Algorithmic Topology & Groups

Lectures by Francis Lazarus & François Dahmani
Notes by Alexis Marchand

Institut Fourier
First semester 2020-21
M2 course

Contents

1 What is an algorithm?

1.1 Turing machines and decision problems

Definition 1.1 (Turing machine)**.** *A **Turing machine** is the data of an alphabet A containing an empty character $\varnothing$, a finite set of states Q and a finite transition table $T \subseteq A \times Q \times A \times Q \times \{L, S, R\}$. The letters L, S, R stand for "left", "stay" and "right" respectively.*

*A **configuration** is encoded by $uqv \in A^* \times Q \times A^*$, where q represents the current state of the machine, u represents the word written on the tape (strictly) to the left of the head and v is the word starting at the head.*

*A **transition** $aqbpD \in T$ means that, if the first letter of v is a and the current state is q, then the first letter becomes b, the current state becomes p and the head moves in the direction given by $D \in \{L, S, R\}$.*

*A Turing machine is **deterministic** if at most one transition applies to a configuration.*

Definition 1.2 (Decision problem)**.** *We consider a problem represented by a **language** $L \subseteq A^*$. A deterministic Turing machine M with an initial state q_i, an accepting state q_a and a rejecting state q_r **solves** L if for every $w \in A^*$, when M is executed starting with configuration $q_i w$, the computations lead to the state q_a (resp. q_r) exactly when $w \in L$ (resp. $w \notin L$).*

*A problem is **decidable** (or solvable) if there is a Turing machine that solves it. It is **semi-decidable** if there is a Turing machine M s.t., when starting with $q_i w$, M stops in q_a if and only if $w \in L$.*

Definition 1.3 (Halting problem)**.** *A Turing machine is in **standard form** if A, Q are finite sets of the form $A = \{\varnothing, 1, 1', 1'', \dots\} \subseteq \{\varnothing\} \cup \left\{1^{(n)},\, n \in \mathbb{N}\right\}$ and $Q = \{q, q', q'', \dots\}$. In this case, transitions can be encoded on the alphabet $\{\varnothing, 1, q, ', R, S, L\}$. Finally, we can replace q by $1'$, $'$ by $1''$, R by $1'''$, etc., encoding T on the alphabet $\{\varnothing, 1, 1', 1'', \dots\}$. This gives the **standard encoding** $[M]$ of the Turing machine M.*

*The **self-halting problem** is to know if the machine M, given $[M]$ as input, will stop in an accepting state.*

*The **halting problem** is to know if, given a Turing machine M and a word w, the machine M will accept w.*

Theorem 1.4. *The self-halting problem is semi-decidable but not decidable.*

Proof. The self-halting problem is clearly semi-decidable: one only needs to construct a Turing machine that can simulate any Turing machine.

Now suppose for contradiction that the self-halting problem L is decidable. It follows that its complement is decidable, so there is a Turing machine S such that S recognizes the standard codes of Turing machines that do not accept themselves. Now feed S with $[S]$; this yields a contradiction. □

Corollary 1.5. *The halting problem is not decidable.*

Definition 1.6 (Universal Turing machine)**.** *A **universal Turing machine** is one that, given $[M]$ and a configuration c, simulates the computation of M starting with c.*

Corollary 1.7. *The halting problem for the universal Turing machine is not decidable.*

1.2 Tractability and complexity

Definition 1.8 (Complexity)**.** *The **time complexity** of a computation on a Turing machine is its number of transitions. The **space complexity** of a computation is the maximal length of the part of the tape used for the computation.*

Note that the space complexity is at most equal to the time complexity.

An algorithm has complexity f if, for every input of size n, the complexity of the computation is at most $f(n)$.

Definition 1.9 (Tractability)**.** *A problem is **tractable** if it can be solved in polynomial time. The set of such problems is denoted by P.*

Definition 1.10 (Multitape Turing machine)**.** *A **k-tape Turing machine** is the data of (A, Q, T), with $T \subseteq A^k \times Q \times A^k \times Q \times \{L, S, R\}^k$. A **configuration** is an element of $Q \times (A^* \times A^*)^k$. The **content** of the k-tape is the projection of the configuration onto $(A^* \times A^*)^k$.*

Theorem 1.11. *For every k-tape Turing machine M_k, there is a 1-tape Turing machine M with an injection of the tape content of M_k into the tape content of M s.t. every computation of M_k using n transitions can be done on M with n^2 transitions.*

Proof. Represent the k tapes by $\mathbb{Z} \times \{1, \dots, k\}$. The alphabet for M is $B = (A \times \{0, 1\})^k$. Every content of M_k can be represented by a word in B^* (where the 0s and 1s represent the position of the heads). The set of states of M is $Q \times (A \cup \{0\})^k$. To simulate a transition of M_k in M, we scan the k words until we find all the 1s, so that we know where the heads are, and then we apply the transition. Since each word has length at most n, we do at most n^2 transitions in M. □

1.3 Random access model

Definition 1.12 (Random access model)**.** *A **random access model** (or **RAM**) is the data of a memory unit R with cells $R[0], R[1], \dots$, an accumulator α which is also a cell, a program unit (i.e. a sequence of instructions), and a controller ℓ (a cell which is incremented at each instruction). Each cell contains integers.*

Here is a list of possible instructions and their interpretations:

- ***Transfer instructions**:* `LOAD`j *($\alpha := R[j]$),* `ILOAD`j *($\alpha := R[R[j]]$),* `STORE`j *($R[j] := \alpha$),* `ISTORE`j *($R[R[j]] := \alpha$) and* `WRITE`x *($\alpha := x$),*
- ***Arithmetic operations**:* `ADD`j *($\alpha := \alpha + R[j]$),* `SUB`j *($\alpha := \alpha - R[j]$) and* `HALF` *($\alpha := \left\lfloor \frac{\alpha}{2} \right\rfloor$),*

- ***Control instructions***: `JZERO`ℓ *(go to* ℓ *if* $\alpha = 0$*),* `JPOS`ℓ *(go to* ℓ *if* $\alpha > 0$*) and* `HALT` *(stop the program).*

Theorem 1.13. *RAMs can simulate Turing machines with the same time complexity: for every Turing machine* $M = (A, Q, T)$*, there exists a RAM* M' *s.t., starting from a memory content representing the initial content of* M*, every transition of* M *corresponds to the execution of a constant number of instructions of* M'*. The contents of the memories of* M *and* M' *do correspond after this execution.*

Lemma 1.14. *After executing* k *instructions on a RAM with input size* n*, the bit length of any number in the memory is at most* $n + k + s_p$*, where* s_p *is the largest bit length of any number in the program.*

Proof. Use induction on k, noting that adding or subtracting two $(n + k + s_p)$-bit numbers gives an $(n + k + s_p + 1)$-bit number. □

Theorem 1.15. *A RAM of complexity* f *can be simulated by a* 1*-tape Turing machine with time complexity* $\mathcal{O}(f^6)$*.*

Proof. First simulate the RAM M with a 3-tape Turing machine M_T (one tape for the memory, one for the accumulator, and one encoding a cell index). For any input of size n, the execution of k instructions in M corresponds to $\mathcal{O}(k^2(k + n))$ transitions in M_T. Then use Theorem 1.11 to get a 1-tape Turing machine. □

1.4 Complexity classes and NP-completeness

Notation 1.16. *Complexities will be computed here on multitape Turing machines (which are equivalent to RAMs and* 1*-tape Turing machines up to polynomial composition).*

Definition 1.17 (Complexity classes)**.** *A problem* L *has complexity* f *if there is a (deterministic) algorithm solving* L *with complexity at most* f*. In particular, a problem has* ***polynomial complexity*** *if it has complexity* $p(n)$ *for some polynomial* p*. It has* ***exponential complexity*** *if it has complexity* $2^{p(n)}$ *for some polynomial* p*.*

(i) *We denote by* P *the class of problems with polynomial (time) complexity.*

(ii) *We denote by* $PSPACE$ *the class of problems with polynomial space complexity.*

(iii) *We denote by* EXP *the class of problems with exponential (time) complexity.*

(iv) *We denote by* NP *the class of problems with nondeterministic polynomial complexity.*

Theorem 1.18. *A problem* L *is in* NP iff *for every* $w \in L$*, there is a* ***certificate*** c *of polynomial size and a deterministic Turing machine called the* ***verifier*** *that accepts* (w, c) *in polynomial time and rejects in any other case.*

Proof. ($\Rightarrow$) If there is a nondeterministic Turing machine M solving L, a certificate for a word $w \in L$ is given by an encoding of a computation starting at w and leading to an accepting state in M. ($\Leftarrow$) Use transitions to (nondeterministically) guess a certificate of bounded size, then execute the verifier. □

Proposition 1.19. $P \subseteq NP \subseteq PSPACE \subseteq EXP$*.*

Definition 1.20 (Karp reduction)**.** *A problem* $I \subseteq A^*$ ***reduces*** *to* $J \subseteq B^*$ *(which we write* $I \leqslant J$*) if there exists a function* $r : A^* \to B^*$ *that is computable by a Turing machine in polynomial time, and s.t.* $I = r^{-1}(J)$*.*

Remark 1.21. *There is also a notion of* ***Turing reduction****, which we will not use: we say that I Turing reduces to J if we can solve I with a Turing machine using an oracle for J (i.e. we can solve problems from J in constant time).*

Definition 1.22 (C-hard and C-complete)**.** *A problem I is called C-**hard** if $J \leqslant I$ for all $J \in C$.*
*If in addition $I \in C$, we say that I is C-**complete**.*

Definition 1.23 (SAT)**.** *A* ***boolean formula*** *P on $X = \{x_1, \dots, x_n\}$ is a word in the smallest subset of $(X \cup \{\neg, \vee, \wedge, (,)\})^*$ that contains X and is stable under the binary operations $\vee, \wedge$ and the unary operation $\neg$. Given an* ***assignment*** *$X \to \{T, F\}$, we can give P a truth value in $\{T, F\}$.*
The formula P is ***satisfiable*** *if there is an assignment $X \to \{T, F\}$ s.t. P evaluates to T.*
The class of satisfiable boolean formulas is denoted by SAT.

Theorem 1.24 (Cook-Levin, 1971)**.** *SAT is NP-complete.*

Proof. It is clear that $SAT \in NP$ (a certificate for a satisfiable formula P is an assignment $X \to \{T, F\}$ s.t. P evaluates to T).

We have to show that SAT is NP-hard: given $I \in NP$, there is a nondeterministic Turing machine M that solves I in polynomial time. Now write a boolean formula simulating the execution of M. □

1.5 Basic algorithms: graphs and string matching

Notation 1.25. *A graph is represented by its* ***adjacency lists****, i.e. we have a list V of vertices, and for each vertex $v \in V$, a list of all neighbours of V.*

Definition 1.26 (Topological order)**.** *Given a graph G with a given source vertex s, a* ***topological order*** *is an ordering of the vertices of G as $s = v_1, v_2, \dots, v_n$ s.t. for all i, there is an edge e_i between v_i and one of the vertices $v_1, \dots, v_{i-1}$.*

Algorithm 1.27 (Breadth-first search)**.** *To compute a topological order on G, we start at s, and at each step i, we arbitrarily choose an edge $e_i = v_j v_i$ with j* minimal *in $\{1, \dots, i-1\}$. This is implemented using a queue, and has complexity $\mathcal{O}(|V| + |E|)$.*

Algorithm 1.28 (Depth-first search)**.** *To compute a topological order on G, we start at s, and at each step i, we arbitrarily choose an edge $e_i = v_j v_i$ with j* maximal *in $\{1, \dots, i-1\}$. This is implemented using a stack, and has complexity $\mathcal{O}(|V| + |E|)$.*

Definition 1.29 (String matching problem)**.** *We consider a word $P \in A^*$ of length m and a text $T \in A^*$ of length n. The* ***string matching problem*** *is to find all occurrences of P in T.*

Notation 1.30. *Given two words U, V, we write*

- *$U \sqsubset V$ if U is a prefix of V,*
- *$U \sqsupset V$ if U is a suffix of V.*

Algorithm 1.31 (Knuth-Morris-Pratt, 1970)**.** *Consider the function $\pi : [1, m] \to [0, m-1]$ defined by*

$$\pi(q) = \max \{k < q,\ P[1, k] \sqsupset P[1, q]\}.$$

In other words, $\pi(q)$ is the length of the longest proper prefix of $P[1, q]$ that is also a suffix of $P[1, q]$.

We start by computing $\pi(q)$ as follows: we know that $\pi(1) = 0$, and to compute $\pi(q+1)$, we check if $P[q+1] = P[\pi(q)+1]$; if this is the case, then $\pi(q+1) = \pi(q) + 1$; otherwise, we try to extend $P[1, \pi(\pi(q))]$ to a suffix of $P[1, q+1]$.

Having computed π in complexity $\mathcal{O}(m)$, we want to compute the following function:

$$\omega(q) = \max \{k \leqslant m,\ P[1, k] \sqsupset T[1, q]\}.$$

In other words, $\omega(q)$ is the longest prefix of P that is also a suffix of $T[1,q]$. Therefore, P is a shift-s pattern in T iff *$\omega(s+m) = m$. The computation of ω is similar to that of π and takes complexity $\mathcal{O}(n)$.*

The complete algorithm yields the positions of all occurrences of P in T and has complexity $\mathcal{O}(n+m)$.

2 Topologie des graphes combinatoires

2.1 Generalités sur les graphes

Definition 2.1 (Graphe)**.** *Un **graphe** G est un quadruplet (V, A, o, ι), où V est un ensemble de **sommets**, A est un ensemble d'**arcs**, $o : A \to V$ est l'application **origine** et $\iota : A \to A$ est une involution sans point fixe.*

Pour $a \in A$, on peut noter $a^{-1} = \iota(a)$.

*Une **arête** de G est une paire $\{a^{\pm 1}\} \subseteq A$. On note $E(G)$ l'ensemble des arêtes.*

Example 2.2. *Un **bouquet de cercles** est un graphe avec un seul sommet.*

Definition 2.3 (Chemins et connexité)**.** *Soit G un graphe. Étant donné $v, w \in V$, un **chemin** γ de v à w (noté $\gamma : v \rightsquigarrow w$) est une suite alternée $(v_0, a_1, v_1, \ldots, v_{k-1}, a_k, v_k)$ de sommets et d'arcs t.q. $o(a_i) = v_{i-1}$ et $o\left(a_i^{-1}\right) = v_i$. On pourra omettre les sommets de la notations.*

*Étant donné $\gamma = (v_0, a_1, v_1, \ldots, v_k)$, le **chemin inverse** de γ est $\gamma^{-1} = \left(v_k, a_k^{-1}, v_{k-1}, \ldots, v_0\right)$.*

*Étant donnés deux chemins γ, λ avec $o(\gamma^{-1}) = o(\lambda)$, on note $\gamma \cdot \lambda$ leur **concaténation**.*

*Un graphe G est dit **connexe** si pour tous sommets $v, w \in V$, il existe un chemin $v \rightsquigarrow w$.*

Definition 2.4 (Morphisme de graphes)**.** *Si G, G' sont deux graphes, un **morphisme** $G \to G'$ est une application $f : A \cup V \to A' \cup V'$ t.q.*

- $f(V) \subseteq V'$,
- $f \circ o = o' \circ f$,
- $f \circ \iota = \iota' \circ f$,

où o' et ι' sont prolongés par l'identité sur V'.

Definition 2.5 (Contraction d'arête)**.** *Soit $e = \{a^{\pm 1}\}$ une arête de G. La **contraction** de e dans G est le graphe $G/e = (V', A', o', \iota')$, où $V' = V/(o(a) = o(a^{-1}))$, $A' = A \setminus \{a^{\pm 1}\}$, et o', ι' sont définis de manière naturelle.*

On a alors un morphisme $G \to G/e$.

On définit de manière analogue G/E' pour $E' \subseteq E(G)$.

Si H est un sous-graphe de G, on notera $G/H = G/E(H)$.

Definition 2.6 (Suppression d'arête)**.** *Soit $e = \{a^{\pm 1}\}$ une arête de G. Le graphe obtenu par **suppression** de e est $G - e = (V, A \setminus e, o, \iota)$.*

Definition 2.7 (Subdivisions et équivalence combinatoire)**.** *Soit $e = \{a^{\pm 1}\}$ une arête de G. La **subdivision élémentaire** de e est le graphe obtenu à partir de G en ajoutant un sommet au milieu de e (i.e. on remplace e par un chemin de longueur 2). De même, on peut subdiviser un ensemble d'arêtes.*

*Deux graphes sont **combinatoirement équivalents** s'ils ont des subdivisions isomorphes.*

*Un **invariant de graphes** est une grandeur qui ne dépend que de la classe combinatoire.*

2.2 Cycles et arbres

Definition 2.8 (Cycles et circuits)**.** *Un **cycle** est un chemin fermé. Un **chemin simple** est un chemin sans répétition de sommets. Un **circuit** est un cycle à permutation près. Un **lacet** est un cycle avec un point base.*

Definition 2.9 (Arbres et forêts)**.** *Une **forêt** est un graphe sans cycle simple. Un **arbre** est une forêt connexe.*

Lemma 2.10. *Soit $T \subseteq G$ un sous-arbre. Alors T s'étend en un arbre maximal dans G.*

Proof. Soit $\mathscr{S}$ l'ensemble des sous-arbres de G contenant T, ordonné par l'inclusion. Si $\mathscr{T} \subseteq \mathscr{S}$ est une chaîne (i.e. une partie totalement ordonnée), alors $\bigcup_{T' \in \mathscr{T}} T'$ est un majorant pour $\mathscr{T}$; ainsi, l'ensemble ordonné $\mathscr{S}$ est inductif. Par le Lemme de Zorn, $\mathscr{S}$ admet un élément maximal. □

Corollary 2.11. *Tout graphe connexe G admet un arbre couvrant T (i.e. tel que $V(T) = V(G)$).*

Proof. Soit $v \in V(G)$. Par le Lemme 2.10, il existe un arbre maximal T dans G contenant v. S'il existe $w \in V(G) \smallsetminus V(T)$, on considère (par connexité) un chemin $\gamma : v \rightsquigarrow w$ (dans G), qu'on écrit $\gamma = (u_0, a_1, u_1, \dots, u_k)$. On pose

$$i = \min \{0 \leqslant j \leqslant k,\ u_j \notin T\}.$$

Alors $u_{i-1} \in T$ et $u_i \notin T$, donc l'ajout de $\left\{u_i, a_i^{\pm 1}\right\}$ à T donne un arbre contenant strictement T ; c'est une contradiction. □

Definition 2.12 (Cordes)**.** *Si T est un arbre couvrant d'un graphe connexe G, toute arête $e \in E(G) \smallsetminus E(T)$ est appelée une **corde**.*

Ainsi G/T est un bouquet de cercles sur les cordes de T dans G.

Notation 2.13. *Soit T un arbre couvrant d'un graphe connexe G.*

- *Pour $u, w \in V$, on note $T[u, w]$ l'unique chemin simple de u à w dans T.*
- *Pour $v \in V$ et $a \in A(G)$, on note $T[v, a]$ le cycle $T[v, o(a)] \cdot a \cdot T[o(a^{-1}), v]$.*
- *Pour a une corde de T, on note $T[a]$ le cycle simple $a \cdot T[o(a^{-1}), o(a)]$.*

2.3 Homotopie et groupe fondamental

Definition 2.14 (Homotopie)**.** *Un **aller-retour** (ou **spur**) est un chemin de la forme (a, a^{-1}). Un chemin sans aller-retour est dit **réduit**.*

*Une **homotopie élémentaire** sur un chemin γ consiste à ajouter ou supprimer un aller-retour dans γ. On note $\sim$ la relation d'**homotopie**, qui est la clôture transitive de l'homotopie élémentaire.*

*Une **homotopie (élémentaire) libre** est une homotopie pour les circuits ; elle sera notée $\overset{\text{libre}}{\sim}$.*

Remark 2.15. (i) *Si $\gamma \sim \gamma'$ et $\lambda \sim \lambda'$, alors $\gamma \cdot \gamma' \sim \lambda \cdot \lambda'$.*

(ii) *Pour tout chemin γ, on a $\gamma \cdot \gamma^{-1} \sim 1$.*

Definition 2.16 (Groupe fondamental)**.** *Soit G connexe et $v \in V$. Alors les classes d'homotopie de lacets de point base v constitue un groupe pour la concaténation, d'élément neutre 1. Ce groupe est appelé le **groupe fondamental** de (G, v), et noté $\pi_1(G, v)$.*

Lemma 2.17. *Chaque classe d'homotopie a un unique chemin réduit.*

Proof. L'existence est claire. Pour l'unicité, soit $\gamma \sim \lambda$ deux chemins réduits. On considère une suite d'homotopies élémentaires de γ à λ :

$$\gamma = \mu_0 \sim \mu_1 \sim \cdots \sim \mu_k = \lambda,$$

choisie t.q. $\sum_{i=0}^{k} |\mu_i|$ soit minimale. Supposons par l'absurde que $k \geqslant 1$. Dans ce cas, on a nécessairement $k \geqslant 2$, car μ_1 a un aller-retour donc n'est pas réduit. On choisit alors $0 \leqslant i \leqslant k$ avec $|\mu_i|$ maximal.

