Undecidability in Topology

Francis Lazarus and Arnaud de Mesmay

November 26, 2020

Contents

The purpose of this lecture is to make explicit the limits of computational topology by showing that some simple and natural questions in topology are undecidable. In order to make the statement precise we need to define the notion of decidability and to specify the description of topological spaces we are interested in. Concerning topological spaces we should consider spaces having a combinatorial description such as finite simplicial complexes[1]. Note that many interesting spaces have such a description: compact topological manifolds of dimensions 2 or 3, compact differentiable manifolds, etc. See [Man14] for a survey. Concerning decidability there are essentially two notions. One refers to the independence of a statement with respect to a logical system. In other words, the statement is undecidable if neither its affirmation nor its negation can be proved from the axioms of the system using its logical rules. The existence of such undecidable statements relates to the first Gödel's incompleteness theorem. The other notion of decidability refers to a family of problems with YES/NO answers, such as testing a property over a family of objects, and expresses the existence of an algorithm to output the answer of any problem in the family. Note that any finite family of problems for which the answers is provable is always decidable

[1] Recall that a simplicial complex is a collection of simplices glued in a nice fashion. It is the total space of an *abstract simplicial complex* over a set V, which is a family of subsets of V closed under the operation of taking non-empty subsets.

in this acception. Indeed, an algorithm to solve the problems just needs to store the correct answer of each problem. Paradoxically, this is valid even if we do not know yet the correct answers since the decidability only claims the existence of an algorithm and not the algorithm itself.

Both notions of decidability may be relevant to computational topology. As an illustration, consider the contractibility problem of deciding if a closed path can be continuously deformed into a point in a simplicial complex. We will prove that there is no algorithm to decide this problem given the path and the simplicial complex as input. As a stronger statement there exists a simplicial complex for which there is no algorithm that decides the contractibility of the closed paths in this simplicial complex. At last, there exists a closed path in some simplicial complex for which it cannot be logically decided if the path is contractible or not.

Most often, undecidability results in topology are shown by first transforming a decision problem into a question concerning combinatorial group theory. In turn, problems about groups are transformed into problems about Turing machines. Ultimately, the proofs of undecidability rely on a reduction to the halting problem for Turing machines. We recommend the survey by Poonen [Poo14] for many undecidable problems in mathematics.

1 The Halting Problem

1.1 Turing Machines

A **Turing machine** is a mathematical model for the notion of computation. It was introduced by Alan Turing in 1936. According to Church-Turing thesis this is a universal model for the mechanization of computation. It was proved equivalent to other notion of computation such as recursive functions and λ-calculus.

Formally, a Turing machine is a triple $(\mathscr{A}, \mathscr{Q}, \mathscr{T})$, where $\mathscr{A}$ is a finite alphabet including a special **blank** character, $\mathscr{Q}$ is a finite set of **states**, and $\mathscr{T} \subset \mathscr{A} \times \mathscr{Q} \times \mathscr{A} \times \mathscr{Q} \times \{R, L\}$ is a **transition table** specifying how the machine operates on **configurations**. Those are words of the form $uqv \in \mathscr{A}^* \times \mathscr{Q} \times \mathscr{A}^*$. Such a configuration represents the machine in state q together with a linear tape marked with the word uv and whose read/write head is on the first letter in v (the empty word is interpreted as a blank). Transition $aqbpD \in \mathscr{T}$ applies to any configuration uqv such that a is the first letter in v. It transforms uqv replacing a with b, the state q by p, and moves the head one step to the left or right according to whether D equals L or R, respectively.

From the computability perspective there is no loss of generality to consider **deterministic** machines for which $aqbpD \in \mathscr{T}$ and $aqb'p'D' \in \mathscr{T}$ implies $b' = b$, $p' = p$ and $D' = D$: reading a letter in some state leads to only one new possible configuration. The machine is **halting** in a given configuration when no transition applies.

Standard coding of Turing machines

A Turing Machine M is in **standard form** if its alphabet is a finite subset of $\Sigma = \{\text{blank}, 1, 1', 1'', 1''', \ldots\}$ and its set of states is a finite subset of $\{q, q', q'', q''', \ldots\}$. One can encode the transition table of M on the six letter alphabet $\{\text{blank}, 1, q, ', R, L\}$

by concatenating its transitions (of the form $1'q'1''q''D$), where the prime symbol is considered as a letter. Finally, replacing $q, ', R, L$ by the respective letters $1', 1'', 1''', 1''''$, we obtain a coding of the transition table over the finite alphabet $\{\text{blank}, 1, 1', 1'', 1''', 1''''\}$. This coding is the **standard code** of M and is denoted by $\lceil M \rceil$.

1.2 Undecidability of the Halting Problem

A set of words $W \subset \mathscr{A}^*$ is **decidable**, or **recursive**, if there exists a turing machine $M = (\mathscr{A}, \mathscr{Q}, \mathscr{T})$ with three states $q_i, q_a, q_r \in \mathscr{Q}$, respectively called *initial, accepting* and *rejecting*, such that for every $w \in \mathscr{A}^*$ the machine M starting from configuration $q_i w$ reaches a halting configuration in state q_a if $w \in W$ and in state q_r otherwise. In particular M always reaches a halting configuration. Note that W is decidable if and only if both W and its complement $\mathscr{A}^* \setminus W$ are semi-decidable. Recall that W is **semi-decidable** if there exists a Turing machine halting in an accepting state if and only if it is given as input a word of W. Although this definition does not require any behavior for words not in W, it is equivalent to assume that the machine never stops given such words. Unfortunately, the same definition was given many names such as **semi-recursive**, **recursively enumerable**, **computably enumerable**, **listable** or **Turing recognizable**. The plurality of names comes from the fact that it is equivalent to require the existence of a Turing machine that enumerates W, *i.e.*, outputs all its words one after the other. A **decision problem** is a set of questions with YES/NO answers. By extension this problem is decidable, or **algorithmically solvable**, if the questions can be encoded as words over a finite alphabet and if the subset of words corresponding to questions with positive answers is decidable.

Consider the **self-halting problem** of deciding if a Turing machine M given as input its own standard code, *i.e.* starting with the configuration $q_i\lceil M \rceil$, will eventually reach a halting configuration in the accepting state.

Theorem 1.1. *The self-halting problem is semi-decidable but not decidable.*

PROOF. That the self-halting problem is semi-decidable is quite clear. Given the standard code of a Turing machine, it is enough to simulate the corresponding machine on this same input. The notion of universal Turing machine (see below) provides such a simulation. By way of contradiction, suppose that the self-halting problem is decidable. Hence, there exists a Turing machine, say S, that recognizes the complementary language. In other words, S halts in the accepting case if the input *does not* correspond to the standard code of a Turing machine that halts in the accepting state on its own input, and runs forever otherwise. Let us run S with the initial configuration $q_i\lceil S \rceil$. If S halts in the accepting state, this means that S does not halt in the accepting state on its own input, a contradiction. So S must run forever, meaning that S does halt in the accepting state on its own input, and we have again reached a contradiction. □

The general **halting problem** is to decide, given a machine M and a starting configuration I if M reaches a halting configuration. Since the self-halting problem is a particular case of the halting problem, we obtain:

Corollary 1.2. *The halting problem is unsolvable.*

Universal Turing Machine

A Turing machine T is said **universal** if for any Turing machine M and any initial configuration C, starting from configuration $q_i[M]C$ the machine T simulates the computation of M from C and halts in its accepting state if and only if this computation eventually stops. Though fastidious, one can write a program in his favourite language, say in C++, to simulate a universal Turing machine. This proves a fortiori its existence. The idea is to traverse the initial configuration C to "read" its state and the current symbol (the one that should lie under the reading head of M). Then, T needs to traverse $[M]$ in order to find the transition that applies. This transition transforms C into a configuration C' and we obtain the configuration $q_i[M]C'$ on T. We can proceed this way until some configuration $q_i[M]C''$ is reached, where C'' is a halting configuration for M. In this case, T should stop in its accepting state. Otherwise, T runs forever.

