

# Computational complexity for presentations of sofic shifts

Justin Cai

April 22, 2020

## Abstract

Given an irreducible presentation of a sofic shift, it is well known that the shift it presents is irreducible and that there is a procedure that yields the unique vertex-minimal presentation for this shift in polynomial time. However, if one was given a reducible graph, there is not necessarily a unique vertex-minimal presentation, and a procedure for the construction of some minimal presentation in this case is unknown. It can be the case where the presentation still presents an irreducible shift, but the previous procedure will not produce the minimal presentation. In this thesis, we show complexity results around these problems.

## 1 Preliminaries

**Definition 1.1.** Let  $\mathcal{A}$  be a finite set. The *full  $\mathcal{A}$ -shift* is the set  $\mathcal{A}^{\mathbb{Z}}$  of all bi-infinite sequences over  $\mathcal{A}$  (i.e. functions from  $\mathbb{Z}$  to  $\mathcal{A}$ , hence the usual notation for the set of all functions from  $\mathbb{Z}$  to  $\mathcal{A}$ ).

A *block* (or *word*) is a finite sequence of letters over some alphabet  $\mathcal{A}$ . Let  $x = (x_i)_{i \in \mathbb{Z}}$  be a bi-infinite sequence. For  $i \leq j$ , the block from the  $i$ th coordinate to the  $j$ th coordinate is denoted

$$x_{[i,j]} \triangleq x_i x_{i+1} \dots x_j.$$

**Definition 1.2.** Let  $\mathcal{F}$  be a set of words over some alphabet. A *subshift* is a subset  $X_{\mathcal{F}}$  of some full shift  $\mathcal{A}^{\mathbb{Z}}$  such that no word in  $\mathcal{F}$  appears in any point of the subshift, defined as

$$X_{\mathcal{F}} \triangleq \left\{ (x_i)_{i \in \mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}} : \forall i, j \in \mathbb{Z}, i \leq j \quad x_{[i,j]} \notin \mathcal{F} \right\}.$$

**Definition 1.3.** A *graph*  $G$  is a 4-tuple  $G = (\mathcal{V}, \mathcal{E}, i, t)$ , where  $\mathcal{V}$  is a finite set of *vertices*,  $\mathcal{E}$  is a finite set of *edges*, and  $i : \mathcal{E} \rightarrow \mathcal{V}$  and  $t : \mathcal{E} \rightarrow \mathcal{V}$  are functions assigning an *initial* and *terminating* vertex for each edge, respectively. For an arbitrary graph  $G$ , let  $\mathcal{V}_G$ ,  $\mathcal{E}_G$ ,  $i_G$ ,

and  $t_G$  denote the graph's vertices, edges, and initial and terminating vertex functions, respectively. If the choice of  $G$  is understood, then the subscripts will be dropped for notational convenience.

For  $I \in \mathcal{V}$ , the *outgoing edges of  $I$*  is the set of edges starting at  $I$ , denoted

$$i^{-1}(I) \triangleq \{e \in \mathcal{E} : i(e) = I\}.$$

Similarly, the *incoming edges of  $I$*  is the set of edges terminating at  $I$ , denoted

$$t^{-1}(I) \triangleq \{e \in \mathcal{E} : t(e) = I\}.$$

A graph is *essential* if all vertices have at least one incoming and outgoing edge; i.e. for all  $I \in \mathcal{V}$ ,  $i^{-1}(I) \neq \emptyset$  and  $t^{-1}(I) \neq \emptyset$ .

**Definition 1.4.** A *labeled graph*  $\mathcal{G}$  is a pair  $\mathcal{G} = (G, \mathcal{L})$ , where  $G$  is a graph and  $\mathcal{L} : \mathcal{E} \rightarrow \mathcal{A}$  is the *labeling function* from the edges of  $G$  onto some finite alphabet  $\mathcal{A}$ .

A labeled graph is *deterministic* if for each vertex, the labels of the outgoing edges at that vertex are all distinct (i.e.  $\mathcal{L}|_{i^{-1}(I)}$  is injective for all  $I \in \mathcal{V}$ ).

**Definition 1.5.** Let  $G$  be a graph. The *edge shift of  $G$*  is the set  $X_G$  of all bi-infinite paths on  $G$ , defined as

$$X_G \triangleq \left\{ (x_i)_{i \in \mathbb{Z}} \in \mathcal{E}^{\mathbb{Z}} : \forall i \in \mathbb{Z} \quad t(x_i) = i(x_{i+1}) \right\}.$$

Define paths.

As a consequence of this definition,  $\mathcal{B}(X_G)$  is the set of all finite paths on  $G$ , so elements of  $\mathcal{B}(X_G)$  are called *paths on  $G$* .

Only if  $G$  is essential. Otherwise, if  $G$  is not essential, then there can be paths not in  $\mathcal{B}(X_G)$ .

**Definition 1.6.** Let  $\mathcal{G} = (G, \mathcal{L})$  be a labeled graph. The *presentation of  $\mathcal{G}$*  is the set  $X_G$  of the labels of all bi-infinite paths from  $X_G$ , defined as the image of  $X_G$  under  $\mathcal{L}_\infty$ :

$$X_G \triangleq \mathcal{L}_\infty(X_G).$$

Define sliding block codes so  $\mathcal{L}_\infty$  makes sense.

We say a word  $w \in \mathcal{B}(X_G)$  is *presented by a path  $\pi \in \mathcal{B}(X_G)$*  if  $\mathcal{L}(\pi) = w$ .

**Definition 1.7.** Let  $\mathcal{G} = (G, \mathcal{L})$  be a labeled graph. For a vertex  $I \in \mathcal{V}_G$ , the *follower set of  $I$*  is the set

$$F(I) \triangleq \{\mathcal{L}(\pi) : \pi \in \mathcal{B}(X_G), i(\pi) = I\}.$$

For a word  $w \in \mathcal{B}(X_G)$ , the *follower set of  $w$*  is the set

$$F(w) \triangleq \{u \in \mathcal{B}(X_G) : wu \in \mathcal{B}(X_G)\}$$

**Definition 1.8.** Let  $\mathcal{G} = (G, \mathcal{L})$  be a labeled graph,  $I$  be some vertex in  $\mathcal{G}$ , and  $w \in \mathcal{B}(X_G)$ . If every path  $\pi$  in  $\mathcal{G}$  that presents  $w$  ends at  $I$ , then we say  $w$  *synchronizes to  $I$* . We say that  $w$  is *synchronizing for  $\mathcal{G}$*  if it synchronizes to some vertex in  $\mathcal{G}$ . If there is a word that synchronizes to  $I$ , then we say that the vertex  $I$  is *synchronizing*. Finally, we denote  $S(\mathcal{G})$  as the set of all synchronizing words for  $\mathcal{G}$ .