- Cas 1 : $\mu_i = uaa^{-1}vbb^{-1}w$, $\mu_{i-1} = uaa^{-1}vw$ et $\mu_{i+1} = uvbb^{-1}w$. Dans ce cas, on peut remplacer μ_i par uvw pour faire décroître strictement $\sum |\mu_i|$.
- Cas 2 : $\mu_i = uaa^{-1}v$ et $\mu_{i-1} = \mu_{i+1} = uv$. Dans ce cas, on peut supprimer μ_i, μ_{i+1} pour faire décroître $\sum |\mu_i|$.
- Cas 3 : $\mu_i = uaa^{-1}av$ et $\mu_{i-1} = \mu_{i+1} = uav$. On peut aussi supprimer μ_i, μ_{i+1}.

Les trois cas contredisent la minimalité de $\sum |\mu_i|$, donc on a nécessairement $k = 0$ et $\gamma = \lambda$. □

Proposition 2.18. *Si B_E est le bouquet de cercles sur l'ensemble E, alors $\pi_1(B_E, *) \cong F(E)$.*

Proof. On écrit $A = E \cup E^{-1}$ (cela revient à choisir une orientation pour chaque arête). Chaque $e \in E$ détermine un lacet (e) ; cela définit une application $E \to \pi_1(B_E, *)$ et donc un morphisme $\varphi : F(E) \to \pi_1(B_E, *)$. Comme $\{(e),\ e \in E\}$ génère $\pi_1(B_E, *)$, φ est surjectif. De plus, si $w \in F(E) \setminus \{1\}$, on écrit w sous forme réduite dans le groupe libre, de telle sorte que le lacet $\varphi(w)$ est réduit, donc non trivial par le Lemme 2.17 ; ainsi, φ est injectif. □

Theorem 2.19. *Soit G un graphe connexe et $v \in V$. Étant donné un arbre couvrant T de G,*

$$\pi_1(G, v) \cong F\left(E(G) \setminus E(T)\right).$$

Proof. On écrit $A = E \cup E^{-1}$. Soit $C = E(G) \setminus E(T)$ l'ensemble des cordes de T. On prétend que $\{T[v, c],\ c \in C\}$ est une base libre de $\pi_1(G, v)$. Notons d'abord que si $\gamma = (a_1, \ldots, a_k)$ est un chemin, alors $\gamma \sim T[v, a_1] \cdot T[v, a_2] \cdots T[v, a_k]$, donc la famille $\{T[v, c],\ c \in C\}$ est génératrice. De plus, elle est libre car chaque arête $c \in C$ est contenue dans un et un seul lacet de la famille. □

Corollary 2.20. *Si G est un graphe connexe et $v \in V$, alors*

$$\operatorname{rk} \pi_1(G, v) = 1 - \chi(G),$$

*où $\chi(G) = |V(G)| - |E(G)|$ est la **caractéristique d'Euler** de G.*

*L'entier $\operatorname{rk} \pi_1(G, v)$ est parfois appelé **nombre cyclomatique** de G ; c'est un invariant de graphes.*

Remark 2.21. *Le groupe fondamental définit un foncteur $\pi_1 : \mathbf{Grph}_* \to \mathbf{Gp}$.*

Proof. Si $f : G \to H$ est un morphisme de graphes, on définit l'image d'un chemin par $(a_1, \ldots, a_k) \mapsto (f(a_1), \ldots, f(a_k))$. On vérifie que $f(\gamma) \sim f(\gamma')$ dès que $\gamma \sim \gamma'$; donc f induit un morphisme de groupes $f_* : \pi_1(G, v) \to \pi_1(H, f(v))$. De plus, on a $(f \circ g)_* = f_* \circ g_*$. □

2.4 Calculs sur le groupe fondamental

Algorithm 2.22. *Pour calculer une base libre de $\pi_1(G, v)$, on calcule d'abord un arbre couvrant T en temps $\mathcal{O}(|E| + |V|) = \mathcal{O}(|E|)$ par parcours en largeur (Algorithme 1.27) et on énumère les $T[v, c]$ pour $c \in E(G) \setminus E(T)$. Ainsi, la complexité totale est $\mathcal{O}(|E| + r|V|)$, où r est le nombre cyclomatique.*

Lemma 2.23. *Si $(x_1, \dots, x_n)$ et $(u_1, \dots, u_n)$ sont deux bases libres de $F(n)$, alors il existe $\sigma \in \mathfrak{S}_n$ t.q. x_i apparaît dans l'expression réduite de $u_{\sigma(i)}$ sur $\{x_1, \dots, x_n\}$ pour tout i.*

Proof. On considère le morphisme $f : F(n) \to F(n)$ donné par $x_i \mapsto u_i$. Ce morphisme stabilise le sous-groupe dérivé, donc induit un morphisme, et en fait un isomorphisme

$$\mathbb{Z}^n \cong F(n)/[F(n), F(n)] \xrightarrow{f} F(n)/[F(n), F(n)] \cong \mathbb{Z}^n.$$

On considère la matrice $A = (u_{ij})_{1 \leqslant i,j \leqslant n}$ de l'isomorphisme $f : \mathbb{Z}^n \to \mathbb{Z}^n$. Comme f est un isomorphisme, on a

$$0 \neq \det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \leqslant i \leqslant n} u_{i,\sigma(i)},$$

donc il existe $\sigma \in \mathfrak{S}_n$ t.q. $\prod_{1 \leqslant i \leqslant n} u_{i,\sigma(i)} \neq 0$. Mais u_{ij} est le nombre d'occurrences de x_j dans l'expression de u_i; d'où le résultat avec la permutation σ ci-dessus. □

Proposition 2.24. *Si T est un arbre de plus court chemin, alors la base retournée par l'Algorithme 2.22 est de longueur totale minimale.*

Proof. On considère une base libre $(\gamma_i)_{1 \leqslant i \leqslant r}$ de $\pi_1(G, v)$. Par le Lemme 2.23, il existe $\sigma \in \mathfrak{S}_n$ t.q. $T[v, c_i]$ apparaît dans l'expression réduite de $\gamma_{\sigma(i)}$ pour tout $1 \leqslant i \leqslant r$. Par conséquent, l'arc c_i apparaît dans $\gamma_{\sigma(i)}$, d'où $\left|\gamma_{\sigma(i)}\right| \geqslant |T[v, c_i]|$. □

Algorithm 2.25. *Soit G un graphe et γ, λ deux chemins. Alors on peut décider si $\gamma \sim \lambda$ (resp. si $\gamma \overset{\text{libre}}{\sim} \lambda$). Pour cela, on trouve un chemin réduit (resp. librement réduit) pour γ, λ (ce qu'on peut effectuer en temps linéaire à l'aide d'une pile). Ensuite, on détermine si les chemins réduits sont égaux (resp. s'ils sont permutation cyclique l'un de l'autre, ce qu'on effectue en temps linéaire à l'aide de l'algorithme KMP, c.f. Algorithme 1.31).*

2.5 Homologie des graphes

Definition 2.26 (Chaînes, cycles et homologie)**.** *Soit G un graphe, avec $A = E \cup E^{-1}$.*

- *Les groupes de **chaînes** de G sont $C_0(G) = \bigoplus_{v \in V} \mathbb{Z}v$ et $C_1(G) = \bigoplus_{e \in E} \mathbb{Z}e$.*
- *Le **bord** est l'opérateur $\partial : C_1(G) \to C_0(G)$ défini par $\partial e = o(e^{-1}) - o(e)$.*
- *Les groupes de **cycles** sont $Z_0(G) = C_0(G)$ et $Z_1(G) = \operatorname{Ker} \partial$.*
- *Les groupes d'**homologie** sont $H_0(G) = Z_0(G)/\operatorname{Im} \partial$ et $H_1(G) = Z_1(G)$.*

Le paramètre G sera parfois omis de la notation.

Notation 2.27. *Étant donné un chemin $\gamma = (a_1, \dots, a_\ell)$, on considère γ comme l'élément $a_1 + \cdots + a_\ell$ de $C_1(G)$, où $a_i = -a_i^{-1}$ si $a_i \notin E$.*

Proposition 2.28. *$H_0(G)$ est isomorphe au groupe abélien libre sur les composantes connexes de G.*

Proof. On définit un morphisme d'**augmentation** $\varepsilon : C_0 \to \bigoplus_{\kappa \in K} \mathbb{Z}\kappa$, où K est l'ensemble des composantes connexes de G, par

$$\varepsilon\left(\sum_{v \in V} n_v v\right) = \sum_{\kappa \in K} \left(\sum_{v \in \kappa} n_v\right) \kappa.$$

Notons que $(\varepsilon \circ \partial)(e) = 0$ pour tout $e \in E$, donc $\operatorname{Im} \partial \subseteq \operatorname{Ker} \varepsilon$. Réciproquement, soit $x = \sum_{v \in V} n_v v \in \operatorname{Ker} \varepsilon$. On suppose que x est de support minimal parmi les éléments de $x + \operatorname{Im} \partial$. Supposons par l'absurde que $x \neq 0$. Alors il existe $v \in V$ t.q. $n_v \neq 0$. Soit κ la composante connexe contenant v ; comme $\sum_{w \in \kappa} n_w = 0$, il existe aussi $w \in \kappa \setminus \{v\}$ t.q. $n_w \neq 0$. Maintenant, v et w sont dans la

même composante connexe, donc il existe un chemin $\gamma = (a_1, \dots, a_\ell)$ de v à w. Ainsi, $\partial\gamma = w - v$, donc $x + n_v\partial\gamma \in x + \operatorname{Im}\partial$, mais $\operatorname{Supp}(x + n_v\partial\gamma) \subsetneq \operatorname{Supp}(x)$, contredisant le choix de x. Donc $x = 0 \in \operatorname{Im}\partial$.

On a prouvé que $\operatorname{Im}\partial = \operatorname{Ker}\varepsilon$, et ε est surjectif, donc on $H_0(G) = C_0/\operatorname{Im}\partial = C_0/\operatorname{Ker}\varepsilon \cong \bigoplus_{\kappa\in K}\mathbb{Z}\kappa$. □

Proposition 2.29. *Tout élément de $Z_1(G)$ se décompose en somme de cycles simples (au sens des graphes).*

Proof. Soit $x = \sum_{e\in E} n_e e \in Z_1(G)$. Soit H le sous-graphe induit par le support de x ; H n'a pas de sommet de degré 1 car $\partial x = 0$; cela implique (comme H est fini), que H contient un cycle simple c. Ainsi, si $a \in c$, l'élément $x' = x - n_a c$ est dans $Z_1(G)$ est a son support $\subsetneq \operatorname{Supp}(x)$. En itérant, on obtient le résultat. □

Corollary 2.30. *Si T est une forêt, alors $H_1(T) = 0$.*

Proposition 2.31. *Soit G un graphe connexe et T un arbre couvrant. Alors $H_1(G)$ est isomorphe au groupe abélien libre sur les cordes de T dans G.*

Le rang de $H_1(G)$ est noté $\beta_1(G)$ et appelé ***premier nombre de Betti****.*

Proof. On note C l'ensemble des cordes. Les cycles $\{T[a],\ a \in C\}$ sont indépendants dans $Z_1(G) = H_1(G)$; montrons qu'ils sont générateurs. Si $x = \sum_{e\in E} n_e e \in Z_1(G)$, alors le cycle $x - \sum_{e\in E} n_e T[e]$ a son support inclus dans T, donc est nul par la Proposition 2.29, d'où $x = \sum_{e\in E} n_e T[e]$. □

Theorem 2.32 (Hurewicz)**.** *Si G est connexe et $v \in V$, alors le morphisme $\varphi : \pi_1(G, v) \to H_1(G)$ défini par $(a_1, \dots, a_k) \mapsto \sum_{i=1}^k a_i$ induit un isomorphisme*

$$\pi_1^{\mathrm{ab}}(G, v) \cong H_1(G).$$

Proof. Le morphisme φ est bien défini car invariant par homotopie. De plus, φ est surjectif d'après la Proposition 2.29, et $\operatorname{Ker}\varphi \supseteq \pi_1'(G, v)$ car $H_1(G)$ est abélien. On montre l'inclusion réciproque en écrivant un élément $x \in \operatorname{Ker}\varphi$ dans la base libre $\{T[v, c],\ c \in C\}$ de $\pi_1(G, v)$; d'où $\operatorname{Ker}\varphi = \pi_1'(G, v)$. □

Remark 2.33. *L'homologie induit des foncteurs H_i : **Grph** $\to$ **AbGp**.*

Proof. Si $f : G \to G'$ est un morphisme de graphes, on définit $f_\sharp : C_i(G) \to C_i(G')$ par $f_\sharp(v) = f(v)$ et

$$f_\sharp(a) = \begin{cases} 0 & \text{si } f(a) \in V(G') \\ f(a) & \text{sinon} \end{cases}.$$

Alors $f_\sharp \circ \partial = \partial' \circ f_\sharp$, donc $f_\sharp$ induit des morphismes $f_* : H_i(G) \to H_i(G')$. □

Definition 2.34 (Homologie à coefficients)**.** *Étant donné un groupe abélien A, on peut définir l'****homologie à coefficients*** *dans A par*

$$H_i(G, A) = H_i(G) \otimes_{\mathbb{Z}} A.$$

2.6 Calculs sur l'homologie

Algorithm 2.35. *Pour calculer une base de $H_1(G)$, on trouve un arbre couvrant T, dont on note C l'ensemble des cordes. Alors $(T[c])_{c\in C}$ est une base de $H_1(G)$, appelée* ***base fondamentale de cycles****.*

Definition 2.36 (Poids d'une base)**.** *Soit $w : E \to \mathbb{R}_{>0}$ une fonction poids sur les arêtes d'un graphe G. Étant donné $\gamma = \sum_{e\in E} n_e e \in C_1(G)$, le* ***poids*** *de γ est*

$$|\gamma|_w = \sum_{e\in E} n_e w(e).$$

Le ***poids d'une base*** *est alors la somme des poids de ses cycles.*

Remark 2.37. *On s'intéresse au problème de calculer une base de $H_1(G)$ de poids minimal. Pour l'homologie à coefficients dans $\mathbb{Z}$, c'est un problème ouvert. Cependant, on va voir comment calculer une telle base pour l'homologie à coefficients dans $\mathbb{Z}/2$.*

Lemma 2.38. *Étant donnée une base $B = (c_1, \dots, c_{\beta_1})$ de $H_1(G, \mathbb{Z}/2)$, on note*

$$\ell(B) = \left(|c_1|_w \leqslant \cdots \leqslant |c_{\beta_1}|_w\right) \in (\mathbb{R}_{>0})^{\beta_1}.$$

Alors B est de poids minimal si et seulement si $\ell(B)$ est minimal pour l'ordre lexicographique.

Proof. Cela utilise la structure de $\mathbb{Z}/2$-espace vectoriel, et donc de **matroïde**, sur $H_1(G, \mathbb{Z}/2)$. En particulier, on utilise la propriété suivante : étant données deux familles libres L, Λ dans $H_1(G, \mathbb{Z}/2)$ avec $|L| < |\Lambda|$, alors il existe un $\lambda \in \Lambda$ t.q. $L \cup \{\lambda\}$ est libre. □

Algorithm 2.39 (Algorithme glouton)**.** *Pour calculer une base minimale de $H_1(G, \mathbb{Z}/2)$, on procède comme suit : on calcule tous les $\mathbb{Z}/2$-cycles de G ; il y en a 2^{β_1}. On les trie par ordre de poids croissant. On commence avec $B = \varnothing$ et, à chaque étape, on examine les cycles dans l'ordre jusqu'à trouvé un cycle $c \notin \langle B \rangle$. On remplace alors B par $B \cup \{c\}$, et on itère jusqu'à ce que $|B| = \beta_1$.*

Implémenté ainsi, l'algorithme glouton a une complexité exponentielle, mais on va voir qu'on peut l'améliorer.

Remark 2.40. *Soit B une base de $H_1(G, \mathbb{Z}/2)$.*

(i) *Soit $b = c + d \in B$. Alors $\{c\} \cup B \smallsetminus \{b\}$ ou $\{d\} \cup B \smallsetminus \{b\}$ est une base. En particulier, si B est minimale, alors tout $b \in B$ est un cycle simple.*

(ii) *Soit $b = pq^{-1} \in B$. Si B est minimale, alors p ou q est un plus court chemin.*

(iii) *Soit $b \in B$. Si B est minimale et v est un sommet de b, alors on peut écrire $b = paq^{-1}$, où a est un arc et p, q sont des plus courts chemins d'origine v.*

Proof. (i) Si $\{c\} \cup B \smallsetminus \{b\}$ et $\{d\} \cup B \smallsetminus \{b\}$ ne sont pas des bases, alors $c, d \in \langle B \smallsetminus \{b\} \rangle$, donc $b = c + d \in \langle B \smallsetminus \{b\} \rangle$, ce qui contredit l'indépendance de B.

(ii) S'il y avait un plus court chemin r entre $o(p)$ et $o(p^{-1})$, on pourrait remplacer b par $pr^{-1} + rq^{-1}$ puis appliquer (i).

(iii) On choisit p de longueur maximale t.q. p est un plus court chemin ; alors q est aussi un plus court chemin par (ii), car pa n'en est pas un. □

Notation 2.41. *Étant donné un arbre de plus courts chemins T_v basé en v, on note $T_v[a]$ le cycle $T_v[v, a]$, pour a une corde de T_v.*

Proposition 2.42. *Pour tout $v \in V$, on note T_v un arbre de plus courts chemins en v et C_v l'ensemble des cordes de T_v. Alors il existe une base minimale de $H_1(G, \mathbb{Z}/2)$ dont les éléments sont de la forme $T_v[a]$, pour $v \in V$ et $a \in C_v$*

Proof. Soit $b \in H_1(G, \mathbb{Z}/2)$. Pour tout $v \in V(b)$, on peut écrire $b = paq^{-1}$ à l'aide de la Remarque 2.40, où p, q sont des plus courts chemins d'origine v. On note d_v le nombre d'arêtes de $b \smallsetminus T_v[a]$ et

$$d_b = \min_{v \in V(b)} d_v.$$

On se donne une base minimale $B = (b_1, \dots, b_{\beta_1})$ avec $\sum_{i=1}^{\beta_1} d_{b_i}$ minimale.

Si $\sum_{i=1}^{\beta_1} d_{b_i} = 0$, alors $\{b_1, \dots, b_{\beta_1}\} \subseteq \{T_v[a],\ v \in V,\ a \in C_v\}$, et on a terminé.

Supposons donc, sans perte de généralité, que $d_{b_1} \neq 0$. Si $b_1 = paq^{-1}$, alors on peut écrire

$$b_1 = pT_v[x, v] + T_v[a] + T_v[v, y]q^{-1}.$$

D'après la Remarque (i), b_1 peut être remplacé par l'un des éléments $pT_v[x, v], T_v[a], T_v[v, y]\, q^{-1}$. Mais $d_{pT_v[x,v]} < d_{b_1}$, etc., ce qui contredit la minimalité de $\sum_{i=1}^{\beta_1} d_{b_i}$. □

Algorithm 2.43 (Algorithme glouton optimisé)**.** *Pour calculer une base minimale de $H_1(G, \mathbb{Z}/2)$, on procède comme suit :*

(i) *On calcule T_v pour tout $v \in V$, à l'aide de l'algorithme de Dijkstra, avec une complexité temporelle en $\mathcal{O}(|A| + |V| \log |V|)$. Au total, il faut donc $\mathcal{O}\left(|A| \cdot |V| + |V|^2 \log |V|\right)$.*

(ii) *On calcule et stocke tous les cycles $T_v[a]$ (ainsi que leurs poids), pour $v \in V$ et $a \in C_v$. À v fixé, il y a β_1 tels cycles, chacun ayant au plus $|V|$ arêtes. Au total, il faut donc $\mathcal{O}\left(\beta_1 |V|^2\right)$.*

(iii) *On trie les $T_v[a]$ en temps $\mathcal{O}(n \log n)$. Comme il y a $\beta_1 |V|$ cycles de cette forme, il faut $\mathcal{O}(\beta_1 |V| \log(\beta_1 |V|))$.*

(iv) *On examine les cycles par ordre croissant ; chaque cycle doit être comparé avec les k cycles déjà sélectionnés ; on peut déterminer si le nouveau cycle est independant des k premiers en temps $\mathcal{O}(k |A|)$ à l'aide d'un pivot de Gauß. On répète cette opération au plus $\beta_1 |V|$ fois, et on a à chaque fois $k \leqslant \beta_1$, donc il faut au total $\mathcal{O}(\beta_1^2 |A| \cdot |V|)$.*

La complexité totale est donc $\mathcal{O}\left(|A|^3 |V|\right)$ car $\beta_1 \leqslant |A|$. En particulier, ce calcul s'effectue en temps polynomial.

2.7 Cohomologie des graphes

Definition 2.44 (Cochaînes, cocycles et cohomologie)**.** *Soit G un graphe, avec $A = E \cup E^{-1}$.*

- *Les groupes de **cochaînes** de G sont $C^i(G) = \mathrm{Hom}_{\mathbb{Z}}(C_i(G), \mathbb{Z})$.*
- *Le **cobord** est l'opérateur $\delta : C^0(G) \to C^1(G)$ défini par $\delta\varphi = \varphi \circ \partial$.*
- *Les groupes de **cocycles** sont $Z^0(G) = \operatorname{Ker} \delta$ et $Z^1(G) = C^1(G)$.*
- *Les groupes de **cohomologie** sont $H^0(G) = Z^0(G)$ et $H^1(G) = Z^1(G)/\operatorname{Im} \delta$.*

Le paramètre G sera parfois omis de la notation.

