiently sortable (in four flips), but $\langle 5,\, 2,\, 3,\, 4,\, 1\rangle$ is not.

$x_1 \neq 1$ does not directly count as a breakpoint, and that $d_b(S) \leq n$ for any sequence of length n. For any $p \leq q \in \mathbb{N}$, we write $\mathcal{I}_q^p$ the sequence $\langle p,\, p+1,\, p+2,\, \ldots,\, q\rangle$. $\mathcal{I}_n^1$ is the *identity.* For a sequence of any length $S = \langle x_1,\, x_2,\, \ldots,\, x_k\rangle$, we write $^\star S$ the sequence obtained by reversing S: $^\star S = \langle x_k,\, x_{k-1},\, \ldots,\, x_1\rangle$. Given an integer p, we write $p + S = \langle p + x_1,\, p + x_2,\, \ldots,\, p + x_k\rangle$.

The *flip* of length r is the operation that consists in reversing the r first elements of the sequence. It transforms

$$S = \langle x_1,\, x_2,\, \ldots,\, x_r,\, x_{r+1},\, \ldots,\, x_n\rangle$$

into

$$S' = \langle x_r,\, x_{r-1},\, \ldots,\, x_1,\, x_{r+1},\, \ldots,\, x_n\rangle.$$

Note that the flip of length 1 does not modify S, and the flip of length n transforms S into $^\star S$.

Property 1. *Given a sequence S' obtained from a sequence S by performing one flip, we have $d_b(S') - d_b(S) \in \{-1, 0, 1\}$.*

A flip from S to S' is said to be *efficient* if $d_b(S') = d_b(S) - 1$, and we reserve the notation $S \to S'$ for such flips. A sequence of size n, different from the identity, is a *deadlock* if it yields no efficient flip, and we write $S \to \perp$. By convention, we underline in a sequence the positions corresponding to possible efficient flips: there are at most two of them, and at least one if the sequence is neither a deadlock nor the identity.

We call *path* a series of flips. A path is *efficient* if each flip is efficient in the series. A sequence S is *efficiently sortable* if there exists an efficient path from S to the identity permutation (equivalently, if it can be sorted in $d_b(S)$ flips). See for example Figure 1.

Let S be a sequence different from the identity, and $\mathbb{T}$ be a set of sequences. We write $S \Longrightarrow \mathbb{T}$ if both following conditions are satisfied:

1. for each $T \in \mathbb{T}$, there exists an efficient path from S to T.
2. for each efficient path from S to the identity, there exists a sequence $T \in \mathbb{T}$ such that the path goes through T.

If $\mathbb{T}$ consists of a single element ($\mathbb{T} = \{T\}$), we may write $S \Longrightarrow T$ instead of $S \Longrightarrow \{T\}$. Note that condition 1. is trivial if $\mathbb{T} = \emptyset$, and condition 2. is trivial if there is no efficient path from S to $\mathcal{I}_n^1$. Note that given a sequence S, there can be several different sets $\mathbb{T}$ such that $S \Longrightarrow \mathbb{T}$. However, two are especially relevant:

Property 2. *Given any sequence $S \neq \mathcal{I}_n^1$,*

$$S \Longrightarrow \mathcal{I}_n^1 \quad \Leftrightarrow \quad S \textit{ is efficiently sortable.}$$
$$S \Longrightarrow \emptyset \quad \Leftrightarrow \quad S \textit{ is not efficiently sortable.}$$

Proof. For $S \Longrightarrow \mathcal{I}_n^1$: condition 1. is true iff there exists an efficient path from S to the identity, that is S is efficiently sortable. Condition 2. is always true.

For $S \Longrightarrow \emptyset$: condition 1. is always true. If there exists at least one efficient path from S to $\mathcal{I}_n^1$, then, since there exists no sequence $T \in \emptyset$, Condition 2. cannot be true. Hence Condition 2. is false when there exists an efficient path from S to the identity and true otherwise, so it is equivalent to the fact that S is not efficiently sortable. □

The following property is easily deduced from the definition.

Property 3. *If $S \Longrightarrow \{S_1, S_2\}$, $S_1 \Longrightarrow \mathbb{T}_1$ and $S_2 \Longrightarrow \mathbb{T}_2$, then $S \Longrightarrow \mathbb{T}_1 \cup \mathbb{T}_2$.*

3 Reduction from 3-SAT

The reduction uses a number of gadget sequences in order to simulate boolean variables and clauses with subsequences. They are organized in two levels (where level-1 gadgets are directly defined by sequences of integers, and level-2 gadgets are defined using a pattern of level-1 gadgets). For each gadget we define, we derive a property characterizing the efficient paths that can be followed if some part of the gadget appears at the head of a sequence.

We have not aimed at providing the smallest possible gadgets (the overall reduction for a formula containing l variables and k clauses creates a stack of $31l + 98k$ elements with $16l + 50k$ breakpoints), and we preferred straightforward proofs and easy-to-combine gadgets over short sequences. A rough analysis shows that the final stack size could easily be reduced to $22l + 71k$, with the same number of breakpoints.

3.1 Level-1 gadgets

3.1.1 Docks

The dock gadget is the simplest we define. Its only goal is to store sequences of the kind ${}^\star\mathcal{I}_q^{p+1}$ (with $p < q$) out of the head of the sequence, without "disturbing" any other part.

Definition 1. *Given two integers p and q with $p < q$, the* dock *for ${}^\star\mathcal{I}_q^{p+1}$ is the sequence*

$$\begin{array}{rcl} \mathit{Dock}(p,q) & = & D \\ \textit{where} \quad D & = & \langle p-1,\, p,\, q+1,\, q+2 \rangle. \end{array}$$

It has the following property:

Property 4. *Let p and q be any integers with $p < q$, $D = \mathit{Dock}(p,q)$, and X and Y be any sequences. We have*

$$\begin{array}{c} {}^\star\mathcal{I}_q^{p+1} \\ X \\ D \\ Y \end{array} \Longrightarrow \begin{array}{c} X \\ \mathcal{I}_{q+2}^{p-1} \\ Y \end{array}$$

Proof. An efficient path from $\langle {}^\star\mathcal{I}_q^{p+1}, X, D, Y \rangle$ to $\langle X, \mathcal{I}_{q+2}^{p-1}, Y \rangle$ is given in Figure 2. For each sequence in the path, we apply the only possible efficient flip, hence every efficient path between $\langle {}^\star\mathcal{I}_q^{p+1}, X, D, Y \rangle$ and $\mathcal{I}_n^1$ (if such a path exists) begins with these two flips, and goes through $\langle X, \mathcal{I}_{q+2}^{p-1}, Y \rangle$. □

$$\boxed{\begin{array}{c} {}^{\star}\mathcal{I}_q^{p+1} \\ X \\ D \\ Y \end{array}} = \begin{array}{c} q \\ q-1 \\ \vdots \\ p+2 \\ p+1 \\ X \\ p-1 \\ \underline{p} \\ q+1 \\ q+2 \\ Y \end{array} \rightarrow \begin{array}{c} p \\ p-1 \\ \underline{{}^{\star}X} \\ p+1 \\ p+2 \\ \vdots \\ q-1 \\ q \\ q+1 \\ q+2 \\ Y \end{array} \rightarrow \begin{array}{c} X \\ p-1 \\ p \\ p+1 \\ p+2 \\ \vdots \\ q-1 \\ q \\ q+1 \\ q+2 \\ Y \end{array} = \boxed{\begin{array}{c} X \\ \mathcal{I}_{q+2}^{p-1} \\ Y \end{array}}$$

Figure 2: Proof of Property 4. (Dock gadget)

3.1.2 Lock

A lock gadget contains three parts: a sequence which is the lock itself, a key element that "opens" the lock, and a test element that checks whether the lock is open.

Definition 2. *For any integer p, $Lock(p)$ is defined by*

$$\begin{array}{rrcl} & Lock(p) & = & (key, test, L) \\ \textit{where} & key & = & p+10 \\ & test & = & p+7 \\ & L & = & p + \big\langle 1,\ 2,\ 9,\ 8,\ 5,\ 6,\ 4,\ 3,\ 11,\ 12 \big\rangle \end{array}$$

Given a lock $(key, test, L) = Lock(p)$, we write

$$L^o = p + \big\langle 1,\ 2,\ 3,\ 4,\ 6,\ 5,\ 8,\ 9,\ 10,\ 11,\ 12 \big\rangle.$$

Sequences L and L^o represent the lock when it is respectively closed or open. If a sequence containing a closed lock has *key* for head element, then efficient flips put the lock in open position. If it has *test* for head element, then it is a deadlock if and only if the lock is closed.

Property 5. *Let p be any integer, $(key, test, L) = Lock(p)$, and X and Y be any sequences. We have*

$$\textbf{a.}\ \begin{array}{c} key \\ X \\ L \\ Y \end{array} \Longrightarrow \begin{array}{c} X \\ L^o \\ Y \end{array} \qquad \textbf{b.}\ \begin{array}{c} test \\ X \\ L^o \\ Y \end{array} \Longrightarrow \begin{array}{c} X \\ \mathcal{I}_{p+12}^{p+1} \\ Y \end{array} \qquad \textbf{c.}\ \begin{array}{c} test \\ X \\ L \\ Y \end{array} \rightarrow \bot$$

Proof. See Figure 3. Note that for readability reasons, the proof is given for $p = 0$. It can obviously be extended to any value of p (each element would then be increased by p). □

We use locks to emulate literals of a boolean formula: variables "hold the keys", and in a first time open the locks corresponding to true literals. Each clause holds three test elements, corresponding to its three literals, and the clause is true if the lock is open for at least one of the test elements.

3.1.3 Hook

A hook gadget contains four parts: two sequences used as delimiters, a *take* element that takes the interval between the delimiters and places it in head, and a *put* element that does the reverse operation. Thus, the

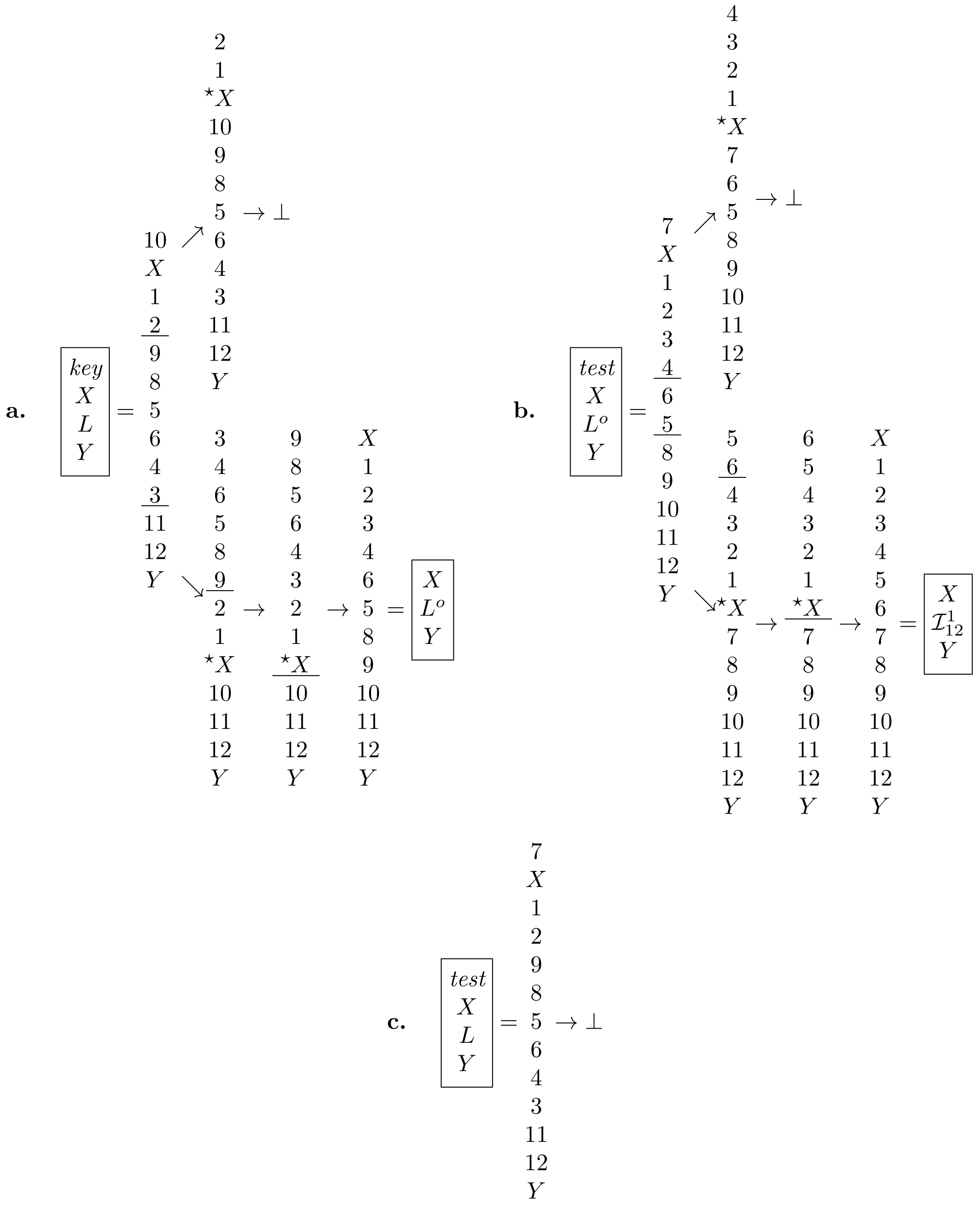


Figure 3: Proof of Property 5. (Lock gadget)

sequence between the delimiters can be stored anywhere until it is called by *take*, and then can be stored back using *put*.