Define  $\mathcal{A}_{\mathcal{G}}$ .

Let  $\mathcal{G}$  be a deterministic labeled graph. It follows that for every vertex  $I$  in  $\mathcal{G}$  and every  $w \in F(I)$ , there is a unique path labeled  $w$  starting at  $I$ . We can define a partial transition function  $\delta_{\mathcal{G}} : \mathcal{V}_{\mathcal{G}} \times \mathcal{A}_{\mathcal{G}}^* \rightarrow \mathcal{V}_{\mathcal{G}}$  with  $\delta_{\mathcal{G}}(I, w) \triangleq t(\pi)$  if there is a path  $\pi$  labeled  $w$  starting at  $I$ . If  $w = \mathcal{L}(\pi)$  and  $\mathcal{L}(\tau)$  for paths  $\pi$  and  $\tau$ , then by determinism,  $\pi = \tau$  so  $t(\pi) = t(\tau)$ , so this function is well defined. It will be useful to make  $\delta_{\mathcal{G}}$  total by first defining  $\mathcal{V}_{\mathcal{G}}^0 \triangleq \mathcal{V}_{\mathcal{G}} \cup \{0\}$ , where  $0$  is a constant distinct from  $\mathcal{V}_{\mathcal{G}}$ . Then, by extending the domain of  $\delta_{\mathcal{G}}$  to  $\mathcal{V}_{\mathcal{G}}^0 \times \mathcal{A}_{\mathcal{G}}^*$  and the codomain to  $\mathcal{V}_{\mathcal{G}}^0$ , define  $\delta_{\mathcal{G}}(I, w) \triangleq 0$  if  $w \notin F(I)$  and  $\delta_{\mathcal{G}}(0, w) = 0$ . Finally, define the subset transition function  $\Delta_{\mathcal{G}} : \mathcal{P}(\mathcal{V}) \times w \rightarrow \mathcal{P}(\mathcal{V})$  with  $\Delta_{\mathcal{G}}(S, w) \triangleq \{\delta_{\mathcal{G}}(I, w) : I \in S \text{ and } \delta_{\mathcal{G}}(I, w) \neq 0\}$ .

**Theorem 1.9.** Let  $\mathcal{G}$  be a deterministic labeled graph, and  $I$  be a vertex in  $\mathcal{G}$ . The following properties of the transition function are true:

- (i)  $w \in F(I)$  if and only if  $\delta_{\mathcal{G}}(I, w) \neq 0$
- (ii)  $w \in \mathcal{B}(\mathcal{X}_{\mathcal{G}})$  if and only if  $\Delta_{\mathcal{G}}(\mathcal{V}_{\mathcal{G}}, w) \neq \emptyset$
- (iii)  $w$  synchronizes to  $I$  if and only if  $\Delta_{\mathcal{G}}(\mathcal{V}_{\mathcal{G}}, w) = \{I\}$

**Definition 1.10.** Let  $\mathcal{G}$  be an essential labeled graph. The  $\mathcal{G}$  kill state graph with alphabet  $\mathcal{A}$  is the labeled graph  $\mathcal{G}^0$  taking the same vertices and edges as  $\mathcal{G}$  with an additional vertex  $0$  and edges such that for each  $a \in \mathcal{A}$  and vertex  $I$  in  $\mathcal{G}$ , if there is no edge starting at  $I$  labeled  $a$ , then there is an edge in  $\mathcal{G}^0$  between  $I$  and  $0$  labeled  $a$ .

**Definition 1.11.** Let  $\mathcal{G}$  and  $\mathcal{H}$  be labeled graphs. The label product of  $\mathcal{G}$  and  $\mathcal{H}$  is the labeled graph  $\mathcal{G} * \mathcal{H}$  such that if there is an edge  $e_1$  in  $\mathcal{G}$  between  $I_1$  and  $J_1$  and an edge  $e_2$  in  $\mathcal{H}$  between  $I_2$  and  $J_2$  with  $\mathcal{L}_{\mathcal{G}}(e_1) = \mathcal{L}_{\mathcal{H}}(e_2)$ , then there is an edge in  $\mathcal{G} * \mathcal{H}$  between  $(I_1, I_2)$  and  $(J_1, J_2)$  labeled  $\mathcal{L}_{\mathcal{G}}(e_1) = \mathcal{L}_{\mathcal{H}}(e_2)$ . That is,

$$\begin{aligned} \mathcal{V}_{\mathcal{G} * \mathcal{H}} &\triangleq \mathcal{V}_{\mathcal{G}} \times \mathcal{V}_{\mathcal{H}} \\ \mathcal{E}_{\mathcal{G} * \mathcal{H}} &\triangleq \{(e_1, e_2) \in \mathcal{E}_{\mathcal{G}} \times \mathcal{E}_{\mathcal{H}} : \mathcal{L}(e_1) = \mathcal{L}(e_2)\} \\ i_{\mathcal{G} * \mathcal{H}}(e_1, e_2) &\triangleq (i_{\mathcal{G}}(e_1), i_{\mathcal{H}}(e_2)) \\ t_{\mathcal{G} * \mathcal{H}}(e_1, e_2) &\triangleq (t_{\mathcal{G}}(e_1), t_{\mathcal{H}}(e_2)) \\ \mathcal{L}_{\mathcal{G} * \mathcal{H}}(e_1, e_2) &\triangleq \mathcal{L}_{\mathcal{G}}(e_1) \quad (= \mathcal{L}_{\mathcal{H}}(e_2)) \end{aligned}$$

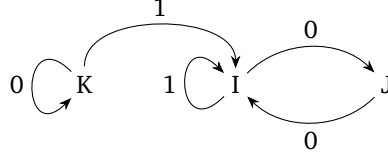
**Theorem 1.12.** If there is a path in  $\mathcal{G} * \mathcal{H}$  labeled  $w$  starting at  $(I, J)$ , then there is a path in  $\mathcal{G}$  labeled  $w$  starting at  $I$  and a path in  $\mathcal{H}$  labeled  $w$  starting at  $J$ .