Proposition 2.45. (i) *Si G est connexe, alors $H^0(G) \cong \mathbb{Z}$.*

(ii) *Si K est l'ensemble des composantes connexes de G, alors $H^0(G) \cong \mathbb{Z}^K$.*

(iii) *Si T est un arbre, alors $H^1(T) = 0$.*

(iv) *Si T est un arbre couvrant de G, et C est l'ensemble des cordes de T, alors $H^1(G) \cong \mathbb{Z}^C$.*

Proof. (i) Soit $\varphi \in H^0(G) = \operatorname{Ker} \delta$. Pour $a \in A$, on a $0 = \delta\varphi(a) = \varphi(o(a^{-1})) - \varphi(o(a))$, donc

$$\varphi\left(o\left(a^{-1}\right)\right) = \varphi(o(a)).$$

Comme c'est vrai pour tout a et que G est connexe, φ est constant, égal à φ_0. On montre alors aisément que l'application $\varphi \mapsto \varphi_0$ est un isomorphisme de groupes $H^0(G) \to \mathbb{Z}$.

(iii) Soit $v \in V(T)$. On définit un "potentiel" $\sigma_T : C^1(T) \to C^0(T)$ par

$$\sigma_T(f) \cdot w = \sum_{a \in T[v,w]} f(a).$$

On a alors $\delta \circ \sigma_T = \mathrm{id}_{C^1(T)}$, d'où $C^1(T) = \operatorname{Im} \delta$, donc $H^1(T) = 0$.

(iv) Soit $\pi : \mathbb{Z}^C \to C^1/\operatorname{Im}\delta$ défini par

$$\pi(\phi)\cdot a = \begin{cases} \phi(c) & \text{si } a \in c \\ 0 & \text{sinon} \end{cases},$$

pour $\phi \in \mathbb{Z}^C$. Remarquons que, pour $g \in C^1(G)$, l'élément $g - g_{|T} = g - \delta\circ\sigma_T\left(g_{|T}\right) \in g + \operatorname{Im}\delta$ s'annule sur T, donc est dans $\operatorname{Im}\pi$. Ainsi, π est surjectif. Soit maintenant $\phi \in \operatorname{Ker}\pi$. Alors $\pi(\phi) = \delta f$ pour un certain $f \in C^0(G)$. Comme $\pi(\phi)$ s'annule sur T, f est constant sur T, donc sur G, d'où $\delta f = 0$ et $\phi = 0$. □

2.8 Revêtements de graphes

Notation 2.46. *Si G est un graphe et $v \in V$, on note* $\operatorname{Star}(v) = \{a \in A,\ o(a) = v\}$.

Definition 2.47 (Revêtement de graphes)**.** *Un morphisme de graphes $p : H \to G$ est un* ***revêtement*** *si p est surjectif, et si pour tout $v \in V(H)$, la restriction $p_{|\operatorname{Star}(v)} : \operatorname{Star}(v) \to \operatorname{Star}(p(v))$ est une bijection.*

On dit alors que G est la ***base*** *et H l'****espace total****.*

Si γ est un chemin dans G, un ***relèvement*** *de γ est un chemin λ dans H t.q. $p(\lambda) = \gamma$.*

Lemma 2.48. *Soit $p : H \to G$ un revêtement.*

(i) *Étant donné un chemin γ dans G d'origine v, et un sommet $w \in p^{-1}(v)$, il existe un unique relèvement λ de γ d'origine w.*

(ii) *Si α, β sont deux chemins homotopes d'origine v dans G, alors leurs relèvements respectifs $\widetilde{\alpha}, \widetilde{\beta}$ de même origine $w \in p^{-1}(v)$ sont homotopes.*

Proof. (i) On écrit $\gamma = (a_1, \ldots, a_k)$. Par définition, il existe un unique $b_1 \in \operatorname{Star}(w)$ t.q. $p(b_1) = a_1$. On itère ce procédé pour obtenir un relèvement de γ.

(ii) On décompose en homotopies élémentaires et on remarque que chaque aller-retour se relève en un aller-retour. □

Definition 2.49 (Action de monodromie)**.** *Soit $p : H \to G$ un revêtement et $v \in V(G)$ un point base. Pour $w \in p^{-1}(v)$ et $[\alpha] \in \pi_1(G, v)$, on note $w \cdot [\alpha]$ l'extrémité de l'unique relèvement $\widetilde{\alpha}$ de α t.q. $o(\widetilde{\alpha}) = w$.*

Ceci définit une action (à droite) $p^{-1}(v) \curvearrowleft \pi_1(G, v)$, appelée ***action de monodromie****. L'image de $\pi_1(G, v)$ dans $\mathfrak{S}_{p^{-1}(v)}$ est appelée* ***groupe de monodromie****.*

Proposition 2.50. *Si $p : (H, w) \to (G, v)$ est un revêtement pointé, alors le morphisme induit*

$$p_* : \pi_1(H, w) \to \pi_1(G, v)$$

est injectif.

Proof. Soit α, β des boucles de point base w dans H. Alors $p_*[\alpha] = p_*[\beta]$ si et seulement si $p(\alpha) \sim p(\beta)$. Par le Lemme 2.48, ceci implique que $\alpha \sim \beta$, i.e. $[\alpha] = [\beta]$. □

Corollary 2.51. *Le groupe libre $F(2)$ de rang 2 contient des sous-groupes libres de tout rang.*

Proposition 2.52. *Soit (G, v) un graphe connexe pointé. Pour tout sous-groupe $U \leqslant \pi_1(G, v)$, il existe un revêtement $p_U : (G_U, w) \to (G, v)$ t.q. $p_{U*}\pi_1(G_U, w) = U$.*

Proof. On fixe un arbre couvrant T de G. On construit $G_U = (V_U, A_U, o_U, \iota_U)$, avec $V_U = V \times (U\backslash\Gamma)$ (où $U\backslash\Gamma$ est l'ensemble des classes à droite de U dans $\Gamma = \pi_1(G, v)$), $A_U = A \times (U\backslash\Gamma)$, $o_U : (a, Ug) \mapsto (o(a), Ug)$ et $\iota_U : (a, Ug) \mapsto (\iota(a), UgT[v, a])$. Pour vérifier que ceci définit bien un graphe, il faut prouver que ι_U est une involution, ce qui est bien le cas car

$$T[v, a] \cdot T\left[v, a^{-1}\right] \sim 1.$$

On définit ensuite un morphisme $p_U : G_U \to G$ par $(v, Ug) \mapsto v$ et $(a, Ug) \mapsto a$. Il est clair que p_U est surjectif et, pour $(w, Ug) \in V_U$, on a

$$\mathrm{Star}_{G_U}(w, Ug) = \mathrm{Star}_G(w) \times \{Ug\},$$

donc $p_{U|_{\mathrm{Star}_{G_U}(w,Ug)}} : \mathrm{Star}_{G_U}(w, Ug) \to \mathrm{Star}_G(w)$ est une bijection, et p_U est un revêtement.

Reste à prouver que $p_{U*}\pi_1(G_U, w) = U$, avec $w = (v, U) \in V_U$. Soit $[\gamma] = [(a_1, \ldots, a_k)] \in \pi_1(G, v)$. Alors $[\gamma] \in p_{U*}\pi_1(G_U, w)$ si et seulement si $w \cdot [\gamma] = w$. Mais

$$w \cdot [\gamma] = (v, U) \cdot [\gamma] = (v, U \cdot T[v, a_1] \cdots T[v, a_k]) = (v, U[\gamma]),$$

car $T[v, a_1] \cdots T[v, a_k] \sim (a_1, \ldots, a_k) = \gamma$. Ainsi, $[\gamma] \in p_{U*}\pi_1(G_U, w)$ si et seulement si $[\gamma] \in U$, d'où le résultat. □

Corollary 2.53 (Nielsen-Schreier)**.** *Tout sous-groupe d'un groupe libre est libre.*

Definition 2.54 (Morphisme de revêtements)**.** *Un* ***morphisme*** *entre deux revêtements $p : H \to G$ et $q : K \to G$ est un morphisme de graphes $f : H \to K$ t.q. $p = q \circ f$.*

Cette définition implique que f lui-même est un revêtement.

Lemma 2.55. *Il existe un morphisme entre deux revêtements pointés $p : (H, v) \to (G, u)$ et $q : (K, w) \to (G, u)$ si et seulement si*

$$p_*\pi_1(H, v) \leqslant q_*\pi_1(K, w).$$

Proof. ($\Rightarrow$) Si $f : H \to K$ est un morphisme, alors $p = qf$ donc $p_* = q_*f_*$ par fonctorialité, d'où l'inclusion voulue. ($\Leftarrow$) Supposons que $p_*\pi_1(H, v) \leqslant q_*\pi_1(K, w)$. On définit $f : H \to K$ par

$$f(x) = w \cdot [p(\gamma)],$$

où γ est un chemin de v à x dans H. Montrons d'abord que cette définition ne dépend pas du choix de γ. En effet, si λ est un autre chemin de v à x, alors

$$w \cdot [p(\gamma)] = w \cdot \left[p\left(\gamma\lambda^{-1}\lambda\right)\right] = w \cdot p_*\left[\gamma\lambda^{-1}\right] \cdot [p(\lambda)] = w \cdot [p(\lambda)],$$

car $p_*[\gamma\lambda^{-1}] \in p_*\pi_1(H, v) \subseteq q_*\pi_1(K, w)$. Ainsi, f est bien définie. On vérifie alors aisément que f induit un morphisme de graphes. □

Theorem 2.56. *Les classes d'isomorphisme de revêtements d'un graphe G sont en correspondance avec les classes de conjugaison des sous-groupes de $\pi_1(G, u)$.*

Cette correspondance transforme un morphisme $(H \to G) \longrightarrow (K \to G)$ entre revêtements en une inclusion à conjugaison près $W_H \leqslant gW_Kg^{-1}$ de sous-groupes de $\pi_1(G, u)$.

En particulier, il existe un unique revêtement de G correspondant au sous-groupe trivial de $\pi_1(G, u)$; ce revêtement est appelé le ***revêtement universel*** *de G.*

Proof. À l'aide du Lemme 2.55, on voit qu'il existe un isomorphisme entre des revêtements (non pointés) $p : H \to G$ et $q : K \to G$ si et seulement si $p_*\pi_1(H, v)$ et $q_*\pi_1(K, w)$ sont conjugués. □

2.9 Graphes quotients

Notation 2.57. *Si G est un graphe, on note* $\mathrm{Aut}(G)$ *le groupe des automorphismes de graphe de G.*

Definition 2.58 (Action sans inversion d'arc)**.** *Soit G un graphe. On dit qu'un sous-groupe $\Gamma \leqslant \mathrm{Aut}(G)$* ***agit sans inversion d'arc*** *si pour tout $g \in \Gamma$ et pour tout $a \in A$, $ga \neq a^{-1}$.*

Definition 2.59 (Graphe quotient)**.** *Soit $\Gamma \leqslant \mathrm{Aut}(G)$ un groupe agissant sans inversion d'arc. On peut alors définir le* ***graphe quotient*** *$G/\Gamma = \left(\overline{V}, \overline{A}, \overline{o}, \overline{\iota}\right)$ par $\overline{V} = \{\Gamma v,\ v \in V(G)\}$, $\overline{A} = \{\Gamma a,\ a \in A(G)\}$, $\overline{o} : \Gamma a \mapsto \Gamma o(a)$ et $\overline{\iota} : \Gamma a \mapsto \Gamma \iota(a)$. L'application $\overline{\iota}$ est une involution sans point fixe car Γ agit sans inversion d'arc, donc G/Γ est bien un graphe.*

De plus, on a un morphisme naturel $p_\Gamma : G \to G/\Gamma$, appelé ***projection****.*

Definition 2.60 (Action libre)**.** *Soit G un graphe. On dit qu'un sous-groupe $\Gamma \leqslant \mathrm{Aut}(G)$* ***agit librement*** *si les deux conditions suivantes sont satisfaites :*

(i) *Γ agit sans inversion d'arc,*

(ii) *Pour tout $g \in \Gamma$ et pour tout $v \in V$, $gv \neq v$.*

Lemma 2.61. *Soit $\Gamma \leqslant \mathrm{Aut}(G)$ un groupe agissant sans inversion d'arc. Alors $p_\Gamma : G \to G/\Gamma$ est un revêtement si et seulement si Γ agit librement.*

Proof. Notons que la projection p_Γ est toujours surjective. Ainsi, il suffit de montrer que $p_{\Gamma|\mathrm{Star}(v)}$ est injective pour tout v si et seulement si Γ agit librement.

($\Leftarrow$) Supposons qu'il existe $v \in V(G)$ t.q. $p_{\Gamma|\mathrm{Star}(v)}$ n'est pas injective. Alors il existe $a \neq b \in \mathrm{Star}(v)$ t.q. $p_\Gamma(a) = p_\Gamma(b)$. Autrement dit, il existe $g \in \Gamma$ t.q. $b = ga$. Ainsi, $g \neq \mathrm{id}$, mais $gv = v$, donc Γ n'agit pas librement.

($\Rightarrow$) Supposons que Γ n'agit pas librement. Alors il existe $g \in \Gamma \smallsetminus \{e\}$ et $v \in V(G)$ t.q. $gv = v$. On considère alors l'ensemble

$$B = \{b \in A(G),\ gb = b\} \subseteq A.$$

Cet ensemble induit un sous-graphe propre $G_B \subsetneq G$. En particulier, on peut trouver un chemin $\gamma = (a_1, \ldots, a_\ell)$ d'origine v et qui n'est pas contenu dans G_B. On considère alors

$$k = \min\left\{1 \leqslant j \leqslant \ell,\ a_j \notin B\right\}.$$

Ainsi $ga_j \neq a_j$ mais $go\left(a_j\right) = o\left(a_j\right)$, donc $p_{\Gamma|\mathrm{Star}(o(a_j))}$ n'est pas injective. □

Proposition 2.62. *Soit $\Gamma \leqslant \mathrm{Aut}(G)$ un groupe agissant librement. Alors, pour tout $v \in V(G)$, on a*

$$\left(p_\Gamma\right)_* \pi_1\left(G, v\right) \trianglelefteq \pi_1\left(G/\Gamma, p_\Gamma(v)\right).$$

Proof. Soit $\alpha \in \left(p_\Gamma\right)_* \pi_1\left(G, v\right)$ et $\gamma \in \pi_1\left(G/\Gamma, p_\Gamma(v)\right)$. On veut prouver que $\gamma^{-1}\alpha\gamma \in \left(p_\Gamma\right)_* \pi_1\left(G, v\right)$, ce qui revient à $v \cdot \gamma^{-1}\alpha\gamma = v$. Mais notons que, par définition de p_Γ, il existe $g \in \Gamma$ t.q. $v \cdot \gamma^{-1} = gv$. Ainsi

$$v \cdot \gamma^{-1}\alpha\gamma = (gv) \cdot \alpha\gamma = g\left(v \cdot \alpha\right) \cdot \gamma = (gv) \cdot \gamma = v.$$ □

2.10 Groupe d'automorphismes d'un revêtement

Definition 2.63 (Automorphismes d'un revêtement)**.** *Étant donné un revêtement $p : H \to G$, on note* $\mathrm{Aut}(p) \leqslant \mathrm{Aut}(H)$ *le groupe des* ***automorphismes*** *de p, i.e. des éléments $f \in \mathrm{Aut}(H)$ t.q. $p \circ f = p$.*

Lemma 2.64. *Si $p : H \to G$ est un revêtement, alors* $\mathrm{Aut}(p)$ *agit librement sur H.*

Proof. Soit $f \in \mathrm{Aut}(p)$. Notons d'abord, que pour $a \in A(H)$, on a $f(a) \neq a^{-1}$, car on aurait sinon $p(a) = p \circ f(a) = p\left(a^{-1}\right) = p\left(a\right)^{-1}$. Ainsi, $\mathrm{Aut}(p)$ agit sans inversion d'arcs.

Soit maintenant $v \in V(H)$ t.q. $f(v) = v$. Pour $w \in V(H)$, on considère un chemin $\alpha : v \rightsquigarrow w$ dans G. Alors on a $p(\alpha) \in \pi_1\left(G, p(v)\right)$ et $w = v \cdot p(\alpha)$, donc

$$f(w) = f\left(v \cdot p(\alpha)\right) = f(v) \cdot p(\alpha) = v \cdot p(\alpha) = w.$$

Ainsi, f agit trivialement sur $V(H)$, d'où on déduit que f agit trivialement sur $A(H)$ car p est un revêtement. Ainsi, $\mathrm{Aut}(p)$ agit librement sur H. □

Proposition 2.65. *Si $\Gamma \leqslant \mathrm{Aut}(G)$ est un groupe agissant librement, alors*

$$\mathrm{Aut}\left(p_\Gamma\right) = \Gamma.$$

Proof. Il est clair que $\Gamma \leqslant \mathrm{Aut}\left(p_\Gamma\right)$. Réciproquement, soit $f \in \mathrm{Aut}\left(p_\Gamma\right)$. Si $v \in V(G)$ est fixé, alors $p_\Gamma \circ f(v) = p_\Gamma(v)$, donc il existe $g \in \Gamma$ t.q. $f(v) = gv$. Mais $g \in \Gamma \leqslant \mathrm{Aut}\left(p_\Gamma\right)$, et $\mathrm{Aut}\left(p_\Gamma\right)$ agit librement sur G par le Lemme 2.64, donc $f = g \in \Gamma$. □

Proposition 2.66. *Soit $p : (H, v) \to (G, u)$ un revêtement, soit $w \in p^{-1}(u)$. Alors $p_*\pi_1(H, v) = p_*\pi_1(H, w)$ si et seulement s'il existe $f \in \mathrm{Aut}(p)$ t.q. $w = f(v)$.*

Proof. ($\Leftarrow$) Si $w = f(v)$ avec $f \in \mathrm{Aut}(p)$, alors $f_*\pi_1(H, v) = \pi_1(H, w)$ car f_* est un isomorphisme de groupes. Ainsi

$$p_*\pi_1(H, v) = p_*f_*\pi_1(H, v) = p_*\pi_1(H, w).$$

($\Rightarrow$) Supposons que $p_*\pi_1\left(H, v\right) = p_*\pi_1\left(H, w\right)$. Étant donné $x \in V(H)$, on définit

$$f(x) = w \cdot p(\alpha),$$

où $\alpha : v \rightsquigarrow x$ dans H. Ceci est bien défini, si $\beta : v \rightsquigarrow x$ est un autre chemin dans H, alors

$$w \cdot p(\alpha) = w \cdot p\left(\alpha\beta^{-1}\right) p\left(\beta\right) = w \cdot p(\beta)$$

car $p\left(\alpha\beta^{-1}\right) \in p_*\pi_1(H, v) = p_*\pi_1(H, w)$. On étend alors naturellement cette définition aux arcs en utilisant le fait que p induit des bijections $\mathrm{Star}(x) \to \mathrm{Star}\left(p(x)\right)$ pour $x \in V(H)$. On a bien $f \in \mathrm{Aut}(p)$ et $f(v) = w$. □

Definition 2.67. *Soit $p : (H, v) \to (G, u)$ un revêtement. S'équivalent :*

(i) $p_*\pi_1(H, v) \trianglelefteq \pi_1(G, u)$.

(ii) $\mathrm{Aut}(p)$ *agit transitivement sur* $p^{-1}(u)$.

Lorsque ces conditions sont satisfaites, on dit que p est un ***revêtement normal*** *(ou* ***galoisien****, ou* ***régulier****).*

Proof. Les conjugués de $p_*\pi_1(H, v)$ dans $\pi_1(G, u)$ sont les $p_*\pi_1(H, w)$ pour $w \in p^{-1}(u)$. Le résultat s'ensuit alors par la Proposition 2.66. □

Proposition 2.68. *Soit $p : (H, v) \to (G, u)$ un revêtement et soit $\Gamma \leqslant \mathrm{Aut}(H)$ un sous-groupe agissant sans inversion d'arc. Alors les morphismes $p : H \to G$ et $p_\Gamma : H \to H/\Gamma$ sont isomorphes (i.e. il existe un isomorphisme $\varphi : H/\Gamma \to G$ t.q. $p = \varphi \circ p_\Gamma$) si et seulement si $\Gamma = \mathrm{Aut}(p)$ et p est normal.*

Proof. ($\Rightarrow$) Si p et p_Γ sont isomorphes, alors $\Gamma = \mathrm{Aut}\left(p_\Gamma\right) = \mathrm{Aut}(p)$ d'après la Proposition 2.65 ; et p_Γ est un revêtement normal d'après la Proposition 2.62, donc p aussi. ($\Leftarrow$) Notons que la projection $H \to H/\mathrm{Aut}(p)$ est isomorphe à $H \to G$ lorsque p est normal. □

Theorem 2.69. *Soit $p : H \to G$ un revêtement. Alors, pour $v \in V(H)$*

$$\mathrm{Aut}(p) \cong N\left(p_*\pi_1(H,v)\right)/p_*\pi_1(H,v),$$

où N désigne le normalisateur dans $\pi_1(G, p(v))$.

Proof. Étant donné $\lambda \in N\left(p_*\pi_1(H,v)\right)$, on a

$$p_*\pi_1\left(H, v\cdot\lambda\right) = \lambda^{-1}p_*\pi_1(H,v)\lambda = p_*\pi_1(H,v).$$

D'après la Proposition 2.66, il existe $f_\lambda \in \mathrm{Aut}(p)$ t.q. $f_\lambda(v) = v\cdot\lambda$. De plus, f_λ est unique car $\mathrm{Aut}(p)$ agit librement (voir Lemme 2.64). On définit ainsi une application

$$\phi : N\left(p_*\pi_1(H,v)\right) \to \mathrm{Aut}(p)$$

par $\lambda \mapsto f_\lambda$.

