Introduction

1.1 Graph Isomorphism

Definition 1.1: An undirected, simple graph G is a set of labelled vertices $V(G)$, and a set of edges, $E(G)$, where $E(G)$ is a set of unordered pairs of vertices from $V(G)$ such that for all $u \in V(G)$, $\{u, u\} \notin E(G)$.

Remark: For this paper, every graph, unless otherwise specified, has vertex set $[n] = \{1, 2, \ldots, n\}$.

Definition 1.2: For a graph $G = \{V, E\}$, if $\{u, v\} \in E$, we say u and v are *adjacent*.

Definition 1.3: Two graphs, G and G', are isomorphic, denoted $G \cong G'$, if there exists a bijection $f : V(G) \to V(G')$ such that for every $u, v \in V(G)$, $\{u, v\} \in E(G)$ if and only if $\{f(u), f(v)\} \in E(G')$.

Remark: Functions are written in a matrix, with the pre-image in the top row and the image in the bottom row. For example, the identity is written

$$\begin{pmatrix} x \\ x \end{pmatrix}.$$

Composition of functions adds a row for each function. For example, the identity composed with its inverse function is

$$\begin{pmatrix} x \\ 1/x \\ 1 \end{pmatrix}.$$

2.1 A graph as a string

Following Luks [1982], a graph can be represented as a binary string using the indicator function for adjacency relations in the graph. Let $\Omega = [1, \ldots, n]$. Let $G = \{\Omega, E\}$ be an undirected, simple graph. Let $\binom{\Omega}{2}$ denote the set of all unordered pairs in Ω (Babai 2018). Let $\delta_G : \binom{\Omega}{2} \to \{0, 1\}$ be the indicator function for the adjacency relations in G, defined by

$$\delta_G(\{x, y\}) = \begin{cases} 1, & \{x, y\} \in E(G) \\ 0, & \text{o/w} \end{cases}.$$

Then δ_G is the binary string representation of G.

Definition 2.4: $\mathrm{Sym}(\Omega)$ (denoted S_Ω) is the group of all bijections $f : \Omega \to \Omega$.

From Definition 1.3, we know that two graphs G and G' are isomorphic if there exists a bijection $f : V(G) \to V(G')$ such that for all $u, v \in V(G)$, $\{u, v\} \in E(G)$ if and only if $\{f(u), f(v)\} \in E(G')$. Since all of the graphs we are discussing are labelled using $[n]$, every isomorphism between two graphs is a function from S_n. In order to define the string isomorphism problem, the following definition is important.

Definition 2.5:
$S_n^{(2)} = \left\{\sigma \in \mathrm{Sym}\ \left(\binom{\Omega}{2}\right) : \exists f \in S_n \text{ s.t. } \forall \omega = \{u, v\} \in \binom{\Omega}{2},\ \sigma(\omega) = \{f(u), f(v)\}\right\}.$

Notice that $S_n^{(2)} \subseteq \mathrm{Sym}(\binom{\Omega}{2})$. There is an added restriction on the bijections in $S_n^{(2)}$ compared to those in $\mathrm{Sym}(\binom{\Omega}{2})$. Every permutation of unordered pairs (i.e. permutation of edges) in $S_n^{(2)}$ can be obtained using a permutation in S_n (i.e. a permutation of the vertices). When $0 < n \leq 3$, $S_n^{(2)} = \mathrm{Sym}(\binom{\Omega}{2})$. When $n > 3$, the two groups are no longer equal. Consider the following example.

Example 2.1: Let

$$\sigma = \begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{1,3\} & \{1,2\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \end{pmatrix}.$$

Notice that $\sigma \in \mathrm{Sym}(\binom{4}{2})$. To see that $\sigma \notin S_4^{(2)}$, we must show that there is no function $f \in S_4$ such that for all $u, v \in [4]$, $\sigma(\{u,v\}) = \{f(u), f(v)\}$. Although there are 24 elements in S_4, there is only one element in S_4 (see f_1 below) that results in mapping $\{1,2\} \to \{1,3\}$ and $\{1,3\} \to \{1,2\}$. We have

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Notice that $\sigma(\{3,4\}) = \{3,4\} \neq \{2,4\} = \{f_1(3), f_1(4)\}$. Since this is the only possible bijection for σ to satisfy the conditions of $S_4^{(2)}$, we know $\sigma \notin S_4^{(2)}$. To make this point more clear, consider the graphs on four vertices below.

(a) G (b) $f_1(V(G))$

Figure 2.1: G and the result of applying f_1 to V(G).

Notice that $\{2,4\} \in E(f_1(V(G))$ but $\{2,4\} \notin E(G)$

Definition 2.6: Let δ_1 and δ_2 be string representations of undirected, simple graphs G_1 and G_2, respectively. Then δ_1 and δ_2 are $S_n^{(2)}$*-isomorphic*, denoted $\delta_1 \cong \delta_2$, if there exists $\sigma \in S_n^{(2)}$ such that $\delta_1 \circ \sigma = \delta_2$.

Given binary strings δ_1 and δ_2, both with length n, the *string isomorphism problem* asks: Does there exist $\sigma \in S_n^{(2)}$ such that $\delta_1 \circ \sigma = \delta_2$? The following example answers this question

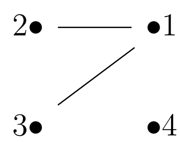

Figure 2.3: G_3, with vertex set $f_2(V(G_1))$.

for a binary string with length 6.

(a) G_1 (b) G_2

Figure 2.2: Two isomorphic graphs on 4 vertices.