Theorem 1.3. *The halting problem for the universal machine T is unsolvable.*

In other words, there is no Turing machine that can decide for any configuration if T eventually stops starting from this configuration. Indeed, such a Turing machine would solve the general halting problem by considering configurations of the form $q_i[M]C$.

2 Decision Problems in Group Theory

Max Dehn (1911) was among the first to work out the connection between topology and combinatorial group theory. He made explicit that answering to certain topological questions about spaces could be used to solve some general problems about group presentations. Recall that a **combinatorial presentation** $\langle S \mid R\rangle$ of a group G is defined by a set S of generators and a set R of words over[2] S, called **relations**, so that G is the quotient of the free group $F(S)$ over S by the normal closure of R in $F(S)$. Hence, the elements of G are classes of words over S where two words are in the same class if one can be transformed into the other by a sequence of insertions or removals of

1. factors ss^{-1} with $s \in S$,
2. or words in R or their inverses.

We shall only consider *finitely presented* groups for which S and R are both finite. Most computational results nonetheless apply to *recursively presented* groups whose set of relations are recursively enumerable.

The universal property of free groups states that every map $S \to G$ from a set S to a group G extends uniquely to a group morphism $F(S) \to G$. A useful extension to group presentations is the following.

[2] By a word over (or in) S we always mean a finite sequence of elements in $S \cup S^{-1}$, where the elements of S^{-1} should be thought of as the inverses of the elements in S.

Theorem 2.1 (von Dyck)**.** *Let R be a set relations over a set S and let $f : S \to G$ be a map from S to a group G. Then, f extends to a morphism $\langle S \mid R\rangle \to G$ if and only if for every relation $r \in R$ we have $f(r) = 1_G$ where $f(r)$ is the natural extension of f to words.*

PROOF. By the universal property of free groups f extends to a morphism $f_S : F(S) \to G$. Denote by $C(R)$ the normal closure of R in $F(S)$. If $f(r) = 1_G$ for every $r \in R$, then $C(R) \subset \ker f_S$ and f_S quotients to a morphism $\langle S \mid R\rangle = F(S)/C(R) \to G$. Conversely, if $F(S)/C(R) \to G$ is an extension of $f : S \to G$, then $F(S) \to F(S)/C(R) \to G$ must be f_S, so that f_S must pass to the quotient. In other words, $C(R) \subset \ker f_S$, implying $f(r) = 1_G$ for every $r \in R$. □

2.1 Tietze Tranformations

Clearly, a group has (infinitely) many presentations. One can indeed replace a presentation $\langle S \mid R\rangle$ by applying the following **Tietze transformations** or their inverses to obtain presentations of the same group.

T1: Add a relation which is a consequence of R.

T2: Add a new generator s with a new relation $s\,w$, where w is any word over S.

Here, by a **consequence** of R it is meant a word r in S representing an element of the normal closure of R in $F(S)$, or equivalently, such that r is in the same class as the trivial word 1 in $\langle S \mid R\rangle$. It is quite remarkable that presentations of the same group are always related by such transformations.

Theorem 2.2. *Two finite presentations represent the same group if and only if one can be obtained from the other by a finite sequence of Tietze transformations and their inverses.*

PROOF. Let $\langle S \mid R\rangle$ and $\langle S' \mid R'\rangle$ be two presentations of the same group. In other words, there is an isomorphism $\langle S' \mid R'\rangle \cong \langle S \mid R\rangle$. The image of any generator $s' \in S'$ under this isomorphism can be expressed as a word $s'(S)$ over S. Similarly, denote by $s(S')$ the image of s by the inverse isomorphism. We have,

$$\langle S \mid R\rangle \cong \langle S \cup S' \mid R \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'}\rangle$$

by repeated applications of T_2. Now, looking at the composition

$$\langle S \cup S' \mid R \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'}\rangle \cong \langle S \mid R\rangle \cong \langle S' \mid R'\rangle$$

we see that the relations in R' and in $\{s \cdot (s(S'))^{-1}\}_{s \in S}$ are consequences of R together with the relations $\{s' \cdot (s'(S))^{-1}\}_{s' \in S'}$ (why?). It follows that

$$\langle S \cup S' \mid R \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'}\rangle \cong \langle S \cup S' \mid R \cup R' \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'} \cup \{s \cdot (s(S'))^{-1}\}_{s \in S}\rangle$$

by repeated applications of T_1. This last presentation is symmetric in prime and unprime symbols and could thus have been derived from $\langle S' \mid R'\rangle$. □

Exercise 2.3. Let r be a word in S that is a consequence of R. Show that r is freely equivalent (*i.e.*, inserting or removing ss^{-1} or $s^{-1}s$ factors) to a word of the form

$$\prod_{j=1}^{k} g_j r_j^{\varepsilon_j} g_j^{-1},$$

where the g_j are words over S, $r_j \in R$, and $\varepsilon_j \in \{-1, 1\}$.

Exercise 2.4. Show that the Tietze transformations T_1 and T_2 indeed produce isomorphic groups. In other words, show that:

$$\langle S \mid R \rangle \cong \langle S \mid R \cup \{r\} \rangle \cong \langle S \cup \{s\} \mid R \cup \{sw\} \rangle,$$

where r is a consequence of R.

2.2 Dehn's Problems

Dehn identified three fundamental algorithmic problems [Sti87]. Let $G = \langle S \mid R \rangle$ be a finitely presented group.

- **The word problem:** decide if a word over S represents the identity in G.
- **The conjugacy problem:** decide if two words over S represent conjugate elements in G.
- **The isomorphism problem:** decide if two combinatorial presentations represent isomorphic groups.

In the late 1940's Markov and Post independently proved that the word problem in semi-groups is unsolvable. The main idea is to encode the transition of a Turing machine as relations in a semi-group. In the end the halting problem becomes equivalent to the word problem in the constructed semi-group. The unsolvability of the word problem for groups is based on similar ideas but singularly more complex. It was eventually shown by P. S. Novikov in 1955 and almost at the same time by Boone. The original article by Novikov was 143 pages long. Thanks to the HNN construction introduced by Higman, Neeumann and Neumann in 1949, Boone (1959) and Britton (1963) succeeded to reduce the proof to approximately 10 pages.

Theorem 2.5 (Novikov, Boone)**.** *There exists a group for which the word problem is unsolvable. In particular, the word problem for groups (given a group* and *a word as input) is unsolvable.*

The simplest example of a group with unsolvable word problem has 4 generators and 12 relations, see Borisov [Bor69]. Since the word problem is a particular case of the conjugacy problem, we immediately infer that

Corollary 2.6. *The conjugacy problem for groups is unsolvable.*

The **generalized word problem** is to decide if a word over the generators S of a presentation P belongs to some subgroup of P specified by a set of generators given as words over S.