- ϕ est un morphisme de groupes : si $\lambda, \mu \in N\left(p_*\pi_1(H,v)\right)$, alors

  $$f_{\lambda\mu}(v) = v\cdot(\lambda\mu) = (v\cdot\lambda)\cdot\mu = f_\lambda(v)\cdot\mu = f_\lambda\left(v\cdot\mu\right) = f_\lambda \circ f_\mu(v).$$

  Par unicité, $f_{\lambda\mu} = f_\lambda \circ f_\mu$, donc $\phi\left(\lambda\mu\right) = \phi\left(\lambda\right)\phi\left(\mu\right)$.

- ϕ est surjectif : si $f \in \mathrm{Aut}(p)$, on choisit un chemin $\widetilde{\lambda} : v \rightsquigarrow f(v)$ dans H, on note $\lambda = \left[p\left(\widetilde{\lambda}\right)\right] \in \pi_1\left(G, p(v)\right)$, et on remarque que

  $$\lambda^{-1}p_*\pi_1\left(H,v\right)\lambda = p_*\pi_1\left(H, f(v)\right) = p_*\pi_1(H,v),$$

  d'après la Proposition 2.66. Ainsi, $\lambda \in N\left(p_*\pi_1(H,v)\right)$ et $f = f_\lambda = \phi\left(\lambda\right)$.

- $\mathrm{Ker}\,\phi = p_*\pi_1(H,v)$. En effet, pour $\lambda \in N\left(p_*\pi_1(H,v)\right)$, on a

  $$\lambda \in \mathrm{Ker}\,\phi \iff f_\lambda = \mathrm{id} \iff v\cdot\lambda = v \iff \lambda \in p_*\pi_1(H,v). \qquad \square$$

3 Combinatorial surfaces

3.1 Definitions

Definition 3.1 (Cellular embedding)**.** *Given a graph G and an oriented surface S, a **cellular embedding** $G \hookrightarrow S$ is a topological embedding such that $S \smallsetminus G$ is a disjoint union of open disks.*

Definition 3.2 (Combinatorial map)**.** *A **(combinatorial) map** is a triple $M = (A, \rho, \iota)$, where A is a set, $\rho \in \mathfrak{S}_A$ is a permutation called the **rotation system**, and $\iota : A \to A$ is a fixed-point-free involution.*

We associate to such a map M a graph $G(M) = (V, A, o, \iota)$, with $V = A/\langle\rho\rangle$ and $o : a \mapsto \langle\rho\rangle\, a$.

*The **monodromy group** (or **cartographic group**) is $\langle\rho, \iota\rangle \leqslant \mathfrak{S}_A$.*

*The map M is said to be **connected** if the graph $G(M)$ is connected, or equivalently, if the monodromy group acts transitively on A.*

*The permutation $\varphi = \rho \circ \iota$ is called the **facial permutation**; a **face** of M is an orbit of $\langle\varphi\rangle$.*

*Given a vertex $v = \langle\rho\rangle\, a$, we define $\mathrm{Star}(v) = \langle\rho\rangle\, a \subseteq A$. Likewise, given a face $f = \langle\varphi\rangle\, a$, we define $\mathrm{Star}(f) = \langle\varphi\rangle\, a \subseteq A$. The cardinal of $\mathrm{Star}(x)$ is called the **degree** of x if x is a vertex or a face.*

The set of vertices (resp. faces) of M is denoted by $V(M)$ (resp. $F(M)$).

Definition 3.3 (Topological realisation of a map)**.** *Given a map $M = (A, \rho, \iota)$, its **topological realisation** is one of the following two equivalent constructions:*

- *Take one k-gon per face of degree k, and glue together every pair of faces corresponding to inverse arcs.*
- *Take one disk per vertex, one strip per arc incident to that vertex, and glue them in the natural way to obtain a surface with boundary. Then glue a disk along every boundary component.*

Remark 3.4. *Given a cellular embedding $\eta : G \hookrightarrow S$, there is an associated map $M(\eta)$ such that the topological realisation $\eta_M : M(\eta) \hookrightarrow S(M(\eta))$ is isomorphic to η.*

Conversely, given a map M with topological realisation $\eta_M : M \hookrightarrow S(M)$, we have an isomorphism $M \cong M(\eta_M)$.

3.2 Ramification and Riemann-Hurwitz Formula

Definition 3.5 (Morphism of maps)**.** *A **morphism** between combinatorial maps $M = (A, \rho, \iota)$ and $N = (B, \sigma, \jmath)$ is a mapping $f : A \to B$ s.t. $\sigma \circ f = f \circ \rho$ and $\jmath \circ f = f \circ \iota$.*

Lemma 3.6. *Let $M = (A, \rho, \iota)$ and $N = (B, \sigma, \jmath)$ be connected maps, and consider a morphism $f : M \to N$.*

(i) *f is surjective on arcs.*

(ii) *f sends stars of vertices (resp. faces) to stars of vertices (resp. faces), so f induces maps $f : V(M) \to V(N)$ and $f : F(M) \to F(N)$.*

(iii) *Given $x \in V(M) \cup F(M)$, the induced map $f : \mathrm{Star}(x) \to \mathrm{Star}(f(x))$ is isomorphic to the quotient map*

$$\mathbb{Z}/(e_x d) \to \mathbb{Z}/d,$$

with $d = \deg f(x)$ and $e_x \geqslant 1$.

(iv) *f induces a group epimorphism $f : \langle \rho, \iota \rangle \to \langle \sigma, \jmath \rangle$ given by $\rho \mapsto \sigma$ and $\iota \mapsto \jmath$, and such that $f \circ \theta = f(\theta) \circ f$ for all $\theta \in \langle \rho, \iota \rangle$.*

*The positive integer e_x is called the **ramification index** of x.*

Proof. Let $a \in A$. By connectedness of M and N, we have $A = \langle \rho, \iota \rangle a$ and $B = \langle \sigma, \jmath \rangle f(a)$. Therefore,

$$f(A) = f(\langle \rho, \iota \rangle a) = \langle \sigma, \jmath \rangle f(a) = B,$$

so f is onto. Take $x \in V(M)$ (the argument is similar if $x \in F(M)$). Then $\mathrm{Star}(x) = \langle \rho \rangle a$, for some $a \in A$, so $f(\mathrm{Star}(x)) = \langle \sigma \rangle f(a) = \mathrm{Star}(f(x))$.

Moreover, for $n \in \mathbb{Z}$, $f(\rho^n a) = \sigma^n f(a)$. It follows that $d = |\langle \sigma \rangle f(a)|$ divides $|\langle \rho \rangle a| = e_x d$, and the map $\rho^n a \mapsto \sigma^n f(a)$ is isomorphic to $\mathbb{Z}/(e_x d) \to \mathbb{Z}/d$. □

Lemma 3.7. *Let $M = (A, \rho, \iota)$ and $N = (B, \sigma, \jmath)$ be connected maps, and consider a morphism $f : M \to N$. Then all the fibres of f have the same size, called the **degree** of f and denoted by $\deg f$.*

Proof. Let $b, b' \in B$. Then by connectedness there exists $\tau \in \langle \sigma, \jmath \rangle$ s.t. $b' = \tau(b)$. Thus, if $\theta \in \langle \rho, \iota \rangle$ is an element of the monodromy group s.t. $\tau = f(\theta)$, then

$$a \in f^{-1}(b) \iff f(a) = b \iff \tau \circ f(a) = b' \iff f \circ \theta(a) = b' \iff \theta(a) \in f^{-1}(b').$$

Therefore, θ induces a bijection $f^{-1}(b) \to f^{-1}(b')$. □

Definition 3.8 (Euler characteristic)**.** *The **Euler characteristic** of a map M is defined by*

$$\chi(M) = |V(M)| - |E(M)| + |F(M)|.$$

*The **genus** of M is $g(M) = 1 - \frac{1}{2}\chi(M)$.*

The classification of combinatorial maps will imply that $g(M)$ is a nonnegative integer.

Proposition 3.9 (Index Formula)**.** *Let $M = (A, \rho, \iota)$ and $N = (B, \sigma, \jmath)$ be connected maps, and consider a morphism $f : M \to N$. For $w \in V(N) \cup F(N)$, we have*

$$\deg f = \sum_{v \in f^{-1}(w)} e_v.$$

Proof. Let $a \in \mathrm{Star}(w)$. Then

$$\deg f = \left|f^{-1}(a)\right| = \sum_{v \in f^{-1}(w)} |\{b \in \mathrm{Star}(v),\ f(b) = a\}| = \sum_{v \in f^{-1}(w)} e_v. \qquad \square$$

Theorem 3.10 (Riemann-Hurwitz)**.** *Let $M = (A, \rho, \iota)$ and $N = (B, \sigma, \jmath)$ be connected maps, and consider a morphism $f : M \to N$. Then*

$$\chi(M) = (\deg f)\,\chi(N) - \sum_{v \in V(M) \cup F(M)} (e_v - 1)\,.$$

Proof. Write $d = \deg f$. Note that $|E(M)| = d\,|E(N)|$. Moreover, the Index Formula (Proposition 3.9) implies that, for all $w \in V(N) \cup F(N)$,

$$d = \sum_{v \in f^{-1}(w)} e_v = \sum_{v \in f^{-1}(w)} (e_v - 1) + \left|f^{-1}(w)\right|.$$

Therefore,

$$\begin{aligned}
\chi(M) &= |V(M)| - |E(M)| + |F(M)| \\
&= \sum_{w \in V(N)} \left|f^{-1}(w)\right| - d\,|E(N)| + \sum_{w \in F(N)} \left|f^{-1}(w)\right| \\
&= \sum_{w \in V(N)} \left(d - \sum_{v \in f^{-1}(w)} (e_v - 1)\right) + \sum_{w \in F(N)} \left(d - \sum_{v \in f^{-1}(w)} (e_v - 1)\right) - d\,|E(N)| \\
&= d\,|V(N)| - d\,|E(N)| + d\,|F(N)| - \sum_{v \in V(M) \cup F(M)} (e_v - 1) \\
&= d\chi(N) - \sum_{v \in V(M) \cup F(M)} (e_v - 1)\,.
\end{aligned}$$

$\square$

3.3 Operations on maps

Definition 3.11 (Dual map)**.** *The **dual** of a map $M = (A, \rho, \iota)$ is the map $M^* = (A, \rho \circ \iota, \iota)$.*

Proposition 3.12. *Let M be a map.*

(i) *M is connected* iff *M^* is connected.*

(ii) *$M^{**} = M$.*

(iii) *$\chi(M) = \chi(M^*)$.*

Proof. (i) M and M^* have the same monodromy group. (ii) $\rho \circ \iota \circ \iota = \rho$ because ι is an involution. (iii) Note that $|E(M^*)| = |E(M)|$, $|V(M^*)| = |F(M)|$ and $|F(M^*)| = |V(M)|$. $\square$

Definition 3.13 (Edge contraction)**.** *Let $M = (A, \rho, \iota)$ be a connected map with at least two edges, and let $e \in E(M)$ be a non-loop edge. The **contraction of** e is the map $M/e = (A \smallsetminus e, \rho', \iota)$, with*

$$\rho'(b) = \begin{cases} \rho(b) & \text{if } \rho(b) \notin e \\ \rho\iota\rho(b) & \text{if } \rho(b) \in e \text{ but } \rho\iota\rho(b) \notin e \\ \rho^2(b) & \text{otherwise} \end{cases}.$$

Proposition 3.14. *If M is connected, then M/e is connected and $\chi(M) = \chi(M/e)$.*

Proof. Note first that $|E(M/e)| = |E(M)| - 1$. Moreover, the new facial permutation $\varphi' = \rho'\iota$ is obtained by removing occurrences of a and a^{-1} (where $e = \{a^{\pm 1}\}$) in the cycles of the facial permutation $\varphi = \rho\iota$; in particular, the number of cycles is unchanged so $|F(M/e)| = |F(M)|$. Similarly, $|V(M/e)| = |V(M)| - 1$. This implies that $\chi(M/e) = \chi(M)$, and connectedness follows from the above analysis of the cycles of φ' and ρ'. □

Definition 3.15 (Edge deletion)**.** *Let $M = (A, \rho, \iota)$ be a map and $e \in E(M)$ be an edge without endpoint of degree* 1*. The **deletion of** e is the map $M - e = (A \setminus e, \rho', \iota)$, where*

$$\rho'(b) = \begin{cases} \rho(b) & \text{if } \rho(b) \notin e \\ \rho^2(b) & \text{if } \rho(b) \in e \text{ but } \rho^2(b) \notin e \\ \rho^3(b) & \text{otherwise} \end{cases}.$$

Definition 3.16 (Regular and singular edges)**.** *An edge $e = \{a^{\pm 1}\}$ of a map M is said to be **regular** if $F(a) \neq F(a^{-1})$ and **singular** otherwise.*

Proposition 3.17. *Let M be a connected map with at least two edges and $e \in E(M)$ be an edge without endpoint of degree* 1*. Then*

$$\chi(M - e) = \begin{cases} \chi(M) & \text{if } e \text{ is regular} \\ \chi(M) + 2 & \text{if } e \text{ is singular} \end{cases}.$$

Proof. Note that $|E(M - e)| = |E(M)| - 1$. Moreover, $|V(M - e)| = |V(M)|$ because e has no endpoint of degree 1. Finally,

$$|F(M - e)| = \begin{cases} |F(M)| - 1 & \text{if } e \text{ is regular} \\ |F(M)| + 1 & \text{if } e \text{ is singular} \end{cases}. \qquad \square$$

Proposition 3.18. *Let M be a connected map and $e \in E(M)$ be a regular edge. Then the following assertions are true as soon as they are well-defined:*

(i) $(M - e)^* = M^*/e$,

(ii) $(M/e)^* = M^* - e$.

3.4 Combinatorial equivalence

Definition 3.19 (Edge subdivision)**.** *Let $M = (A, \rho, \iota)$ be a map and $e = \{a^{\pm 1}\} \in E(M)$. Then the **edge subdivision** S_eM is the map $(A \amalg \{b^{\pm 1}\}, \rho', \iota')$, with $\iota'_{|A} = \iota$, $\iota'(b) = b^{-1}$, and*

$$\rho'(c) = \begin{cases} b & \text{if } \rho(c) = a \\ \rho(a) & \text{if } c = b \\ b^{-1} & \text{if } c = a \\ a & \text{if } c = b^{-1} \\ \rho(c) & \text{otherwise} \end{cases}.$$

In other words, we add a new vertex at the middle of e.

Proposition 3.20. *If M is connected, then S_eM is connected and $\chi(S_eM) = \chi(M)$.*

Definition 3.21 (Face subdivision)**.** *Let $M = (A, \rho, \iota)$ be a map and $a, b \in A$ s.t. $F(a) = F(b)$. The **face subdivision** $S_{a,b}M$ is the map $(A \amalg \{c^{\pm 1}\}, \rho', \iota')$, with $\iota'_{|A} = \iota$, $\iota'(c) = c^{-1}$, and, if $a \neq b$,*

$$\rho'(d) = \begin{cases} c & \text{if } d = a^{-1} \\ \rho(a^{-1}) & \text{if } d = c \\ c^{-1} & \text{if } d = b^{-1} \\ \rho(b^{-1}) & \text{if } d = c^{-1} \\ \rho(d) & \text{otherwise} \end{cases}.$$

The definition is similar if $a = b$. In other words, we add a new edge linking the end vertices of a and b.

Proposition 3.22. *If M is connected, then $S_{a,b}M$ is connected and $\chi(S_{a,b}M) = \chi(M)$.*

Definition 3.23 (Combinatorial equivalence)**.** ***Combinatorial equivalence** is the equivalence relation on combinatorial maps generated by edge and face subdivisions.*

Remark 3.24. *Combinatorial equivalence is stable under edge deletion and contraction.*

Proposition 3.25. *The number of connected components and the Euler characteristic are invariant under combinatorial equivalence.*

3.5 Classification of oriented maps

Definition 3.26 (Normal maps)**.** (i) *The **normal sphere** M_0 is $(\{a^{\pm 1}\}, (a, a^{-1}), (a, a^{-1}))$.*

(ii) *The **normal connected sum of g tori** M_g is (A_g, ρ_g, ι_g), where $A_g = \left\{a_1^{\pm 1}, b_1^{\pm 1}, \ldots, a_g^{\pm 1}, b_g^{\pm 1}\right\}$, with ι_g defined in the obvious way and*

$$\rho_g = \left(a_1, b_1^{-1}, a_1^{-1}, b_1, \ldots, a_g, b_g^{-1}, a_g^{-1}, b_g\right).$$

In the definitions above, the permutations ρ, ι are given by their cyclic representations in $\mathfrak{S}_A$.

Lemma 3.27. *Every finite connected map is combinatorially equivalent to a map with a single vertex.*

Proof. Let T be a spanning tree of the underlying graph $G(M)$. If $G(M)$ is not a single non-loop edge, then we may contract inductively the edges of T in M to get a map with a single vertex. Otherwise, if $G(M)$ is a single non-loop edge, then we may subdivide the only face of M to get two parallel edges, and apply the above. □

Lemma 3.28. *Every finite connected map is combinatorially equivalent to a **reduced map**, i.e. a map with a single vertex and either a single face or a single edge.*

Proof. By Lemma 3.27, we may assume that M has a single vertex. Now let T^* be a spanning tree of M^*. If $G(M^*)$ is not a single non-loop edge, then we may contract inductively the edges of T^* in M^* to get a new map N^*; hence $N = N^{**}$ is reduced and combinatorially equivalent to M by Proposition 3.18. □

Lemma 3.29. *Let M be a reduced map that is not a sphere. In this case, the facial permutation $\varphi \in \mathfrak{S}_A$ is cyclic. Then, for every $a \in A$, there is an arc $b \in A \setminus \{a^{\pm 1}\}$ s.t.*

$$\varphi = \left(a, \ldots, b, \ldots, a^{-1}, \ldots, b^{-1}, \ldots\right).$$

Proof. Write $\varphi = (a, X, a^{-1}, Y)$. Assume for contradiction that $b^{-1} \in X$ for all $b \in X$. Consider the ρ-orbit of a^{-1}. Since $\rho = \varphi \circ \iota$, it is easy to see that $\langle \rho \rangle a^{-1}$ is of the form $\left\{a^{-1}, b^{(1)}, b^{(2)}, \ldots\right\}$ with $b^{(i)} \in X$. In particular, $a \notin \langle \rho \rangle a^{-1}$; but this contradicts the fact that M is reduced and hence has a single vertex. □

Theorem 3.30. *Let M be a finite connected map. Then M is combinatorially equivalent to a normal map M_g for a unique $g \geqslant 0$.*

Proof. Uniqueness is clear because $\chi(M_g) = 2 - 2g$ for all $g \geqslant 0$, and χ is invariant under combinatorial equivalence.

For existence, we may assume that M is reduced by Lemma 3.28 and we may write its facial permutation as

$$\varphi = \left(a, X, b, Y, a^{-1}, Z, b^{-1}, W, T_k\right)$$

by Lemma 3.29, where $T_k = \left(a_1, b_1, a_1^{-1}, b_1^{-1}, \ldots, a_k, b_k, a_k^{-1}, b_k^{-1}\right)$. The goal is to make k larger and apply induction. Performing $S_{\varphi^{-1}(a),a^{-1}}$ and removing $\{b^{\pm 1}\}$, we get an equivalent map whose facial permutation is

$$\varphi' = \left(a, X, W, T_k, c, Z, Y, a^{-1}, c^{-1}\right).$$

(Check this by drawing the face of M!) Now, performing $S_{c,a^{-1}}$ and removing $\{a^{\pm 1}\}$, we get an equivalent map whose facial permutation is

$$\varphi'' = \left(Z, Y, X, W, T_k, c, d, c^{-1}, d^{-1}\right).$$

Setting $a_{k+1} = c$ and $b_{k+1} = d$, we have shown that M is equivalent to the reduced map whose facial permutation is

$$\varphi'' = (Z, Y, X, W, T_{k+1}).$$

It follows by induction on $|Z| + |Y| + |X| + |W|$ that M is equivalent to a reduced map whose facial permutation is T_g for some $g \geqslant 1$; this map is M_g. □

Remark 3.31. *The proof of the topological classification of surfaces is obtained by first triangulating a surface, and then applying the method of Theorem 3.30.*

3.6 Path homotopy in oriented maps

Definition 3.32 (Path homotopy)**.** *Let M be a map. A **path** (resp. **loop**, **circuit**) in M is a path (resp. loop, circuit) in the underlying graph $G(M)$.*

*Given a face f of M, we denote by ∂f the boundary circuit of f. If $\partial f = uv^{-1}$ for some paths u, v, we say that u, v are **complementary subpaths** of f.*

*An **elementary homotopy** is either of the following:*

- *The addition or removal of a spur,*
- *The replacement of a subpath of a face by a complementary subpath.*

*A **free elementary homotopy** is an elementary homotopy for a circuit.*

The homotopy (resp. free homotopy) relation, denoted by $\sim$ (resp. $\overset{\text{free}}{\sim}$) is the equivalence relation generated by elementary (free) homotopies.