Definition 3. *For any integer p, Hook(p) is defined by*

$$\begin{array}{rrcl} & \mathit{Hook}(p) & = & (\mathit{take}, \mathit{put}, G, H) \\ \textit{where} & \mathit{take} & = & p+10 \\ & \mathit{put} & = & p+7 \\ & G & = & p+\big\langle 3,\ 4\big\rangle \\ & H & = & p+\big\langle 12,\ 11,\ 6,\ 5,\ 9,\ 8,\ 2,\ 1\big\rangle. \end{array}$$

Given a hook $(\mathit{take}, \mathit{put}, G, H) = \mathit{Hook}(p)$, we write

$$\begin{array}{rcl} G' & = & p+\big\langle 12,\ 11,\ 6,\ 5,\ 4,\ 3\big\rangle \\ H' & = & p+\big\langle 10,\ 9,\ 8,\ 2,\ 1\big\rangle \\ G'' & = & p+\big\langle 3,\ 4,\ 5,\ 6,\ 7\big\rangle \\ H'' & = & p+\big\langle 12,\ 11,\ 10,\ 9,\ 8,\ 2,\ 1\big\rangle. \end{array}$$

Property 6. *Let p be an integer, $(\mathit{take}, \mathit{put}, G, H) = \mathit{Hook}(p)$, and X, Y and Z be any sequences. We have*

$$\textbf{a.}\quad \begin{array}{c} \mathit{take} \\ X \\ G \\ Y \\ H \\ Z \end{array} \Longrightarrow \begin{array}{c} Y \\ G' \\ {}^\star X \\ H' \\ Z \end{array} \qquad\qquad \textbf{b.}\quad \begin{array}{c} \mathit{put} \\ X \\ G' \\ {}^\star Y \\ H' \\ Z \end{array} \Longrightarrow \begin{array}{c} Y \\ G'' \\ X \\ H'' \\ Z \end{array} \qquad\qquad \textbf{c.}\quad \begin{array}{c} G'' \\ X \\ H'' \\ Y \end{array} \Longrightarrow \begin{array}{c} X \\ {}^\star\mathcal{I}_{p+12}^{p+1} \\ Y \end{array}$$

Proof. See Figure 4 (with $p = 0$). □

3.1.4 Fork

A fork gadget implements choices. It contains two parts delimiting a sequence X. Any efficient path encountering a fork gadget follows one of two tracks, where either X or ${}^\star X$ appears at the head of the sequence at some point. Sequence X would typically contain a series of triggers for various gadgets (*key*, *take*, etc.), so that X and ${}^\star X$ differ in the order in which the gadgets are triggered.

Definition 4. *For any integer p, Fork(p) is defined by*

$$\begin{array}{rrcl} & \mathit{Fork}(p) & = & (E, F) \\ \textit{where} & E & = & p+\big\langle 11,\ 8,\ 7,\ 3\big\rangle \\ & F & = & p+\big\langle 10,\ 9,\ 6,\ 12,\ 13,\ 4,\ 5,\ 15,\ 14,\ 2,\ 1\big\rangle. \end{array}$$

Given a fork $(E, F) = \mathit{Fork}(p)$, we write

$$\begin{array}{rcl} F^1 & = & p+\big\langle 10,\ 9,\ 6,\ 7,\ 8,\ 11,\ 12,\ 13,\ 14,\ 15,\ 5,\ 4,\ 3,\ 2,\ 1\big\rangle \\ F^2 & = & p+\big\langle 3,\ 7,\ 8,\ 11,\ 10,\ 9,\ 6,\ 12,\ 13,\ 4,\ 5,\ 15,\ 14,\ 2,\ 1\big\rangle \end{array}$$

Property 7. *Let p be an integer, $(E, F) = \mathit{Fork}(p)$, and X, Y be any sequences. We have*

$$\textbf{a.}\quad \begin{array}{c} E \\ X \\ F \\ Y \end{array} \Longrightarrow \left\{ \begin{array}{c} X \\ F^1 \\ Y \end{array} , \begin{array}{c} {}^\star X \\ F^2 \\ Y \end{array} \right\} \qquad\qquad \textbf{b.}\quad \begin{array}{c} F^1 \\ Y \end{array} \Longrightarrow \begin{array}{c} {}^\star\mathcal{I}_{p+15}^{p+1} \\ Y \end{array} \qquad\qquad \textbf{c.}\quad \begin{array}{c} F^2 \\ Y \end{array} \Longrightarrow \begin{array}{c} {}^\star\mathcal{I}_{p+15}^{p+1} \\ Y \end{array}$$

a.

$$\boxed{\begin{array}{c} \mathit{take} \\ X \\ G \\ Y \\ H \\ Z \end{array}} = \begin{array}{c} 10 \\ X \\ 3 \\ 4 \\ Y \\ 12 \\ 11 \\ 6 \\ \underline{5} \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} \to \begin{array}{c} 5 \\ 6 \\ 11 \\ 12 \\ \underline{{}^\star Y} \\ 4 \\ 3 \\ {}^\star X \\ 10 \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} \to \begin{array}{c} Y \\ 12 \\ 11 \\ 6 \\ 5 \\ 4 \\ 3 \\ {}^\star X \\ 10 \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} = \boxed{\begin{array}{c} Y \\ G' \\ {}^\star X \\ H' \\ Z \end{array}}$$

b.

$$\boxed{\begin{array}{c} \mathit{put} \\ X \\ G' \\ {}^\star Y \\ H' \\ Z \end{array}} = \begin{array}{c} 7 \\ X \\ 12 \\ \underline{11} \\ 6 \\ 5 \\ 4 \\ 3 \\ {}^\star Y \\ 10 \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} \to \begin{array}{c} 11 \\ 12 \\ {}^\star X \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ \underline{{}^\star Y} \\ 10 \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} \to \begin{array}{c} Y \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ X \\ 12 \\ 11 \\ 10 \\ 9 \\ 8 \\ 2 \\ 1 \\ Z \end{array} = \boxed{\begin{array}{c} Y \\ G'' \\ X \\ H'' \\ Z \end{array}}$$

c.

$$\boxed{\begin{array}{c} G'' \\ X \\ H'' \\ Y \end{array}} = \begin{array}{c} 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ X \\ 12 \\ 11 \\ 10 \\ 9 \\ \underline{8} \\ 2 \\ 1 \\ Y \end{array} \to \begin{array}{c} 8 \\ 9 \\ 10 \\ 11 \\ 12 \\ \underline{{}^\star X} \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \\ Y \end{array} \to \begin{array}{c} X \\ 12 \\ 11 \\ 10 \\ 9 \\ 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \\ Y \end{array} = \boxed{\begin{array}{c} X \\ {}^\star \mathcal{I}^1_{12} \\ Y \end{array}}$$

Figure 4: Proof of Property 6. (Hook Gadget)

Proof. See Figures 5 and 6 (with $p = 0$). □

3.2 Level-2 gadgets

In this section, we define new gadgets based on the four level-1 gadgets. From now on, each property proof uses exclusively properties from smaller gadgets. In order to help the reader follow the ever-present references, we use the following notations. Bold font is used to emphasise the “active” parts of the gadget currently having an element at the head of the sequence. For each relation $S \Longrightarrow T$, we give the relevant reference below (e.g. $S \underset{4.}{\Longrightarrow} T$ if it is obtained from Property 4). Finally, a summary of all gadget properties (either level-1 or -2) is given in Figure 7.

3.2.1 Literals

The following gadget is used only once in the reduction. It contains the locks corresponding to all literals of the formula.

Definition 5. *Let p and m be two integers, $\mathit{Literals}(p,m)$ is defined by*

$$\begin{aligned} \mathit{Literals}(p,m) &= (\mathit{key}_1, \ldots, \mathit{key}_m, \mathit{test}_1, \ldots, \mathit{test}_m, \Lambda) \\ \mathit{where} \quad \Lambda &= \langle L_1,\, L_2,\, \ldots,\, L_m \rangle \\ \forall i \in [\![1\,;\,m]\!]\,,\ (\mathit{key}_i, \mathit{test}_i, L_i) &= \mathit{Lock}(p + 12(i-1)) \end{aligned}$$

Let O and I be two disjoint subsets of $[\![1\,;\,m]\!]$. We write Λ_I^O the sequence obtained from Λ by

- *replacing L_i by L_i^o for all $i \in O$,*
- *replacing L_i by $\mathcal{I}_{p+12i}^{p+12i-11}$ for all $i \in I$.*

Elements of O correspond to open locks in Λ_I^O, while elements of I correspond to open locks which have moreover been tested. Note that $\Lambda_\emptyset^\emptyset = \Lambda$, and that $\Lambda_{[\![1\,;\,m]\!]}^\emptyset = \mathcal{I}_{p+12m}^{p+1}$.

Property 8. *Let p and m be two integers, $(\mathit{key}_1, \ldots, \mathit{key}_m, \mathit{test}_1, \ldots, \mathit{test}_m, \Lambda) = \mathit{Literals}(p,m)$, O and I be two disjoint subsets of $[\![1\,;\,m]\!]$, and X be any sequence. We have*

$$\textbf{a.} \quad \forall i \in [\![1\,;\,m]\!] - O - I, \quad \begin{matrix} \mathit{key}_i \\ X \\ \Lambda_I^O \end{matrix} \Longrightarrow \begin{matrix} X \\ \Lambda_I^{O \cup \{i\}} \end{matrix}$$

$$\textbf{b.} \quad \forall i \in O, \quad \begin{matrix} \mathit{test}_i \\ X \\ \Lambda_I^O \end{matrix} \Longrightarrow \begin{matrix} X \\ \Lambda_{I \cup \{i\}}^{O - \{i\}} \end{matrix}$$

$$\textbf{c.} \quad \forall i \in [\![1\,;\,m]\!] - O, \quad \begin{matrix} \mathit{test}_i \\ X \\ \Lambda_I^O \end{matrix} \rightarrow \bot$$

Proof. The proof follows from Property 5.

a. Let $i \in [\![1\,;\,m]\!] - O - I$. Then Λ_I^O can be written $\Lambda_I^O = \langle A,\, L_i,\, B \rangle$. Hence

$$\begin{aligned} &\langle \mathit{key}_i,\, X,\, \Lambda_I^O \rangle \\ &= \langle \boldsymbol{\mathit{key}_i},\, X,\, A,\, \boldsymbol{L_i},\, B \rangle \\ &\underset{5.\mathrm{a}}{\Longrightarrow} \langle X,\, A,\, L_i^o,\, B \rangle \\ &= \langle X,\, \Lambda_I^{O \cup \{i\}} \rangle \end{aligned}$$

$$\begin{tikzcd}[column sep=small]
 & \begin{array}{c}{}^\star X\\3\\7\\8\\11\\10\\9\\6\\12\\13\\4\\5\\15\\14\\2\\1\\Y\end{array} = \boxed{\begin{array}{c}{}^\star X\\F^2\\Y\end{array}} & & \begin{array}{c}13\\12\\11\\8\\7\\6\\9\\10\\{}^\star X\\3\\4\\5\\15\\14\\2\\1\\Y\end{array} \arrow[r] & \bot & \\
\textbf{a.}\quad \boxed{\begin{array}{c}E\\X\\F\\Y\end{array}} = \begin{array}{c}11\\8\\7\\3\\\underline{X}\\10\\9\\\underline{6}\\12\\13\\4\\5\\15\\14\\2\\1\\Y\end{array} \arrow[ur] \arrow[dr] & & & & & \\
 & \begin{array}{c}6\\9\\10\\{}^\star X\\\underline{3}\\7\\8\\11\\12\\13\\4\\5\\15\\14\\2\\1\\Y\end{array} \arrow[r] & \begin{array}{c}3\\X\\10\\9\\6\\7\\8\\11\\12\\\underline{13}\\4\\5\\15\\\underline{14}\\2\\1\\Y\end{array} \arrow[r] \arrow[uur] & \begin{array}{c}14\\15\\5\\\underline{4}\\13\\12\\11\\8\\7\\6\\9\\10\\{}^\star X\\3\\2\\1\\Y\end{array} \arrow[r] & \begin{array}{c}4\\5\\15\\14\\13\\12\\11\\8\\7\\6\\9\\10\\\underline{{}^\star X}\\3\\2\\1\\Y\end{array} \arrow[r] & \begin{array}{c}X\\10\\9\\6\\7\\8\\11\\12\\13\\14\\15\\5\\4\\3\\2\\1\\Y\end{array} = \boxed{\begin{array}{c}X\\F^1\\Y\end{array}}
\end{tikzcd}$$

$$\textbf{b.}\quad \boxed{\begin{array}{c}F^1\\Y\end{array}} = \begin{array}{c}10\\9\\6\\7\\\underline{8}\\11\\12\\13\\14\\15\\5\\4\\3\\2\\1\\Y\end{array} \rightarrow \begin{array}{c}8\\7\\\underline{6}\\9\\10\\11\\12\\13\\14\\15\\5\\4\\3\\2\\1\\Y\end{array} \rightarrow \begin{array}{c}6\\7\\8\\9\\10\\11\\12\\13\\14\\\underline{15}\\5\\4\\3\\2\\1\\Y\end{array} \rightarrow \begin{array}{c}15\\14\\13\\12\\11\\10\\9\\8\\7\\6\\5\\4\\3\\2\\1\\Y\end{array} = \boxed{\begin{array}{c}{}^\star\mathcal{I}^1_{15}\\Y\end{array}}$$