Theorem 2.7. *The generalized word problem is unsolvable.*

Theorem 2.8 (Adyan 1957, Rabin 1958)**.** *The isomorphism problem for groups is unsolvable.*

A **Markov property** for groups is one that is satisfied by at least one group with finite presentation and such that there exists a group H with finite presentation such that any group including H as a subgroup does not satisfy the property. Being the trivial group, or being Abelian are Markov properties (why?). Being the fundamental group of a 3-manifold is also a Markov property because there exist finitely presentable groups which cannot appear as subgroups of 3–manifold groups.

Theorem 2.9 (Adyan, Rabin)**.** *If P is a Markov property, then the problem of deciding if a finite presentation satisfies P is unsolvable.*

While those negative results assert that the basic decision problems in group theory are unsolvable *in general*, there are positive results for specific classes of groups. For instance, as we saw in a previous lecture, the word and conjugacy problems are solvable for surface groups. It results from the classification of surfaces that the isomorphism problem is also solvable for surface groups. A much stronger result claims that those problems are solvable for the class of fundamental groups of closed, orientable 3–manifolds. However, none of those groups are algorithmically recognizable. Indeed, the trivial group occurs as the fundamental group of a surface group and of a closed, orientable 3–manifold group. The recognition of such groups would thus allow to decide whether a given finite presentation describes the trivial group, in contradiction with Theorem 2.8. See also the survey on decision problems for 3–manifolds by Aschenbrenner, Friedl and Wilton [AFW15] for more details.

We postpone the proof of the undecidability of the word problem to Section 4. In the next section, we shall deduce the undecidability of topological problems from the above negative results in group theory.

3 Decision Problems in Topology

3.1 The Contractibility and Transformation Problems

Given a closed path in a simplicial complex, the **contractibility problem** is to decide if the path can be deformed continuously to a point in the complex. Likewise, given two closed path in a simplicial complex, the **transformation problem** is to decide if the paths can be deformed continuously one into the other in the complex. These are extensions of the corresponding problems we saw in the lecture on the homotopy test for surfaces.

Proposition 3.1. *The word and conjugacy problems respectively reduce to the contractibility and transformation problems in 2-complexes.*

The proof uses a simple construction that associates a two dimensional complex $\boldsymbol{\mathscr{C}(\langle S \mid R\rangle)}$ with every group presentation $\langle S \mid R\rangle$. The complex is built from a bouquet of circles, one for each generator in S, and a set of disks, one for each non-trivial[3] relation $r \in R$. If $r = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$, the boundary circle of the corresponding disk is subdivided into k subarcs and glued along the bouquet of circles in such a way that the ith arc is mapped onto the circle corresponding to generator s_i traversed in the same ($\varepsilon_i = 1$) or opposite ($\varepsilon_i = -1$) direction. By a repeated application of the Seifert–van Kampen theorem[4], the fundamental group of the resulting two dimensional complex is isomorphic to $\langle S \mid R\rangle$:

$$\pi_1(\mathscr{C}(\langle S \mid R\rangle)) \cong \langle S \mid R\rangle.$$

Note that the bouquet of circles can be seen as a graph with one vertex and with one loop edge per generator. This graph is the **1-skeleton** of $\mathscr{C}(\langle S \mid R\rangle)$.

PROOF OF PROPOSITION 3.1. Given a word $w = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ on the generators of a presentation $\langle S \mid R\rangle$, we consider the closed path ℓ_w of length k whose ith edge is the loop edge of the 1-skeleton of $\mathscr{C}(\langle S \mid R\rangle)$ corresponding to s_i, traversed in the same ($\varepsilon_i = 1$) or opposite ($\varepsilon_i = -1$) direction. The homotopy class of ℓ_w in $\mathscr{C}(\langle S \mid R\rangle)$ is the class of w in $\langle S \mid R\rangle$, so that w represents the identity in $\langle S \mid R\rangle$ if and only if ℓ_w is contractible. Namely, the word problem for w in $\langle S \mid R\rangle$ reduces to the contractibility problem for ℓ_w in $\mathscr{C}(\langle S \mid R\rangle)$. Now, given two words u and v and their corresponding closed paths ℓ_u and ℓ_w in $\mathscr{C}(\langle S \mid R\rangle)$ we saw in the lecture on the homotopy test that ℓ_u and ℓ_w are (freely) homotopic if and only if their homotopy classes are conjugates in the fundamental group of $\mathscr{C}(\langle S \mid R\rangle)$. It follows that the conjugacy problem for u and v is equivalent to the transformation problem for ℓ_u and ℓ_w. □

Exercise 3.2. A 2-complex can be described as a graph, allowing loop and multiple edges, and a collection of polygons, allowing monogons and bigons, such that the boundary of each polygon is attached to a closed path in the graph. Each side of the boundary should be attached to a single edge, but the closed path need not be simple.

The barycentric subdivision of such a 2-complex is obtained by first inserting a vertex in the middle of each edge in the graph and in the middle of each side of the polygons, then triangulating each polygon by inserting a vertex at the center and joining this vertex to the boundary vertices (including the new ones) with new edges. Show that three barycentric subdivisions of $\mathscr{C}(\langle S \mid R\rangle)$ always suffice to obtain a simplicial complex.

Corollary 3.3. *There exists a 2-dimensional complex for which the contractibility problem is unsolvable. In particular, the contractibility problem is unsolvable for 2-complexes. The same is true for the transformation problem.*

---

[3]For each trivial relation "1" we may also attach a sphere to the vertex of the bouquet. See the construction of Section 3.2.

[4]The version we need here is the following. If $X = U \cup D$ is a CW complex obtained by attaching a disk D along its boundary to the 1-skeleton of a connected CW complex U, then (omitting the base point) $\pi_1(X)$ is the quotient of $\pi_1(U)$ by the normal subgroup generated by the loop $\partial D \to U$.

PROOF. This follows directly from Theorem 2.5 and the previous Proposition 3.1. □

In fact, there exists a 2-dimensional complex and a closed path in this complex such that the contractibility of the path cannot be decided! The proof relies on the theory of Diophantine equations. In the famous list of 23 problems published in 1900 by Hilbert, the tenth problem asks for an algorithm to decide if a multivariable polynomial equation with integer coefficients has a solution in integers. Such equations are said **Diophantine** when one is indeed looking for integral solutions. In 1970, Matiyasevich succeeded to prove that Hilbert tenth problem is unsolvable by showing that any semi-decidable set of natural numbers is Diophantine, *i.e.*, has the form

$$\{n \in \mathbb{N} \mid \exists (n_1, \ldots, n_k) \in \mathbb{Z}^k : p(n, n_1, \ldots, n_k) = 0\}$$

for some polynomial p with integer coefficients in $k+1$ variables. Now, the set of statements in any formal system with recursively enumerable description (axioms and inference rules) can be numbered so that the theorems form a semi-decidable subset. By Gödel first incompleteness theorem, such a system, assuming it can express basic facts about natural numbers, has a statement that can neither be proved or disproved in the system (such as stating its own consistency, which cannot be proved by Gödel second incompleteness theorem). If n is the number of an undecidable statement and p is the Diophantine equation for the set of theorems, then it cannot be decided if $p(n,\cdot)$ has a solution. (See [Jon82, CM14] for explicit constructions.) More precisely, it cannot be proved that $p(n,\cdot)$ has no solution (if $p(n,\cdot)$ had a solution, this solution would provide its own proof). Hence, considering a Turing machine M that looks for a solution of $p(n,\cdot)$, we cannot prove that the machine runs indefinitely given $p(n,\cdot)$ as input. In Section 4 we shall construct, for every Turing machine and every input, a group presentation P with a word w in its generators such that the machine eventually halts after being given the input if and only if w represents the identity in P. This provides a 2-complex $\mathscr{C}(P)$ and a closed path corresponding to (an encoding of) $p(n,\cdot)$ for which we cannot prove that the path is non-contractible.