Definition 3.33 (Fundamental group)**.** *Given paths $p \sim q$ and $p' \sim q'$, we have $p \cdot p' \sim q \cdot q'$.*

*Therefore, the set of homotopy classes of loops with given basepoint $v \in V(M)$ forms a group for concatenation, denoted by $\pi_1(M, v)$ and called the **fundamental group** of M at v.*

Lemma 3.34. *Two loops α, β based at v are freely homotopic* iff $[\alpha]$ *and* $[\beta]$ *are conjugate in $\pi_1(M, v)$.*

Proof. Assume that α, β are freely homotopic. Then there is a sequence

$$\alpha = \alpha_0 \overset{\text{free}}{\sim} \alpha_1 \overset{\text{free}}{\sim} \cdots \overset{\text{free}}{\sim} \alpha_n = \beta$$

of free elementary homotopies.

We now prove by induction on i that there is a path λ_i s.t. $\alpha \sim \lambda_i \alpha_i \lambda_i^{-1}$. This is clear for $i = 0$. Assume the result has been proved at rank i. Since there is a free elementary homotopy $\alpha_i \overset{\text{free}}{\sim} \alpha_{i+1}$, there are circuit permutations α_i', α_{i+1}' of α_i, α_{i+1} respectively, s.t. there is an elementary homotopy $\alpha_i' \sim \alpha_{i+1}'$. Now let p (resp. q) be the subpath of the circuit containing α_i, α_i' (resp. $\alpha_{i+1}, \alpha_{i+1}'$) from the basepoint of α_i (resp. α_{i+1}) to the basepoint of α_i' (resp. α_{i+1}'). Then $\alpha_i \sim p\alpha_i' p^{-1}$ and $\alpha_{i+1} \sim q\alpha_{i+1}' q^{-1}$. Therefore,

$$\alpha \sim \lambda_i \alpha_i \lambda_i^{-1} \sim \lambda_i p \alpha_i' p^{-1} \lambda_i^{-1} \sim \lambda_i p \alpha_{i+1}' p^{-1} \lambda_i^{-1} \sim \lambda_i p q^{-1} \alpha_{i+1} q p^{-1} \lambda_i^{-1},$$

so it suffices to set $\lambda_{i+1} = \lambda_i p q^{-1}$.

Finally, take $\ell = \lambda_n$, which must be a loop. □

Lemma 3.35. *Let α, β be paths in M. The following are equivalent:*

(i) $\alpha \sim \beta$.

(ii) $\alpha\beta^{-1} \sim 1$.

(iii) $\alpha\beta^{-1} \overset{\text{free}}{\sim} 1$.

Proof. (i) ⇒ (ii) If $\alpha \sim \beta$, then $\alpha\beta^{-1} \sim \beta\beta^{-1} \sim 1$. (ii) ⇒ (i) If $\alpha\beta^{-1} \sim 1$, then $\alpha \sim \alpha\beta^{-1}\beta \sim \beta$. (ii) ⇒ (iii) Clear. (iii) ⇒ (ii) If $\alpha\beta^{-1} \overset{\text{free}}{\sim} 1$, then by Lemma 3.34, there is a loop ℓ s.t. $\alpha\beta^{-1} \sim \ell \cdot 1 \cdot \ell^{-1} \sim 1$. □

3.7 Presentation of the fundamental group

Lemma 3.36. *Let T be a spanning tree of a map M.*

(i) *$\pi_1(M, v)$ has group presentation*

$$\pi_1(M, v) = \langle E(M) \mid E(T), \{\partial f,\ f \in F(M)\} \rangle .$$

(ii) *If C is the set of chords of T, then $\pi_1(M, v)$ has group presentation*

$$\pi_1(M, v) = \langle C \mid r_f,\ f \in F(M) \rangle ,$$

where r_f denotes the sequence of arcs of ∂f not in T.

Proof. (i) Given a path $\sigma = (a_1, \ldots, a_k)$, we denote $T[v, \sigma] = T[v, a_1] \cdots T[v, a_k]$. If σ is a loop based at w, then we have

$$T[v, \sigma] \sim T[v, w] \cdot \sigma \cdot T[w, v] .$$

Note moreover that:

- If $\{a^{\pm 1}\} \in E(T)$, then $T[v, a] \sim 1$.
- If $f \in F(M)$, then $T[v, \partial f] \sim 1$ because $\partial f \sim 1$ since ∂f is a complementary subpath of the trivial path in f.

Now define a group homomorphism $\psi : F(E(M)) \to \pi_1(M, v)$ by $\psi(a) = T[v, a]$ (where one arc representative has been chosen for each edge). It is clear that ψ is onto because $\psi(E(M))$ generates $\pi_1(G(M), v)$, and $\pi_1(M, v)$ is a quotient of the latter. Moreover, $\operatorname{Ker} \psi = \langle\langle E(T), \{\partial f,\ f \in F(M)\} \rangle\rangle$ because elementary homotopies in $\pi_1(M, v)$ correspond to the given relations. This proves the result.

(ii) This follows from (i) after applying a **Tietze transformation** to the given presentation: in general,

$$\langle X \mid R \rangle \cong \langle X \cup \{x\} \mid R \cup \{xw\} \rangle$$

for all $w \in F(X)$. □

Example 3.37. *Recall that M_g is the normal map of genus g (c.f. Definition 3.26).*

(i) $\pi_1(M_0, *) = 1$.

(ii) $\pi_1(M_g, *) = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1, b_1] \cdots [a_g, b_g] \rangle$.

Remark 3.38. *The fundamental group is invariant under combinatorial equivalence.*

Corollary 3.39. *Any finite connected map has fundamental group isomorphic to one of the groups of Example 3.37.*

3.8 Coverings of oriented maps

Definition 3.40 (Covering)**.** *A morphism of maps $p : M \to N$ is a **covering** if its restriction to stars of vertices and faces are bijections. Note that p is automatically onto by Lemma 3.6.*

Lemma 3.41. *Let $p : M \to N$ be a covering.*

(i) *Given a path γ in M with origin v, and a vertex $w \in p^{-1}(v)$, there is a unique lift λ of γ with origin w.*

(ii) *If α, β are two homotopic paths with origin v in M, then their respective lifts $\widetilde{\alpha}, \widetilde{\beta}$ with origin $w \in p^{-1}(v)$ are homotopic.*

*This gives the **monodromy action** $p^{-1}(v) \curvearrowleft \pi_1(N, v)$ as for graphs.*

Proof. (ii) A spur lifts to a spur, and complementary subpaths lift to complementary subpaths (because p induces bijections on stars of faces). □

Corollary 3.42. *If $p : (M, w) \to (N, v)$ is a covering, then*

$$p_* : \pi_1(M, w) \to \pi_1(N, v)$$

is injective.

Proposition 3.43. *Let M be a map and $v \in V(M)$. For every subgroup $U \leqslant \pi_1(M, v)$, there is a connected covering $p_U : (M_U, w) \to (M, v)$ s.t. $(p_U)_* \pi_1(M_U, w) = U$.*

Proof. Let T be a spanning tree for M. For $a \in A$, write $\gamma_a = T[v, a]$. The map $M_U = (A_U, \rho_U, \iota_U)$ is defined by $A_U = A \times (\Gamma \backslash U)$ (where $\Gamma \backslash U$ is the set of right cosets of U in $\Gamma = \pi_1(M, v)$), $\rho_U(a, Ug) = (\rho(a), Ug)$ and $\iota_U(a, Ug) = (a^{-1}, Ug[\gamma_a])$. Note that M_U is connected because $\langle \rho, \iota \rangle \curvearrowright A$ transitively and $\{[\gamma_a],\ a \in A\}$ generates Γ. Moreover, p_U is a covering because $\mathrm{Star}_{M_U}(a, Ug) = \mathrm{Star}_M(a) \times \{Ug\}$; moreover, if $\varphi_U = \rho_U \circ \iota_U$ is the facial permutation, we check that $\varphi_U^k(a, Ug) = (a, Ug)$ iff k is a multiple of $\deg(\langle \varphi \rangle a)$, so p_U also induces bijections on stars of faces. The rest of the proof is similar to Proposition 2.52. □

Example 3.44. *In Proposition 3.43:*

- *If $U = 1$, we get the **universal cover** of M,*
- *If $U = \pi_1'(M, v)$, M_U is called the **homology cover** of M,*
- *If $U = \pi_1(M, v)^2$, M_U is called the $\mathbb{Z}/2$**-homology cover** of M.*

Theorem 3.45. *The isomorphism classes of connected coverings of a map M are in bijection with the conjugacy classes of subgroups of $\pi_1(M, v)$.*

Proof. The proof is similar to Theorem 2.56. □

3.9 Quotient maps

Definition 3.46 (Quotient map)**.** *Let M be a map and $\Gamma \leqslant \mathrm{Aut}(M)$. The **quotient** $M/\Gamma = (A_\Gamma, \rho_\Gamma, \iota_\Gamma)$ is defined by $A_\Gamma = \{\Gamma a,\ a \in A\}$, $\rho_\Gamma(\Gamma a) = \Gamma\rho(a)$ and $\iota_\Gamma(\Gamma a) = \Gamma\iota(a)$.*

We then have a natural (surjective) morphism $p_\Gamma : M \to M/\Gamma$.

Note that, if Γ acts with arc inversions, the involution ι_Γ may not be fixed-point-free. To deal with this, we will view an arc a s.t. $\iota_\Gamma(a) = a$ as a half-edge. All the theory remains valid with this addition (both for graphs and for maps).

Remark 3.47. *Given a map M, the action $\mathrm{Aut}(M) \curvearrowright A$ is free.*

Definition 3.48 (Free action)**.** *Let M be a map.*

- *An automorphism $f \in \mathrm{Aut}(M)$ is **fixed-point-free** if $f(x) \neq x$ for all $x \in V(M) \cup F(M)$, or equivalently $f(a) \notin \langle\rho\rangle a \cup \langle\varphi\rangle a$ for all $a \in A$.*
- *A subgroup $\Gamma \leqslant \mathrm{Aut}(M)$ **acts freely** if every $f \in \Gamma \setminus \{\mathrm{id}\}$ is fixed-point-free.*

Proposition 3.49. *Let M be a map and $\Gamma \leqslant \mathrm{Aut}(M)$. Then the projection $p_\Gamma : M \to M/\Gamma$ is a covering* iff *Γ acts freely.*

Proof. Note that p_Γ is surjective, so it is a covering iff its restrictions to stars are injective, i.e. for $a \in A$ and $b \in \langle\rho\rangle a \cup \langle\varphi\rangle a$, $\Gamma a = \Gamma b$ implies that $a = b$. This is true iff Γ acts freely: if $\Gamma a = \Gamma b$, then we may write $b = \gamma a$ for some $\gamma \in \Gamma$, and γ has a fixed vertex or face since $b \in \langle\rho\rangle a \cup \langle\varphi\rangle a$; therefore $\gamma = \mathrm{id}$ if Γ acts freely. □

Remark 3.50. *The results of Section 2.9 on quotient graphs remain valid (after removing the assumption that groups act without arc inversion).*

Proposition 3.51. *If $p : M \to N$ is a covering and $v \in V(N)$, then*

$$\mathrm{Aut}(p) \cong N\left(p_*\pi_1(N, v)\right) / p_*\pi_1(N, v).$$

Proof. The proof is similar to Theorem 2.69. □

3.10 Hurwitz' Theorem

Theorem 3.52 (Hurwitz, 1893)**.** *If M is a map with genus $g \geqslant 2$, then*

$$|\mathrm{Aut}(M)| \leqslant 84(g-1).$$

Proof. Let $\Gamma = \mathrm{Aut}(M)$ and consider the projection $p_\Gamma : M \to M/\Gamma$. Note that Γ acts transitively on $p_\Gamma^{-1}(x)$ for $x \in A(M/\Gamma) \cup V(M/\Gamma) \cup F(M/\Gamma)$. Therefore, given $w \in W = V(M/\Gamma) \cup F(M/\Gamma)$, all vertices in $p_\Gamma^{-1}(w)$ have the same degree, so they all have the same ramification index; denote it by e_w.

The Riemann-Hurwitz Formula (Theorem 3.10) implies that

$$\chi(M) = (\deg p_\Gamma)\,\chi(M/\Gamma) - \sum_{v \in V(M) \cup F(M)} (e_v - 1) = (\deg p_\Gamma)\,\chi(M/\Gamma) - \sum_{w \in W} \left|p_\Gamma^{-1}(w)\right| (e_w - 1).$$

But $|p_\Gamma(w)|\, e_w = \deg p_\Gamma$ by the Index Formula (Proposition 3.9); moreover $\deg p_\Gamma = |\Gamma|$ because the action $\Gamma \curvearrowright A$ is free. Therefore

$$\chi(M) = |\Gamma|\,\chi(M/\Gamma) - \sum_{w \in W} (\deg p_\Gamma)\left(1 - \frac{1}{e_w}\right) = -|\Gamma| \underbrace{\left(\sum_{w \in W}\left(1 - \frac{1}{e_w}\right) - \chi(M/\Gamma)\right)}_{Q}.$$

In other words,

$$2(g-1) = |\Gamma|\, Q,$$

so it suffices to prove that $Q \geqslant \frac{1}{42}$. Note first that $Q > 0$ because $g \geqslant 2$.

- If $\chi(M/\Gamma) \leqslant -2$, then $Q \geqslant 2$.
- If $\chi(M/\Gamma) = 0$, then we must have

$$Q = \sum_{w \in W} \left(1 - \frac{1}{e_w}\right) \geqslant \frac{1}{2},$$

because the sum must have at least one nonzero term since $Q > 0$, and each nonzero term is at least $\frac{1}{2}$.

- If $\chi(M/\Gamma) = 2$, then $\sum_{w \in W} \left(1 - \frac{1}{e_w}\right) = Q + \chi(M/\Gamma) > 2$, so $|W'| \geqslant 3$ where $W' = \{w \in W,\, e_w > 1\}$.
  - If $|W'| \geqslant 5$, then $\sum_{w \in W} \left(1 - \frac{1}{e_w}\right) \geqslant \frac{5}{2}$, so $Q \geqslant \frac{1}{2}$.
  - If $|W'| = 4$, then $\sum_{w \in W} \left(1 - \frac{1}{e_w}\right) \geqslant \frac{3}{2} + \frac{2}{3}$, so $Q \geqslant \frac{1}{6}$.
  - If $|W'| = 3$, then $\sum_{w \in W} \left(1 - \frac{1}{e_w}\right) \geqslant \frac{1}{2} + \frac{2}{3} + \frac{6}{7}$, so $Q \geqslant \frac{1}{42}$. □

Definition 3.53 (Hurwitz maps)**.** *A map M for which $|\mathrm{Aut}(M)| = 84(g-1)$ is called a **Hurwitz map**.*

The above proof of Hurwitz' Theorem implies that a Hurwitz map must have exactly three branch values, with ramification indices $2, 3, 7$ respectively.

Actually, one can show that there are Hurwitz maps. They have genus at least 3, and an example (in genus 3) is the Klein quartic.

3.11 Branched coverings and monodromy

Definition 3.54 (Branched covering)**.** *A **branched covering** (or **ramified covering**) is a continuous mapping $p : S' \to S$ between compact surfaces with a finite set $\Sigma \subseteq S$, called the **singular set**, s.t. p induces a covering $S' \setminus p^{-1}(\Sigma) \to S \setminus \Sigma$, and for all $w \in \Sigma$ and $\widetilde{w} \in p^{-1}(w)$, there are charts around $w, \widetilde{w}$ in which p is $z \mapsto z^k$ in $\mathbb{C}$. The integer k is called the **ramification index**.*

*The points of Σ are called **branch values** and the points of $p^{-1}(\Sigma)$ are called **ramification points**.*

Remark 3.55 (Topological realisation of a morphism)**.** *Consider a morphism $f : M \to N$ of combinatorial maps. The map M may be triangulated as follows: add a vertex of type $*$ inside each face and one of type $\circ$ at the middle of each edge (or at the end of self-opposite edges), then link each face vertex with all the vertices on the boundary of the face. Let $\bullet$ be the type of ordinary vertices. This gives a triangulation of the topological realisation $S(M)$ in which each pair of triangles corresponds to an arc. Perform the same triangulation on N and use the mapping $f : A(M) \to A(N)$ to construct a mapping $\overline{f} : S(M) \to S(N)$. Then $\overline{f}$ is a branched covering.*

Remark 3.56 (Relation between the monodromy group of a combinatorial map and that of a covering)**.** *Let M be a combinatorial map and consider its triangulation as constructed in Remark 3.55. If $M_t = (\{a\}, \mathrm{id}, \mathrm{id})$ is the **trivial map**, then there is a canonical morphism $p_M : M \to M_t$. The topological realisation of p_M is a branched covering of the sphere with branch values $*, \circ, \bullet$.*

Now note that $\pi_1(S(M_t) \setminus \{*, \circ, \bullet\}) \cong F(\lambda, \mu)$, where λ is a loop around $\bullet$ and μ is a loop around $\circ$. Therefore, the branched covering p_M induces an action $F(\lambda, \mu) \curvearrowright S(M) \setminus p_M^{-1}(*, \circ, \bullet)$. Recalling that $S(M) \setminus p_M^{-1}(*, \circ, \bullet)$ is triangulated, with each pair of triangles corresponding to an arc of M, we check that the action of λ corresponds to the action of ρ on A and the action of μ corresponds to the action of ι on A.

Hence, the monodromy action $F(\lambda, \mu) \curvearrowright S(M) \setminus p_M^{-1}(*, \circ, \bullet)$ corresponds to the action of the monodromy group $\langle \rho, \iota \rangle$ on A.

4 The homotopy test

Remark 4.1. *Consider a combinatorial map M. We consider two fundamental problems:*

(i) *The **contractibility problem**, i.e. determining whether or not a given loop is null-homotopic,*

(ii) *The **transformation problem**, i.e. determining whether or not two given circuits are freely homotopic.*

Noting that the universal cover of a map M is a tiling of the plane by the Cayley complex of the fundamental group $\pi_1(M)$, it follows that those problems are equivalent to the following two problems in $\pi_1(M)$, respectively,

(i) *The **word problem**, i.e. determining whether or not a word in the generators is trivial,*

(ii) *The **conjugacy problem**, i.e. determining whether or not two words in the generators are conjugate.*

4.1 Van Kampen diagrams

Remark 4.2. *If X is a topological space, then a loop $\gamma : \mathbb{S}^1 \to X$ is contractible* iff *there is a continuous map $\overline{\gamma} : \mathbb{D}^2 \to X$ s.t. $\overline{\gamma}_{|\mathbb{S}^1} = \gamma$. We are now going to express this idea in the combinatorial framework.*

Definition 4.3 (Disk diagram)**.** *Given a map M, a **disk diagram** over M is a sphere map D with one face marked as the **outer face** ω, and with a labelling $\ell : A(D) \to A(M)$ s.t.*

- *Opposite arcs are labelled with opposite arcs, i.e. $\iota \circ \ell = \ell \circ \iota$,*
- *The label of each inner face of D is a face of M, i.e. for all $f \in F(D) \setminus \{\omega\}$, $\ell(\partial f) = \partial g$ for some $g \in F(M)$.*

We shall denote $\partial D = \partial \omega$.

*A disk diagram is **reduced** if for every pair of inner faces sharing a vertex in D, their labels are not inverse to each other.*

Lemma 4.4 (Van Kampen, 1933)**.** *A closed path in a map M is contractible* iff *it is the label of the outer face of a reduced disk diagram over M.*

Proof. ($\Leftarrow$) If c is the label of the outer face of a reduced disk diagram D over M, then c is homotopic to a point in D (since D is topologically a sphere), and the corresponding sequence of homotopies induces a homotopy from c to a point in M.

($\Rightarrow$) Assume that c is contractible, i.e. there is a sequence

$$1 = c_0 \sim c_1 \sim c_2 \sim \cdots \sim c_k = c,$$

of elementary homotopies. We construct inductively a disk diagram for c_i as follows:

- If $c_i \sim c_{i+1}$ is the addition of a spur (a, a^{-1}), then simply add an edge $\{a^{\pm 1}\}$ with one degree 1 endpoint to the disk diagram of c_i.
- If $c_i \sim c_{i+1}$ is a path replacement in a face f, add a face labelled by ∂f to the disk diagram of c_i.

This gives a disk diagram for c. We can reduce it by merging faces with a common vertex and inverse labels. □

Definition 4.5 (Annular diagram)**.** *An **annular diagram** is a disk diagram with two (instead of one) marked faces.*

Lemma 4.6 (Schupp, 1968)**.** *Two closed paths c and d are freely homotopic* iff *there exists a reduced annular diagram over M whose marked faces are labelled by c and d respectively.*

Proof. We know that $c \overset{\text{free}}{\sim} d$ iff there is a path p s.t. $cpd^{-1}p^{-1}$ is contractible. Now use the Van Kampen Lemma and transform a disk diagram for $cpd^{-1}p^{-1}$ into an annular diagram for c, d. □

4.2 Combinatorial Gauß-Bonnet Formula

Theorem 4.7 (Gauß-Bonnet)**.** *Let S be a surface with boundary, equipped with a Riemannian metric. If K is the Gaussian curvature of S and k_g is the geodesic curvature along ∂S, then*

$$\int_S K \, \mathrm{d}s + \int_{\partial S} k_g \, \mathrm{d}\ell = 2\pi\chi(S).$$

Definition 4.8 (Map with boundary)**.** *A map with **boundary** is a map M together with an assignement $b : F(M) \to \{0, 1\}$. Faces f s.t. $b(f) = 1$ are considered as boundary faces. A vertex v is called **inner** if none of the faces f s.t. $\mathrm{Star}(f) \cap \mathrm{Star}(v) \neq \varnothing$ is a boundary face. Otherwise, v is called a **boundary vertex**. We denote by V^0 (resp. V^∂) the set of inner (resp. boundary) vertices.*

Definition 4.9 (Angular assignement)**.** *Consider a map $M = (A, \rho, \iota)$ with boundary. The **corners** of M are the pairs $(a, \rho(a))$ for $a \in A$. We denote by C the set of corners. An **angular assignment** for M is an assignment $\theta : C \to \mathbb{R}$ s.t. the following condition holds for all $f \in F(M)$:*

$$\sum_{c \in f} \theta(c) = \frac{1}{2} \deg f - 1.$$

(In writing this condition as above, we consider that the circle has length 1.)
*If $v \in V$, its **curvature** is defined by*

- $\kappa(v) = 1 - \sum_{c \in v} \theta(c)$ *if* $v \in V^0$,
- $\tau(v) = \frac{1}{2} - \sum_{c \in v} \theta(c)$ *if* $v \in V^\partial$.