Figure 5: Proof of Properties 7.a and 7.b (Fork gadget).

c.

$$\begin{tikzcd}
 & & \begin{array}{c} 13\\ 12\\ 6\\ 9\\ 10\\ 11\\ 8\\ 7\\ 3\\ 4\\ 5\\ 15\\ 14\\ 2\\ 1\\ Y \end{array} \arrow[r] & \perp & & & & & \\
\boxed{\begin{array}{c} F^2\\ Y \end{array}} \arrow[r, phantom, "="] & \begin{array}{c} 3\\ 7\\ 8\\ 11\\ 10\\ 9\\ 6\\ 12\\ 13\\ \hline 4\\ 5\\ 15\\ 14\\ \hline 2\\ 1\\ Y \end{array} \arrow[ur] \arrow[dr] & & & & & & & \\
 & & \begin{array}{c} 14\\ 15\\ 5\\ 4\\ \hline 13\\ 12\\ 6\\ 9\\ 10\\ 11\\ 8\\ 7\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 4\\ 5\\ 15\\ 14\\ 13\\ 12\\ 6\\ 9\\ 10\\ 11\\ 8\\ 7\\ \hline 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 7\\ 8\\ 11\\ 10\\ 9\\ \hline 6\\ 12\\ 13\\ 14\\ 15\\ 5\\ 4\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 9\\ 10\\ 11\\ \hline 8\\ 7\\ 6\\ 12\\ 13\\ 14\\ 15\\ 5\\ 4\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 11\\ 10\\ 9\\ 8\\ 7\\ 6\\ \hline 12\\ 13\\ 14\\ 15\\ 5\\ 4\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 6\\ 7\\ 8\\ 9\\ 10\\ 11\\ 12\\ 13\\ 14\\ 15\\ \hline 5\\ 4\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r] & \begin{array}{c} 15\\ 14\\ 13\\ 12\\ 11\\ 10\\ 9\\ 8\\ 7\\ 6\\ 5\\ 4\\ 3\\ 2\\ 1\\ Y \end{array} \arrow[r, phantom, "="] & \boxed{\begin{array}{c} {}^{\star}\mathcal{I}^1_{15}\\ Y \end{array}}
\end{tikzcd}$$

Figure 6: Proof of Property 7.c (Fork gadget).

Dock gadget

$$\left\langle {}^{\star}\boldsymbol{\mathcal{I}_q^{p+1}},\, X,\, \boldsymbol{D},\, Y \right\rangle \underset{4.}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{q+2}^{p-1},\, Y \right\rangle$$

Lock gadget

$$\left\langle \boldsymbol{key},\, X,\, \boldsymbol{L},\, Y \right\rangle \underset{5.\text{a}}{\Longrightarrow} \left\langle X,\, L^{o},\, Y \right\rangle$$

$$\left\langle \boldsymbol{test},\, X,\, \boldsymbol{L^{o}},\, Y \right\rangle \underset{5.\text{b}}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{p+12}^{p+1},\, Y \right\rangle$$

$$\left\langle \boldsymbol{test},\, X,\, \boldsymbol{L},\, Y \right\rangle \underset{5.\text{c}}{\rightarrow} \perp$$

Hook gadget

$$\left\langle \boldsymbol{take},\, X,\, \boldsymbol{G},\, Y,\, \boldsymbol{H},\, Z \right\rangle \underset{6.\text{a}}{\Longrightarrow} \left\langle Y,\, G',\, {}^{\star}X,\, H',\, Z \right\rangle$$

$$\left\langle \boldsymbol{put},\, X,\, \boldsymbol{G'},\, {}^{\star}Y,\, \boldsymbol{H'},\, Z \right\rangle \underset{6.\text{b}}{\Longrightarrow} \left\langle Y,\, G'',\, X,\, H'',\, Z \right\rangle$$

$$\left\langle \boldsymbol{G''},\, X,\, \boldsymbol{H''},\, Y \right\rangle \underset{6.\text{c}}{\Longrightarrow} \left\langle X,\, {}^{\star}\mathcal{I}_{p+12}^{p+1},\, Y \right\rangle$$

Fork gadget

$$\left\langle \boldsymbol{E},\, X,\, \boldsymbol{F},\, Y \right\rangle \underset{7.\text{a}}{\Longrightarrow} \left\{ \begin{matrix} \left\langle X,\, F^{1},\, Y \right\rangle \\ \left\langle {}^{\star}X,\, F^{2},\, Y \right\rangle \end{matrix} \right\}$$

$$\left\langle \boldsymbol{F^{1}},\, Y \right\rangle \underset{7.\text{b}}{\Longrightarrow} \left\langle {}^{\star}\mathcal{I}_{p+15}^{p+1},\, Y \right\rangle$$

$$\left\langle \boldsymbol{F^{2}},\, Y \right\rangle \underset{7.\text{c}}{\Longrightarrow} \left\langle {}^{\star}\mathcal{I}_{p+15}^{p+1},\, Y \right\rangle$$

Literals gadget

$$\forall i \notin O \cup I,\ \left\langle \boldsymbol{key_i},\, X,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{8.\text{a}}{\Longrightarrow} \left\langle X,\, \Lambda_I^{O\cup\{i\}} \right\rangle$$

$$\forall i \in O,\ \left\langle \boldsymbol{test_i},\, X,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{8.\text{b}}{\Longrightarrow} \left\langle X,\, \Lambda_{I\cup\{i\}}^{O-\{i\}} \right\rangle$$

$$\forall i \notin O,\ \left\langle \boldsymbol{test_i},\, X,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{8.\text{c}}{\rightarrow} \perp$$

Variable gadget

$$\left\langle \boldsymbol{\nu},\, X,\, \boldsymbol{V},\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{9.\text{a}}{\Longrightarrow} \left\{ \begin{matrix} \left\langle X,\, V^{1},\, Y,\, \Lambda_I^{O\cup P} \right\rangle \\ \left\langle X,\, V^{2},\, Y,\, \Lambda_I^{O\cup N} \right\rangle \end{matrix} \right\}$$

$$\left\langle \boldsymbol{V^{1}},\, X,\, \boldsymbol{D},\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{9.\text{b}}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{p+31}^{p+1},\, Y,\, \Lambda_I^{O\cup N} \right\rangle$$

$$\left\langle \boldsymbol{V^{2}},\, X,\, \boldsymbol{D},\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{9.\text{c}}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{p+31}^{p+1},\, Y,\, \Lambda_I^{O\cup P} \right\rangle$$

Clause gadget

$$\left\langle \boldsymbol{\gamma},\, X,\, \boldsymbol{\Gamma},\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{10.}{\Longrightarrow} \left\{ \begin{matrix} \left\langle X,\, \Gamma^{1},\, Y,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \right\rangle \text{ iff } a \in O \\ \left\langle X,\, \Gamma^{2},\, Y,\, \Lambda_{I\cup\{b\}}^{O-\{b\}} \right\rangle \text{ iff } b \in O \\ \left\langle X,\, \Gamma^{3},\, Y,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \text{ iff } c \in O \end{matrix} \right\}$$

$$\left\langle \boldsymbol{\Gamma^{1}},\, Y,\, \Delta,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{11.\text{a}}{\Longrightarrow} \left\langle Y,\, \mathcal{I}_{p+62}^{p+1},\, Z,\, \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \right\rangle$$

$$\left\langle \boldsymbol{\Gamma^{2}},\, Y,\, \Delta,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{11.\text{b}}{\Longrightarrow} \left\langle Y,\, \mathcal{I}_{p+62}^{p+1},\, Z,\, \Lambda_{I\cup\{a,c\}}^{O-\{a,c\}} \right\rangle$$

$$\left\langle \boldsymbol{\Gamma^{3}},\, Y,\, \Delta,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle \underset{11.\text{c}}{\Longrightarrow} \left\langle Y,\, \mathcal{I}_{p+62}^{p+1},\, Z,\, \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \right\rangle$$

Figure 7: Compilation of all gadget properties. As a general rule, X, Y, Z can be any sequences, O and I any disjoint subsets of $[\![1\,;\,m]\!]$. See respective definitions and properties for specific constraints and notations

b. Let $i \in O$. Then Λ_I^O can be written $\Lambda_I^O = \langle A,\, L_i^o,\, B\rangle$. Hence

$$\begin{aligned}&\langle \mathit{test}_i,\, X,\, \Lambda_I^O\rangle\\ &= \langle \boldsymbol{test_i},\, X,\, A,\, \boldsymbol{L_i^o},\, B\rangle\\ &\underset{5.\mathrm{b}}{\Longrightarrow} \langle X,\, A,\, \mathcal{I}_{p+12i}^{p+12i-11},\, B\rangle\\ &= \langle X,\, \Lambda_{I\cup\{i\}}^{O-\{i\}}\rangle\end{aligned}$$

c. Let $i \in [\![1\,;\,m]\!] - O$. If $i \in I$, then $\mathit{test}_i \in \mathcal{I}_{p+12i}^{p+12i-11} \subset \Lambda_I^O$, and $\langle \mathit{test}_i,\, X,\, \Lambda_I^O\rangle$ is not a valid sequence (it contains a duplicate). Otherwise, $i \in [\![1\,;\,m]\!] - O - I$, and Λ_I^O can be written $\Lambda_I^O = \langle A,\, L_i,\, B\rangle$. Hence

$$\langle \mathit{test}_i,\, X,\, \Lambda_I^O\rangle = \langle \boldsymbol{test_i},\, X,\, A,\, \boldsymbol{L_i},\, B\rangle \underset{5.\mathrm{c}}{\rightarrow} \perp$$

□

3.2.2 Variable

In the following two sections, we assume that p_Λ and m are two fixed integers, and we define the *Literals*(,g)adget $(\mathit{key}_1, \ldots, \mathit{key}_m, \mathit{test}_1, \ldots, \mathit{test}_m, \Lambda) = \mathit{Literals}(p_\Lambda, m)$. Thus, we can use elements key_i and test_i for $i \in [\![1\,;\,m]\!]$, and sequences Λ_I^O for any disjoint subsets O and I of $[\![1\,;\,m]\!]$.

We now define a gadget simulating a boolean variable x_i. It holds two series of *key* elements: the ones with indices in P (resp. N) open the locks corresponding to literals of the form x_i (resp. $\neg x_i$). When the triggering element, ν, is brought to the head, a choice has to be made between P and N, and the locks associated with the chosen set (and only them) are open.

Definition 6. *Let P, N be two disjoint subsets of $[\![1\,;\,m]\!]$ ($P = \{p_1, p_2, \ldots, p_q\}$, $N = \{n_1, n_2, \ldots, n_{q'}\}$) and p be an integer, Variable(P, N, p) is defined by*

$$\begin{aligned} \mathit{Variable}(P,N,p) &= (\nu, V, D)\\ \textit{where}\quad (\mathit{take}, \mathit{put}, G, H) &= \mathit{Hook}(p+2)\\ (E,F) &= \mathit{Fork}(p+14)\\ \textit{in}\quad \nu &= \mathit{take}\\ V &= \langle G,\, E,\, \mathit{key}_{p_1},\, \ldots,\, \mathit{key}_{p_q},\, \mathit{put},\, \mathit{key}_{n_1},\, \ldots,\, \mathit{key}_{n_{q'}},\, F,\, H\rangle\\ D &= \mathit{Dock}(p+2, p+29)\end{aligned}$$

Given a variable gadget $(\nu, V, D) = \mathit{Variable}(P, N, p)$, we write

$$\begin{aligned} V^1 &= \langle G'',\, \mathit{key}_{n_1},\, \ldots,\, \mathit{key}_{n_{q'}},\, F^1,\, H''\rangle\\ V^2 &= \langle G'',\, \mathit{key}_{p_q},\, \ldots,\, \mathit{key}_{p_1},\, F^2,\, H''\rangle\end{aligned}$$

where G'', H'', F^1, F^2, come from the definitions of Hook (Definition 3) and Fork (Definition 4).

The following property determines the possible behavior of a variable gadget. It is illustrated by Figure 8.