Remark 3.4. The results in this section extend to four dimensional manifolds since any finitely presented group can be realized as the fundamental group of a 4-manifolds that can effectively be computed (Dehn 1910).

3.2 The Homeomorphism Problem

The **homeomorphism problem** is to decide if two given combinatorial spaces, say simplicial complexes, are homeomorphic. Since we know that the isomorphism problem is unsolvable (Theorem 2.8), it is tempting to use the 2-complex $\mathscr{C}(P)$ associated to a group presentation P to reduce the isomorphism problem to the homeomorphism problem and conclude that this last one is also unsolvable. Indeed, if the complexes $\mathscr{C}(P)$ and $\mathscr{C}(Q)$ corresponding to the group presentations P and Q are homeomorphic, then their fundamental groups, hence P and Q, are isomorphic. However, different presentations of the same group may lead to non-homeomorphic 2-complexes so that we cannot conclude that the group are distinct when the corresponding 2-complexes are not homeomorphic. As a simple example consider the presentations $\langle \{s\} \mid \{s\} \rangle$,

$\langle \{s\} \mid \{s, s\} \rangle$, and $\langle \{s\} \mid \{s, 1\} \rangle$ of the trivial group. The corresponding 2-complexes are respectively homeomorphic to a disk, a sphere, and a sphere attached to a disk through a point. In order to prove the unsolvability of the homeomorphism problem one needs a presentation-invariant construction of a complex whose fundamental group is the given group. This was eventually achieved by Markov, using four dimensional manifolds rather than 2-complexes. Markov's proof is based on a Seifert and Threlfall construction (1934) using manifold surgery. Following Stillwell, we shall rely on a construction of Boone, Haken and Poénaru (1968).

Theorem 3.5 (Markov, 1958)**.** *The homeomorphism problem is unsolvable for manifolds of dimension* 4 *or larger.*

PROOF. Given two presentations P and Q we shall construct 4-manifold complexes $\mathscr{C}'(P)$ and $\mathscr{C}'(Q)$ such that $P \cong Q$ if and only if $\mathscr{C}'(P)$ and $\mathscr{C}'(Q)$ are homeomorphic. Since isomorphic presentations are related by Tietze transformations (Theorem 2.2) a solution is to provide a construction whose homeomorphism type is invariant by Tietze transformations. The above examples show that this is not the case for $\mathscr{C}(P)$. It turns out that the extra sphere arising from the trivial relation in the examples is essentially the only obstruction to an invariant construction. To overcome this problem Boone et al. introduce three modifications.

1. If P has p generators and m relations and Q has q generators and n relations, first add $p+n+1$ trivial relations (1) to P and $q+m+1$ trivial relations to Q. Denote by $P \star (p+n+1)$ and $Q \star (q+m+1)$ the resulting presentations.

2. Replace the 2-complexes $\mathscr{C}(P)$ and $\mathscr{C}(Q)$ by their thickening in $\mathbb{R}^5$. First note that any 2-complex $\mathscr{C}$ can be triangulated (see Exercise 3.2) and that any such triangulation has a piecewise linear (PL) embedding in $\mathbb{R}^5$. For $\varepsilon > 0$, let $\mathscr{C}^\varepsilon$ be the set of points at distance at most ε from $\mathscr{C}$ in $\mathbb{R}^5$. When ε is small enough $\mathscr{C}^\varepsilon$ deform retracts[5] onto $\mathscr{C}$, hence has the same fundamental group as $\mathscr{C}$. Moreover, $\mathscr{C}^\varepsilon$ can be triangulated and such a triangulation can be computed from $\mathscr{C}$. We set $\mathscr{C}'(P)$ to the boundary of the 5-manifold $\mathscr{C}^\varepsilon(P \star (p+n+1))$ and $\mathscr{C}'(Q)$ to the boundary of $\mathscr{C}^\varepsilon(Q \star (q+m+1))$.

3. In order to prove the invariance by Tietze transformations, replace the addition of a consequence relation (T_1) by four transformations T_{11}, T_{12}, T_{13} and T_{14}:

   T_{11} : replace a relation r by $s s^{-1} r$ or $s^{-1} s r$ for some generator s,

   T_{12} : replace a relation $u v w$ by its cyclic permutation $v w u$,

   T_{13} : replace a relation r by r^{-1},

   T_{14} : replace r by $r r'$ where r, r' are the ith and jth relations, $i \neq j$.

   Hence, transformation T_{1i} replaces a relation rather than adding a new one. It clearly produces isomorphic presentations (prove it!).

[5]A **retraction** is a continuous map from a topological space onto a subspace whose restriction to the subspace is the identity map. A **deformation retraction** is a homotopy between the identity map and a retraction.

Claim 1. Let $P = \langle S \mid R\rangle$ and $P' = \langle S \mid R \cup \{r\}\rangle$, where r is a consequence of R. Then $P \star 2$ may be converted to $P' \star 1$ using transformations $T_{11},\dots,T_{14}$ and T_2 and their inverses.

PROOF. By Exercise 2.3, we may write $r = \prod_{j=1}^{k} g_j r_j^{\varepsilon_j} g_j^{-1}$. By a combination of $T_{11},\dots,T_{14}$ and their inverses, we can transform the second of the two extra relations in $P \star 2$ into $g_j r_j^{\varepsilon_j} g_j^{-1}$. We can then use transformation T_{14} to accumulate such factors in the first extra relation, resetting each time the second extra relation to 1 by the reverse transformations used to get $g_j r_j^{\varepsilon_j} g_j^{-1}$. The details are left to the reader. □

Claim 2. If P and Q are isomorphic then we can transform $P \star (n+m+1)$ into $Q \star (n+m+1)$ using a sequence of transformations $T_{11},\dots,T_{14}$ and T_2 and their inverses.

PROOF. Let $P = \langle S \mid R\rangle$ and $Q = \langle S' \mid R'\rangle$. Using the notations in the proof of Theorem 2.2 we first transform $P \star (p+n+1)$ into $\langle S \cup S' \mid R \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'}\rangle \star (p+n+1)$ by repeated applications of T_2. We further mimic the proof of Theorem 2.2 using combinations of transformations $T_{11},\dots,T_{14}$ in place of T_1. By Claim 1, we obtain this way the isomorphic presentation $\langle S \cup S' \mid R \cup R' \cup \{s' \cdot (s'(S))^{-1}\}_{s' \in S'}, \{s \cdot (s(S'))^{-1}\}_{s \in S}\rangle \star 1$ which is symmetric in prime and unprime symbols and could thus have been derived from $Q \star (q+m+1)$. □

Claim 3. If presentation P_2 results from presentation P_1 by a transformation $T_{11},\dots,T_{14}$ or T_2, then $\mathscr{C}^\varepsilon(P_2)$ is homeomorphic to $\mathscr{C}^\varepsilon(P_1)$.