Add theorem showing that  $\mathcal{X}_{\mathcal{G}}$  and  $\mathcal{X}_{\mathcal{G}}$  are shift spaces.

Add theorem showing that shift spaces are uniquely defined by a language.

## 2 Irreducibility

Consider the reducible graph  $\mathcal{G}$ :



The shift that subgraph induced by  $I$  and  $J$  is the even shift, and every word presented by a path starting from  $K$  is presented by some path starting at  $I$  and  $J$ . Hence, this graph presents the even shift. Additionally, it is also follower-separated as  $01 \in F(K) \setminus F(I)$ ,  $1 \in F(K) \setminus F(J)$ , and  $1 \in F(I) \setminus F(J)$ .

When do follower-separated reducible graphs present irreducible shifts? We will first look at a simple class of reducible graphs.

Let  $\mathcal{G} \rightarrow \mathcal{H}$  be an essential, deterministic, follower-separated graph with two irreducible components that induce two subgraphs, namely  $\mathcal{G}$  and  $\mathcal{H}$ , such that there is exactly one edge starting in  $\mathcal{G}$  and ending in  $\mathcal{H}$ . Some properties of  $\mathcal{G} \rightarrow \mathcal{H}$  are that the vertices of  $\mathcal{G}$  and  $\mathcal{H}$  partition the vertices of  $\mathcal{G} \rightarrow \mathcal{H}$ , both  $\mathcal{G}$  and  $\mathcal{H}$  are essential, any vertex in  $\mathcal{H}$  is reachable from any vertex in  $\mathcal{G} \rightarrow \mathcal{H}$ , and no vertex in  $\mathcal{G}$  is reachable from any vertex in  $\mathcal{H}$ .

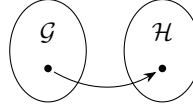


Figure 1: Representation of  $\mathcal{G} \rightarrow \mathcal{H}$ .

Related to a comment below, but this is just a corollary of [Lind and Marcus 3.3.16] and the nature of  $\mathcal{G} \rightarrow \mathcal{H}$

**Theorem 2.1.** Every word  $u \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  can be extended on the right to a word  $uw \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  that synchronizes to a vertex  $I$  in  $\mathcal{H}$ .

*Proof.* Let  $u \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$ . As  $\mathcal{G} \rightarrow \mathcal{H}$  is deterministic and follower-separated, then by [Lind and Marcus 3.3.16], we can extend  $u$  on the right to  $uw \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  so that  $uw$  synchronizes to some vertex  $J$ . As  $I$  is a vertex in  $\mathcal{H}$ ,  $I$  can be reached from  $J$ , so let  $v$  be the label of a path from  $I$  to  $J$ . Then,  $uwv \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  and any path presenting  $uwv$  must end at  $J$ , so  $uwv$  synchronizes to  $I$ .  $\square$

**Corollary 2.2.** Every vertex in  $\mathcal{H}$  is synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ .

*Proof.* For a vertex  $I$  in  $\mathcal{H}$ , take any word  $u \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  and use Theorem 2.1 to synchronize it to  $I$ . Hence, there is a word that synchronizes to  $I$ , so  $I$  is synchronizing.  $\square$

Probably will expand this later. Argue that  $uwv$  is synchronizing, so  $F(uwv) = F(J)$  for some vertex  $J$  in  $\mathcal{H}$ , so  $F(uwv) = F(J) \subseteq \bigcup_{K \in \mathcal{V}_{\mathcal{H}}} F(K) = \mathcal{B}(\mathcal{X}_{\mathcal{H}})$

**Lemma 2.3.** Let  $u \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$ . If  $u \notin \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ , then  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is reducible.

*Proof.* By Theorem 2.1, we can extend  $u$  on the right to a word  $uw \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$  so that any path presenting  $uw$  ends at some vertex  $I$  in  $\mathcal{H}$ . Hence, for any word  $v \in F(uw)$ , a path presenting  $uwv$  ends at some vertex in  $\mathcal{H}$ , so  $F(uwv) \subseteq \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ . As  $u \notin \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ , we have  $u \notin F(uwv)$ . Thus, there is no word in  $\mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$  joining the word  $uw$  and  $u$ , so  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is reducible.  $\square$

**Theorem 2.4.**  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible if and only if  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ .

*Proof.* Suppose  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, and let  $w \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$ . By Lemma 2.3, as  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, then  $w \in \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ , so  $\mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}) \subseteq \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ . By construction of  $\mathcal{G} \rightarrow \mathcal{H}$ , we have  $\mathcal{B}(\mathcal{X}_{\mathcal{H}}) \subseteq \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$ . Therefore,  $\mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}) = \mathcal{B}(\mathcal{X}_{\mathcal{H}})$  so  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ . Conversely, suppose  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ . As  $\mathcal{X}_{\mathcal{H}}$  is irreducible, then so is  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$ .  $\square$

**Corollary 2.5.** If  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, then  $\mathcal{X}_{\mathcal{G}} \subseteq \mathcal{X}_{\mathcal{H}}$ .

*Proof.* By Theorem 2.4, if  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, then  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ . As  $\mathcal{X}_{\mathcal{G}} \subseteq \mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$ , then  $\mathcal{X}_{\mathcal{G}} \subseteq \mathcal{X}_{\mathcal{H}}$ .  $\square$

**Theorem 2.6.** If  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, then no vertex in  $\mathcal{G}$  is synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ .

*Proof.* Suppose there were a vertex  $I$  in  $\mathcal{G}$  that is synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ . Let  $v$  be a word that synchronizes to  $I$  in  $\mathcal{G} \rightarrow \mathcal{H}$ . By Corollary 2.2, every vertex in  $\mathcal{H}$  is synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ , so let  $J$  be some vertex in  $\mathcal{H}$  and  $u$  be a word that synchronizes to  $J$  in  $\mathcal{G} \rightarrow \mathcal{H}$ . As  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible, there is a word  $w \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$  such that  $uwv \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$ . However, any path presenting  $uwv$  must first visit  $J$  (as  $u$  is synchronizing) and then visit  $I$ , implying that  $I$  is reachable from  $J$ . But this contradicts the structure of  $\mathcal{G} \rightarrow \mathcal{H}$ , so no vertex in  $\mathcal{G}$  can be synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ .  $\square$

**Theorem 2.7.**  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$  if and only if  $S(\mathcal{G} \rightarrow \mathcal{H}) \subseteq S(\mathcal{H})$ .

*Proof.* Suppose  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ . Let  $w \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$  synchronize to some vertex  $I$  in  $\mathcal{G} \rightarrow \mathcal{H}$ . If  $\pi$  is some path in  $\mathcal{H}$  presenting  $w$ , then it must end at  $I$ . By Theorem 2.6,  $I$  cannot be a vertex in  $\mathcal{G}$ , so it must be a vertex in  $\mathcal{H}$ . Therefore, every path in  $\mathcal{H}$  presenting  $w$  ends at  $I$ , so  $S(\mathcal{G} \rightarrow \mathcal{H}) \subseteq S(\mathcal{H})$ .

Conversely, suppose  $S(\mathcal{G} \rightarrow \mathcal{H}) \subseteq S(\mathcal{H})$ . Let  $u \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$ . By Theorem 2.1, we can extend  $u$  to a word  $uw \in \mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}})$  that synchronizes to some vertex  $I$  in  $\mathcal{G} \rightarrow \mathcal{H}$ . Hence,  $uw$  is synchronizing for  $\mathcal{G} \rightarrow \mathcal{H}$ , so it is also synchronizing for  $\mathcal{H}$ . But if  $uw$  is synchronizing for  $\mathcal{H}$ , then by definition,  $uw \in \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ . Therefore,  $\mathcal{B}(\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}}) \subseteq \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ , so  $\mathcal{X}_{\mathcal{G} \rightarrow \mathcal{H}} = \mathcal{X}_{\mathcal{H}}$ .  $\square$

**Theorem 2.8.** If  $w \in S(\mathcal{G} \rightarrow \mathcal{H})$  but  $w \notin S(\mathcal{H})$ , then  $w \notin \mathcal{B}(\mathcal{X}_{\mathcal{H}})$ .

*Proof.* As  $w \in S(\mathcal{G} \rightarrow \mathcal{H})$ , there is a vertex  $I$  in  $\mathcal{G} \rightarrow \mathcal{H}$  such that every path in  $\mathcal{G} \rightarrow \mathcal{H}$  presenting  $w$  ends at  $I$ . If  $w \notin S(\mathcal{H})$ , then either  $w \notin \mathcal{B}(X_{\mathcal{H}})$  or for every vertex  $J$  in  $\mathcal{H}$  there is a path in  $\mathcal{H}$  that presents  $w$  but does not end at  $J$ . Hence if the latter condition were true, then this implies there is a path in  $\mathcal{H}$  that presents  $w$  and does not end at  $I$ . But this path is also in  $\mathcal{G} \rightarrow \mathcal{H}$  and presents  $w$ , so it should end at  $I$ , which is a contradiction. Therefore,  $w \notin \mathcal{B}(X_{\mathcal{H}})$ .  $\square$

**Theorem 2.9.**  $X_{\mathcal{G} \rightarrow \mathcal{H}}$  is irreducible if and only if  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  and for all vertices  $I$  in  $\mathcal{G}$  there is a word  $w$  and vertex  $J$  in  $\mathcal{H}$  such that  $\delta_{\mathcal{G} \rightarrow \mathcal{H}}(I, w) = \delta_{\mathcal{G} \rightarrow \mathcal{H}}(J, w)$ .

*Proof.* Suppose  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  and for all vertices  $I$  in  $\mathcal{G}$  there is a word  $w$  and vertex  $J$  in  $\mathcal{H}$  such that  $\delta_{\mathcal{G} \rightarrow \mathcal{H}}(I, w) = \delta_{\mathcal{G} \rightarrow \mathcal{H}}(J, w)$ . Let  $w \in \mathcal{B}(X_{\mathcal{G} \rightarrow \mathcal{H}})$  and  $\pi$  be a path in  $\mathcal{G} \rightarrow \mathcal{H}$  presenting  $w$ . If  $\pi$  starts in  $\mathcal{H}$ , then  $w \in \mathcal{B}(X_{\mathcal{H}})$ . Otherwise,  $\square$

### 3 Subshift testing

---

**Algorithm 1** Subshift testing

---

**Require:**  $\mathcal{G}$  and  $\mathcal{H}$  are deterministic, irreducible labeled graphs

```

1: procedure IS_SUBSHIFT( $\mathcal{G}, \mathcal{H}$ )
2:   for  $I \in \mathcal{V}_{\mathcal{G}}$  do
3:      $X \leftarrow \mathcal{V}_{\mathcal{H}}$ 
4:      $w \leftarrow \epsilon$ 
5:     repeat
6:        $J \leftarrow$  any element in  $X$ 
7:       find a word  $u$  such that  $\delta_{\mathcal{G}}(I, u) \neq 0$  and  $\delta_{\mathcal{H}}(J, u) = 0$ 
8:       if  $u$  exists then
9:          $w \leftarrow wu$ 
10:         $I \leftarrow \delta_{\mathcal{G}}(I, u)$ 
11:         $X \leftarrow \Delta_{\mathcal{H}}(X, u)$ 
12:        if  $X = \emptyset$  then
13:          return false
14:        end if
15:      end if
16:    until  $u$  does not exist
17:  end for
18:  return true
19: end procedure

```

---

**Theorem 3.1.** If  $\mathcal{G}$  and  $\mathcal{H}$  are essential, deterministic labeled graphs, then Algorithm 1 always terminates and returns true if and only if  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$ .

*Proof.* First, we need to show that for the loop on lines 8-19, if  $I_0$  is the value of  $I$  before entering the loop, the invariants

- (i)  $\delta_{\mathcal{G}}(I_0, w) = I$
- (ii)  $I \neq 0$
- (iii)  $\Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w) = X$

hold before the beginning of each iteration the loop. Additionally, we need to show that the loop always terminates.