Example 2.2: Consider graphs G_1 and G_2 in Figure 2.2. In this case, we consider $\Omega = [1, 2, 3, 4]$. A bijection that produces an isomorphism between G_1 and G_2 is f_2,

$$f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

If we apply f_2 to $V(G_1)$, the resulting graph is G_3 (Figure 2.3). We now construct the binary string representation of each graph. We have

$$\delta_{G_1} = \begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and

$$\delta_{G_2} = \begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We also have

$$\mathrm{Sym}\ (\Omega) = S_4.$$

To show that $\delta_{G_1} \cong \delta_{G_2}$, we must find $\sigma \in S_4^{(2)}$ such that $\delta_{G_1} \circ \sigma = \delta_{G_2}$. We simply record the effect on $E(G_1)$ of applying f_2 to $V(G_1)$. We have

$$\sigma = \begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{1,2\} & \{2,4\} & \{2,3\} & \{1,4\} & \{1,3\} & \{3,4\} \end{pmatrix}.$$

Then

$$\delta_{G_1} \circ \sigma = \begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{1,2\} & \{2,4\} & \{2,3\} & \{1,4\} & \{1,3\} & \{3,4\} \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \delta_{G_2},$$

as desired. Hence, $\delta_{G_1} \cong \delta_{G_2}$.

Lemma 2.1: $S_n^{(2)}$ is a subgroup of $\mathrm{Sym}(\binom{[n]}{2})$.

Proof. Let $\sigma, \eta \in S_n^{(2)}$. Since $S_n^{(2)} \subseteq \mathrm{Sym}\left(\binom{[n]}{2}\right)$, $\sigma, \eta \in \mathrm{Sym}\left(\binom{[n]}{2}\right)$. Moreover, $\mathrm{Sym}\left(\binom{[n]}{2}\right)$ is a group. Hence, $\sigma \circ \eta \in \mathrm{Sym}\left(\binom{[n]}{2}\right)$. Now, by definition there exists $f_\sigma,\ f_\eta \in S_n$ such that for all $\omega = \{u, v\} \in \mathrm{Sym}(\binom{[n]}{2})$, $\sigma(\{u,v\}) = \{f_\sigma(u), f_\sigma(v)\}$ and $\eta(\{u,v\}) = \{f_\eta(u), f_\eta(v)\}$. Since $f_\sigma, f_\eta \in S_n$, $f_\sigma \circ f_\eta \in S_n$. Let $\omega = \{u, v\} \in \mathrm{Sym}(\binom{[n]}{2})$. Consider $\sigma \circ \eta(\{u,v\})$. We have

$$\sigma \circ \eta(\{u,v\}) = \sigma(\{f_\eta(u), f_\eta(v)\}) = \{f_\sigma \circ f_\eta(u), f_\sigma \circ f_\eta(v)\}.$$

Hence, $\sigma \circ \eta \in S_n^{(2)}$. Lastly, consider $f_\sigma^{-1} \in S_n$. Let $\sigma^{-1}(\{u,v\}) = \{f_\sigma^{-1}(u), f_\sigma^{-1}(v)\}$. Hence, $\sigma^{-1} \in S_n^{(2)}$. Observe,

$$\sigma \circ \sigma^{-1}(\{u,v\}) = \sigma(\{f_\sigma^{-1}(u), f_\sigma^{-1}(v)\}) = \{f_\sigma \circ f_\sigma^{-1}(u), f_\sigma \circ f_\sigma^{-1}(v)\} = \{u, v\}.$$

By a similar argument, $\sigma^{-1}\sigma(\{u,v\}) = \{u,v\}$. Hence, $S_n^{(2)}$ is a subgroup of $\mathrm{Sym}(\binom{[n]}{2})$. $\square$

Lemma 2.2: Two graphs are isomorphic if and only if their string representations are $S_n^{(2)}$-isomorphic.

Proof. Let B_1 and B_2 be binary string representations of undirected graphs G_1 and G_2, respectively.

$\rightarrow$

Suppose $G_1 \cong G_2$. By Definition **??**, there exists bijection $g : V(G_1) \rightarrow V(G_2)$ such that for all $u, v \in V(G_1)$, $\{u, v\} \in E(G_1)$ if and only if $\{g(u), g(v)\} \in E(G_2)$. Notice that $g \in S_n$. Let $\sigma : \binom{[n]}{2} \rightarrow \binom{[n]}{2}$ where $\sigma(\{u, v\}) = \{g(u), g(v)\}$. Then $\sigma \in S_n^{(2)}$. Let $u, v \in [n]$. Consider $B_2 \circ \sigma(\{u, v\})$. We have

$$B_2 \circ \sigma(\{u, v\}) = B_2(\{g(u), g(v)\}) = B_1(\{u, v\}).$$

The last equality follows because $\{u, v\} \in E(G_1)$ if and only if $\{g(u), g(v)\} \in E(G_2)$. This means $B_1(\{u, v\} = 1$ if and only if $B_2(\{g(u), g(v)\}) = 1$. Hence, $B_2 \cong B_1$.

$\leftarrow$

Suppose $B_1 \cong B_2$. By Definition 2.6, there exists $\sigma \in S_n^{(2)}$ such that $B_1 \circ \sigma = B_2$. Let $\omega = \{u, v\} \in \binom{[n]}{2}$. There exists $f_\sigma \in S_n$ such that $\sigma(\omega) = \{f_\sigma(u), f_\sigma(v)\}$. We have

$$B_2(\{u, v\}) = B_1 \circ \sigma(\{u, v\}) = B_1(\{f_\sigma(u), f_\sigma(v)\}).$$

This means that $B_2(\{u, v\}) = 1$ if and only if $B_1(\{f_\sigma(u), f_\sigma(v)\}) = 1$. In other words, $\{u, v\} \in E(G_2)$ if and only if $\{f_\sigma(u), f_\sigma(v)\} \in E(G_1)$. Hence, $G_1 \cong G_2$. $\square$