Mathematics for Computer Science (30470023) Spring 2020

Lecture 11 — May 9, 2020

Instructor: Prof. Andrew C. Yao *Scribes: Boyang Chen, Jiatu Li*

1 Overview

Recall that we have learned some basic concepts about graph theory and algorithms, including Eulerian cycle problem and an algorithm for it. Also we have partially shown why a similar problem, the Hamiltonian cycle problem, is "harder" than the Eulerian cycle problem. The techniques we used are important for computer science, since they make it possible to lay a solid foundation for new areas such as cryptography, and the influence has spread to other scientific areas.

In this lecture, we will move on to study the hardness of the Hamiltonian problem. We will firstly complete our reduction of Eulerian to Hamiltonian, and then introduce several other problems on graphs that are equivalently hard with the Hamiltonian.

2 The hardness of Hamiltonian problem

Suppose $G = (V, E)$, we want to find a graph $G' = (V', E')$ such that G has a Eulerian cycle if and only if G' has a Hamiltonian cycle. If this is possible, we can solve the Eulerian cycle problem with a Hamiltonian cycle solver, which means that Eulerian cycle problem is "easier". Note that a Eulerian cycle is a path

$$v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} \dots \xrightarrow{e_{l-1}} v_l,$$

such that $v_1 = v_l$, and $\{e_1, e_2, \dots, e_{l-1}\} = E$.

It's natural to see that, we can create a graph $G' = (V', E')$ such that the *vertices* of it represent the *edges* of G. More preciously, let $V' = E$, $\{e_i, e_j\} \in E'$ if and only if e_i and e_j shares a common endpoint in G.

Theorem 2.1. If G contains a Eulerian cycle, G' contains a Hamiltonian cycle. ♢

Proof. Suppose G has a Eulerian cycle, there is a path

$$v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} \dots \xrightarrow{e_{l-1}} v_l = v_1,$$

such that each edge appears exactly once in it. We can also consider this path as a path on G' as

$$e_1 \to e_2 \to \dots \to e_{l-1} \to e_1,$$

where each *vertex* in G' occurs exactly once besides e_1. As a result, there must be a Hamiltonian cycle in G'. □

But the converse of the theorem is not true, which means that this reduction is actually not valid. Consider the graph in Fig **??**. There exists a Hamiltonian cycle in G' since it is simply a triangle, but the sequence does not correspond to a Eulerian cycle in G. The problem of our construction is that, we lost some sense of direction of movement on the edges in the original graph during this transformation.

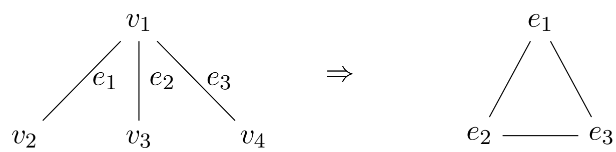


Figure 1: A counterexample for the simple transformation.

In order to solve the problem, we can put three vertices $e'_i, e_i, e''_i \in V''$ on an edge $e_i \in G$,

$$v_i \xrightarrow{e'_i \quad e_i \quad e''_i} v_j,$$

to form a graph $G'' = (V'', E'')$. It's clear that $|V''| = 3\,|E|$. Two vertices in V'' are connected, if they are "adjacent", i.e. one of the situations hold

1. they are two adjacent vertices on the same edge in G;
2. they lay on two edges that shares a common endpoint in G, and each of them is the *closest* vertex to the endpoint on its own edge.

Figure **??** shows the new graph G'' for the counterexample of our original attempt.

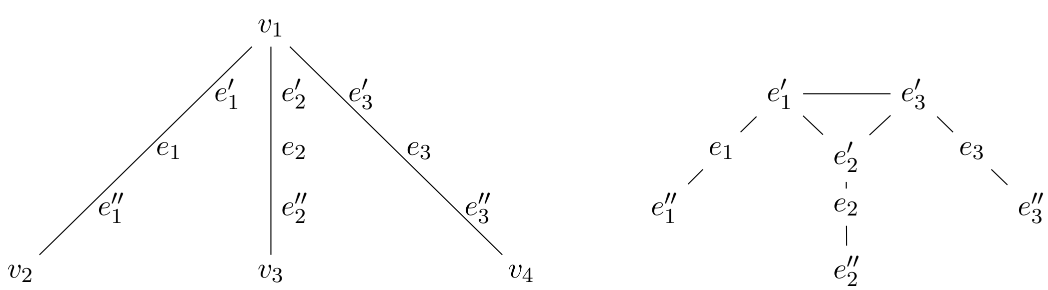


Figure 2: New transformation.