Theorem 4.10 (Combinatorial Gauß-Bonnet)**.** *Let M be a map with boundary, equipped with an angular assignment. Assume that ∂M is composed of disjoint simple cycles. Then*

$$\sum_{v \in V^0} \kappa(v) + \sum_{v \in V^\partial} \tau(v) = \chi(M).$$

Proof. We have

$$\sum_{v \in V^0} \kappa(v) = \sum_{v \in V^0} \left(1 - \sum_{c \in v} \theta(c)\right) = \left|V^0\right| - \sum_{c \in v \in V^0} \theta(c),$$

and similarly $\sum_{v \in V^\partial} \tau(v) = \frac{1}{2}\left|V^\partial\right| - \sum_{c \in v \in V^\partial} \theta(c)$. Therefore,

$$\begin{aligned}
\sum_{v \in V^0} \kappa(v) + \sum_{v \in V^\partial} \tau(v) &= |V| - \frac{1}{2}\left|V^\partial\right| - \sum_{c \in v \in V} \theta(c) \\
&= |V| - \frac{1}{2}\left|V^\partial\right| - \sum_{c \in f \in F} \theta(c) \\
&= |V| - \frac{1}{2}\left|V^\partial\right| - \sum_{f \in F} \left(\frac{1}{2} \deg f - 1\right) \\
&= |V| - \frac{1}{2}\left|V^\partial\right| - \frac{1}{2} \sum_{f \in F} \deg f + |F| \,.
\end{aligned}$$

But $\sum_{f\in F} \deg f = 2\,|E| - \left|E^\partial\right|$, so that

$$\sum_{v\in V^0} \kappa(v) + \sum_{v\in V^\partial} \tau(v) = |V| - |E| + |F| - \frac{1}{2}\left(\left|V^\partial\right| - \left|E^\partial\right|\right) = \chi(M),$$

since $\left|V^\partial\right| = \left|E^\partial\right|$ because ∂M is composed of disjoint simple cycles. □

4.3 Quad systems

Definition 4.11 (Quad system)**.** *A **quad system**, or **quadrangulated map**, is a map in which all faces have degree* 4*.*

Proposition 4.12. *Every map is equivalent to a quad system.*

Proof. Let M be a map. We assume that M is not a sphere. Then Lemma 3.28 implies that M is equivalent to a map with a single vertex and a single face. Introduce a new vertex $*$ in the face, connect it to all boundary vertices, and erase all the original edges. This yields a quadrangulation of M. □

Lemma 4.13. *Let M be a map and M_q be the equivalent quad system obtained by the process of Proposition 4.12. Given a path c in M, a homotopic path of length at most $2\,|c|$ in M_q can be computed in $\mathcal{O}(|c|)$ time.*

Moreover, all the precomputations on M are done in $\mathcal{O}(|M|)$ time.

Proof. Note that any edge e in M is homotopic to the path of length 2 in M_q connecting $*$ to the two endpoints of e. We can precompute and store all those length 2 paths. Then, given c, we replace each edge by the corresponding length 2 path. □

4.4 Reduction to canonical form

Definition 4.14 (Turn sequence)**.** *Given a closed path $c = (a_0, \dots, a_n)$ in a map $M = (A, \rho, \iota)$, its **turn** at i is the element $t_i \in \mathbb{Z}/d_i$ (where $d_i = \deg(\langle\rho\rangle\, a_{i+1})$) s.t. $a_{i+1} = \rho^{t_i} \circ \iota(a_i)$. The **turn sequence** of c is the word $t_0 \cdots t_{n-1}$.*

*A **bracket** in a path is a subpath with turn sequence 12^*1 or $\overline{12^*1}$, where $\overline{k} = -k$.*

Lemma 4.15 (Four bracket)**.** *Let D be a nonsingular (i.e. ∂D is a simple cycle) quadrangulated disk whose interior vertices have degree at least* 4*. Then ∂D contains at least four brackets.*

Proof. Equip D with the constant angular assignment $\frac{1}{4}$. The Gauß-Bonnet Formula (Theorem 4.10) yields

$$\sum_{v\in V^0} \kappa(v) + \sum_{v\in V^\partial} \tau(v) = \chi(D) = 1.$$

For $v \in V^0$, we have $\deg v \geqslant 4$, so $\kappa(v) = 1 - \sum_{c\in v} \theta(v) \leqslant 0$. It follows that $\sum_{v\in V^\partial} \tau(v) \geqslant 1$. But, for $v \in V^\partial$, the number of corners of v is $\deg v - 1$, so

$$\tau(v) = \frac{1}{4}(3 - \deg v).$$

Either $\deg v = 2$ and $\tau(v) = \frac{1}{4}$, or $\deg v = 3$ and $\tau(v) = 0$, or $\deg v \geqslant 4$ and $\tau(v) \leqslant \frac{1}{4}$. Hence,

$$\left|\left\{v \in V^\partial,\ \deg v = 2\right\}\right| \geqslant \left|\left\{v \in V^\partial,\ \deg v \geqslant 4\right\}\right| + 4.$$

This gives at least four brackets in ∂D. □

Corollary 4.16. *A nontrivial contractible circuit in a quad system with minimum degree at least* 4 *must contain a spur or a bracket.*

Proof. Suppose that c is contractible and does not contain any spur. By the Van Kampen Lemma (Lemma 4.4), c bounds a disk diagram D. Consider the dual graph H^* on the inner faces of D.

- If H^* is connected, then D is nonsingular and $c = \partial D$ must therefore contain four brackets by the Four Bracket Lemma (Lemma 4.15).
- Otherwise, each of the connected components correspond to nonsingular disks, so they contain four brackets, two of which are subpaths of c. □

Definition 4.17 (Bracket flattening)**.** *A **bracket flattening** consists in replacing a bracket and the two incident edges by the "straight line" between their endpoints. Some care must be taken when the two indicident edges share an endpoint, or when these edges are part of the bracket.*

Algorithm 4.18 (Dehn)**.** *To decide whether or not a given loop c in a quad system with minimum degree at least 4 is null-homotopic, apply successive bracket flattenings and spur removals. These operations decrease strictly the length of c, so the process has to stop, reaching either a trivial loop if c is contractible, or a loop without bracket or spur otherwise.*

Definition 4.19 (Convex vertex)**.** *A vertex v on a path c is called **convex** if its turn is 1.*

Definition 4.20 (Reduced circuit)**.** *A circuit without spur, bracket or convex vertex is called **reduced**.*

Proposition 4.21. *In a quad system with minimum degree at least 5, every free homotopy class contains a unique reduced circuit.*

Proof. Existence. We may perform spur removals and bracket flattenings to remove all spurs and brackets. If there is a convex vertex, take a maximal subsequence of the turn sequence of the form 2^*12^* containing it. This corresponds to a subpath p bounding an L-shaped sequence of quadrilaterals that lie to the right. Replace p by the complementary path bounding the same sequence of quadrilaterals. This decreases the number of convex vertices by 1 (because the quad system has minimum degree at least 5).

Uniqueness. Consider two reduced circuit c, d that are freely homotopic. By Schupp's Lemma (Lemma 4.6), c and d bound a reduced annular diagram D. First note that the two boundaries of D must be simple because c and d are reduced.

Now remark that the Four Bracket Lemma (Lemma 4.15) becomes the Five Bracket Lemma if we assume that the minimum degree is at least 5. Using this, prove that the interior faces of D cannot contain any interior vertex. Conclude that $c = d$. □

4.5 The homotopy test

Lemma 4.22. *The reduced form of a circuit c can be computed in $\mathcal{O}(|c|)$ time.*

Algorithm 4.23 (Homotopy test)**.** *Given two circuits c, d in M, we can decided in $\mathcal{O}(|M| + |c| + |d|)$ time whether or not $c \overset{\text{free}}{\sim} d$ as follows:*

(i) *Reduce M to a quad system M_q in $\mathcal{O}(|M|)$ time.*

(ii) *Compute circuits c', d' corresponding to c, d in M_q in $\mathcal{O}(|c| + |d|)$ time as in Lemma 4.13.*

(iii) *Use Lemma 4.22 to reduce c' and d' in $\mathcal{O}(|c| + |d|)$ time.*

(iv) *Check whether the reduced words are equal using the KMP Algorithm (Algorithm 1.31).*

Corollary 4.24. *The word and conjugacy problems of the surface groups*

$$\Gamma_g = \langle a_1, b_1, \dots, a_g, b_g \mid [a_1, b_1] \cdots [a_g, b_g] \rangle$$

can be solved in linear time.

Proof. The word problem in Γ_g amounts to the contractibility problem in M_g, which can be solved by Dehn's Algorithm (Algorithm 4.18). The conjugacy problem amounts to the transformation problem, for which Algorithm 4.23 gives a solution if $g \geqslant 2$ (so that vertices in the quadrangulation of M_g have degree at least 5). If $g = 1$, then $\Gamma_g \cong \mathbb{Z}^2$ is abelian, so the conjugacy problem is no other than the word problem. □

5 Undecidability in topology

5.1 Group presentations

Definition 5.1 (Group presentation)**.** *Given a set S (called the set of **generators**) and a set $R \subseteq F(S)$ (called the set of **relations**), the group with **presentation** $\langle S \mid R \rangle$ is by definition $F(S)/\langle\langle R \rangle\rangle$.*

*We say that a group Γ is **finitely presented** if there are finite sets S, R s.t. $\Gamma \cong \langle S \mid R \rangle$.*

Proposition 5.2. *Any mapping $S \to \Gamma$ extends uniquely to a morphism $F(S) \to \Gamma$.*

Theorem 5.3 (Von Dyck)**.** *Let R be a set of relations on S. Then a mapping $f : S \to \Gamma$ extends (uniquely) to a morphism $\overline{f} : \langle S \mid R \rangle \to \Gamma$ iff $f(R) = 1$.*

Definition 5.4 (Tietze transformations)**.** *Consider a presentation $\langle S \mid R \rangle$. **Tietze transformations** are the following operations:*

(T_1) $\langle S \mid R \rangle \longmapsto \langle S \mid R \cup \{r\} \rangle$, *with* $r \in \langle\langle R \rangle\rangle \subseteq F(S)$.

(T_2) $\langle S \mid R \rangle \longmapsto \langle S \cup \{s\} \mid R \cup \{sw\} \rangle$, *with* $w \in F(S)$.

Applying a Tietze transformation does not change the isomorphism type of the presentation.

Theorem 5.5. *Two finite presentations represent the same group* iff *they are related by a finite sequence of Tietze transformations.*

Proof. ($\Leftarrow$) This is clear. ($\Rightarrow$) Consider an isomorphism $\varphi : \langle S' \mid R' \rangle \overset{\cong}{\to} \langle S \mid R \rangle$ between two finite presentations. We claim that $R' \subseteq \left\langle\left\langle R \cup \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \right\rangle\right\rangle$ in $F(S \cup S')$. Indeed, by Tietze transformations, there is an isomorphism

$$\psi : \left\langle S \cup S' \mid R \cup \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \right\rangle \overset{\cong}{\to} \langle S \mid R \rangle$$

with $\psi(s) = s$ for $s \in S$ and $\psi(s') = \varphi(s')$ for $s' \in S'$. In particular, $(\varphi^{-1} \circ \psi)_{|\langle S' \rangle} = \mathrm{id}$, so $\varphi^{-1} \circ \psi(R') = R' = 1$, which implies (by injectivity of $\varphi^{-1} \circ \psi$) that $R' \subseteq \left\langle\left\langle R \cup \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \right\rangle\right\rangle$ in $F(S \cup S')$.

Therefore, we have the following sequence of Tietze transformations starting from $\langle S \mid R \rangle$:

$$\begin{aligned}
\langle S \mid R \rangle &\overset{(T_2)}{\cong} \left\langle S \cup S' \mid R \cup \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \right\rangle \\
&\overset{(T_1)}{\cong} \left\langle S \cup S' \mid R \cup R' \cup \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \right\rangle \\
&\overset{(T_1)}{\cong} \left\langle S \cup S' \mid R \cup R' \left\{ s' \varphi(s')^{-1} \right\}_{s' \in S'} \cup \left\{ s \varphi^{-1}(s)^{-1} \right\}_{s \in S} \right\rangle.
\end{aligned}$$

By symmetry, the last presentation can also be obtained from $\langle S' \mid R' \rangle$ after a finite sequence of Tietze transformations. □

5.2 Dehn's decision problems in group theory

Definition 5.6 (Dehn's problems)**.** *Consider a group presentation* $\Gamma = \langle S \mid R \rangle$*.*

(i) *The* ***word problem*** *asks whether a given word in* S *is trivial in* Γ*.*

(ii) *The* ***generalised word problem*** *asks whether a given word in* S *belongs to a subgroup of* Γ *defined by a given set of generators.*

(iii) *The* ***conjugacy problem*** *asks whether two given words in* S *are conjugate in* Γ*.*

(iv) *The* ***isomorphism problem*** *asks whether* $\langle S \mid R \rangle$ *is isomorphic to some other presentation* $\langle S' \mid R' \rangle$*.*

Theorem 5.7. (i) (Markov, Post 1947) *The word problem is unsolvable for semigroups.*

(ii) (Novikov 1955, Boone, Britton 1959) *The word problem is unsolvable for groups.*

(iii) (Borisov 1969) *There is a group with four generators and twelve relations with unsolvable word problem.*

Corollary 5.8. *The conjugacy problem and the generalised word problem are unsolvable.*

Proof. The word problem reduces to the conjugacy problem since $w = 1$ iff w is conjugated to 1. Similarly, the word problem reduces to the generalised word problem. □

Theorem 5.9 (Adyan 1957, Rabin 1958)**.** *The isomorphism problem is undecidable.*

Definition 5.10 (Markov properties)**.** *A* ***Markov property*** *for groups is a property* $\mathscr{P}$ *that is invariant under group isomorphism and s.t.*

(i) *There is a finite presentation* $\langle S \mid R \rangle$ *satisfying* $\mathscr{P}$*,*

(ii) *There is a finite presentation* $\langle S' \mid R' \rangle$ *s.t. any group containing* $\langle S' \mid R' \rangle$ *does not satisfy* $\mathscr{P}$*.*

Theorem 5.11 (Adyan, Rabin)**.** *Given a Markov property* $\mathscr{P}$*, the problem of deciding if a given presentation satisfies* $\mathscr{P}$ *is unsolvable.*

Example 5.12. *The following are examples of Markov properties:*

- *Being trivial,*
- *Being abelian,*
- *Being nilpotent,*
- *Being simple,*
- *Being the fundamental group of a 3-manifold,*
- *Being hyperbolic.*

Therefore, all those properties are undecidable.

5.3 Decision problems in topology

Definition 5.13 (Topological decision problems)**.** *Consider a complex $\mathcal{C}$.*

(i) *The **contractibility problem** asks whether a path is contractible in $\mathcal{C}$.*

(ii) *The **transformation problem** asks whether two circuits are freely homotopic in $\mathcal{C}$.*

Proposition 5.14. *The word and conjugacy problem reduce to the contractibility and transformation problem respectively.*

Proof. Given a presentation $\langle S \mid R\rangle$ and a word w on S, build a complex $\mathcal{C}$ by glueing one disk per relation r on a bouquet of circles indexed by S. Using the Seifert-Van Kampen Theorem, we have

$$\pi_1\mathcal{C} \cong \langle S \mid R\rangle .$$

Now the word w can be considered as a loop in $\mathcal{C}$, so that $w = 1$ in $\langle S \mid R\rangle$ iff $w \sim 1$ in $\mathcal{C}$. □

Corollary 5.15. *There exists a 2-dimensional complex for which the contractibility and transformation problems are unsolvable.*

Proof. Consider a group $\langle S \mid R\rangle$ for which the word and conjugacy problems are unsolvable (using Theorem 5.7) and construct the associated complex as in the proof of Proposition 5.14. □

Remark 5.16. *In fact, using Matiyasevich's 1970 solution of Hilbert's Tenth Problem on the solvability of diophantine systems, we can prove the existence of a 2-complex and a loop in it s.t. we can neither prove nor disprove that the loop is contractible.*

5.4 $\mathbb{Z}^2$-machines

Definition 5.17 ($\mathbb{Z}^2$-machine)**.** *A $\mathbb{Z}^2$-**machine** over a basis $\beta \geqslant 2$ is the data of:*

- *ℓ-**transformations**, i.e. partial functions $\mathbb{Z}^2 \to \mathbb{Z}^2$ given by*
$$\left(\beta^2 U + A_\ell, \beta V + B_\ell\right) \xrightarrow{\ell} \left(\beta U + C_\ell, \beta^2 V + D_\ell\right),$$
where $A_\ell, D_\ell \in \{0, \dots, \beta^2 - 1\}$, $B_\ell, C_\ell \in \{0, \dots, \beta - 1\}$ are fixed integers,
- *r-**transformations**, i.e. partial functions $\mathbb{Z}^2 \to \mathbb{Z}^2$ given by*
$$\left(\beta U + A_r, \beta^2 V + B_r\right) \xrightarrow{r} \left(\beta^2 U + C_r, \beta V + D_r\right),$$
where $A_r, D_r \in \{0, \dots, \beta - 1\}$, $B_r, C_r \in \{0, \dots, \beta^2 - 1\}$ are fixed integers.

We write $(X, Y) \xrightarrow{s} (X', Y')$ (with $s \in \{\ell, r\}$) if there is a s-transformation from (X, Y) to (X', Y'); we write $(X, Y) \xrightarrow{*} (X', Y')$ if there is a sequence of ℓ and r-transformations from (X, Y) to (X', Y'); finally, we denote by $\overset{*}{\leftrightarrow}$ the equivalence relation generated by $\xrightarrow{*}$.

Remark 5.18. *A Turing machine may be encoded by a $\mathbb{Z}^2$-machine.*

Proof. Consider a Turing machine $M = (A, Q, T)$. Set $\beta = |A| + |Q|$. Recall that a configuration of M is an element $uqv \in A^* \times Q \times A^*$. We fix a bijection $B : A \amalg Q \xrightarrow{\cong} \{0, \dots, \beta - 1\}$. This can be extended to an injection $B : (A \amalg Q)^* \hookrightarrow \mathbb{Z}$ by interpreting each letter in a word as a digit in the basis β. Hence, interpreting each configuration uqv as the pair $(B(uq), B(\overline{v})) \in \mathbb{Z}^2$ (where $\overline{v}$ is the word v in the reverse order), a left transition

$$(uc)q(av) \longmapsto up(cbv)$$

in M gives rise to a transition $\mathbb{Z}^2 \to \mathbb{Z}^2$ given by

$$\left(\beta^2 B(u) + B(cq), \beta B(\overline{v}) + B(a)\right) \longmapsto \left(\beta B(u) + B(p), \beta^2 B(\overline{v}) + B(bc)\right).$$

Therefore, if we associate to each left transition $t = qapbL \in T$ the ℓ-transformations given by $A_\ell = B(cq)$, $B_\ell = B(a)$, $C_\ell = B(p)$ and $D_\ell = B(bc)$ for $c \in A$, and similarly for right transitions, we get a $\mathbb{Z}^2$-machine whose transformations correspond to transitions in M. □

5.5 HNN extensions

Definition 5.19 (HNN extension)**.** *Consider a group Γ, together with subgroups $A, B \leqslant \Gamma$ and an isomorphism $\varphi : A \xrightarrow{\cong} B$. The **HNN extension** of Γ over φ is the group*

$$\Gamma *_\varphi = (\Gamma * \langle t \rangle) \,/\, \left\langle\!\!\left\langle t^{-1} a t \varphi(a)^{-1},\ a \in A \right\rangle\!\!\right\rangle .$$

In other words, if $\Gamma = \langle S \mid R \rangle$, then

$$\Gamma *_\varphi = \left\langle S \cup \{t\} \mid R \cup \left\{ t^{-1} a t \varphi(a)^{-1},\ a \in A \right\} \right\rangle .$$

*The letter t is called the **stable generator**.*

Remark 5.20. *HNN extensions arise naturally in topology in the same way as amalgamated free products do:*

- *If a space X is the union of two intersecting spaces A, B, then $\pi_1 X \cong (\pi_1 A) *_{\pi_1(A \cap B)} (\pi_1 B)$.*
- *If a space Y is obtained from a space X by glueing two boundary components A, B via a homeomorphism $\varphi : A \xrightarrow{\cong} B$, then $\pi_1 Y \cong (\pi_1 X) *_{\varphi_*}$.*

Lemma 5.21 (Britton, 1963)**.** *Let $g_i \in \Gamma$ and $\varepsilon_i \in \{\pm 1\}$ s.t.*

$$g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n \overset{\Gamma *_\varphi}{=} 1.$$

Then one of the following holds:

- *$n = 0$ and $g_0 \overset{\Gamma}{=} 1$,*
- *There exists an i s.t. $\varepsilon_i = -1$, $\varepsilon_{i+1} = +1$ and $g_i \in A$,*
- *There exists an i s.t. $\varepsilon_i = +1$, $\varepsilon_{i+1} = -1$ and $g_i \in B$,*

Theorem 5.22 (Normal form for HNN extensions)**.** *Let T_A (resp. T_B) be a set of right coset representatives for A (resp. B) in Γ s.t. $1 \in T_A$ (resp. $1 \in T_B$). Then every element $w \in \Gamma *_\varphi$ may be written uniquely as*

$$w = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n,$$

with $g_i \in \Gamma$, $\varepsilon_i \in \{\pm 1\}$, and such that

(i) *If $\varepsilon_i = 1$, then $g_i \in T_B$,*

(ii) *If $\varepsilon_i = -1$, then $g_i \in T_A$,*

(iii) *There is no factor of the form $t^\varepsilon 1 t^{-\varepsilon}$.*

Proof. Existence. If $w \in \Gamma *_\varphi$, then since $\Gamma *_\varphi$ is generated by $\Gamma \cup \{t\}$, we may write

$$w = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n,$$

where conditions (i)-(iii) may not be satisfied. If for example $\varepsilon_n = 1$, write $g_n = b g_n'$ for some $b \in B$ and $g_n' \in T_B$. Thus:

$$\begin{aligned} w &= g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t b g_n' \\ &= g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} a t g_n', \end{aligned}$$

where $a = \varphi^{-1}(b)$. Proceeding inductively, we thus reduce the number of values of i for which conditions (i)-(iii) are not satisfied, until we get a word satisfying the required conditions.