PROOF. The claim is trivial for transformations T_{12} and T_{13} since the 2-complexes $\mathscr{C}(P_1)$ and $\mathscr{C}(P_2)$ are the same in those cases. Consider now the transformation T_{11} applied to P_1. It replaces one of its relations r by $ss^{-1}r$ (or $s^{-1}sr$). Let P_0 be P_1 minus the relation r, which is also P_2 minus the relation $ss^{-1}r$. The 2-complex $\mathscr{C}(P_1)$ is obtained from $\mathscr{C}(P_0)$ by attaching a disk D to the closed curve corresponding to r in the 1-skeleton of $\mathscr{C}(P_0)$. Disk D intersects the thickening $\mathscr{C}^\varepsilon(P_0)$ in a simple closed curve ℓ_1 which cuts D into a smaller disk D_1 outside $\mathscr{C}^\varepsilon(P_0)$. So, $\mathscr{C}^\varepsilon(P_1)$ is the union of $\mathscr{C}^\varepsilon(P_0)$ and the thickening D_1^ε of D_1. Likewise, $\mathscr{C}^\varepsilon(P_2)$ is the union of $\mathscr{C}^\varepsilon(P_0)$ and the thickening D_2^ε of a disk D_2 that intersects $\mathscr{C}^\varepsilon(P_0)$ in a simple closed curve ℓ_2. Now, ℓ_1 and ℓ_2 differ by a thin "tongue" close to the path ss^{-1}. Hence, there is a homeomorphism (in fact an ambient isotopy) of $\mathscr{C}^\varepsilon(P_0)$ sending ℓ_2 to ℓ_1. We can extend this homeomorphism to an homeomorphism between $\mathscr{C}^\varepsilon(P_2) = \mathscr{C}^\varepsilon(P_0) \cup D_2^\varepsilon$ and $\mathscr{C}^\varepsilon(P_1) = \mathscr{C}^\varepsilon(P_0) \cup D_1^\varepsilon$. Similar constructions hold for the last two transformations T_{14} and T_2. See [Sti93, Sec. 9.4.4] for the details. □

We are now ready to prove that $\mathscr{C}'(P)$ and $\mathscr{C}'(Q)$ are homeomorphic if and only if P and Q are isomorphic. Recall that the fundamental group of $\mathscr{C}^\varepsilon(P \star (p+n+1))$ is $P \star (p+n+1) \cong P$. Since $\mathscr{C}^\varepsilon(P \star (p+n+1))$ is a 5-manifold, removing its 2-dimensional core $\mathscr{C}(P \star (p+n+1))$ does not change its fundamental group. Moreover, since $\mathscr{C}^\varepsilon(P \star (p+n+1)) \setminus \mathscr{C}(P \star (p+n+1))$ deform retracts onto the boundary of $\mathscr{C}^\varepsilon(P \star (p+n+1))$ they also have the same fundamental group. We conclude that $\pi_1(\mathscr{C}'(P)) \cong P$. Likewise, $\pi_1(\mathscr{C}'(Q)) \cong Q$. It follows that P and Q are isomorphic whenever $\mathscr{C}'(P)$ and $\mathscr{C}'(Q)$ are homeomorphic.

Suppose now that P and Q are isomorphic. According to Claim 2, $P\star(p+n+1)$ can be converted to $Q\star(q+m+1)$ using a sequence of transformations $T_{11},\dots,T_{14}$ and T_2 and their inverses. Following Claim 3, $\mathscr{C}^\varepsilon(P\star(p+n+1))$ and $\mathscr{C}^\varepsilon(Q\star(q+m+1))$ are homeomorphic and so are their boundaries $\mathscr{C}'(P)$ and $\mathscr{C}'(Q)$. $\square$

Exercise 3.6. Prove that any finite 2-dimensional simplicial complex has a PL embedding in $\mathbb{R}^5$.

Exercise 3.7. Provide the details in the proof of the above Claim 1.

Quite surprisingly, while there is no algorithm to decide whether two 2-complexes have isomorphic fundamental groups, the homeomorphism problem for 2-complexes is solvable! This results from the existence of a normal form for 2-complexes due to Whittlesey [Whi58, Whi60]. This normal form easily leads to an equivalence between the homeomorphism problem for 2-complexes and the graph isomorphism problem [STP94, DWW00]. The homeomorphism problem is also solvable for closed, oriented, triangulated 3-manifolds as recently proved by Kuperberg [Kup15]. The proof relies on the geometrization theorem conjectured by Thurston and proved by Perelman. This geometrization theorem provides a canonical decomposition of 3-manifolds into elementary pieces that can be algorithmically recognized.

4 Proof of the Undecidability of the Group Problems

In this Section we give a complete proof of Theorems 2.5, 2.7 and 2.8. We follow the proof by Stillwell [Sti82, Sti93][6]. A first step is two replace Turing machines by the $\mathbb{Z}^2$-machine formalism.

4.1 $\mathbb{Z}^2$-Machines

We can interpret a Turing machine $M=(\mathscr{A},\mathscr{Q},\mathscr{T})$ as a set of transformations over $\mathbb{Z}^2$. To this end we associate with every letter and state of M a distinct digit in base β between 0 and $\beta-1$, where $\beta=|\mathscr{A}|+|\mathscr{Q}|$. For a word w in $(\mathscr{A}\cup\mathscr{Q})^*$, let $\mathscr{B}(w)$ be the integer in base β whose digits are associated with the letters and states of w, in the same order. We encode a configuration uqv of M as a couple $(\mathscr{B}(uq),\mathscr{B}(\bar v))$ of integers, where $\bar v=\overline{v_1v_2\dots v_k}=v_k\dots v_2v_1$. Every transition of M may be interpreted as a partial transformation over $\mathbb{Z}^2$. Precisely, we associate with every transition $aqbpL$ the l**-transformations**:

$$(\beta^2U+\mathscr{B}(cq),\beta V+\mathscr{B}(a))\xrightarrow{l}(\beta U+\mathscr{B}(p),\beta^2V+\mathscr{B}(bc))$$

corresponding to the transitions $\mathscr{B}^{-1}(U)cqa\overline{\mathscr{B}^{-1}(V)}\mapsto\mathscr{B}^{-1}(U)pcb\overline{\mathscr{B}^{-1}(V)}$. Those transformations can be written as

$$(\beta^2U+A_l,\beta V+B_l)\xrightarrow{l}(\beta U+C_l,\beta^2V+D_l)$$

[6] Another interesting but incomplete presentation is proposed by Andrews [And05].

for some appropriate numbers A_l, B_l, C_l, D_l. Those four numbers determine the l-transformation. Note that a single transition gives rise to a number $|\mathscr{A}|$ of l-transformations, one for each $c \in \mathscr{A}$. Similarly, every transition $a\,q\,b\,p\,R$ is associated the r**-transformations**:

$$(\beta U + \mathscr{B}(q), \beta^2 V + \mathscr{B}(c\,a)) \xrightarrow{r} (\beta^2 U + \mathscr{B}(b\,p), \beta V + \mathscr{B}(c))$$

which write

$$(\beta U + A_r, \beta^2 V + B_r) \xrightarrow{r} (\beta^2 U + C_r, \beta V + D_r)$$

for appropriate A_r, B_r, C_r, D_r.