Clearly,  $I = I_0$  and  $w = \epsilon$  before entering the loop, so  $\Delta_{\mathcal{G}}(I_0, w) = \delta_{\mathcal{G}}(I, \epsilon) = I$ . As  $I_0 \in \mathcal{V}_{\mathcal{G}}$ , we have that  $I \neq 0$ . Finally, as  $X = \mathcal{V}_{\mathcal{G}}$  before entering the loop,  $\Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w) = \Delta_{\mathcal{H}}(X, \epsilon) = X$ , so the invariants hold before entering the loop.

Suppose the invariants were true before the current iteration of the loop and  $I$ ,  $J$ ,  $w$ , and  $X$  had the values  $I_n$ ,  $J_n$ ,  $w_n$  and  $X_n$ , respectively. Furthermore, suppose the loop does not exit after the current iteration. Because of this, then the algorithm must enter the if statement on line 8 (and not enter the if statement on line 12), so there is a word  $u$  such that  $\delta_{\mathcal{G}}(I_n, u) \neq 0$  and  $\delta_{\mathcal{H}}(J_n, u) = 0$ . We can see that  $w = w_n u$ ,  $I = \delta_{\mathcal{G}}(I_n, u)$ , and  $X = \Delta_{\mathcal{H}}(X_n, u)$  at the end of the current iteration, so from this, we can see

$$\delta_{\mathcal{G}}(I_0, w) = \delta_{\mathcal{G}}(I_0, w_n u) = \delta_{\mathcal{G}}(\delta_{\mathcal{G}}(I_0, w_n), u) = \delta_{\mathcal{G}}(I_n, u) = I$$

and similarly,

$$\Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w) = \Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w_n u) = \Delta_{\mathcal{H}}(\Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w_n), u) = \Delta_{\mathcal{H}}(X_n, u) = X.$$

Therefore, all the invariants hold before the next iteration of the loop. Finally, note that as  $\delta_{\mathcal{H}}(J_n, u) = 0$  and  $J_n \in X$ ,  $|X|$  is strictly less than  $|X|$ . This guarantees the loop terminates as if the exit condition is never true, then  $|X| = 0$  will be true for some iteration so  $X = \emptyset$  and the algorithm exits on line 13.

Now, we will show the correctness of the algorithm. Suppose algorithm returns false. Then  $X = \emptyset$  so from the invariants,  $\delta_{\mathcal{G}}(I_0, w) = I \neq 0$  so  $w \in \mathcal{B}(X_{\mathcal{G}})$  and  $\Delta_{\mathcal{H}}(\mathcal{V}_{\mathcal{H}}, w) = \emptyset$  so  $w \notin \mathcal{B}(X_{\mathcal{H}})$ . Therefore,  $X_{\mathcal{G}} \not\subseteq X_{\mathcal{H}}$ .

Conversely, suppose  $X_{\mathcal{G}} \not\subseteq X_{\mathcal{H}}$ . That is, there is a word  $w \in \mathcal{B}(X_{\mathcal{G}})$  but  $w \notin \mathcal{B}(X_{\mathcal{H}})$ . As  $w \in \mathcal{B}(X_{\mathcal{G}})$ , then  $\delta_{\mathcal{G}}(I^*, w) \neq 0$  for some vertex  $I^*$  in  $\mathcal{G}$ . As  $w \notin \mathcal{B}(X_{\mathcal{H}})$ , then  $\delta_{\mathcal{H}}(J, w) = 0$  for all vertices  $J$  in  $\mathcal{H}$ . As the algorithm will eventually have  $I$  take the value of  $I^*$  on line 7, we can see that  $w$  satisfies the conditions for a word  $u$  such that  $\delta_{\mathcal{G}}(I, u) \neq 0$  and  $\delta_{\mathcal{H}}(J, u) = 0$ , so the algorithm enters the if statement on line 8. We can see the value of  $X$  is updated to  $\emptyset$  as  $\delta_{\mathcal{H}}(J, u) = 0$  for all vertices  $J$  in  $\mathcal{H}$ , so the algorithm returns false.  $\square$



## 4 Minimality

This section will probably hardness of sofic shift problems. As the one of the earlier sections that was written, this could be rewritten and streamlined a bit with the other sections. Other things to do: define "irreducible shift" decision problem. Give reduction from GI to irreducible shift, conclude irreducible shift is GI-hard. Give reduction from irreducible shift to minimality, conclude minimality is GI-hard.

Move this to an appropriate section.

**Theorem 4.1.** If  $\mathcal{G} = (G, \mathcal{L})$  is the minimizing right resolving presentation of an irreducible sofic shift  $X$  and  $X$  is an  $N$ -step shift of finite type, then  $X_G \cong X_{\mathcal{G}}$ .

*Proof.* Let  $x, y$  be walks in  $X_G$ . Suppose  $\mathcal{L}_{\infty}(x) = \mathcal{L}_{\infty}(y)$ . For any  $i$ , the paths  $x_{[i-N, i-1]}$  and  $y_{[i-N, i-1]}$  present the same word. Because that word is of length  $N$ , the word is synchronizing for  $\mathcal{G}$  (from 3.4.17), so those paths end at the same vertex. Since  $\mathcal{L}(x_{[i]}) = \mathcal{L}(y_{[i]})$ ,  $\mathcal{G}$  is right resolving, and  $x_{[i-N, i-1]}$  and  $y_{[i-N, i-1]}$  end at the same vertex, then  $x_{[i]} = y_{[i]}$  and hence  $x = y$ , so  $\mathcal{L}_{\infty}$  is injective. By definition,  $\mathcal{L}_{\infty}$  is surjective. Therefore,  $\mathcal{L}_{\infty}$  is bijective and a conjugacy from  $X_G$  to  $X_{\mathcal{G}}$ .  $\square$

Move this to an appropriate section.

**Lemma 4.2.** If  $X$  and  $Y$  are shift spaces, then  $\mathcal{B}(X) \subseteq \mathcal{B}(Y)$  if and only if  $X \subseteq Y$ .

*Proof.* Let  $x$  be a point in  $X$ . Then every word that appears in  $x$  is in  $\mathcal{B}(X)$ . Since  $\mathcal{B}(X) \subseteq \mathcal{B}(Y)$ , then every word that appears in  $x$  is in  $\mathcal{B}(Y)$ , so  $x \in Y$ , hence  $X \subseteq Y$ .