Uniqueness. Assume that

$$g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n} g_n = h_0 t^{\eta_1} h_1 \cdots h_{m-1} t^{\eta_m} h_m,$$

where the two words satisfy conditions (i)-(iii). In other words,

$$g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n} \left(g_n h_m^{-1}\right) t^{-\eta_m} h_{m-1}^{-1} \cdots h_1^{-1} t^{-\eta_1} h_0^{-1} = 1.$$

By Britton's Lemma (Lemma 5.21), there must be a factor of the form $t^{-1}at$ (with $a \in A$) or tbt^{-1} (with $b \in B$). If such a factor arises inside one of the given words, then we have (for instance) $\varepsilon_i = -1$, $\varepsilon_{i+1} = 1$ and $g_i \in A$. But then condition (ii) implies that $g_i \in T_A$; and $T_A \cap A = \{1\}$, which gives a factor of the form $t^{-1}1t$, contradicting (iii). Therefore, the factor of the form $t^{-1}at$ or tbt^{-1} must be at the junction between the two words, i.e. we must have $\varepsilon_n = \eta_m$ and $(g_n h_m^{-1}) \in A$ if for example $\varepsilon_n = -1$. But then (ii) implies that $g_n, h_m \in T_A$, and $Ag_n = Ah_m$, so $g_n = h_m$. This proves that $g_n = h_m$ and $\varepsilon_n = \eta_m$; inductively, we see that the two words are the same. □

Corollary 5.23. (i) Γ *(and hence A and B) embed naturally as subgroups of* $\Gamma *_\varphi$.

(ii) $\mathbb{Z}$ *embeds as a subgroup of* $\Gamma *_\varphi$ *via* $n \mapsto t^n$.

In particular, $\Gamma *_\varphi$ *is a group containing* Γ *and in which A and B are related by an inner automorphism.*

Proposition 5.24. *If* Γ *is torsion-free, then so is* $\Gamma *_\varphi$.

5.6 Undecidability of the generalised word problem

Notation 5.25. *We introduce the group*

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

We define a mapping $p : \mathbb{Z}^2 \to K$ *by*

$$p : (u, v) \mapsto (x^u y^v)^{-1} z (x^u y^v).$$

Lemma 5.26. $p(\mathbb{Z}^2)$ *is a free basis of a subgroup of K. In particular, $p : \mathbb{Z}^2 \to K$ is injective.*

Proof. Consider a word

$$w = p(u_1, v_1)^{j_1} \cdots p(u_n, v_n)^{j_n} \in K$$

that is reduced over $p(\mathbb{Z}^2)$, i.e. such that $(u_{i+1}, v_{i+1}) \neq (u_i, v_i)$ for all i. In other words

$$w = \left(x^{-u_1} y^{-v_1}\right) z^{j_1} \left(x^{u_1 - u_2} y^{v_1 - v_2}\right) z^{j_2} \cdots z^{j_n} (x^{u_n} y^{v_n}).$$

It is clear from this expression that if $w = 1$, then $n = 0$. This means that $p(\mathbb{Z}^2)$ is free. □

Lemma 5.27. *Let M be a Turing machine and consider the associated $\mathbb{Z}^2$-machine. To every ℓ-transformation, we associate a morphism between subgroups of K*

$$\varphi_\ell : \left\langle x^{\beta^2}, y^\beta, p(A_\ell, B_\ell) \right\rangle \to \left\langle x^\beta, y^{\beta^2}, p(C_\ell, D_\ell) \right\rangle,$$

defined by $x^{\beta^2} \mapsto x^\beta$, $y^\beta \mapsto y^{\beta^2}$ *and* $p(A_\ell, B_\ell) \mapsto p(C_\ell, D_\ell)$.

Then φ_ℓ is a well-defined group isomorphism, and there is a similar notion for r-transformations.

Proof. Consider the inner automorphism ρ_ℓ (resp. θ_ℓ) conjugating by $x^{A_\ell} y^{B_\ell}$ (resp. $x^{C_\ell} y^{D_\ell}$). Then

$$\rho_\ell \left(\left\langle x^{\beta^2}, y^\beta, p(A_\ell, B_\ell) \right\rangle\right) = \left\langle x^{\beta^2}, y^\beta, z \right\rangle,$$
$$\theta_\ell \left(\left\langle x^\beta, y^{\beta^2}, p(C_\ell, D_\ell) \right\rangle\right) = \left\langle x^\beta, y^{\beta^2}, z \right\rangle.$$

Moreover, consider the isomorphism $\alpha : \left\langle x^{\beta^2}, y^\beta, z \right\rangle \to \left\langle x^\beta, y^{\beta^2}, z \right\rangle$ given by $x^{\beta^2} \mapsto x^\beta$, $y^\beta \mapsto y^{\beta^2}$ and $z \mapsto z$. Then

$$\varphi_\ell = \theta_\ell^{-1} \circ \alpha \circ \rho_\ell.$$ □

Lemma 5.28. *Given a ℓ-transformation, consider the HNN extension $K*_{\varphi_\ell}$ with stable generator t_ℓ. The ℓ-transformation under consideration sends (u,v) to (u',v')* iff

$$t_\ell^{-1} p(u,v)\, t_\ell \overset{K*_{\varphi_\ell}}{=} p(u',v'),$$

and similarly for r-transformations.

Proof. ($\Rightarrow$) Write $u = \beta^2 U + A_\ell$, $v = \beta V + B_\ell$, $u' = \beta U + C_\ell$ and $v' = \beta^2 V + D_\ell$. Check that $\varphi_\ell(p(u,v)) \overset{K}{=} p(u',v')$, so that $t_\ell^{-1} p(u,v)\, t_\ell \overset{K*_{\varphi_\ell}}{=} p(u',v')$.

($\Leftarrow$) Suppose that $t_\ell^{-1} p(u,v) t_\ell p(u',v')^{-1} \overset{K*_{\varphi_\ell}}{=} 1$. By Britton's Lemma (Lemma 5.21), $p(u,v) \in \left\langle x^{\beta^2}, y^\beta, p(A_\ell, B_\ell) \right\rangle$. Hence, we may write (in K)

$$\begin{aligned} p(u,v) &= x^{\beta^2 j_1} y^{\beta j_2} p(A_\ell,B_\ell)^{j_3} x^{\beta^2 j_4} \cdots p(A_\ell,B_\ell)^{j_n} \\ &= p\left(\beta^2 U_1 + A_\ell, \beta V_1 + B_\ell\right)^{i_1} \cdots p\left(\beta^2 U_k + A_\ell, \beta V_k + B_\ell\right)^{i_k} x^{\beta^2 a} y^{\beta b}. \end{aligned}$$

By considering the abelianisation K_{ab}, we see that $a = b = 0$. Now since $p(\mathbb{Z}^2)$ freely generates a subgroup of K, we must have $(u,v) = (\beta^2 U + A_\ell, \beta V + B_\ell)$ for some U, V. Hence

$$p(u',v') = t_\ell^{-1} p(u,v) t_\ell = p\left(\beta U + C_\ell, \beta^2 V + D_\ell\right),$$

so $(u',v') = (\beta U + C_\ell, \beta^2 V + D_\ell)$. □

Notation 5.29. *Consider the group*

$$K_Z = \left(\left((K*_{\varphi_\ell})*_{\varphi'_\ell}\right)*_{\varphi_r}\right) * \cdots,$$

obtained by taking successive HNN extensions over all isomorphisms φ_ℓ and φ_r corresponding to ℓ and r-transformations respectively. We denote by T_ℓ, T_r the set of stable generators of K_Z corresponding to ℓ and r-transformations respectively.

Lemma 5.30. *$(u',v') \overset{*}{\leftrightarrow} (u,v)$ if and only if $p(u',v') \in \langle p(u,v), T_\ell, T_r \rangle$ in K_Z.*

Proof. ($\Rightarrow$) This follows from Lemma 5.28.

($\Leftarrow$) Suppose that

$$p(u',v') = \tau_0 p(u,v)^{j_1} \tau_1 p(u,v)^{j_2} \tau_2 \cdots \tau_{k-1} p(u,v)^{j_k} \tau_k,$$

with $\tau_i \in \langle T_\ell, T_r \rangle$. By Britton's Lemma (Lemma 5.21), the above product must contain a factor of the form $t_s^\varepsilon w t_s^{-\varepsilon}$ with w in the domain or codomain of φ_s (and $s \in \{\ell, r\}$). Hence

$$t_s^\varepsilon w t_s^{-\varepsilon} = t_s^\varepsilon p(u,v)^{k_0} t_s^{-\varepsilon} = \left(t_s^\varepsilon p(u,v) t_s^{-\varepsilon}\right)^{k_0} = p(u_0,v_0)^{k_0},$$

with $(u,v) \overset{s}{\leftrightarrow} (u_0,v_0)$. Therefore, we may inductively reduce the above product to

$$p(u',v') = p(u_1,v_1)^{k_1} \cdots p(u_\ell,v_\ell)^{k_\ell},$$

with $(u_i,v_i) \overset{*}{\leftrightarrow} (u,v)$. But by freeness of $p(\mathbb{Z}^2)$, we get $\ell = 1$ and $k_1 = 1$, so $(u',v') = (u_1,v_1) \overset{*}{\leftrightarrow} (u,v)$. □

Lemma 5.31. *Assume that the $\mathbb{Z}^2$-machine is obtained from a deterministic Turing machine, and that (u_0,v_0) is a halting configuration, i.e. there is no transformation starting from it.*

Then $(u,v) \overset{*}{\leftrightarrow} (u_0,v_0)$ if and only if $(u,v) \overset{*}{\to} (u_0,v_0)$.

Proof. Consider a minimal sequence of transformations

$$(u, v) = (u_n, v_n) \leftrightarrow (u_{n-1}, v_{n-1}) \leftrightarrow \cdots \leftrightarrow (u_0, v_0)\,.$$

Since (u_0, v_0) is a halting configuration, the last transition has to be $\rightarrow$. Moreover, if we have

$$(u_{i+2}, v_{i+2}) \leftarrow (u_{i+1}, v_{i+1}) \rightarrow (u_i, v_i)\,,$$

then $(u_i, v_i) = (u_{i+2}, v_{i+2})$ because the Turing machine is assumed to be deterministic (so there is at most one transition from each state). This is impossible by minimality of the sequence of transformations. Hence, every transition $\rightarrow$ has to be preceded by $\rightarrow$. Inductively, we have

$$(u, v) = (u_n, v_n) \rightarrow (u_{n-1}, v_{n-1}) \rightarrow \cdots \rightarrow (u_0, v_0)\,. \qquad \square$$

Theorem 5.32. *There exists a finitely presented group Γ together with a finitely generated subgroup H for which the generalised word problem is undecidable.*

Proof. Let M be the universal Turing machine, which is deterministic. We consider the associated $\mathbb{Z}^2$-machine. We may assume that M has only one halting state corresponding to $(u_0, v_0) \in \mathbb{Z}^2$. Now take $\Gamma = K_Z$ constructed as above (c.f. Notation 5.29) and let

$$H = \langle p\,(u_0, v_0)\,, T_\ell, T_r \rangle \leqslant \Gamma.$$

By Lemmas 5.30 and 5.31, the halting problem for M reduces to the generalised word problem for (Γ, H). But the former is undecidable by Corollary 1.7, and so is the latter. $\square$

5.7 Undecidability of the word and isomorphism problems

Theorem 5.33. *There exists a finitely presented group L for which the word problem is undecidable.*

Proof. By Theorem 5.32, there is a group Γ together with a subgroup H s.t. the generalised word problem for (Γ, H) is undecidable. Consider $\varphi = \mathrm{id}_H : H \xrightarrow{\cong} H$ and let

$$L = \Gamma *_\varphi,$$

with stable generator k. By Britton's Lemma (Lemma 5.21), for $g \in \Gamma$, $[g, k] = 1$ if and only if $g \in H$. Therefore, (a particular instance of) the word problem for L reduces to the generalised word problem for (Γ, H); the latter is undecidable, and so is the former. $\square$

Theorem 5.34. *There exists a finitely generated free group F s.t. determining if a group is isomorphic to F is undecidable. In particular, the isomorphism problem is undecidable.*

Proof. By Theorem 5.33, there exists a finitely presented group L for which the word problem is undecidable. Moreover, L was constructed by successive HNN extensions starting from the torsion-free group $K \cong \mathbb{Z}^2 * \mathbb{Z}$, so L is torsion-free by Proposition 5.24. Consider a finite presentation $L = \langle S \mid R \rangle$. Define an abstract set of letters $S' = \{h_s,\ s \in S\}$. Now, for $w \in F(S)$, define

$$L(w) = \left\langle S \cup S' \mid R \cup \left\{h_s^{-1} w h_s s^{-1},\ s \in S\right\} \right\rangle.$$

Note that, if $w \overset{L}{=} 1$, then $L(w) = F\,(S')$. Conversely, if $w \overset{L}{\neq} 1$, then w has infinite order since L is torsion-free, and each element $s \in S$ induces an isomorphism $\varphi_s : \langle w \rangle \xrightarrow{\cong} \langle s \rangle$ by conjugation by h_s. Therefore,

$$L(w) = \left(\left(L *_{\varphi_{s_1}}\right) *_{\varphi_{s_2}}\right) * \cdots\,,$$

so $L(w)$ is obtained from L, and therefore from K, by successive HNN extensions. But $K \cong \mathbb{Z}^2 * \mathbb{Z}$ is not free, so neither is $L(w)$. This proves that

$$w \overset{L}{=} 1 \iff L(w) \cong F\,(S')\,.$$

Therefore, the word problem for L reduces to determining if a group is isomorphic to $F\,(S')$. Since the former is undecidable, so is the latter. $\square$

5.8 Undecidability of the homeomorphism problem

Remark 5.35. *Given a group presentation $\langle S \mid R\rangle$, Proposition 5.14 constructs a complex $\mathcal{C}$ s.t. $\pi_1\mathcal{C} \cong \langle S \mid R\rangle$, and s.t. a word w is trivial in $\langle S \mid R\rangle$* iff *the corresponding loop is contractible in $\mathcal{C}$.*

To reduce the isomorphism problem to the homeomorphism problem, it is tempting to construct the complexes $\mathcal{C}, \mathcal{C}'$ from two presentations $\langle S \mid R\rangle, \langle S' \mid R'\rangle$ respectively and check if $\mathcal{C} \cong \mathcal{C}'$. However, this is not equivalent in general to $\langle S \mid R\rangle \cong \langle S' \mid R'\rangle$. The reason for this is essentially that there can be trivial relations: for instance, consider the presentations $\langle s \mid s\rangle$ and $\langle s \mid s, s\rangle$ of the trivial group. The corresponding complexes are a disc with its boundary and a sphere with marked equator, respectively, so they are not homeomorphic.

The solution to this issue will be to construct a new complex, that is invariant under (some variations of) Tietze transformations.

Notation 5.36. *Given a presentation $G = \langle S \mid R\rangle$, we write*

$$G \star k = \langle S \mid R \cup \{1, \dots, 1\}\rangle$$

for the same presentation with k trivial relations added.

Notation 5.37. *Let $G = \langle S \mid R\rangle$ and $G' = \langle S' \mid R'\rangle$ be two group presentations. We associate 4-manifolds M, M' to G, G' respectively constructed as follows:*

- *Replace G by $G \star (p + m' + 1)$ and G' by $G' \star (p' + m + 1)$, with $p = |S|$, $p' = |S'|$, $m = |R|$ and $m' = |R'|$.*
- *Consider the complexes $\mathcal{C}, \mathcal{C}'$ given by Proposition 5.14.*
- *Triangulate $\mathcal{C}, \mathcal{C}'$ and get simplicial complexes after performing at most two barycentric subdivisions.*
- *Piecewise linearly embed $\mathcal{C}, \mathcal{C}'$ in $\mathbb{R}^5$: to do this, place the vertices in general position in $\mathbb{R}^5$ (i.e. such that any six vertices are affinely independent), for instance by considering the curve $t \mapsto (t, t^2, t^3, t^4, t^5)$, then piecewise linearly embed the faces of $\mathcal{C}, \mathcal{C}'$ as triangles and check that this gives an embedding of $\mathcal{C}, \mathcal{C}'$.*
- *Thicken the resulting complexes in $\mathbb{R}^5$, i.e. consider the ε-neighbourhoods $\mathcal{C}^\varepsilon, \mathcal{C}'^\varepsilon$ for ε small enough.*
- *Take the boundary and set $M = \partial\mathcal{C}^\varepsilon$ and $M' = \partial\mathcal{C}'^\varepsilon$.*

Lemma 5.38. *Consider the following alternative Tietze transformations:*

(T_{11}) $\langle S \mid R\rangle \longmapsto \langle S \mid R \cup \{s^\varepsilon s^{-\varepsilon} r\} \setminus \{r\}\rangle$, *with $r \in R$, $s \in S$ and $\varepsilon \in \{\pm 1\}$.*

(T_{12}) $\langle S \mid R\rangle \longmapsto \langle S \mid R \cup \{vwu\} \setminus \{uvw\}\rangle$, *with $uvw \in R$.*

(T_{13}) $\langle S \mid R\rangle \longmapsto \langle S \mid R \cup \{r^{-1}\} \setminus \{r\}\rangle$, *with $r \in R$.*

(T_{14}) $\langle S \mid R\rangle \longmapsto \langle S \mid R \cup \{rr'\} \setminus \{r\}\rangle$, *with $r \neq r' \in R$.*

Then (T_{11})-(T_{14}) preserve the isomorphism type of the presentation. Moreover, any two isomorphic group presentations can be related by a sequences of transformations among (T_{11})-(T_{14}), (T_2) (c.f. Definition 5.4), and their inverses.

Proof. Note that, if $G = \langle S \mid R\rangle$ and $G' = \langle S \mid R \cup \{r\}\rangle$ (with $r \in \langle\langle R\rangle\rangle$), then $G \star 2$ may be connected to $G' \star 1$ by (T_{11})-(T_{14}), (T_2). Then apply Theorem 5.5. □

Lemma 5.39. *If G_2 is a group presentation resulting from G_1 by any of the transformations among (T_{11})-(T_{14}), (T_2), then the 4-manifolds M_1, M_2 constructed in Notation 5.37 from G_1, G_2 are homeomorphic.*

Corollary 5.40. *The homeomorphism problem for 4-manifolds is undecidable.*

Proof. Lemmas 5.38 and 5.39 imply that the isomorphism problem reduces to the homeomorphism problem for 4-manifolds. The former is undecidable by Theorem 5.34, and so is the latter. □

6 Geometry of the word problem

6.1 Cayley graphs and Cayley 2-complexes

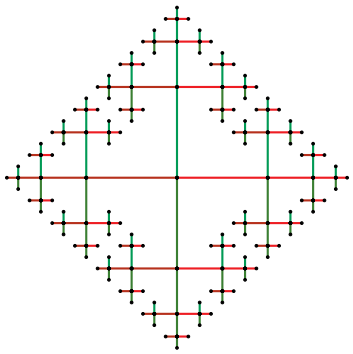
Definition 6.1 (Cayley graph)**.** *Let G be a group with a generating set S (we may assume S to be symmetric, i.e. $S = S^{-1}$). The* ***Cayley graph*** *of G for S is the graph $\mathrm{Cay}_S G$ with vertex set G and arc set*

$$A = \left\{(g, gs)\,,\ g \in G,\ s \in S^{\pm 1}\right\},$$

with $o(g, gs) = g$ and $\iota(g, gs) = (gs, g)$.

There is a natural left action $G \curvearrowright \mathrm{Cay}_S G$ by graph automorphisms, and this action is free and transitive on the vertices.