Property 9. *Let P, N be two disjoint subsets of $[\![1\,;\,m]\!]$, p be an integer, X and Y be two sequences, O, I be two disjoint subsets of $[\![1\,;\,m]\!]$, and $(\nu, V, D) = \mathit{Variable}(P, N, p)$. For sub-property (a.) we require that $(P \cup N) \cap (O \cup I) = \emptyset$, for (b.) that $N \cap (O \cup I) = \emptyset$, and for (c.) that $P \cap (O \cup I) = \emptyset$ (these conditions are in fact necessarily satisfied by construction since all sequences considered are permutations). We have*

$$\textbf{a.}\quad \begin{array}{c}\nu\\X\\V\\Y\\\Lambda_I^O\end{array} \Longrightarrow \left\{\begin{array}{c}X\\V^1\\Y\\\Lambda_I^{O\cup P}\end{array},\ \begin{array}{c}X\\V^2\\Y\\\Lambda_I^{O\cup N}\end{array}\right\} \qquad \textbf{b.}\quad \begin{array}{c}V^1\\X\\D\\Y\\\Lambda_I^O\end{array} \Longrightarrow \begin{array}{c}X\\\mathcal{I}_{p+31}^{p+1}\\Y\\\Lambda_I^{O\cup N}\end{array} \qquad \textbf{c.}\quad \begin{array}{c}V^2\\X\\D\\Y\\\Lambda_I^O\end{array} \Longrightarrow \begin{array}{c}X\\\mathcal{I}_{p+31}^{p+1}\\Y\\\Lambda_I^{O\cup P}\end{array}$$

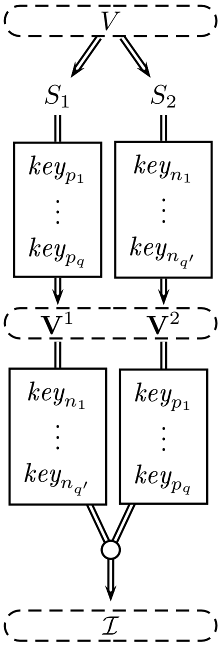

V
S_1
S_2
key_{p_1} ⋮ key_{p_q}
key_{n_1} ⋮ $key_{n_{q'}}$
$\mathbf{V}^1$
$\mathbf{V}^2$
key_{n_1} ⋮ $key_{n_{q'}}$
key_{p_1} ⋮ key_{p_q}
$\mathcal{I}$

Figure 8: Initially, a variable gadget contains mainly the sequence V. Property 9a proves that two paths are possible, leading to sequences containing either V^1 or V^2. Along the first (resp. second) path, the locks with indices in P (resp. N) are opened. By Property 9b (resp. c), there exists a path transforming V^1 (resp. V^2) into the identity over $[\![p+1\,;\,p+31]\!]$, which opens the remaining locks.

Proof.

a. $\langle \nu,\, X,\, V,\, Y,\, \Lambda_I^O \rangle$

$$= \langle \boldsymbol{take},\, X,\, \boldsymbol{G},\, E,\, key_{p_1},\, \dots,\, key_{p_q},\, put,\, key_{n_1},\, \dots,\, key_{n_{q'}},\, F,\, \boldsymbol{H},\, Y,\, \Lambda_I^O \rangle$$

$$\underset{6.\mathrm{a}}{\Longrightarrow} \langle \boldsymbol{E},\, key_{p_1},\, \dots,\, key_{p_q},\, put,\, key_{n_1},\, \dots,\, key_{n_{q'}},\, \boldsymbol{F},\, G',\, {}^\star X,\, H',\, Y,\, \Lambda_I^O \rangle$$

$$\underset{7.\mathrm{a}}{\Longrightarrow} \{S_1, S_2\} \quad \text{(where sequences } S_1 \text{ and } S_2 \text{ are described below)}$$

First,

$$S_1 = \langle \boldsymbol{key_{p_1}},\, key_{p_2},\, \dots,\, key_{p_q},\, put,\, key_{n_1},\, \dots,\, key_{n_{q'}},\, F^1,\, G',\, {}^\star X,\, H',\, Y,\, \boldsymbol{\Lambda_I^O} \rangle$$

$$\underset{8.\mathrm{a}}{\Longrightarrow} \langle \boldsymbol{key_{p_2}},\, \dots,\, key_{p_q},\, put,\, key_{n_1},\, \dots,\, key_{n_{q'}},\, F^1,\, G',\, {}^\star X,\, H',\, Y,\, \boldsymbol{\Lambda_I^{O\cup\{p_1\}}} \rangle$$

$$\vdots$$

$$\underset{8.\mathrm{a}}{\Longrightarrow} \langle \boldsymbol{put},\, key_{n_1},\, \dots,\, key_{n_{q'}},\, F^1,\, \boldsymbol{G'},\, {}^\star X,\, \boldsymbol{H'},\, Y,\, \Lambda_I^{O\cup P} \rangle$$

$$\underset{6.\mathrm{b}}{\Longrightarrow} \langle X,\, G'',\, key_{n_1},\, \dots,\, key_{n_{q'}},\, F^1,\, H'',\, Y,\, \Lambda_I^{O\cup P} \rangle$$

$$= \langle X,\, V^1,\, Y,\, \Lambda_I^{O\cup P} \rangle$$

Second,

$$\begin{aligned}
S_2 &= \left\langle \boldsymbol{key_{n_{q'}}},\, key_{n_{q'-1}},\, \ldots,\, key_{n_1},\, put,\, key_{p_q},\, \ldots,\, key_{p_1},\, F^2,\, G',\, {}^\star X,\, H',\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{key_{n_{q'-1}}},\, \ldots,\, key_{n_1},\, put,\, key_{p_q},\, \ldots,\, key_{p_1},\, F^2,\, G',\, {}^\star X,\, H',\, Y,\, \boldsymbol{\Lambda_I^{O\cup\{n_{q'}\}}} \right\rangle \\
&\vdots \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{put},\, key_{p_q},\, \ldots,\, key_{p_1},\, F^2,\, \boldsymbol{G'},\, {}^\star X,\, \boldsymbol{H'},\, Y,\, \Lambda_I^{O\cup N} \right\rangle \\
&\underset{6.b}{\Longrightarrow} \left\langle X,\, G'',\, key_{p_q},\, \ldots,\, key_{p_1},\, F^2,\, H'',\, Y,\, \Lambda_I^{O\cup N} \right\rangle \\
&= \left\langle X,\, V^2,\, Y,\, \Lambda_I^{O\cup N} \right\rangle
\end{aligned}$$

b. $\left\langle V^1,\, X,\, D,\, Y,\, \Lambda_I^O \right\rangle$

$$\begin{aligned}
&= \left\langle \boldsymbol{G''},\, key_{n_1},\, \ldots,\, key_{n_{q'}},\, F^1,\, \boldsymbol{H''},\, X,\, D,\, Y,\, \Lambda_I^O \right\rangle \\
&\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{key_{n_1}},\, key_{n_2},\, \ldots,\, key_{n_{q'}},\, F^1,\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{key_{n_2}},\, \ldots,\, key_{n_{q'}},\, F^1,\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \boldsymbol{\Lambda_I^{O\cup\{n_1\}}} \right\rangle \\
&\vdots \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{F^1},\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \Lambda_I^{O\cup N} \right\rangle \\
&\underset{7.b}{\Longrightarrow} \left\langle \boldsymbol{{}^\star\mathcal{I}_{p+29}^{p+15}},\, \boldsymbol{{}^\star\mathcal{I}_{p+14}^{p+3}},\, X,\, \boldsymbol{D},\, Y,\, \Lambda_I^{O\cup N} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{p+31}^{p+1},\, Y,\, \Lambda_I^{O\cup N} \right\rangle
\end{aligned}$$

c. $\left\langle V^2,\, X,\, D,\, Y,\, \Lambda_I^O \right\rangle$

$$\begin{aligned}
&= \left\langle \boldsymbol{G''},\, key_{p_q},\, \ldots,\, key_{p_1},\, F^2,\, \boldsymbol{H''},\, X,\, D,\, Y,\, \Lambda_I^O \right\rangle \\
&\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{key_{p_q}},\, key_{p_{q-1}},\, \ldots,\, key_{p_1},\, F^2,\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{key_{p_{q-1}}},\, \ldots,\, key_{p_1},\, F^2,\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \boldsymbol{\Lambda_I^{O\cup\{p_q\}}} \right\rangle \\
&\vdots \\
&\underset{8.a}{\Longrightarrow} \left\langle \boldsymbol{F^2},\, {}^\star\mathcal{I}_{p+14}^{p+3},\, X,\, D,\, Y,\, \Lambda_I^{O\cup P} \right\rangle \\
&\underset{7.c}{\Longrightarrow} \left\langle \boldsymbol{{}^\star\mathcal{I}_{p+29}^{p+15}},\, \boldsymbol{{}^\star\mathcal{I}_{p+14}^{p+3}},\, X,\, \boldsymbol{D},\, Y,\, \Lambda_I^{O\cup P} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle X,\, \mathcal{I}_{p+31}^{p+1},\, Y,\, \Lambda_I^{O\cup P} \right\rangle
\end{aligned}$$

□

3.2.3 Clause

The following gadget simulates a 3-clause in a boolean formula. It holds the *test* elements for three locks, corresponding to three literals. When the triggering element, γ, is at the head of a sequence, three distinct efficient paths may be followed. In each such path, one of the three locks is tested: in other words, any efficient path leading to the identity requires one of the locks to be open.

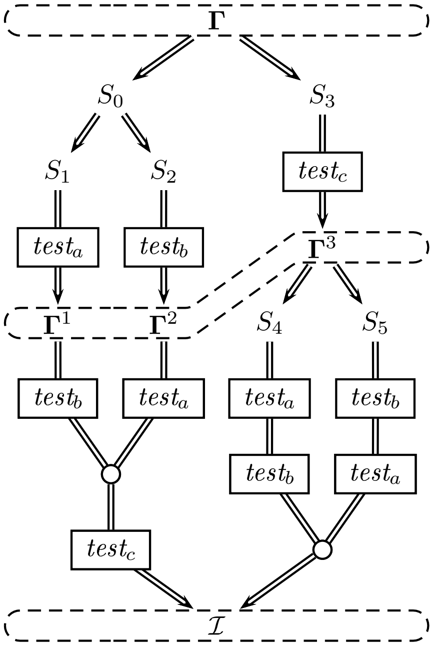


Figure 9: Initially, a clause gadget contains mainly the sequence Γ. Property 10 proves that three paths may be possible, leading to sequences containing either Γ^1, Γ^2 or Γ^3. Because of the *test* elements, each path requires one lock to be open (either a, b or c). By Property 11a (resp. b, c), there exists a path transforming Γ^1 (resp. Γ^2, Γ^3) into the identity over $[\![p+1\,;\,p+62]\!]$, provided the remaining locks are open.

Definition 7. *Let $a, b, c \in [\![1\,;\,m]\!]$ be pairwise distinct integers and p be an integer, $Clause(a, b, c, p)$ is defined by*

$$\begin{array}{rcl}
Clause(a,b,c,p) & = & (\gamma, \Gamma, \Delta) \\
\textit{where} \quad (E_1, F_1) & = & Fork(p+2) \\
(E_2, F_2) & = & Fork(p+45) \\
(take_1, put_1, G_1, H_1) & = & Hook(p+21) \\
(take_2, put_2, G_2, H_2) & = & Hook(p+33) \\
D_1 & = & Dock(p+2, p+17) \\
D_2 & = & Dock(p+21, p+60) \\
\textit{in} \quad \gamma & = & take_1 \\
\Gamma & = & \left\langle G_1,\, E_1,\, take_2,\, put_1,\, test_c,\, F_1,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, H_1 \right\rangle \\
\Delta & = & \left\langle D_1,\, D_2 \right\rangle
\end{array}$$

Given a clause gadget $(\gamma, \Gamma, \Delta) = Clause(a, b, c, p)$, we write

$$\begin{array}{rcl}
\Gamma^1 & = & \left\langle G_1'',\, test_c,\, F_1^1,\, G_2'',\, test_b,\, F_2^1,\, H_2'',\, H_1'' \right\rangle \\
\Gamma^2 & = & \left\langle G_1'',\, test_c,\, F_1^1,\, G_2'',\, test_a,\, F_2^2,\, H_2'',\, H_1'' \right\rangle \\
\Gamma^3 & = & \left\langle G_1'',\, take_2,\, F_1^2,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, H_1'' \right\rangle
\end{array}$$

The following two properties determine the possible behavior of a clause gadget. They are illustrated by Figure 9.