Conversely, let  $w$  be a word in  $\mathcal{B}(X)$ . Then  $w$  occurs in some  $x \in X$ . Since  $X \subseteq Y$ , we have  $x \in Y$ , so  $w$  occurs in some  $x \in Y$ . Hence,  $w \in \mathcal{B}(Y)$ .  $\square$

Let  $\mathcal{G}$  and  $\mathcal{H}$  be labeled graphs,  $I$  be a vertex from  $\mathcal{G}$ , and  $J$  be a vertex from  $\mathcal{H}$ . Define the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $J$  as the disjoint union of the two graphs, adding an edge starting at  $I$  and ending at  $J$ , and adding a self loop on  $J$ . Label these two new edges with a symbol that does not appear in either graph. Since  $\mathcal{G}$  and  $\mathcal{H}$  are subgraphs of a graph connecting the two, it follows that the presentations of the individual graphs are subshifts of a presentation of a graph connecting the two - any bi-infinite walk in one of the graphs is a bi-infinite walk of the corresponding subgraph of the connected graphs. Additionally, observe that the graph is reducible, as any path starting in  $\mathcal{H}$  cannot end in  $\mathcal{G}$ .

**Theorem 4.3.** Let  $\mathcal{G}$  and  $\mathcal{H}$  be irreducible graphs, and  $\mathcal{K}$  be the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $J$ . If  $X_{\mathcal{K}}$  is irreducible, then  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$ .

*Proof.* First, suppose that  $X_{\mathcal{K}}$  is irreducible, and let  $u \in \mathcal{B}(X_{\mathcal{G}})$ . There is a path in  $\mathcal{G}$  that presents  $u$ , hence there is a path in the  $\mathcal{G}$  subgraph of  $\mathcal{K}$  that presents  $u$ . From the irreducibility of  $\mathcal{G}$ , there is a path from the terminating vertex of a path presenting  $u$  to

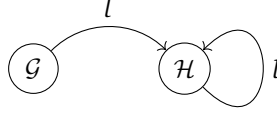


Figure 2: A graph connecting  $\mathcal{G}$  to  $\mathcal{H}$ .

$I$ . Let  $v$  be the word such path presents and  $l$  be the label of the edge connecting  $\mathcal{G}$  to  $\mathcal{H}$ , so that we have  $uvl \in \mathcal{B}(X_{\mathcal{K}})$  and  $u \in \mathcal{B}(X_{\mathcal{K}})$ . As  $X_{\mathcal{K}}$  is irreducible, there exists a word  $w \in \mathcal{B}(X_{\mathcal{K}})$  such that  $uvlwu \in \mathcal{B}(X_{\mathcal{K}})$ . A path presenting  $uvlwu$  must have the subpath presenting  $wu$  visit vertices only from the  $\mathcal{H}$  subgraph of  $\mathcal{K}$ . This implies that there is a path in  $\mathcal{H}$  presenting  $u$ , so we have  $u \in \mathcal{B}(X_{\mathcal{H}})$  and therefore  $\mathcal{B}(X_{\mathcal{G}}) \subseteq \mathcal{B}(X_{\mathcal{H}})$ , and  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  via Lemma 1.  $\square$

**Theorem 4.4.** Let  $\mathcal{G}$  and  $\mathcal{H}$  be irreducible, minimal, right-resolving presentations. If  $X_{\mathcal{G}} = X_{\mathcal{H}}$ , then there exists a pair of vertices  $(I, J) \in (\mathcal{V}_{\mathcal{G}} \times \mathcal{V}_{\mathcal{H}})$  such that both the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $J$  and the graph connecting  $\mathcal{H}$  to  $\mathcal{G}$  via  $J$  and  $I$  both present irreducible shifts.

Equivalently, if for every pair of vertices  $(I, J) \in (\mathcal{V}_{\mathcal{G}}, \mathcal{V}_{\mathcal{H}})$  the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $J$  and the graph connecting  $\mathcal{H}$  to  $\mathcal{G}$  via  $J$  and  $I$  do not both present irreducible shifts.

*Proof.* Suppose  $X_{\mathcal{G}} = X_{\mathcal{H}}$ . Since  $\mathcal{G}$  and  $\mathcal{H}$  are irreducible, minimal, right-resolving presentations of the same shift, they must be isomorphic. Let  $(\partial\Phi, \Phi)$  be a graph isomorphism between them. Choose an arbitrary vertex  $I$  from  $\mathcal{G}$ , and then let  $\mathcal{K}$  be the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $\partial\Phi(I)$ . Let  $f$  be the self loop on  $\partial\Phi(I)$  added in the construction of  $\mathcal{K}$ , and  $\mathcal{H}^+$  be the  $\mathcal{H}$  of  $\mathcal{K}$  subgraph plus  $f$ . As  $\mathcal{H}$  is irreducible, then  $\mathcal{H}^+$  is irreducible. It suffices to show that  $X_{\mathcal{K}} = X_{\mathcal{H}^+}$  to show  $X_{\mathcal{K}}$  is irreducible.

Let  $u$  be a word from  $\mathcal{B}(X_{\mathcal{K}})$ , and  $\pi$  be a path that presents it. Without loss of generality, assume  $u$  and  $\pi$  are nonempty. If  $\pi$  starts in  $\mathcal{H}^+$ , then  $u \in \mathcal{B}(X_{\mathcal{H}^+})$ . Otherwise, it starts in  $\mathcal{G}$  and either ends in  $\mathcal{G}$  or ends in  $\mathcal{H}^+$ . For the case of  $\pi$  ending in  $\mathcal{G}$ , then  $\Phi(\pi)$  is a path in  $\mathcal{H}$  presenting  $u$ , as  $(\partial\Phi, \Phi)$  is a graph isomorphism, so  $u \in \mathcal{B}(X_{\mathcal{H}^+})$ . For the case of  $\pi$  ending in  $\mathcal{H}^+$ , we can split  $\pi$  into  $\pi = \pi_1 e \pi_2$ , where  $\pi_1$  and  $\pi_2$  are (possibly empty) paths from  $\mathcal{G}$  and  $\mathcal{H}^+$ , respectively, and  $e$  is the edge connecting  $\mathcal{G}$  and  $\mathcal{H}$ . Note that  $\Phi(\pi_0)$  is a path in  $\mathcal{H}$  and that it terminates at  $\partial\Phi(I)$  as  $\pi_0$  terminates at  $I$ , assuming  $\pi_0$  is nonempty. From this, we have that  $\Phi(\pi_0) f \pi_1$  is path in  $\mathcal{H}^+$  that presents  $u$ , so  $u \in \mathcal{B}(X_{\mathcal{H}^+})$ .