Example 6.2. *For $G = F(a, b)$ and $S = \{a, b\}$, we get the following graph:*



$\mathrm{Cay}_{\{a,b\}} F(a, b)$

Definition 6.3 (Cayley 2-complex)**.** *Given a presentation $G = \langle S \mid R\rangle$, the* ***Cayley 2-complex*** *$X^{(2)}(S, R)$ is the cell complex with only one vertex, with arcs indexed by $S \cup S^{-1}$, and with 2-cells indexed by R, each 2-cell being glued on the 1-skeleton along the corresponding word $w \in R$.*

Example 6.4. *If $G = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1, b_1] \cdots [a_g, b_g]\rangle$, then the topological realisation of $X^{(2)}$ is the surface of genus g.*

Theorem 6.5. *$\pi_1\left(X^{(2)}(S, R), \bullet\right) \cong \langle S \mid R\rangle$ (and the isomorphism sends the loop indexed by $s \in S$ to the letter $s \in \langle S \mid R\rangle$).*

Proof. Note first that $\pi_1\left(X^{(1)}, \bullet\right) \cong F(S)$. By definition, we have an exact sequence

$$1 \to \langle\langle R\rangle\rangle \to F(S) \to \langle S \mid R\rangle \to 1.$$

Moreover, we have an exact sequence

$$1 \to \operatorname{Ker} p \to \pi_1\left(X^{(1)}, \bullet\right) \xrightarrow{p} \pi_1\left(X^{(2)}, \bullet\right) \to 1.$$

An element $w \in \operatorname{Ker} p$ is a loop corresponding to a 2-cell, i.e. to an element of $\langle\langle R\rangle\rangle$; therefore $\operatorname{Ker} p = \langle\langle R\rangle\rangle$ and the above two exact sequences fit into a commutative diagram. □

Proposition 6.6. *If $X = X^{(2)}(S, R)$, then the 1-skeleton of the universal cover $\widetilde{X}$ is isomorphic to $\mathrm{Cay}_S \langle S \mid R\rangle$.*

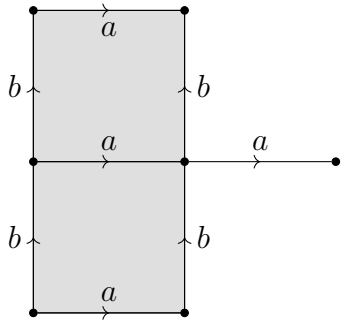
In particular, there is a proper and free action $\langle S \mid R\rangle \curvearrowright \widetilde{X}$.

Note that $\widetilde{X}$ is sometimes called the Cayley 2-complex.

6.2 Van Kampen diagrams

Definition 6.7 (Van Kampen diagram)**.** *Let $G = \langle S \mid R\rangle$. Take a word $w \in (S \amalg S^{-1})^*$ with $w \overset{G}{=} 1$. Then a **Van Kampen diagram** for w is a finite planar simply connected 2-complex Δ with (oriented) edges labelled by $S \amalg S^{-1}$, (unoriented) 2-cells labelled by R, and such that, for each 2-cell π of label $r_\pi \in R$, $\partial\pi$ is labelled by a cyclic permutation of $r_\pi^{\pm 1}$, and $\partial\Delta$ is labelled by w.*

Example 6.8. *Consider $\mathbb{Z}^2 = \langle a, b \mid [a, b]\rangle$ and $w = abaa^{-1}ba^{-1}b^{-1}b^{-1} \overset{\mathbb{Z}^2}{=} 1$. Then the following is a Van Kampen diagram for w:*

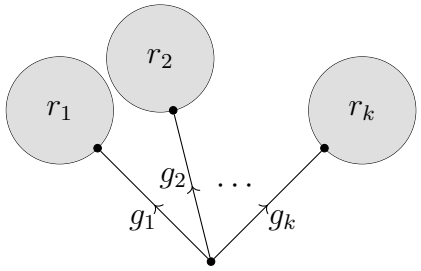


Note that w may have other Van Kampen diagrams. Moreover, Van Kampen diagrams have no reason to be subcomplexes of the universal cover of $X^{(2)}(S, R)$.

Proposition 6.9. *Let $G = \langle S \mid R\rangle$. Then a word $w \in (S \amalg S^{-1})^*$ is trivial in G* iff *there exists a Van Kampen diagram for w.*

Proof. ($\Leftarrow$) Let Δ be a Van Kampen diagram for w. Recall that Δ is simply connected, so its boundary $\partial\Delta$ is a contractible loop labelled by w. But homotopies in Δ corresponds to multiplying by conjugates of elements of R. In particular, homotopies do not change the value of a word in G, which implies that $w \overset{G}{=} 1$.

($\Rightarrow$) Write $w = \prod_i g_i r_i g_i^{-1}$, with $g_i \in G$ and $r_i \in R$, and consider the following Van Kampen diagram:



It may be reduced after performing some folds. □

Definition 6.10 (Combinatorial area)**.** *Let $G = \langle S \mid R\rangle$. The **combinatorial area** of a word $w \overset{G}{=} 1$ is the minimal number of 2-cells in a Van Kampen diagram for w, or equivalently, the minimal number of relators needed to express w as a trivial word.*

6.3 Isoperimetry and Dehn functions

Definition 6.11 (Dehn function)**.** *The **Dehn function** of $\langle S \mid R\rangle$ is*

$$D_{\langle S|R\rangle} : n \in \mathbb{N} \longmapsto \max_{\substack{|w|_S \leqslant n \\ w=1}} \mathrm{Area}(w).$$

Given a function $F \geqslant D$, one says that an inequality

$$\mathrm{Area}(w) \leqslant F\left(|w|_S\right)$$

*is an **isoperimetric inequality**. Note that such an inequality holds for all $w \overset{G}{=} 1$* iff *$F \geqslant D$.*

Proposition 6.12. *Given two finite presentations $\langle S \mid R\rangle, \langle S' \mid R'\rangle$ of a same group G with respective Dehn functions D, D', there exists a constant $A \geqslant 1$ such that, for all $n \in \mathbb{N}$,*

$$D(n) \leqslant A \cdot D'(An).$$

In particular, it makes sense to say that the Dehn function of a finitely presented group is linear, quadratic, polynomial, exponential, etc.

Proof. First choose $A_0 = \max_{s\in S} |s|_{S'}$, so that

$$|w|_{S'} \leqslant A_0 |w|_S$$

for all w. Then choose $A_1 = \max_{r'\in R'} \mathrm{Area}_R(r')$, so that

$$\mathrm{Area}_R(w) \leqslant A_1 \mathrm{Area}_{R'}(w)$$

for all $w \overset{G}{=} 1$. Now, if $A = \max\{A_0, A_1\}$, then

$$\mathrm{Area}_R(w) \leqslant A\,\mathrm{Area}_{R'}(w) \leqslant A \cdot D'(|w|_{S'}) \leqslant A \cdot D'(A|w|_S). \qquad \square$$

Proposition 6.13. *Let $G = \langle S \mid R\rangle$ be a finite presentation with Dehn function D. Then the word problem for G is solvable* iff *there exists a function $T \geqslant D$ that is computable by a Turing machine.*

Proof. ($\Leftarrow$) Given a word w, compute $t = T(|w|_S)$, then enumerate all possible Van Kampen diagrams with at most $Lt + |w|_S$ edges, where $L = \max_{r\in R} |r|_S$. If $w \overset{G}{=} 1$, then it must appear as the boundary of one of those diagrams.

($\Rightarrow$) Make a list of all trivial words of length at most n (since the word problem is solvable), find a Van Kampen diagram (by enumeration of all possible diagrams of small enough length) for each trivial word, and look at the number of 2-cells of each diagram to obtain an upper-bound for the area. $\square$

Corollary 6.14. *There exists a finite group presentation whose Dehn function grows faster than any computable function.*

Proof. By Theorem 5.33, there exists a finitely presented group whose word problem is undecidable. Therefore, by Proposition 6.13, the Dehn function of the corresponding presentation grows faster than any computable function. $\square$

Example 6.15. *Consider the surface group $S_g = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1, b_1]\cdots[a_g, b_g]\rangle$ with $g \geqslant 2$. The Cayley graph of G (with respect to the generating set $\{a_1, b_1, \ldots, a_g, b_g\}$) is the plane tiled by $4g$-gons, with $4g$ tiles at each vertex. Dehn's original idea to solve the word problem for S_g was to notice that each loop in this graph contains a subword of length at least 5 that is also a subword of a relation; therefore, this subword can be replaced by a subword of length at most 3. In other words, if $w \overset{G}{=} 1$ and $|w|_S \geqslant 1$, then there exist $h \in G$ and $r \in R$ s.t.*

$$\left|whrh^{-1}\right|_S < |w|_S.$$

This implies that

$$D(n) \leqslant n,$$

so the Dehn function of a surface group is linear, and therefore surface groups have a solvable word problem.

6.4 Lower bounds on Dehn functions

Proposition 6.16. *Let $G = \langle S \mid R\rangle$ be a presentation; denote by $\widetilde{X}^{(2)}$ the universal cover of the Cayley 2-complex. Given a Van Kampen diagram Δ for a word $w \in (S \amalg S^{-1})^*$ with $w \overset{G}{=} 1$, there exists a continuous map*

$$\varphi : \Delta \to \widetilde{X}^{(2)}$$

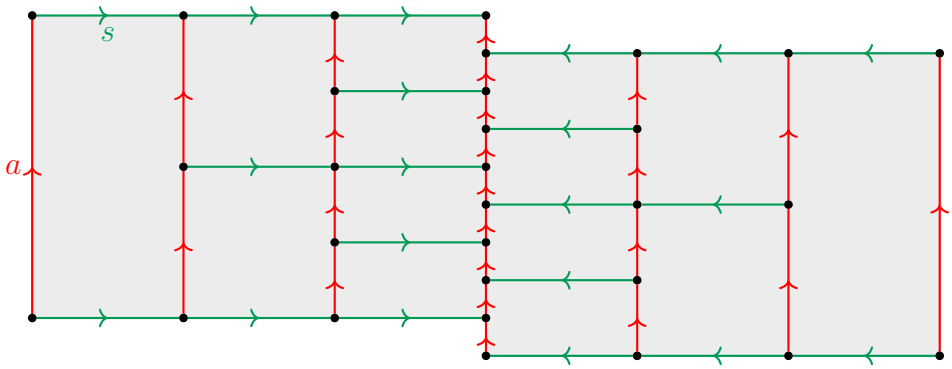
that preserves the labelling of edges.

*Moreover, if φ is an embedding and if $\widetilde{X}^{(2)}$ is **aspherical** (i.e. $\pi_2\widetilde{X}^{(2)} = 1$), then Δ has minimal area, i.e.* $\mathrm{Area}(w) = \mathrm{Area}(\Delta)$.

Sketch of proof. Argue by induction on the number of cells of Δ. The result is clear if Δ has only one cell. In the general case, send $\partial\Delta$ to $\mathrm{Cay}_S G = \widetilde{X}^{(1)}$ by following the word w. Take a cell intersecting $\partial\Delta$; there is a corresponding cell in $\widetilde{X}^{(2)}$; homotope through both cells and apply induction.

If $\varphi : \Delta \to \widetilde{X}^{(2)}$ is an embedding, assume for contradiction that there exists another Van Kampen diagram Δ' with smaller area but same boundary. Glue the two diagram Δ, Δ' along their boundary to obtain $\Delta \cup_{\partial\Delta} \Delta'$. This yields a spherical diagram $\Delta \cup_{\partial\Delta} \Delta' \to \widetilde{X}^{(2)}$. Since $\widetilde{X}^{(2)}$ is aspherical, we can conclude that two adjacent cells in $\Delta \cup_{\partial\Delta} \Delta'$ are identified. This allows one to induct on $\mathrm{Area}(\Delta)$. □

Example 6.17. *Consider the Baumslag-Solitar group $BS_{1,2} = \langle a, s \mid s^{-1}asa^{-2}\rangle$. We have the following Van Kampen diagram for $w = s^{-n}as^n a^{-1}s^{-n}a^{-1}s^n a$ (here for $n = 3$):*



This diagram is embedded in $\widetilde{X}^{(2)}$ and has exponentially many cells. Moreover, $\widetilde{X}^{(2)}$ is aspherical (in fact, it is homeomorphic to the product of a tree with $\mathbb{R}$). It follows that the Dehn function of $BS_{1,2}$ is at least exponential.

6.5 Small cancellation presentations

Definition 6.18 (Pieces)**.** *Given a presentation $\langle S \mid R\rangle$, we denote by R_* the collection of cyclic permutations of the words r, r^{-1} for $r \in R$.*

*A **piece** of $\langle S \mid R\rangle$ is a common prefix of two distinct words in R_*.*

Example 6.19. (i) *Let $G_1 = \langle a, b, c \mid bcabacda\rangle$. Then pieces are $a^{\pm 1}, b^{\pm 1}, c^{\pm 1}, ab, b^{-1}a^{-1}$.*

(ii) *Let $G_2 = \langle a, b \mid (ab)^5\rangle$. Then words of R_* are $(ab)^5, (ba)^5, (b^{-1}a^{-1})^5, (a^{-1}b^{-1})^5$. In particular, there are no pieces.*

(iii) *Let $G_3 = \langle a, b \mid [a, b]\rangle$. Pieces are $a^{\pm 1}, b^{\pm 1}$.*

Remark 6.20. *If Δ is a Van Kampen diagram for a word w and if α is a path in Δ that bounds two 2-cells C_1, C_2, then:*

- *Either α is labelled by a piece,*
- *Or Δ is not reduced at α, i.e. the labels of $\partial C_1, \partial C_2$ are inverses of each other.*

Definition 6.21 (Small cancellation conditions)**.** *Let $\lambda \in (0,1]$. The presentation $\langle S \mid R\rangle$ is said to satisfy the $\mathcal{C}'(\lambda)$* ***small cancellation condition*** *if, given $r \in R_*$ and a prefix u of r that is a piece, we have*

$$|u| < \lambda\,|r|\,.$$

In other words, pieces are small as compared to the relators to which they belong.

Example 6.22. (i) *The presentations G_1, G_3 of Example 6.19 satisfy $\mathcal{C}'\left(\frac{1}{4}+\varepsilon\right)$ for all $\varepsilon > 0$.*

(ii) *The presentation G_2 of Example 6.19 satisfies $\mathcal{C}'(\lambda)$ for all $\lambda \in (0,1]$.*

(iii) *Let $\Gamma_g = \langle a_1, b_1, \dots, a_g, b_g \mid [a_1,b_1]\cdots[a_g,b_g]\rangle$. Then Γ_g satisfies $\mathcal{C}'\left(\frac{1}{4g}+\varepsilon\right)$ for all $\varepsilon > 0$.*

Note in particular that Γ_g satisfies $\mathcal{C}'\left(\frac{1}{6}\right)$ if $g \geqslant 2$.

6.6 Greendlinger's Lemma

Theorem 6.23 (Greendlinger 1961)**.** *Let $\langle S \mid R\rangle$ be a presentation satisfying $\mathcal{C}'(\lambda)$ with $\lambda \leqslant \frac{1}{6}$. Let Δ be an area minimising Van Kampen diagram for a trivial word w in $\langle S \mid R\rangle$ s.t.*

- *Δ has at least one cell,*
- *w is cyclically reduced,*
- *w does not contain any subword that is trivial in $\langle S \mid R\rangle$.*

Then there exists a subpath α of $\partial\Delta$ bounding a 2-cell C and s.t.

$$|\alpha| > (1-3\lambda)\,|\partial C|\,.$$

Note that, for $\lambda = \frac{1}{6}$, this conclusion is exactly the condition needed to make Dehn's Algorithm work.

Proof. Assume for contradiction that all subpaths α of $\partial\Delta$ bounding a 2-cell C satisfy $|\alpha| \leqslant (1-3\lambda)\,|\partial C|$. Since Δ is planar, it may be realised on the sphere $\mathbb{S}^2$. Construct a dual diagram Γ as follows:

- There is one vertex v_C of Γ in the interior of each cell C of Δ.
- For every maximal subpath α adjacent to two cells C_1, C_2 of Δ, there is an edge e_α between v_{C_1} and v_{C_2} in Γ, with e_α transverse to α.
- There is a vertex v_∞ in the outer face of Δ with edges between v_∞ and every vertex v_C s.t. the cell C is adjacent to $\partial\Delta$.

Note that this construction can be done without any crossing between the edges of Γ, i.e. in such a way that Γ is planar. Observe also that Γ has no 1-gon (because boundaries of cells of Δ are cyclically reduced, i.e. there is no edge of Δ bounding only one face) and no bigon (because we only construct edges of Γ through maximal boundary subpaths). Therefore, the faces of Γ are polygons with at least three sides.

(Remark: another way to construct Γ is to first replace all degree 2 vertices of Δ by edges, and then to take the dual of the graph, which can be seen as a spherical combinatorial map.)

Write v, e, f for the numbers of vertices, edges and faces of Γ. Since Γ is embedded on the sphere, we have

$$v - e + f = \chi(\Gamma) = 2.$$

Moreover, since the faces of Γ have at least three sides, it follows that

$$2e = \sum_{p \in F(\Gamma)} \deg p \geqslant 3f,$$

i.e. $f \leqslant \frac{2}{3}e$. Combining this with the equality obtained from the Euler characteristic yields

$$v - 1 \geqslant 1 + \frac{1}{3}e. \qquad (*)$$

We now define a weight function on $V(\Gamma)$ as follows:

- Given C_1, C_2 two cells of Δ, every edge between v_{C_1} and v_{C_2} adds $\frac{1}{2}$ to the weights of v_{C_1} and v_{C_2}.
- Given a cell C adjacent to $\partial\Delta$, every edge between v_C and v_∞ adds 1 to the weight of v_C.

Let us give a lower bound on the weight of v_C, for C a cell of Δ.

- *Case* 1: C is not adjacent to $\partial\Delta$. Then condition $\mathcal{C}'(\lambda)$ implies that C has $> \frac{1}{\lambda}$ adjacent cells in Δ (this follows from the fact that all maximal boundary subpaths of Δ must correspond to pieces of $\langle S \mid R\rangle$ since Δ has minimal area), so v_C has weight $> \frac{1}{2\lambda} \geqslant 3$.
- *Case* 2: there is exactly one maximal boundary subpath α of ∂C in $\partial\Delta$. Then by assumption, $|\alpha| \leqslant (1 - 3\lambda)\,|\partial C|$, or in other words $|\partial C \setminus \alpha| \geqslant 3\lambda\,|\partial C|$. Hence $\mathcal{C}'(\lambda)$ implies that C has $> \frac{1}{\lambda} \cdot 3\lambda = 3$ adjacent cells in Δ. Hence, v_C has weight at least $\frac{4}{2} + 1 = 3$.
- *Case* 3: there are two or more maximal subpaths of ∂C in $\partial\Delta$. Hence, there are at least two cells of Δ adjacent to C, so v_C has weight at least $\frac{2}{2} + 1 + 1 = 3$.

In all cases, we see that v_C has weight at least 3.

Now the sum of all weights is e, and all vertices (except for v_∞) have weight at least 3; therefore

$$e \geqslant 3(v - 1).$$

Combining with $(*)$ yields $e \geqslant 3 + e$, which is a contradiction. □

Corollary 6.24. *If a presentation satisfies $\mathcal{C}'\left(\frac{1}{6}\right)$, then its Dehn function is linear.*
In particular, its word problem is solvable by Proposition 6.13.

Proof. Take a Van Kampen diagram Δ of minimal area for a trivial word w. By Greendlinger's Lemma (Theorem 6.23), one can homotope w to a strictly shorter word by removing one cell. It follows that $\mathrm{Area}(w) \leqslant |w|$. □

Remark 6.25. *In fact, having a linear Dehn function is a characterisation of word-hyperbolic groups.*

Example 6.26. *Consider $G_n = \langle x, y \mid (xy)\,(xy^2)\cdots(xy^n)\rangle$. Then, for all $\varepsilon > 0$, if n is large enough, G_n satisfies $\mathcal{C}'(\varepsilon)$.*

Proposition 6.27. *If $G = \langle S \mid R\rangle$ satisfies $\mathcal{C}'\left(\frac{1}{6}\right)$, then the universal cover $\widetilde{X}^{(2)}$ of the Cayley 2-complex is aspherical.*
In particular, G has cohomological dimension at most 2.

Sketch of proof. Assume for contradiction that $\widetilde{X}^{(2)}$ contains a spherical diagram. Remove one cell from it to obtain a Van Kampen diagram and apply Greendlinger's Lemma (Theorem 6.23) to find a large piece. □

Theorem 6.28. *Let $G = \langle S \mid R\rangle$ be a presentation satisfying $\mathcal{C}'\left(\frac{1}{8}\right)$. Then*

(i) *The group G is infinite.*

(ii) *If a word g satisfies $g^k \overset{G}{=} 1$, then there are words h, w s.t. $hgh^{-1} = w$ and $w^k \in R$.*

References

[1] N. Brady, T. Riley, and H. Short. *The Geometry of the Word Problem for Finitely Generated Groups.*

[2] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms.*

[3] J. Gross and T. Tucker. *Topological Graph Theory.*

[4] B. Mohar and C. Thomassen. *Graphs on Surfaces.*

[5] C. Papadimitriou. *Computational Complexity.*

[6] J. Stillwell. *Classical Topology and Combinatorial Group Theory.*

[7] A. Wigderson. *P, NP and Mathematics — a computational complexity perspective.*