For numbers X, Y, X', Y', we write $(X, Y) \xrightarrow{s} (X', Y')$ if (X', Y') is the result of an s-transformation, $s \in \{l, r\}$, applied to (X, Y). More generally, we write

$$(X, Y) \xrightarrow{*} (X', Y')$$

if (X', Y') is obtained from (X, Y) by applying a finite sequence of transformations. Hence, M changes from a configuration to another one by a sequence of transitions if and only if $(X, Y) \xrightarrow{*} (X', Y')$ for the corresponding $\mathbb{Z}^2$-couples. We finally write

$$(X, Y) \xleftrightarrow{*} (X', Y')$$

if there exist $\mathbb{Z}^2$-couples $(X, Y) = (X_0, Y_0), (X_1, Y_1), \ldots, (X_n, Y_n) = (X', Y')$ such that, for $0 \le i < n$, either $(X_i, Y_i) \xrightarrow{s_i} (X_{i+1}, Y_{i+1})$ or $(X_{i+1}, Y_{i+1}) \xrightarrow{s_i} (X_i, Y_i)$, where $s_i \in \{l, r\}$.

We shall prove that the halting problem for Turing machines is Turing reducible to the generalized word problem. For this, we consider the $\mathbb{Z}^2$-machine Z corresponding to an arbitrary deterministic Turing machine. We then construct a group K_Z and a 1-1 map $p : \mathbb{Z}^2 \to K_Z$ so that the statement

Z, starting from some $(u, v) \in \mathbb{Z}^2$, eventually stops

is equivalent to $p(u, v)$ belonging to a certain subgroup of K_Z. We start recalling fundamental constructions in group theory.

4.2 Useful Constructs in Combinatorial Group Theory

Free Groups and Free Products

Recall that a free group over a set S is the group $F(S) = \langle S \mid - \rangle$ of words over S modulo the insertion of trivial relations $s\,s^{-1}$ and $s^{-1}s$, $s \in S$.

A relation between elements of a group is any product of those elements and their inverses which is the identity in the group. A relation is **reduced** if it does not contain two inverse consecutive factors. A subgroup H of a group G is free if H is isomorphic to a free group. A subset $S \subset G$ is a **free basis** for the subgroup it generates if there is no non-trivial reduced relations between the elements of S. In this case, the subgroup generated by S is a free subgroup isomorphic to $F(S)$.

The **free product** of two groups with presentations $\langle S \mid R \rangle$ and $\langle S' \mid R' \rangle$ is the group $\langle S \mid R \rangle * \langle S' \mid R' \rangle := \langle S \cup S' \mid R \cup R' \rangle$ (here, S, S' must be considered as disjoint sets even when $\langle S \mid R \rangle \cong \langle S' \mid R' \rangle$). The free product only depends on the group factors and not on the used presentations[7]. The **normal form theorem for free products** says that

[7]Free products can be defined by a universal property.

any non-trivial element of $G * H$ may be uniquely written as an alternating product of non-trivial elements of G and non-trivial elements of H. In particular, G and H embeds as subgroups of $G * H$.

HNN Extension and Britton's Lemma

Given a group $G = \langle S \mid R\rangle$ and an isomorphism $\varphi : A \to B$ between two subgroups A and B of G, Graham Higman, Bernhard Neumann et Hanna Neumann (1949) established the existence of a group $G*_\varphi$ containing G as a subgroup and such that $\varphi : A \to B$ becomes an inner automorphism (A and B are conjugate subgroups) in $G*_\varphi$. More precisely,

Definition 4.1. The **HNN extension** of G relatively to φ is the group

$$G*_\varphi := \langle S \cup \{t\} \mid R \cup \{\varphi(a) = t^{-1} a t\}_{a\in A}\rangle$$

where t is a new generator qualified as **stable**.

An essential property of HNN extensions is the existence of some kind of normal forms.

Theorem 4.2 (Normal forms for HNN extensions)**.** *Let T_A be a set of right coset representatives of A in G, with $1 \in T_A$. Similarly, let T_B be a set of right coset representatives of B in G, with $1 \in T_B$. Every element of $G*_\varphi$ can be written uniquely in the* normal form *$g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} g_n$, for some $g_i \in G$, $\varepsilon_i \in \{-1, 1\}$ satisfying*

- *$\varepsilon_i = 1$ implies $g_i \in T_B$,*
- *$\varepsilon_i = -1$ implies $g_i \in T_A$,*
- *there is no subsequence $t^\varepsilon 1 t^{-\varepsilon}$ with $\varepsilon \in \{-1, 1\}$.*

It results in the following Britton's lemma.

Lemma 4.3 (Britton, 1963)**.** *If a product $g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \dots t^{\varepsilon_n} g_n$ represents the identity in $G*_\varphi$, where $g_0 \in G$, $g_i \in G$ and $\varepsilon_i \in \{-1, 1\}$, $\forall i \in [1, n]$, then either $n = 0$ and $g_0 =_G 1$, or for some $i \in [1, n-1]$ we have*

- *either $\varepsilon_i = -1, \varepsilon_{i+1} = 1$ and $g_i \in A$,*
- *or $\varepsilon_i = 1, \varepsilon_{i+1} = -1$ and $g_i \in B$.*

Another easy consequence of the normal form theorem is that G, A, B and $\mathbb{Z}$ (generated by the stable generator) embed in $G*_\varphi$ (the normal forms of their elements reduce to themselves).

4.3 Undecidability of the Generalized Word Problem

Let

$$K = \langle x, y, z \mid [x, y] \rangle \quad \text{and} \quad p: \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & K \\ (u, v) & \longmapsto & (x^u y^v)^{-1} z x^u y^v \end{array}$$

Note that $K \cong \langle x, y \mid [x, y] \rangle * \langle z \mid - \rangle \cong \mathbb{Z}^2 * \mathbb{Z}$.

Lemma 4.4. *The image of $\mathbb{Z}^2$ under the map p forms a free basis of a free subgroup of K. In particular, p is one-to-one.*

PROOF. Let $w = p(u_1, v_1)^{j_1} \cdot p(u_2, v_2)^{j_2} \ldots p(u_n, v_n)^{j_n}$ be a *reduced* product of $p(u, v)$ factors, *i.e.*, such that $(u_i, v_i) \neq (u_{i+1}, v_{i+1})$ and $j_i \neq 0$. Substituting the $p(u_i, v_i)$ with their values and using that x and y commute in K, we get

$$w =_K x^{-u_1} y^{-v_1} z^{j_1} x^{u_1 - u_2} y^{v_1 - v_2} z^{j_2} \ldots x^{u_{n-1} - u_n} y^{v_{n-1} - v_n} z^{j_n} x^{u_n} y^{v_n}$$

From the normal form theorem of free products, if w is the identity in K, then it contains a factor $x^{u_i - u_{i+1}} y^{v_i - v_{i+1}}$ which is 1 in $\langle x, y \mid [x, y] \rangle$. However this is in contradiction with the hypothesis that $(u_i, v_i) \neq (u_{i+1}, v_{i+1})$. It follows that the $p(u_i, v_i)$ constitute a free basis. $\square$

With every l-transformation, we associate a morphism

$$\phi_l :< x^{\beta^2}, y^{\beta}, p(A_l, B_l) > \longrightarrow < x^{\beta}, y^{\beta^2}, p(C_l, D_l) >$$

between the two subgroups of K respectively generated by $x^{\beta^2}, y^{\beta}, p(A_l, B_l)$ and $x^{\beta}, y^{\beta^2}, p(C_l, D_l)$. This morphism is defined by $x^{\beta^2} \mapsto x^{\beta}$, $y^{\beta} \mapsto y^{\beta^2}$ and $p(A_l, B_l) \mapsto p(C_l, D_l)$. That this indeed defines a morphism is not obvious, see the next lemma. We similarly associate with every r-transformation the morphism

$$\phi_l :< x^{\beta}, y^{\beta^2}, p(A_r, B_r) > \longrightarrow < x^{\beta^2}, y^{\beta}, p(C_r, D_r) >$$

defined by $x^{\beta} \mapsto x^{\beta^2}$, $y^{\beta^2} \mapsto y^{\beta}$, $p(A_r, B_r) \mapsto p(C_r, D_r)$.