Hence, we have  $\mathcal{B}(X_{\mathcal{K}}) \subseteq \mathcal{B}(X_{\mathcal{H}^+})$ , and from the construction of  $\mathcal{K}$ , we also have

$\mathcal{B}(X_{\mathcal{H}^+}) \subseteq \mathcal{B}(X_{\mathcal{K}})$ , so  $\mathcal{B}(X_{\mathcal{K}}) = \mathcal{B}(X_{\mathcal{H}^+})$  and  $X_{\mathcal{K}} = X_{\mathcal{H}^+}$ . Thus, we have shown the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $\partial\Phi(I)$  presents an irreducible shift. A similar argument can be made showing that the graph connecting  $\mathcal{H}$  to  $\mathcal{G}$  via  $\partial\Phi(I)$  and  $I$  presents an irreducible shift (start from “...and then let  $\mathcal{K}$ ”, and replace  $\mathcal{G} \mapsto \mathcal{H}, \mathcal{H} \mapsto \mathcal{G}, I \mapsto \partial\Phi(I), \partial\Phi(I) \mapsto I, \mathcal{H}^+ \mapsto \mathcal{G}^+, \Phi(\pi_0) \mapsto \Phi^{-1}(\pi_0)$ ).  $\square$

**Theorem 4.5.** Given an oracle for minimizing a reducible presentation, deciding if two irreducible, minimal, right-resolving labeled graphs are isomorphic can be determined in polynomial time.

*Proof.* Let the decision procedure be as follows: for every pair of vertices  $(I, J) \in (\mathcal{V}_{\mathcal{G}} \times \mathcal{V}_{\mathcal{H}})$  between the graphs, construct and set  $\mathcal{G}_I \rightarrow \mathcal{H}_J$  as the graph connecting  $\mathcal{G}$  to  $\mathcal{H}$  via  $I$  and  $J$ , and similarly, construct and set  $\mathcal{H}_J \rightarrow \mathcal{G}_I$  as the graph connecting  $\mathcal{H}$  to  $\mathcal{G}$  via  $J$  and  $I$ . Then, using the oracle, minimize  $\mathcal{G}_I \rightarrow \mathcal{H}_J$  and check if it is strongly connected (that is, irreducible), and if so, then from Theorem 2, we know we can set  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  to be true. Similarly, minimize  $\mathcal{H}_J \rightarrow \mathcal{G}_I$  and check if it is strongly connected, and if so, set  $X_{\mathcal{H}} \subseteq X_{\mathcal{G}}$  to be true. If at any point both  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  and  $X_{\mathcal{H}} \subseteq X_{\mathcal{G}}$  are set to true, then  $X_{\mathcal{G}} = X_{\mathcal{H}}$  and thus can conclude  $\mathcal{G} \cong \mathcal{H}$  (as  $\mathcal{G}$  and  $\mathcal{H}$  are unique, minimal, and irreducible presentations). If you find that after every pair of vertices that one or both of  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  and  $X_{\mathcal{H}} \subseteq X_{\mathcal{G}}$  were not set to true, then we have that for all pairs of vertices, the presentations of the pair of graphs constructed were not both irreducible, as if they were, then both  $X_{\mathcal{G}} \subseteq X_{\mathcal{H}}$  and  $X_{\mathcal{H}} \subseteq X_{\mathcal{G}}$  would be true, so via Theorem 3, we have that  $X_{\mathcal{G}} \neq X_{\mathcal{H}}$  and can conclude  $\mathcal{G} \not\cong \mathcal{H}$  (as again,  $\mathcal{G}$  and  $\mathcal{H}$  are irreducible, minimal, right-resolving graphs).

The worst case runtime of the decision procedure is if  $\mathcal{G} \not\cong \mathcal{H}$ , as we minimize and check strongly connected-ness twice (of a graph that is potentially the size of both  $\mathcal{G}$  and  $\mathcal{H}$ ) for each pair of vertices, so the runtime is  $O((V + E) \cdot V^2)$ , where  $V$  is the number of vertices of one graph and  $E$  is the number of edges of one graph.  $\square$

## 5 Graph isomorphisms

**Definition 5.1.** An *undirected graph* is a pair  $G = (V, E)$ , where  $V$  is a finite set of vertices and  $E \subseteq V \times V$  is a symmetric and irreflexive relation on  $V$ .

**Definition 5.2.** Given undirected graphs  $G = (V_G, E_G)$  and  $H = (V_H, E_H)$ , an isomorphism from  $G$  to  $H$  is a bijection  $\varphi : V_G \rightarrow V_H$  such that for all  $I, J \in V_G$ ,  $(I, J) \in E_G$  if and only if  $(\varphi(I), \varphi(J)) \in E_H$ . If there is an isomorphism from  $G$  to  $H$ , then we say  $G$  and  $H$  are isomorphic.

Given labeled graphs  $\mathcal{G}$  and  $\mathcal{H}$ , an isomorphism from  $\mathcal{G}$  to  $\mathcal{H}$  is a pair of bijections  $\partial\Phi : \mathcal{V}_{\mathcal{G}} \rightarrow \mathcal{V}_{\mathcal{H}}$  and  $\Phi : \mathcal{E}_{\mathcal{G}} \rightarrow \mathcal{E}_{\mathcal{H}}$  such that for all  $e \in \mathcal{E}_{\mathcal{G}}$ ,  $i_{\mathcal{H}}(\Phi(e)) = \partial\Phi(i_{\mathcal{G}}(e))$ ,  $t_{\mathcal{H}}(\Phi(e)) = \partial\Phi(t_{\mathcal{G}}(e))$ , and  $\mathcal{L}_{\mathcal{H}}(\Phi(e)) = \mathcal{L}_{\mathcal{G}}(e)$ .