Property 10. *Let X and Y be any sequences, and O, I be two disjoint subsets of $[\![1\,;\,m]\!]$. We have*

$$\begin{array}{c}\gamma\\ X\\ \Gamma\\ Y\\ \Lambda_I^O\end{array} \Longrightarrow \mathbb{T}$$

where $\mathbb{T}$ contains from 0 to 3 sequences, and is defined by:

$$\begin{array}{c}X\\ \Gamma^1\\ Y\\ \Lambda_{I\cup\{a\}}^{O-\{a\}}\end{array} \in \mathbb{T} \textit{ iff } a \in O \qquad \begin{array}{c}X\\ \Gamma^2\\ Y\\ \Lambda_{I\cup\{b\}}^{O-\{b\}}\end{array} \in \mathbb{T} \textit{ iff } b \in O \qquad \begin{array}{c}X\\ \Gamma^3\\ Y\\ \Lambda_{I\cup\{c\}}^{O-\{c\}}\end{array} \in \mathbb{T} \textit{ iff } c \in O$$

Proof.

$$\begin{aligned}
&\big\langle \gamma,\, X,\, \Gamma,\, Y,\, \Lambda_I^O \big\rangle\\
&= \big\langle \boldsymbol{take_1},\, X,\, \boldsymbol{G_1},\, E_1,\, take_2,\, put_1,\, test_c,\, F_1,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, \boldsymbol{H_1},\, Y,\, \Lambda_I^O \big\rangle\\
&\underset{6.\mathrm{a}}{\Longrightarrow} \big\langle \boldsymbol{E_1},\, take_2,\, put_1,\, test_c,\, \boldsymbol{F_1},\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \Lambda_I^O \big\rangle\\
&\underset{7.\mathrm{a}}{\Longrightarrow} \{S_0, S_3\}
\end{aligned}$$

$$\begin{aligned}
S_0 &= \big\langle \boldsymbol{take_2},\, put_1,\, test_c,\, F_1^1,\, \boldsymbol{G_2},\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, \boldsymbol{H_2},\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \Lambda_I^O \big\rangle\\
&\underset{6.\mathrm{a}}{\Longrightarrow} \big\langle \boldsymbol{E_2},\, test_a,\, put_2,\, test_b,\, \boldsymbol{F_2},\, G'_2,\, {}^\star F_1^1,\, test_c,\, put_1,\, H'_2,\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \Lambda_I^O \big\rangle\\
&\underset{7.\mathrm{a}}{\Longrightarrow} \{S_1, S_2\}
\end{aligned}$$

$S_1 = \big\langle \boldsymbol{test_a},\, put_2,\, test_b,\, F_2^1,\, G'_2,\, {}^\star F_1^1,\, test_c,\, put_1,\, H'_2,\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \boldsymbol{\Lambda_I^O} \big\rangle$

if $a \notin O$ then $S_1 \underset{8.\mathrm{c}}{\rightarrow} \perp$

if $a \in O$ then

$$\begin{aligned}
S_1 &\underset{8.\mathrm{b}}{\Longrightarrow} \big\langle \boldsymbol{put_2},\, test_b,\, F_2^1,\, \boldsymbol{G'_2},\, {}^\star F_1^1,\, test_c,\, put_1,\, \boldsymbol{H'_2},\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \big\rangle\\
&\underset{6.\mathrm{b}}{\Longrightarrow} \big\langle \boldsymbol{put_1},\, test_c,\, F_1^1,\, G''_2,\, test_b,\, F_2^1,\, H''_2,\, \boldsymbol{G'_1},\, {}^\star X,\, \boldsymbol{H'_1},\, Y,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \big\rangle\\
&\underset{6.\mathrm{b}}{\Longrightarrow} \big\langle X,\, G''_1,\, test_c,\, F_1^1,\, G''_2,\, test_b,\, F_2^1,\, H''_2,\, H''_1,\, Y,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \big\rangle\\
&= \big\langle X,\, \Gamma^1,\, Y,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \big\rangle
\end{aligned}$$

$S_2 = \big\langle \boldsymbol{test_b},\, put_2,\, test_a,\, F_2^2,\, G'_2,\, {}^\star F_1^1,\, test_c,\, put_1,\, H'_2,\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \boldsymbol{\Lambda_I^O} \big\rangle$

if $b \notin O$ then $S_2 \underset{8.\mathrm{c}}{\rightarrow} \perp$

if $b \in O$ then

$$\begin{aligned}
S_2 &\underset{8.\mathrm{b}}{\Longrightarrow} \big\langle \boldsymbol{put_2},\, test_a,\, F_2^2,\, \boldsymbol{G'_2},\, {}^\star F_1^1,\, test_c,\, put_1,\, \boldsymbol{H'_2},\, G'_1,\, {}^\star X,\, H'_1,\, Y,\, \Lambda_{I\cup\{b\}}^{O-\{b\}} \big\rangle\\
&\underset{6.\mathrm{b}}{\Longrightarrow} \big\langle \boldsymbol{put_1},\, test_c,\, F_1^1,\, G''_2,\, test_a,\, F_2^2,\, H''_2,\, \boldsymbol{G'_1},\, {}^\star X,\, \boldsymbol{H'_1},\, Y,\, \Lambda_{I\cup\{b\}}^{O-\{b\}} \big\rangle\\
&\underset{6.\mathrm{b}}{\Longrightarrow} \big\langle X,\, G''_1,\, test_c,\, F_1^1,\, G''_2,\, test_a,\, F_2^2,\, H''_2,\, H''_1,\, Y,\, \Lambda_{I\cup\{b\}}^{O-\{b\}} \big\rangle\\
&= \big\langle X,\, \Gamma^2,\, Y,\, \Lambda_{I\cup\{b\}}^{O-\{b\}} \big\rangle
\end{aligned}$$

$$S_3 = \left\langle \boldsymbol{test_c},\, put_1,\, take_2,\, F_1^2,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, G_1',\, {}^\star X,\, H_1',\, Y,\, \boldsymbol{\Lambda_I^O} \right\rangle$$

if $c \notin O$ then $S_3 \underset{8.c}{\rightarrow} \bot$

if $c \in O$ then

$$\begin{aligned}
S_3 &\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{put_1},\, take_2,\, F_1^2,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, \boldsymbol{G_1'},\, {}^\star X,\, \boldsymbol{H_1'},\, Y,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \\
&\underset{6.b}{\Longrightarrow} \left\langle X,\, G_1'',\, take_2,\, F_1^2,\, G_2,\, E_2,\, test_a,\, put_2,\, test_b,\, F_2,\, H_2,\, H_1'',\, Y,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \\
&= \left\langle X,\, \Gamma^3,\, Y,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle
\end{aligned}$$

□

Property 11. *Let Y and Z be any sequences, and O, I be two disjoint subsets of $[\![1\,;\,m]\!]$. We have*

$$\textbf{a.}\quad \textit{If } b, c \in O, \textit{ then } \boxed{\begin{array}{c} \Gamma^1 \\ Y \\ \Delta \\ Z \\ \Lambda_I^O \end{array}} \Longrightarrow \boxed{\begin{array}{c} Y \\ \mathcal{I}_{p+62}^{p+1} \\ Z \\ \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \end{array}}$$

$$\textbf{b.}\quad \textit{If } a, c \in O, \textit{ then } \boxed{\begin{array}{c} \Gamma^2 \\ Y \\ \Delta \\ Z \\ \Lambda_I^O \end{array}} \Longrightarrow \boxed{\begin{array}{c} Y \\ \mathcal{I}_{p+62}^{p+1} \\ Z \\ \Lambda_{I\cup\{a,c\}}^{O-\{a,c\}} \end{array}}$$

$$\textbf{c.}\quad \textit{If } a, b \in O, \textit{ then } \boxed{\begin{array}{c} \Gamma^3 \\ Y \\ \Delta \\ Z \\ \Lambda_I^O \end{array}} \Longrightarrow \boxed{\begin{array}{c} Y \\ \mathcal{I}_{p+62}^{p+1} \\ Z \\ \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \end{array}}$$

Proof.

$$\begin{aligned}
\textbf{a.}\quad & \left\langle \Gamma^1,\, Y,\, \Delta,\, Z,\, \Lambda_I^O \right\rangle \\
&= \left\langle \boldsymbol{G_1''},\, test_c,\, F_1^1,\, G_2'',\, test_b,\, F_2^1,\, H_2'',\, \boldsymbol{H_1''},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_I^O \right\rangle \\
&\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{test_c},\, F_1^1,\, G_2'',\, test_b,\, F_2^1,\, H_2'',\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, D_1,\, D_2,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle \\
&\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{F_1^1},\, G_2'',\, test_b,\, F_2^1,\, H_2'',\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \\
&\underset{7.b}{\Longrightarrow} \left\langle \boldsymbol{{}^\star\mathcal{I}_{p+17}^{p+3}},\, G_2'',\, test_b,\, F_2^1,\, H_2'',\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, \boldsymbol{D_1},\, D_2,\, Z,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle \boldsymbol{G_2''},\, test_b,\, F_2^1,\, \boldsymbol{H_2''},\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \Lambda_{I\cup\{c\}}^{O-\{c\}} \right\rangle \\
&\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{test_b},\, F_2^1,\, {}^\star\mathcal{I}_{p+45}^{p+34},\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \boldsymbol{\Lambda_{I\cup\{c\}}^{O-\{c\}}} \right\rangle \\
&\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{F_2^1},\, {}^\star\mathcal{I}_{p+45}^{p+34},\, {}^\star\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \right\rangle \\
&\underset{7.b}{\Longrightarrow} \left\langle \boldsymbol{{}^\star\mathcal{I}_{p+60}^{p+46}},\, \boldsymbol{{}^\star\mathcal{I}_{p+45}^{p+34}},\, \boldsymbol{{}^\star\mathcal{I}_{p+33}^{p+22}},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, \boldsymbol{D_2},\, Z,\, \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle Y,\, \mathcal{I}_{p+19}^{p+1},\, \mathcal{I}_{p+62}^{p+20},\, Z,\, \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \right\rangle \\
&= \left\langle Y,\, \mathcal{I}_{p+62}^{p+1},\, Z,\, \Lambda_{I\cup\{b,c\}}^{O-\{b,c\}} \right\rangle
\end{aligned}$$

b. $\left\langle \Gamma^2,\, Y,\, \Delta,\, Z,\, \Lambda_I^O \right\rangle$

$= \left\langle \boldsymbol{G''_1},\, \mathit{test}_c,\, F_1^1,\, G''_2,\, \mathit{test}_a,\, F_2^2,\, H''_2,\, \boldsymbol{H''_1},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_I^O \right\rangle$

$\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{\mathit{test}_c},\, F_1^1,\, G''_2,\, \mathit{test}_a,\, F_2^2,\, H''_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle$

$\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{F_1^1},\, G''_2,\, \mathit{test}_a,\, F_2^2,\, H''_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda^{O-\{c\}}_{I\cup\{c\}} \right\rangle$

$\underset{7.b}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}^{p+3}_{p+17}},\, G''_2,\, \mathit{test}_a,\, F_2^2,\, H''_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \boldsymbol{D_1},\, D_2,\, Z,\, \Lambda^{O-\{c\}}_{I\cup\{c\}} \right\rangle$

$\underset{4.}{\Longrightarrow} \left\langle \boldsymbol{G''_2},\, \mathit{test}_a,\, F_2^2,\, \boldsymbol{H''_2},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \Lambda^{O-\{c\}}_{I\cup\{c\}} \right\rangle$

$\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{\mathit{test}_a},\, F_2^2,\, {}^{\star}\mathcal{I}^{p+34}_{p+45},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \boldsymbol{\Lambda^{O-\{c\}}_{I\cup\{c\}}} \right\rangle$

$\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{F_2^2},\, {}^{\star}\mathcal{I}^{p+34}_{p+45},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \Lambda^{O-\{a,c\}}_{I\cup\{a,c\}} \right\rangle$

$\underset{7.c}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}^{p+46}_{p+60}},\, \boldsymbol{{}^{\star}\mathcal{I}^{p+34}_{p+45}},\, \boldsymbol{{}^{\star}\mathcal{I}^{p+22}_{p+33}},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, \boldsymbol{D_2},\, Z,\, \Lambda^{O-\{a,c\}}_{I\cup\{a,c\}} \right\rangle$

$\underset{4.}{\Longrightarrow} \left\langle Y,\, \mathcal{I}^{p+1}_{p+19},\, \mathcal{I}^{p+20}_{p+62},\, Z,\, \Lambda^{O-\{a,c\}}_{I\cup\{a,c\}} \right\rangle$

$= \left\langle Y,\, \mathcal{I}^{p+1}_{p+62},\, Z,\, \Lambda^{O-\{a,c\}}_{I\cup\{a,c\}} \right\rangle$

c. $\left\langle \Gamma^3,\, Y,\, \Delta,\, Z,\, \Lambda_I^O \right\rangle$

$= \left\langle \boldsymbol{G''_1},\, \mathit{take}_2,\, F_1^2,\, G_2,\, E_2,\, \mathit{test}_a,\, \mathit{put}_2,\, \mathit{test}_b,\, F_2,\, H_2,\, \boldsymbol{H''_1},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_I^O \right\rangle$

$\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{\mathit{take}_2},\, F_1^2,\, \boldsymbol{G_2},\, E_2,\, \mathit{test}_a,\, \mathit{put}_2,\, \mathit{test}_b,\, F_2,\, \boldsymbol{H_2},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_I^O \right\rangle$

$\underset{6.a}{\Longrightarrow} \left\langle \boldsymbol{E_2},\, \mathit{test}_a,\, \mathit{put}_2,\, \mathit{test}_b,\, \boldsymbol{F_2},\, G'_2,\, {}^{\star}F_1^2,\, H'_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_I^O \right\rangle$

$\underset{7.a}{\Longrightarrow} \{S_4, S_5\}$

$S_4 = \left\langle \boldsymbol{\mathit{test}_a},\, \mathit{put}_2,\, \mathit{test}_b,\, F_2^1,\, G'_2,\, {}^{\star}F_1^2,\, H'_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle$

$\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{\mathit{put}_2},\, \mathit{test}_b,\, F_2^1,\, \boldsymbol{G'_2},\, {}^{\star}F_1^2,\, \boldsymbol{H'_2},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda^{O-\{a\}}_{I\cup\{a\}} \right\rangle$

$\underset{6.b}{\Longrightarrow} \left\langle \boldsymbol{F_1^2},\, G''_2,\, \mathit{test}_b,\, F_2^1,\, H''_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda^{O-\{a\}}_{I\cup\{a\}} \right\rangle$