Lemma 4.5. *The maps ϕ_l and ϕ_r are well-defined isomorphisms.*

PROOF. Let ρ_l be the (inner) automorphism acting by conjugation by $x^{-A_l} y^{-B_l}$. This morphism sends $< x^{\beta^2}, y^{\beta}, p(A_l, B_l) >$ isomorphically onto $< x^{\beta^2}, y^{\beta}, z >$. Similarly, we have an inner automorphism θ_l sending $< x^{\beta}, y^{\beta^2}, p(C_l, D_l) >$ onto $< x^{\beta}, y^{\beta^2}, z >$. Note that $< x^{\beta^2}, y^{\beta}, z >$ as a subgroup of K is equal to $< x^{\beta^2}, y^{\beta} > * < z >$ (show inclusion in both directions) and similarly $< x^{\beta}, y^{\beta^2}, z >=< x^{\beta}, y^{\beta^2} > * < z >$. Now, the map $x^{\beta^2} \mapsto x^{\beta}, y^{\beta} \mapsto y^{\beta^2}$ induces an isomorphism $\alpha :< x^{\beta^2}, y^{\beta} > \longrightarrow < x^{\beta}, y^{\beta^2} >$ between subgroups of $\langle x, y \mid [x, y] \mid \simeq \rangle \mathbb{Z}^2$. The "free product" of this isomorphism with the identity over $< z >$ is an isomorphism. We can thus set $\phi_l = \theta_l^{-1} \circ (\alpha * Id_{<z>}) \circ \rho_l$, noting that both sides of the equality coincide on x^{β^2}, y^{β} and $p(A_\ell B_\ell)$. An analogous proof holds for ϕ_r. $\square$

We can thus consider the HNN extension $K*_{\phi_l}$ of K by ϕ_l. Let t_l be the stable generator of this extension.

Lemma 4.6. *$(u,v)\xrightarrow{l}(u',v')$ if and only if $t_l^{-1}p(u,v)t_l = p(u',v')$ in $K*_{\phi_l}$. Likewise, $(u,v)\xrightarrow{r}(u',v')$ if and only if $t_r^{-1}p(u,v)t_r = p(u',v')$ in $K*_{\phi_r}$.*

PROOF. If $(u,v)\xrightarrow{l}(u',v')$ then for some numbers U,V : $u=\beta^2U+A_l, v=\beta V+B_l, u'=\beta U+C_l, v'=\beta^2V+D_l$. It easily follows that $\phi_l(p(u,v))=p(u'v')$, whence $t_l^{-1}p(u,v)t_l = p(u',v')$ in $K*_{\phi_l}$. Conversely, suppose that $t_l^{-1}p(u,v)t_lp(u',v')^{-1}=1$. By Britton's Lemma 4.3 applied to $K*_{\phi_l}$, we have $p(u,v)\in<x^{\beta^2},y^{\beta},p(A_l,B_l)>$. Hence,

$$p(u,v)=x^{\beta^2j_1}y^{\beta j_2}p(A_l,B_l)^{j_3}x^{\beta^2j_4}\dots p(A_l,B_l)^{j_n} \tag{1}$$

for some integers $j_1,j_2,\dots,j_n$. Using trivial relations and the commutation of x and y, the right-hand side of (1) may be written as

$$p(\beta^2U_1+A_l,\beta V_1+B_l)^{j_3}\cdot p(\beta^2U_2+A_l,\beta V_2+B_l)^{j_6}\dots p(\beta^2U_k+A_l,\beta V_k+B_l)^{j_n}x^{\beta^2a}y^{\beta b}$$

for some $U_1,V_1,U_2,V_2,\dots U_k,V_k,a,b$. Making x,y and z commute (by abelianizing K) in this equality, we deduce that $a=b=0$. By Lemma 4.4, we then conclude that the right-hand side of (1) reduces to a single factor $p(\beta^2U+A_l,\beta V+B_l)$ for which $u=\beta^2U+A_l$ and $v=\beta V+B_l$. We thus compute in $K*_{\phi_l}$ that $t_l^{-1}p(u,v)t_l=\phi_l(p(u,v))=p(\beta U+C_l,\beta^2V+D_l)$. It then follows from the hypothesis $p(u',v')=t_l^{-1}p(u,v)t_l$ and Lemma 4.4 that $u'=\beta U+C_l$ et $v'=\beta^2V+C_l$. In other words, $(u,v)\xrightarrow{l}(u',v')$. The case of an r-transformation may be treated the same way. □

Denote by K_Z the group obtained from K by the successive HNN extensions by the morphisms ϕ_l and ϕ_r associated with all the l and r-transformations of Z. Clearly, the resulting group does not depend on the order of successive extensions. Since a group embeds in all its extensions, Lemma 4.6 remains valid in K_Z. Denote by $\{t_l\}$ and $\{t_r\}$ the stable generators of all the HNN extensions corresponding to the morphisms ϕ_l and ϕ_r.

Lemma 4.7. *$(u',v')\overset{*}{\longleftrightarrow}(u,v)$ if and only if $p(u',v')\in<p(u,v),\{t_r\},\{t_l\}>\subset K_Z$.*

PROOF. By repeated applications of Lemma 4.6, if $(u',v')\overset{*}{\longleftrightarrow}(u,v)$ then there exists $w\in<\{t_l\},\{t_r\}>\subset K_Z$ such that $p(u',v')=w^{-1}p(u,v)w$. In particular, $p(u',v')\in<p(u,v),\{t_r\},\{t_l\}>$. Conversely, suppose that $p(u',v')\in<p(u,v),\{t_r\},\{t_l\}>$. Hence, $p(u',v')$ may be written

$$T_0p(u,v)^{j_1}T_1p(u,v)^{j_2}\dots p(u,v)^{j_k}T_k \tag{2}$$

for some integers $j_1,j_2,\dots,j_k$ and words $T_0,T_1,\dots,T_k$ in $<\{t_r\},\{t_l\}>$. Since the value $p(u',v')$ of this product is in K, it follows by induction on the number of HNN extensions from K to K_Z and by Britton's lemma that this product contains a factor of the form $t_s^{\pm1}wt_s^{\mp1}$, where w is in the domain or codomain of ϕ_s. From (2) we must have $w=p(u,v)^j$ for some $j\in\{j_1,j_2,\dots,j_k\}$. Arguing as in the second part of the proof of Lemma 4.6, we deduce that

$$t_s^{\pm1}wt_s^{\mp1}=t_s^{\pm1}p(u,v)^jt_s^{\mp1}=(t_s^{\pm1}p(u,v)t_s^{\mp1})^j=p(u'',v'')^j$$

where either $(u,v) \xrightarrow{s} (u'',v'')$ or $(u,v) \xleftarrow{s} (u'',v'')$ depending on the signs in the t_s exponents. In particular, the fact that $p(u,v)^j$ is in the (co)domain of ϕ_s implies that the s-transformation (or its inverse) corresponding to t_s applies to (u,v). Substituting $p(u'',v'')^j$ to $t_s^{\pm 1} p(u,v)^j t_s^{\mp 1}$ in (2) we get a new expression in terms of the T_i's, $p(u,v)$ and $p(u'',v'')$. Iterating the process we eliminate the t_s factors to obtain

$$p(u',v') = p(u_1,v_1)^{j_1} p(u_2,v_2)^{j_2} \dots p(u_k,v_k)^{j_k}$$

where $(u_i,v_i) \overset{*}{\longleftrightarrow} (u,v)$ for each i. Lemma 4.4 allows to conclude that the right-hand side reduces to a single $p(u_i,v_i)$ with $(u_i,v_i) = (u',v')$, so that $(u',v') \overset{*}{\longleftrightarrow} (u,v)$. □