**Definition 5.3.** Define the decision problem  $\text{GI}$  to be the set of all pairs of isomorphic undirected graphs:

$$\text{GI} \triangleq \{(G, H) : G \text{ and } H \text{ are isomorphic undirected graphs}\}$$

Similarly, define the decision problem  $\text{LGI}$  to be the set of all pairs of isomorphic labeled graphs:

$$\text{LGI} \triangleq \{(\mathcal{G}, \mathcal{H}) : \mathcal{G} \text{ and } \mathcal{H} \text{ are isomorphic labeled graphs}\}$$

**Definition 5.4.** Let  $A$  be some decision problem. We say  $A$  is *GI-hard* if  $\text{GI}$  is polynomial-time Turing reducible to  $A$ . We say  $A$  is *GI-complete* if  $A$  is  $\text{GI-hard}$  and  $A$  is polynomial-time Turing reducible to  $\text{GI}$ .

**Theorem 5.5.**  $\text{LGI}$  is  $\text{GI-hard}$ .

*Proof.* First, we will show that  $\text{LGI}$  is  $\text{GI-hard}$ . Let  $G$  and  $H$  be undirected graphs. Construct the labeled graph  $\mathcal{G}$  with  $\mathcal{V}_{\mathcal{G}} \triangleq V_G$ ,  $\mathcal{E}_{\mathcal{G}} \triangleq E_G$  and for all  $I, J \in \mathcal{E}_{\mathcal{G}}$ ,  $i_{\mathcal{G}}(I, J) \triangleq I$ ,  $t_{\mathcal{G}}(I, J) \triangleq J$ , and  $\mathcal{L}_{\mathcal{G}}(I, J) \triangleq \ell$ . Construct the labeled graph  $\mathcal{H}$  in a similar fashion. Obviously, this construction can be done in polynomial-time with respect to the size of  $G$  and  $H$ .

Suppose  $\varphi$  is an isomorphism from  $G$  to  $H$ . Define the map  $\partial\Phi : \mathcal{V}_{\mathcal{G}} \rightarrow \mathcal{V}_{\mathcal{H}}$  with  $\partial\Phi(I) \triangleq \varphi(I)$  for  $I \in \mathcal{V}_{\mathcal{G}}$  and  $\Phi : \mathcal{E}_{\mathcal{G}} \rightarrow \mathcal{E}_{\mathcal{H}}$  with  $\Phi(I, J) \triangleq (\varphi(I), \varphi(J))$  for  $I, J \in \mathcal{E}_{\mathcal{G}}$ . Let  $(I, J) \in \mathcal{E}_{\mathcal{G}}$ . Then,

$$\begin{aligned} \partial\Phi(i_{\mathcal{G}}(I, J)) &= \partial\Phi(I) \\ &= \varphi(I) \\ &= i_{\mathcal{H}}(\varphi(I), \varphi(J)) \quad (\star) \\ &= i_{\mathcal{H}}(\Phi(I, J)), \end{aligned}$$

and  $(\star)$  is well-defined as  $(I, J) \in \mathcal{E}_{\mathcal{G}} = E_G$  if and only if  $(\varphi(I), \varphi(J)) \in E_H = \mathcal{E}_{\mathcal{H}}$ . A similar deduction can be used to show  $\partial\Phi(t_{\mathcal{G}}(I, J)) = t_{\mathcal{H}}(\Phi(I, J))$ . As  $\varphi$  is a bijection from  $V_G$  to  $V_H$ , then  $\partial\Phi$  is a bijection from  $\mathcal{V}_{\mathcal{G}}$  to  $\mathcal{V}_{\mathcal{H}}$ . One can check that for  $\Phi^{-1}(I, J) \triangleq (\varphi^{-1}(I), \varphi^{-1}(J))$ ,  $\Phi^{-1} \circ \Phi = id_{\mathcal{E}_{\mathcal{G}}}$  and  $\Phi \circ \Phi^{-1} = id_{\mathcal{E}_{\mathcal{H}}}$  so  $\Phi$  is a bijection from  $\mathcal{G}$  to  $\mathcal{H}$ . Hence,  $(\partial\Phi, \Phi)$  is an isomorphism from  $\mathcal{G}$  to  $\mathcal{H}$ .

Conversely, suppose  $(\partial\Phi, \Phi)$  is an isomorphism from  $\mathcal{G}$  to  $\mathcal{H}$ . Define  $\varphi : V_G \rightarrow V_H$  with  $\varphi(I) \triangleq \partial\Phi(I)$  for  $I \in V_G$ . Note that for  $(I, J) \in \mathcal{E}_{\mathcal{H}}$ ,  $(I, J) = (i_{\mathcal{H}}(I, J), t_{\mathcal{H}}(I, J))$ . If  $(I, J) \in E_G$ , then

$$\begin{aligned} i_{\mathcal{H}}(\Phi(I, J)) &= \partial\Phi(i_{\mathcal{G}}(I, J)) \\ &= \partial\Phi(I) \\ t_{\mathcal{H}}(\Phi(I, J)) &= \partial\Phi(t_{\mathcal{G}}(I, J)) \\ &= \partial\Phi(J), \end{aligned}$$

so  $\Phi(I, J) = (i_{\mathcal{H}}(\Phi(I, J)), t_{\mathcal{H}}(\Phi(I, J))) = (\partial\Phi(I), \partial\Phi(J)) = (\varphi(I), \varphi(J))$ . Therefore, as  $\Phi(I, J) \in \mathcal{E}_{\mathcal{H}} = E_H$ , then  $(\varphi(I), \varphi(J)) \in E_H$ . Similarly, note that for  $I, J \in E_{\mathcal{G}}$ ,  $(I, J) = (i_{\mathcal{G}}(I, J), t_{\mathcal{G}}(I, J))$ . If  $(\varphi(I), \varphi(J)) \in E_H$ , then

$$\begin{aligned} i_{\mathcal{H}}(\Phi(I, J)) &= \partial\Phi(i_{\mathcal{G}}(I, J)) \\ &= \partial\Phi(I) \\ t_{\mathcal{H}}(\Phi(I, J)) &= \partial\Phi(t_{\mathcal{G}}(I, J)) \\ &= \partial\Phi(J), \end{aligned}$$

□