$\underset{7.c}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}^{p+3}_{p+17}},\, G''_2,\, \mathit{test}_b,\, F_2^1,\, H''_2,\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \boldsymbol{D_1},\, D_2,\, Z,\, \Lambda^{O-\{a\}}_{I\cup\{a\}} \right\rangle$

$\underset{4.}{\Longrightarrow} \left\langle \boldsymbol{G''_2},\, \mathit{test}_b,\, F_2^1,\, \boldsymbol{H''_2},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \Lambda^{O-\{a\}}_{I\cup\{a\}} \right\rangle$

$\underset{6.c}{\Longrightarrow} \left\langle \boldsymbol{\mathit{test}_b},\, F_2^1,\, {}^{\star}\mathcal{I}^{p+34}_{p+45},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \boldsymbol{\Lambda^{O-\{a\}}_{I\cup\{a\}}} \right\rangle$

$\underset{8.b}{\Longrightarrow} \left\langle \boldsymbol{F_2^1},\, {}^{\star}\mathcal{I}^{p+34}_{p+45},\, {}^{\star}\mathcal{I}^{p+22}_{p+33},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, D_2,\, Z,\, \Lambda^{O-\{a,b\}}_{I\cup\{a,b\}} \right\rangle$

$\underset{7.b}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}^{p+46}_{p+60}},\, \boldsymbol{{}^{\star}\mathcal{I}^{p+34}_{p+45}},\, \boldsymbol{{}^{\star}\mathcal{I}^{p+22}_{p+33}},\, Y,\, \mathcal{I}^{p+1}_{p+19},\, \boldsymbol{D_2},\, Z,\, \Lambda^{O-\{a,b\}}_{I\cup\{a,b\}} \right\rangle$

$\underset{4.}{\Longrightarrow} \left\langle Y,\, \mathcal{I}^{p+1}_{p+19},\, \mathcal{I}^{p+20}_{p+62},\, Z,\, \Lambda^{O-\{a,b\}}_{I\cup\{a,b\}} \right\rangle$

$= \left\langle Y,\, \mathcal{I}^{p+1}_{p+62},\, Z,\, \Lambda^{O-\{a,b\}}_{I\cup\{a,b\}} \right\rangle$

$$\begin{aligned}
S_5 &= \left\langle \boldsymbol{test_b},\, put_2,\, test_a,\, F_2^2,\, G_2',\, {}^{\star}F_1^2,\, H_2',\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, D_1,\, D_2,\, Z,\, \boldsymbol{\Lambda_I^O} \right\rangle \\
&\underset{8.\mathrm{b}}{\Longrightarrow} \left\langle \boldsymbol{put_2},\, test_a,\, F_2^2,\, \boldsymbol{G_2'},\, {}^{\star}F_1^2,\, \boldsymbol{H_2'},\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \right\rangle \\
&\underset{6.\mathrm{b}}{\Longrightarrow} \left\langle \boldsymbol{F_1^2},\, G_2'',\, test_a,\, F_2^2,\, H_2'',\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, D_1,\, D_2,\, Z,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \right\rangle \\
&\underset{7.\mathrm{c}}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}_{p+17}^{p+3}},\, G_2'',\, test_a,\, F_2^2,\, H_2'',\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, \boldsymbol{D_1},\, D_2,\, Z,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle \boldsymbol{G_2''},\, test_a,\, F_2^2,\, \boldsymbol{H_2''},\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \Lambda_{I\cup\{a\}}^{O-\{a\}} \right\rangle \\
&\underset{6.\mathrm{c}}{\Longrightarrow} \left\langle \boldsymbol{test_a},\, F_2^2,\, {}^{\star}\mathcal{I}_{p+45}^{p+34},\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \boldsymbol{\Lambda_{I\cup\{a\}}^{O-\{a\}}} \right\rangle \\
&\underset{8.\mathrm{b}}{\Longrightarrow} \left\langle \boldsymbol{F_2^2},\, {}^{\star}\mathcal{I}_{p+45}^{p+34},\, {}^{\star}\mathcal{I}_{p+33}^{p+22},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, D_2,\, Z,\, \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \right\rangle \\
&\underset{7.\mathrm{c}}{\Longrightarrow} \left\langle \boldsymbol{{}^{\star}\mathcal{I}_{p+60}^{p+46}},\, \boldsymbol{{}^{\star}\mathcal{I}_{p+45}^{p+34}},\, \boldsymbol{{}^{\star}\mathcal{I}_{p+33}^{p+22}},\, Y,\, \mathcal{I}_{p+19}^{p+1},\, \boldsymbol{D_2},\, Z,\, \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \right\rangle \\
&\underset{4.}{\Longrightarrow} \left\langle Y,\, \mathcal{I}_{p+19}^{p+1},\, \mathcal{I}_{p+62}^{p+20},\, Z,\, \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \right\rangle \\
&= \left\langle Y,\, \mathcal{I}_{p+62}^{p+1},\, Z,\, \Lambda_{I\cup\{a,b\}}^{O-\{a,b\}} \right\rangle
\end{aligned}$$

□

3.3 Reduction

Let ϕ be a boolean formula over l variables in conjunctive normal form, such that each clause contains exactly three literals. We write k the number of clauses, $m = 3k$ the total number of literals, and $\{\lambda_1, \dots, \lambda_m\}$ the set of literals. Let $n = 31l + 62k + 12m$ (thus, $n = 31l + 98k$).

Definition 8. *We define the sequence S_ϕ as the permutation of $[\![1\,;\,n]\!]$ obtained by:*

$$\begin{aligned}
&(key_1, \dots, key_m, test_1, \dots, test_m, \Lambda) = \mathit{Literals}(31l + 62k, m) \\
&\textit{For all } i \in [\![1\,;\,l]\!] \\
&\quad P_i = \{ j \in [\![1\,;\,m]\!] \mid \lambda_j = x_i \} \\
&\quad N_i = \{ j \in [\![1\,;\,m]\!] \mid \lambda_j = \neg x_i \} \\
&\quad (\nu_i, V_i, D_i) = \mathit{Variable}(P_i, N_i, 31(i-1)) \\
&\textit{For all } i \in [\![1\,;\,k]\!] \\
&\quad (a_i, b_i, c_i) = \textit{ indices such that the i-th clause of } \phi \textit{ is } \lambda_{a_i} \vee \lambda_{b_i} \vee \lambda_{c_i} \\
&\quad (\gamma_i, \Gamma_i, \Delta_i) = \mathit{Clause}(a_i, b_i, c_i, 31l + 62(i-1)) \\
&S_\phi = \left\langle \nu_1, \dots, \nu_l, \gamma_1, \dots, \gamma_k, V_1, \dots, V_l, \Gamma_1, \dots, \Gamma_k, D_1, \dots, D_l, \Delta_1, \dots, \Delta_k, \Lambda_\emptyset^\emptyset \right\rangle
\end{aligned}$$

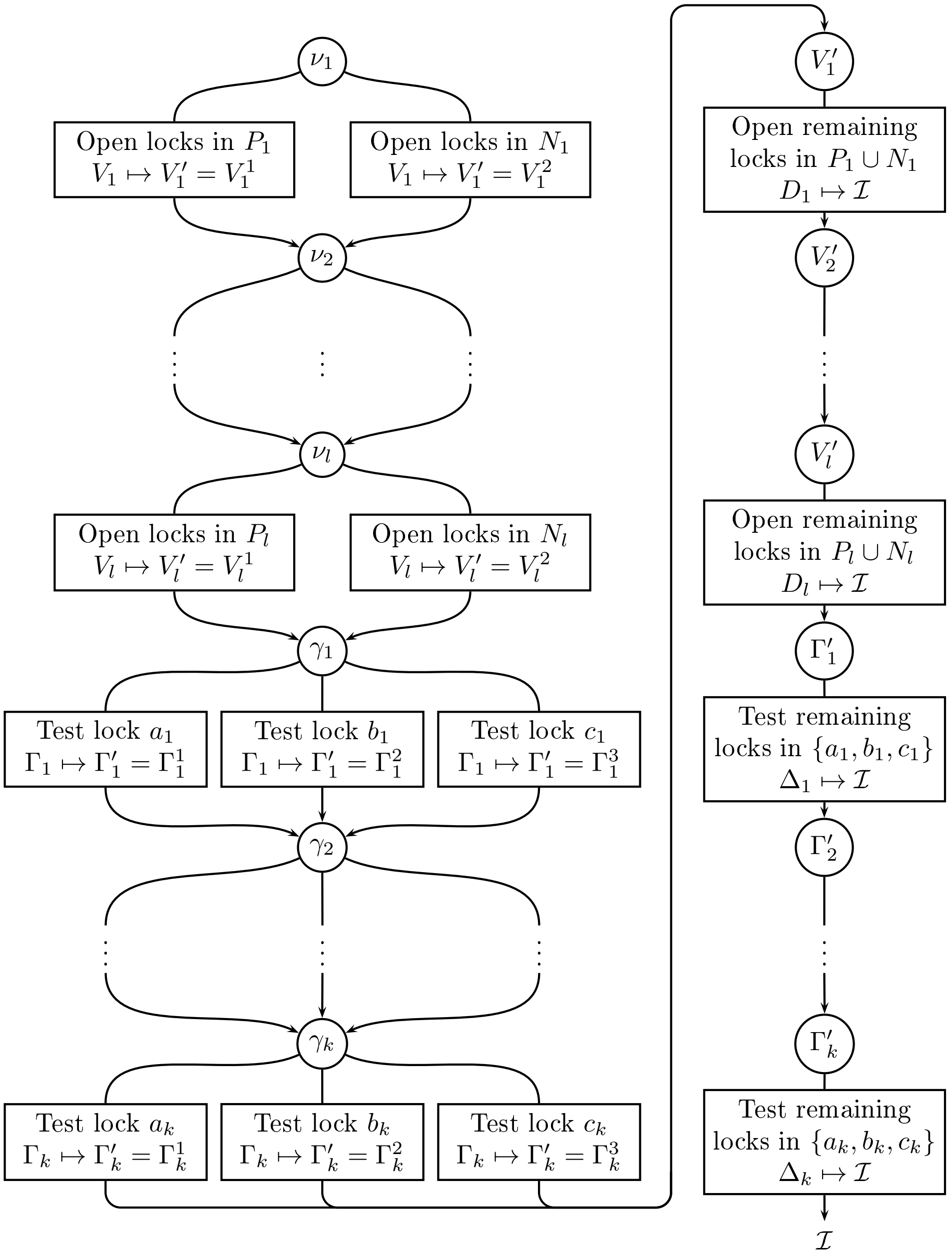
Two things should be noted in this definition. First, elements key_i and $test_i$ are used in the clause and variable gadgets, although they are not explicitly stated in the parameters (cf. Definitions 6 and 7). Second, one could assume that literals are sorted in the formula ($\phi = (\lambda_1 \vee \lambda_2 \vee \lambda_3) \wedge \dots$), so that $a_i = 3i - 2$, $b_i = 3i - 1$ and $c_i = 3i$, but it is not necessary since these values are not used in the following.

We now aim at proving Theorem 18 (p. 25), which states that S_ϕ is efficiently sortable if and only if the formula ϕ is satisfiable. Several preliminary lemmas are necessary, and the overall process is illustrated in Figure 10.

3.3.1 Variable assignment

Definition 9. *Let $r \in [\![0\,;\,l]\!]$. An* r-assignment *is a partition $\mathcal{P} = (T, F)$ of $[\![1\,;\,r]\!]$. An l-assignment is called a* full *assignment. Using notations from Definition 8, we define the sequence $S_\phi[\mathcal{P}]$ by:*

$$S_\phi = \left\langle \nu_1,\dots,\nu_l,\gamma_1,\dots,\gamma_k,V_1,\dots,V_l,\Gamma_1,\dots,\Gamma_k,D_1,\dots,D_l,\Delta_1,\dots,\Delta_k,\Lambda^{\emptyset}_{\emptyset}\right\rangle$$



ν_1
Open locks in P_1 $V_1 \mapsto V_1' = V_1^1$
Open locks in N_1 $V_1 \mapsto V_1' = V_1^2$
ν_2
ν_l
Open locks in P_l $V_l \mapsto V_l' = V_l^1$
Open locks in N_l $V_l \mapsto V_l' = V_l^2$
γ_1
Test lock a_1 $\Gamma_1 \mapsto \Gamma_1' = \Gamma_1^1$
Test lock b_1 $\Gamma_1 \mapsto \Gamma_1' = \Gamma_1^2$
Test lock c_1 $\Gamma_1 \mapsto \Gamma_1' = \Gamma_1^3$
γ_2
γ_k
Test lock a_k $\Gamma_k \mapsto \Gamma_k' = \Gamma_k^1$
Test lock b_k $\Gamma_k \mapsto \Gamma_k' = \Gamma_k^2$
Test lock c_k $\Gamma_k \mapsto \Gamma_k' = \Gamma_k^3$
V_1'
Open remaining locks in $P_1 \cup N_1$ $D_1 \mapsto \mathcal{I}$
V_2'
V_l'
Open remaining locks in $P_l \cup N_l$ $D_l \mapsto \mathcal{I}$
Γ_1'
Test remaining locks in $\{a_1, b_1, c_1\}$ $\Delta_1 \mapsto \mathcal{I}$
Γ_2'
Γ_k'
Test remaining locks in $\{a_k, b_k, c_k\}$ $\Delta_k \mapsto \mathcal{I}$
$\mathcal{I}$