Lemma 4.8. *Let $(u_0,v_0) \in \mathbb{Z}^2$ corresponds to a halting configuration of Z. Then, $(u,v) \overset{*}{\longleftrightarrow} (u_0,v_0)$ if and only if $(u,v) \xrightarrow{*} (u_0,v_0)$.*

Proof. On the one hand, we cannot have $(u,v) \xleftarrow{s} (u_0,v_0)$ since (u_0,v_0) is halting. On the other hand, $(u,v) \xleftarrow{s} (u',v') \xrightarrow{s'} (u'',v'')$ implies $(u,v) = (u'',v'')$ since Z is deterministic. We can thus assume that this pattern does not occur in $(u,v) \overset{*}{\longleftrightarrow} (u_0,v_0)$. It follows that $(u,v) \xrightarrow{*} (u_0,v_0)$. □

Proof of Theorem 2.7. let Z be the $\mathbb{Z}^2$-machine corresponding to a universal Turing machine T. Up to a simple modification, we can assume that T has a unique halting configuration corresponding to some (u_0,v_0) for Z. It follows from Lemmas 4.7 and 4.8 that T eventually halts starting from a configuration with $\mathbb{Z}^2$ code (u,v) if and only if $p(u,v)$ belongs to the subgroup $< p(u_0,v_0), \{t_r\}, \{t_l\} >$ of K_Z. This last generalized word problem is thus unsolvable by Corollary 1.2. □

Proof of Theorem 2.5. Let $H =< p(u_0,v_0), \{t_r\}, \{t_l\} > \subset K_Z$. Consider the HNN extension $L := K_Z *_{Id_H}$ and let k be the stable generator of this extension. By Britton's lemma $p(u,v) k p(u,v)^{-1} k^{-1} =_L 1$ if and only if $p(u,v) \in H$. Hence, the above unsolvable generalized word problem reduces to the word problem. □

Proof of Theorem 2.8. The unsolvability of the isomorphism problem results from Theorem 2.9 since being isomorphic to the trivial group is a Markov property. For completeness we nonetheless provide an independent proof based on the above construction. First note that if all the nontrivial elements of a group have infinite order, this remains true for the nontrivial elements of any HNN extension of the group. This can be proved by applying Britton's lemma to the powers of the normal form of an element (exercise). In particular, the nontrivial elements of $K = \langle x,y,z \mid [x,y] \rangle$ have infinite order, so that this will be true for any further HNN extensions.

Let $\langle S \mid R \rangle$ be the presentation of $L = K_Z *_{Id_H}$ naturally obtained by the successive extensions as in the proof of Theorem 2.5. In particular, $S = \{x,y,z\} \cup \{t_l\} \cup \{t_r\} \cup \{k\}$. For a word w in S, we consider the group with presentation

$$L(w) := \langle S \cup \{k_s\}_{s \in S} \mid R \cup \{k_s^{-1} w k_s = s\}_{s \in S} \rangle$$

We claim that w represents the identity in L if and only if $L(w)$ is isomorphic to the free group over S. Indeed, if $w =_L 1$ then the new relations in $L(w)$ reduce to $1 = s$, whence

$L(w) = \langle \{k_s\}_{s\in S} \mid -\rangle$. Conversely, if $w \neq 1$ then w, like the s's, has infinite order in L. It follows that $w \mapsto s$ defines an isomorphism of cyclic infinite groups. Hence, $L(w)$ may be viewed as resulting from a sequence of HNN extensions with stable generators $\{k_s\}_{s\in S}$. In particular, L embeds in $L(w)$, implying that the word problem for $L(w)$ is unsolvable. On the other hand, if $L(w)$ was isomorphic to a free group then the word problem for $L(w)$ would be solvable, a contradiction. Hence, $L(w)$ is not isomorphic to a free group, thus proving the claim. It follows that this instance of the isomorphism problem reduces to an unsolvable word problem. □

References

[AFW15] Matthias Aschenbrenner, Stefan Friedl, and Henry Wilton. Decision problems for 3–manifolds and their fundamental groups. *Geometry & Topology Monographs*, 19(1):201–236, 2015.

[And05] Uri Andrews. Undecidable problems in topology. https://math.berkeley.edu/~hutching/teach/215b-2005/andrews.ps, May 2005.

[Bor69] V. V. Borisov. Simple examples of groups with unsolvable word problem. *Mathematical Notes*, 6(5):768–775, 1969.

[CM14] Merlin Carl and Boris Zelikovich Moroz. On a diophantine representation of the predicate of provability. *Journal of Mathematical Sciences*, 199(1):36–52, 2014.

[DWW00] Colm Ó Dúnlaing, Colum Watt, and David Wilkins. Homeomorphism of 2-complexes is equivalent to graph isomorphism. *International Journal of Computational Geometry & Applications*, 10(5):453–476, 2000.

[Jon82] James P Jones. Universal diophantine equation. *The journal of symbolic logic*, 47(03):549–571, 1982.

[Kup15] Greg Kuperberg. Algorithmic homeomorphism of 3-manifolds as a corollary of geometrization. Technical report, arXiV, 2015. https://arxiv.org/abs/1508.06720.

[Man14] Ciprian Manolescu. Triangulations of manifolds. *ICCM Not*, 2(2):21–23, 2014.

[Poo14] Bjorn Poonen. *Interpreting Gödel: Critical Essays*, chapter Undecidable problems: a sampler, pages 211–241. Cambridge University Press, 2014.

[Sti82] John Stillwell. The word problem and the isomorphism problem for groups. *Bull. Amer. Math. Soc.*, 6(1):33–56, 1982.

[Sti87] John Stillwell. *Papers on group theory and topology*. Springer-Verlag, New York, 1987.

[Sti93] John Stillwell. *Classical topology and combinatorial group theory*, volume 72. Springer-Verlag, New York, 1993.

[STP94] John Shawe-Taylor and Tomaž Pisanski. Homeomorphism of 2-complexes is graph isomorphism complete. *SIAM J. Comput.*, 23(1):120–132, 1994.

[Whi58] E. F. Whittelsey. Classification of finite 2-complexes. *Proceedings of the American Mathematical Society*, 9(6):841–845, 1958.

[Whi60] E. F. Whittlesey. Finite surfaces. a study of finite 2-complexes. part ii. the canonical form. *Mathematics Magazine*, 34(2):67–80, 1960.