Figure 10: Description of an efficient sorting of S_ϕ. Circular nodes correspond to head elements or sequences especially relevant (landmarks). We start with the head element of S_ϕ: ν_1. From each landmark, one, two or three paths are possible before reaching the next landmark, each path having its own effects, stated in rectangles, on the sequence. Possible effects are: transforming a subsequence of S_ϕ (symbol $\mapsto$), opening a lock, testing a lock (such a path requires the lock to be open). The top-left quarter, from ν_1 to ν_l, is studied in Section 3.3.1; the bottom-left quarter, from γ_1 to γ_k, is studied in Section 3.3.2; and the right half, from V_1' to Γ_k', is studied in Section 3.3.3. Indices are removed from identity sequences ($\mathcal{I}$) for readability.

$$\textit{For all } i \in [\![1\,;\,r]\!]\,, \quad V_i' = \begin{cases} V_i^1 \textit{ if } i \in T \\ V_i^2 \textit{ if } i \in F \end{cases}$$

$$O = \bigcup_{i \in T} P_i \cup \bigcup_{i \in F} N_i$$

$$S_\phi[\mathcal{P}] = \big\langle \nu_{r+1}, \ldots, \nu_l, \gamma_1, \ldots, \gamma_k, V_1', \ldots, V_r', V_{r+1}, \ldots, V_l, \\ \Gamma_1, \ldots, \Gamma_k, D_1, \ldots, D_l, \Delta_1, \ldots, \Delta_k, \Lambda_\emptyset^O \big\rangle$$

Property 12. *Let $r \in [\![0\,;\,l]\!]$ with $r < l$, $\mathcal{P} = (T, F)$ be any r-assignment, $\mathcal{P}_1 = (T \cup \{r+1\}, F)$ and $\mathcal{P}_2 = (T, F \cup \{r+1\})$. Then*

$$S_\phi[\mathcal{P}] \Longrightarrow \{S_\phi[\mathcal{P}_1], S_\phi[\mathcal{P}_2]\}$$

Proof. This is a direct application of Property 9.a on variable $(\nu_{r+1}, V_{r+1}, D_{r+1})$, using sequences:

$$X = \big\langle \nu_{r+2}, \ldots, \nu_l, \gamma_1, \ldots, \gamma_k, V_1', \ldots, V_r' \big\rangle$$
$$Y = \big\langle V_{r+2}, \ldots, V_l, \Gamma_1, \ldots, \Gamma_k, D_1, \ldots, D_l, \Delta_1, \ldots, \Delta_k \big\rangle$$

□

With the following lemma, we ensure that any sequence of efficient flips from S_ϕ begins with a full assignment of the boolean variables, and every possible assignment can be reached using only efficient flips.

Lemma 13.

$$S_\phi \Longrightarrow \{S_\phi[\mathcal{P}] \mid \mathcal{P} \textit{ full assignment}\}$$

Proof. We prove $S_\phi \Longrightarrow \{S_\phi[\mathcal{P}] \mid \mathcal{P}\ r-\text{assignment}\}$ by induction for all $r \in [\![0\,;\,l]\!]$, and the lemma is deduced from the case $r = l$.

There is only one 0-assignment, which is $\mathcal{P}_0 = (\emptyset, \emptyset)$, and $S_\phi = S_\phi[\mathcal{P}_0]$. Consider now any $r < l$. We use notations $\mathcal{P}_1$ and $\mathcal{P}_2$ from Property 12. Then any $(r+1)$-assignment can be written $\mathcal{P}_1$ or $\mathcal{P}_2$, where $\mathcal{P}$ is some r-assignment. We have

$$S_\phi \Longrightarrow \{S_\phi[\mathcal{P}] \mid \mathcal{P}\ r\text{-assignment}\} \text{ by induction hypothesis}$$
$$S_\phi \Longrightarrow \{S_\phi[\mathcal{P}_1], S_\phi[\mathcal{P}_2] \mid \mathcal{P}\ r\text{-assignment}\} \text{ by Property 12}$$
$$= \{S_\phi[\mathcal{P}'] \mid \mathcal{P}'\ (r+1)\text{-assignment}\}$$

□

3.3.2 Going through clauses

Now that each variable is assigned a boolean value, we need to verify with each clause that this assignment satisfies the formula ϕ. This is done by selecting, for each clause, a literal which is true, and testing the corresponding lock. As in Definition 8, for any $i \in [\![1\,;\,k]\!]$ we write (a_i, b_i, c_i) the indices such that the i-th clause of ϕ is $\lambda_{a_i} \vee \lambda_{b_i} \vee \lambda_{c_i}$ (thus, $a_i, b_i, c_i \in [\![1\,;\,m]\!]$).

Definition 10. *Let $t \in [\![0\,;\,k]\!]$ and $\mathcal{P}$ be a full assignment. A* t-selection *σ is a subset of $[\![1\,;\,m]\!]$ such that*

- $|\sigma| = t$
- *for each $i \in [\![1\,;\,t]\!]$, $|\{a_i, b_i, c_i\} \cap \sigma| = 1$*

A t-selection σ and a full assignment $\mathcal{P} = (T, F)$ are compatible*, if, for every $i \in \sigma$, literal λ_i is true according to assignment $\mathcal{P}$ (that is, $\lambda_i = x_j$ and $j \in T$, or $\lambda_i = \neg x_j$ and $j \in F$).*

A k-selection is called a full *selection. Given a t-selection σ and a full assignment $\mathcal{P} = (T, F)$ which are compatible, we define the sequence $S_\phi[\mathcal{P}, \sigma]$ by:*

$$\text{For all } i \in [\![1\,;\,l]\!]\,, \quad V'_i = \begin{cases} V_i^1 \text{ if } i \in T \\ V_i^2 \text{ if } i \in F \end{cases}$$

$$\text{For all } i \in [\![1\,;\,t]\!]\,, \quad \Gamma'_i = \begin{cases} \Gamma_i^1 \text{ if } a_i \in \sigma \\ \Gamma_i^2 \text{ if } b_i \in \sigma \\ \Gamma_i^3 \text{ if } c_i \in \sigma \end{cases}$$

$$O = \bigcup_{i \in T} P_i \cup \bigcup_{i \in F} N_i - \sigma$$

$$I = \sigma$$

$$S_\phi[\mathcal{P}, \sigma] = \left\langle \gamma_{t+1}, \ldots, \gamma_k, V'_1, \ldots, V'_l, \Gamma'_1, \ldots, \Gamma'_t, \Gamma_{t+1}, \ldots, \Gamma_k, D_1, \ldots, D_l, \Delta_1, \ldots, \Delta_k, \Lambda_I^O \right\rangle$$

Property 14. *Let $\mathcal{P}$ be a full assignment and $t \in [\![0\,;\,k]\!]$, $t < k$. Let σ' be a $(t+1)$-selection compatible with $\mathcal{P}$, then there exists a t-selection σ compatible with $\mathcal{P}$ such that $\sigma \subset \sigma'$.*

Proof. It is obtained by $\sigma = \sigma' - \{a_{t+1}, b_{t+1}, c_{t+1}\}$. It is trivially a t-selection included in σ, and it is compatible with $\mathcal{P}$ (all selected literals in σ are also selected in σ', and thus are true according to $\mathcal{P}$). □

Property 15. *Let $t \in [\![0\,;\,k]\!]$, $t < k$, $\mathcal{P}$ be a full assignment, and σ be a t-selection compatible with $\mathcal{P}$.*

$$S_\phi[\mathcal{P}, \sigma] \Longrightarrow \{S_\phi[\mathcal{P}, \sigma'] \mid \sigma' \ (t+1)\text{-selection compatible with } \mathcal{P}; \sigma \subset \sigma'\}$$

Note that the right-hand side can be the empty set, in which case $S_\phi[\mathcal{P}, \sigma] \Longrightarrow \emptyset$.

Proof. First note that there are 3 $(t+1)$-selections such that $\sigma \subset \sigma'$, and they are $\sigma'_1 = \sigma \cup \{a_{t+1}\}$, $\sigma'_2 = \sigma \cup \{b_{t+1}\}$, and $\sigma'_3 = \sigma \cup \{c_{t+1}\}$. Since σ is compatible with $\mathcal{P}$, σ'_1 is compatible with $\mathcal{P}$ iff literal $\lambda_{a_{t+1}}$ is true in $\mathcal{P}$ (and similarly with couples $(\sigma'_2, \lambda_{b_{t+1}})$ and $(\sigma'_3, \lambda_{c_{t+1}})$). We now define sequences X and Y and sets I and O such that $S_\phi[\mathcal{P}, \sigma] = \left\langle \gamma_{t+1},\, X,\, \Gamma_{t+1},\, Y,\, \Lambda_I^O \right\rangle$, that is:

$$X = \left\langle \gamma_{t+2}, \ldots, \gamma_k, V'_1, \ldots, V'_l, \Gamma'_1, \ldots, \Gamma'_t \right\rangle$$

$$Y = \left\langle \Gamma_{t+2}, \ldots, \Gamma_k, D_1, \ldots, D_l, \Delta_1, \ldots, \Delta_k, \right\rangle$$

$$O = \bigcup_{i \in T} P_i \cup \bigcup_{i \in F} N_i - \sigma$$

$$I = \sigma$$

Using Property 10 on clause gadget $(\gamma_{t+1}, \Gamma_{t+1}, \Delta_{t+1})$, we obtain:

$$S_\phi[\mathcal{P}, \sigma] \Longrightarrow \mathbb{T}$$

where $\mathbb{T}$ is defined by:

$$\left\langle X,\, \Gamma_{t+1}^1,\, Y,\, \Lambda_{I \cup \{a_{t+1}\}}^{O - \{a_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad a_{t+1} \in O$$

$$\left\langle X,\, \Gamma_{t+1}^2,\, Y,\, \Lambda_{I \cup \{b_{t+1}\}}^{O - \{b_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad b_{t+1} \in O$$

$$\left\langle X,\, \Gamma_{t+1}^3,\, Y,\, \Lambda_{I \cup \{c_{t+1}\}}^{O - \{c_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad c_{t+1} \in O$$

Note that $a_{t+1} \notin \sigma$, hence $a_{t+1} \in O$ iff $\exists i \in T$ s.t. $a_{t+1} \in P_i$ or $\exists i \in F$ s.t. $a_{t+1} \in N_i$. Equivalently, $a_{t+1} \in O$ iff $\lambda_{a_{t+1}}$ is a positive occurrence of a variable assigned True in $\mathcal{P}$, or a negative occurrence of a variable assigned False in $\mathcal{P}$. Finally, $a_{t+1} \in O$ iff σ'_1 is compatible with $\mathcal{P}$. Likewise, $b_{t+1} \in O$ iff σ'_2 is compatible with $\mathcal{P}$, and $c_{t+1} \in O$ iff σ'_3 is compatible with $\mathcal{P}$.

$$\begin{aligned}
S_\phi[\mathcal{P}, \sigma'_1] &= \left\langle X,\, \Gamma^1_{t+1},\, Y,\, \Lambda^{O-\{a_{t+1}\}}_{I\cup\{a_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad \sigma'_1 \text{ is compatible with } \mathcal{P} \\
S_\phi[\mathcal{P}, \sigma'_2] &= \left\langle X,\, \Gamma^2_{t+1},\, Y,\, \Lambda^{O-\{b_{t+1}\}}_{I\cup\{b_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad \sigma'_2 \text{ is compatible with } \mathcal{P} \\
S_\phi[\mathcal{P}, \sigma'_3] &= \left\langle X,\, \Gamma^3_{t+1},\, Y,\, \Lambda^{O-\{c_{t+1}\}}_{I\cup\{a_{t+1}\}} \right\rangle \in \mathbb{T} \quad \text{iff} \quad \sigma'_3 \text{ is compatible with } \mathcal{P}
\end{aligned}$$

Thus $\mathbb{T}$ is indeed the set of sequences $S_\phi[\mathcal{P}, \sigma']$ where σ' is a $(t+1)$-selection which contains σ and is compatible with $\mathcal{P}$: the property is proved. □

With the following lemma, we ensure that after the truth assignment, every efficient path starting from S_ϕ needs to select a literal in each clause, under the constraint that the selection is compatible with the assignment.

Lemma 16. *Let $\mathcal{P}$ be a full assignment. Then*

$$S_\phi[\mathcal{P}] \Longrightarrow \{S_\phi[\mathcal{P}, \sigma] \mid \sigma \textit{ full selection compatible with } \mathcal{P}\}$$

Proof. The proof follows the same pattern as the one of Lemma 13, that is, we prove

$$S_\phi[\mathcal{P}] \Longrightarrow \{S_\phi[\mathcal{P}, \sigma] \mid \sigma \text{ } t\text{-selection compatible with } \mathcal{P}\}$$

by induction for all $t \in [\![0\,;\,k]\!]$, and the lemma is deduced from the case $t = k$.

There is only one 0-selection, which is $\sigma_0 = \emptyset$, it is compatible with $\mathcal{P}$, and $S_\phi[\mathcal{P}] = S_\phi[\mathcal{P}, \sigma_0]$. Consider now any $t < k$. We have

$$\begin{aligned}
S_\phi[\mathcal{P}] &\Longrightarrow \{S_\phi[\mathcal{P}, \sigma] \mid \sigma \text{ } t\text{-selection compatible with } \mathcal{P}\} \text{ (by induction hypothesis)} \\
S_\phi[\mathcal{P}] &\Longrightarrow \{S_\phi[\mathcal{P}, \sigma'] \mid \sigma' \text{ } (t+1)\text{-selection compatible with } \mathcal{P} \text{ and} \\
&\qquad\qquad \exists \sigma \text{ } t\text{-selection compatible with } \mathcal{P},\, \sigma \subset \sigma'\} \text{ by Property 15} \\
&= \{S_\phi[\mathcal{P}, \sigma'] \mid \sigma' \text{ } (t+1)\text{-selection compatible with } \mathcal{P}\} \text{ by Property 14}
\end{aligned}$$

□

3.3.3 Beyond clauses

Lemma 17. *Let $\mathcal{P}$ be a full assignment and σ be a full selection, such that $\mathcal{P}$ and σ are compatible (provided such a pair exists for ϕ). Then*

$$S_\phi[\mathcal{P}, \sigma] \Longrightarrow \mathcal{I}^1_n$$

Proof. Write $\mathcal{P} = (T, F)$. Since σ is a full selection, $S_\phi[\mathcal{P}, \sigma]$ can be written (see Definition 10):

$$\begin{aligned}
&\text{For all } i \in [\![1\,;\,l]\!]\,, \quad V'_i = \begin{cases} V^1_i \text{ if } i \in T \\ V^2_i \text{ if } i \in F \end{cases} \\
&\text{For all } i \in [\![1\,;\,k]\!]\,, \quad \Gamma'_i = \begin{cases} \Gamma^1_i \text{ if } a_i \in \sigma \\ \Gamma^2_i \text{ if } b_i \in \sigma \\ \Gamma^3_i \text{ if } c_i \in \sigma \end{cases} \\
&O = \bigcup_{i \in T} P_i \cup \bigcup_{i \in F} N_i - \sigma \\
&I = \sigma \\
&S_\phi[\mathcal{P}, \sigma] = \left\langle V'_1, \ldots, V'_l, \Gamma'_1, \ldots, \Gamma'_k, D_1, \ldots, D_l, \Delta_1, \ldots, \Delta_k, \Lambda^O_I \right\rangle
\end{aligned}$$

We extend the definition of set O to O_r, for any $r \in \llbracket 0\,;\,l \rrbracket$, as follows:

$$O_r = \bigcup_{0<i\leq r} (P_i \cup N_i) \cup \bigcup_{i\in T} P_i \cup \bigcup_{i \in F} N_i - \sigma$$

Note that $O_0 = O$, and that $O_l = \llbracket 1\,;\,m \rrbracket - \sigma$.

$$\begin{aligned}
S_\phi[\mathcal{P},\sigma] &= \left\langle \boldsymbol{V_1'}, \dots, V_l', \Gamma_1', \dots, \Gamma_k', \boldsymbol{D_1}, \dots, D_l, \Delta_1, \dots, \Delta_k, \boldsymbol{\Lambda_I^{O_0}} \right\rangle \\
&\underset{9.\text{b/c}}{\Longrightarrow} \left\langle \boldsymbol{V_2'}, \dots, V_l', \Gamma_1', \dots, \Gamma_k', \mathcal{I}_{31}^1, \boldsymbol{D_2} \dots, D_l, \Delta_1, \dots, \Delta_k, \boldsymbol{\Lambda_I^{O_1}} \right\rangle \\
&\underset{9.\text{b/c}}{\Longrightarrow} \left\langle \boldsymbol{V_3'}, \dots, V_l', \Gamma_1', \dots, \Gamma_k', \mathcal{I}_{31}^1, \mathcal{I}_{62}^{32}, \boldsymbol{D_3} \dots, D_l, \Delta_1, \dots, \Delta_k, \boldsymbol{\Lambda_I^{O_2}} \right\rangle \\
&\dots \\
&\underset{9.\text{b/c}}{\Longrightarrow} \left\langle \Gamma_1', \dots, \Gamma_k', \boldsymbol{\mathcal{I}_{31}^1, \mathcal{I}_{62}^{32}, \dots, \mathcal{I}_{31l}^{31l-30}}, \Delta_1, \dots, \Delta_k, \Lambda_I^{O_l} \right\rangle \\
&= \left\langle \Gamma_1', \dots, \Gamma_k', \mathcal{I}_{31l}^1, \Delta_1, \dots, \Delta_k, \Lambda_I^{O_l} \right\rangle
\end{aligned}$$

Finally, for the last part, we use a similar procedure, with the following sets, for $t \in \llbracket 0\,;\,k \rrbracket$:

$$\begin{aligned}
O_t' &= \llbracket 1\,;\,m \rrbracket - \left(\sigma \cup \bigcup_{0<i\leq t} \{a_i, b_i, c_i\} \right) \\
I_t' &= \sigma \cup \bigcup_{0<i\leq t} \{a_i, b_i, c_i\}
\end{aligned}$$

Note that $O_0' = O_l$, $I_0' = I$, $O_k' = \emptyset$, $I_k' = \llbracket 1\,;\,m \rrbracket$, and more importantly, for $i > t$, assuming that $a_i \in \sigma$ (cases $b_i \in \sigma$ and $c_i \in \sigma$ are similar), then $a_i \in I_t'$, $b_i \in O_t'$ and $c_i \in O_t'$. Hence we can successively apply Property 11 (either .a, .b or .c) on each clause gadgets.

$$\begin{aligned}
&\left\langle \boldsymbol{\Gamma_1'}, \dots, \Gamma_k', \mathcal{I}_{31l}^1, \boldsymbol{\Delta_1}, \dots, \Delta_k, \boldsymbol{\Lambda_{I_0'}^{O_0'}} \right\rangle \\
&\underset{11.}{\Longrightarrow} \left\langle \boldsymbol{\Gamma_2'}, \dots, \Gamma_k', \mathcal{I}_{31l}^1, \mathcal{I}_{31l+62}^{31l+1}, \boldsymbol{\Delta_2}, \dots, \Delta_k, \boldsymbol{\Lambda_{I_1'}^{O_1'}} \right\rangle \\
&\underset{11.}{\Longrightarrow} \left\langle \boldsymbol{\Gamma_3'}, \dots, \Gamma_k', \mathcal{I}_{31l}^1, \mathcal{I}_{31l+62}^{31l+1}, \mathcal{I}_{31l+124}^{31l+63}, \boldsymbol{\Delta_3}, \dots, \Delta_k, \boldsymbol{\Lambda_{I_2'}^{O_2'}} \right\rangle \\
&\dots \\
&\underset{11.}{\Longrightarrow} \left\langle \mathcal{I}_{31l}^1, \boldsymbol{\mathcal{I}_{31l+62}^{31l+1}, \mathcal{I}_{31l+124}^{31l+63}, \dots, \mathcal{I}_{31l+62k}^{31l+62k-61}}, \Lambda_{I_k'}^{O_k'} \right\rangle \\
&= \left\langle \mathcal{I}_{31l}^1, \mathcal{I}_{31l+62k}^{31l+1}, \Lambda_{\llbracket 1\,;\,m \rrbracket}^{\emptyset} \right\rangle \\
&= \left\langle \mathcal{I}_{31l}^1, \mathcal{I}_{31l+62k}^{31l+1}, \mathcal{I}_{31l+62k+12m}^{31l+62k+1} \right\rangle \\
&= \mathcal{I}_n^1
\end{aligned}$$

□

Theorem 18.

$$S_\phi \Longrightarrow \mathcal{I}_n^1 \textit{ iff } \phi \textit{ is satisfiable.}$$

Proof. Assume first that $S_\phi \Longrightarrow \mathcal{I}_n^1$. By Lemma 13, since $S_\phi \Longrightarrow \{S_\phi[\mathcal{P}] \mid \mathcal{P}$ full assignment$\}$, there exists a full assignment $\mathcal{P} = (T, F)$ such that the path from S_ϕ to the identity uses $S_\phi[\mathcal{P}]$. Note that $S_\phi[\mathcal{P}] \Longrightarrow \mathcal{I}_n^1$. Now, by Lemma 16, since $S_\phi[\mathcal{P}] \Longrightarrow \{S_\phi[\mathcal{P}, \sigma] \mid \sigma$ full selection compatible with $\mathcal{P}\}$, there exists a full selection σ, compatible with $\mathcal{P}$, such that the path from $S_\phi[\mathcal{P}]$ to the identity uses $S_\phi[\mathcal{P}, \sigma]$. Consider the truth assignment $x_i :=$ True $\Leftrightarrow i \in T$. Then each clause of ϕ contains at least one literal that is true (the literal whose index is in σ), and thus ϕ is satisfiable.

Assume now that ϕ is satisfiable: consider any truth assignment making ϕ true, write T the set of indices such that $x_i =$ True, and $F = [\![1\,;\,l]\!] - T$. Write also σ a set containing, for each clause of ϕ, the index of one literal being true under this assignment. Then σ is a full selection, compatible with the full assignment $\mathcal{P} = (T, F)$. By Lemma 13, there exists an efficient path from S_ϕ to $S_\phi[\mathcal{P}]$. By Lemma 16, there exists an efficient path from $S_\phi[\mathcal{P}]$ to $S_\phi[\mathcal{P}, \sigma]$. And by Lemma 17, there exists an efficient path from $S_\phi[\mathcal{P}, \sigma]$ to the identity. Thus sequence S_ϕ is efficiently sortable. □

Using Theorem 18, we can now prove the main result of the paper.

Theorem 19. *The following problems are* NP*-hard:*

- *Sorting By Prefix Reversals (MIN-SBPR)*
- *deciding, given a sequence S, whether S can be sorted in $d_b(S)$ flips*

Proof. By reduction from 3-SAT. Given any formula ϕ, create S_ϕ (see Definition 8, the construction requires a linear time). By Theorem 18, the minimum number of flips necessary to sort S_ϕ is $d_b(S_\phi)$ iff ϕ is satisfiable. □

4 Conclusion

In this paper, we have shown that the Pancake Flipping problem is NP-hard, thus answering a long-standing open question. We have also provided a stronger result, namely, deciding whether a permutation can be sorted with no more than one flip per breakpoint is also NP-hard.

Among related important problems, the last one having an open complexity is now the burnt variant of the Pancake Flipping problem. An interesting insight into this problem is given in a recent work from Labarre and Cibulka [13], where the authors characterize a subclass of permutations that can be sorted in polynomial time, using the breakpoint graph [1]. Another development consists in trying to improve the approximation ratio of 2 for the Pancake Flipping problem, both in its burnt and unburnt versions.

References

[1] V. Bafna and P. Pevzner. Genome rearrangements and sorting by reversals. In *FOCS*, pages 148–157. IEEE, 1993.

[2] P. Berman, S. Hannenhalli, and M. Karpinski. 1.375-approximation algorithm for sorting by reversals. In R. Möhring and R. Raman, editors, *ESA*, volume 2461 of *Lecture Notes in Computer Science*, pages 200–210. Springer, 2002.

[3] P. Berman and M. Karpinski. On some tighter inapproximability results (extended abstract). In J. Wiedermann, P. van Emde Boas, and M. Nielsen, editors, *ICALP*, volume 1644 of *Lecture Notes in Computer Science*, pages 200–209. Springer, 1999.

[4] B. Chitturi, W. Fahle, Z. Meng, L. Morales, C.O. Shields, I. Sudborough, and W. Voit. An $(18/11)n$ upper bound for sorting by prefix reversals. *Theoretical Computer Science*, 410(36):3372–3390, 2009.

[5] J. Cibulka. On average and highest number of flips in pancake sorting. *Theoretical Computer Science*, 412(8-10):822–834, 2011.

[6] D. Cohen and M. Blum. On the problem of sorting burnt pancakes. *Discrete Applied Mathematics*, 61(2):105–120, 1995.

[7] H. Dweighter. *American Mathematics Monthly*, 82(1), 1975.

[8] J. Fischer and S. Ginzinger. A 2-approximation algorithm for sorting by prefix reversals. In G. S. Brodal and S. Leonardi, editors, *ESA*, volume 3669 of *Lecture Notes in Computer Science*, pages 415–425. Springer, 2005.

[9] W. Gates and C. Papadimitriou. Bounds for sorting by prefix reversal. *Discrete Mathematics*, 27(1):47–57, 1979.

[10] S. Hannenhalli and P. Pevzner. Transforming cabbage into turnip: polynomial algorithm for sorting signed permutations by reversals. In *STOC*, pages 178–189. ACM, 1995.

[11] M. Heydari and I. Sudborough. On sorting by prefix reversals and the diameter of pancake networks. In *Proceedings of the First Heinz Nixdorf Symposium on Parallel Architectures and Their Efficient Use*, pages 218–227, London, UK, 1993. Springer-Verlag.

[12] M. Heydari and I. Sudborough. On the diameter of the pancake network. *Journal of Algorithms*, 25(1):67–94, October 1997.

[13] A. Labarre and J. Cibulka. Polynomial-time sortable stacks of burnt pancakes. *Theoretical Computer Science*, 412(8-10):695–702, 2011.