Clearly a Eulerian cycle in G corresponds to a Hamiltonian cycle in G''. Conversely, suppose there is a Hamiltonian cycle in G', in order to go through the "middle vertex" put on each edge, three vertices put on the same edge should be adjacent on the cycle, which means that we can ensure the correctness of the direction.

Theorem 2.2. G has a Eulerian cycle if and only if G'' has a Hamiltonian cycle. $\diamondsuit$

Proof. By the previous theorem it's easy to see that G has a Eulerian cycle implies that G'' has a Hamiltonian. Conversely, suppose G'' has a Hamiltonian cycle, it must go through all the vertices on G'' and in particular, it must go through e_i for all i. Since e_i has only two neighbors, either we travel by the path $e_i' \to e_i \to e_i''$ or by the path $e_i'' \to e_i \to e_i'$. Let the former situation be $L(e_i)$ and the latter one be $R(e_i)$, by the definition of the graph G'', there must be a cycle

$$L/R(e_{p_1}) \to L/R(e_{p_2}) \to \cdots \to L/R(e_{p_m}) \to L/R(e_{p_1})$$

for some permutation $p \in S_m$, where $m = |E|$. Since the direction is determined by L or R, such cycle must correspond to a sequence of edges in G, where (1) each edge occurs exactly once; (2) the adjacent edges in the sequence shares the same endpoint; (3) we can go through the edges in the sequence with correct direction. Thus it forms a Eulerian cycle in G. $\square$

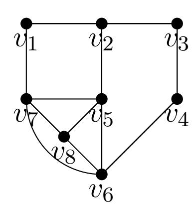
By the construction above, we have already shown that the Eulerian is reducible to the Hamiltonian. We will be *extremely* happy if we can show that there is no way to reduce Hamiltonian to Eulerian. Unfortunately, we don't know how to prove this statement.

But mathematicians do believe that the reduction is impossible. If it were possible to transform G to G', such that G is Hamiltonian if and only if G' is Eulerian, it will be easy for us to find the criteria for Hamiltonian problem. Since the mathematicians and computer scientists fail to find a simple combinatorial criteria for Hamiltonian for hundreds of years, either the reduction is impossible or it is extremely complex.

The computer scientists also develop a framework in which we can formally define the reduction. In the next section, we will introduce more problems that are *equivalently hard* with the Hamiltonian cycle problem. Moreover, we know that they are inside the complexity class NP-complete, which means that if there is an "efficient" algorithm for it, thousands of problems can be efficiently solved, and we can show that P = NP.

3 Some computationally hard problems

Definition 3.1 (Clique). Let $G = (V, E)$, a clique in G is a subset $V' \subseteq V$ s.t. $\forall u, v \in V', \{u, v\} \in E$. Given a graph G, let $\omega(G)$ be the maximum size of any clique in G. $\diamondsuit$



As for the graph above, we can find a clique of order 4: $\{5, 6, 7, 8\}$ and this is the maximum clique. In fact, consider the independent sets: $\{1, 3, 5\}$, $\{2, 4, 7\}$,$\{6\}$,$\{8\}$, if V' is a clique of the graph G, then it would intersect every set at most once, so the clique sizepp cannot exceed 4.

Then the problem we concern is given a graph G, and integer k, decide whether there exists a clique of order k. That is, let $\omega(G)$ be the maximum size of any clique in G, decide if $\omega(G) \geq k$ or not.

Definition 3.2 (Independent Set). Independent set W in $G = (V, E)$ is $\forall u, w \in W$,$(u, w) \notin E$, and given a graph G, let $d(G)$ be the maximum size of any independent set in G. $\diamondsuit$

As for the graph above, we can find an independent set of order 3: $\{1, 3, 5\}$, and we can divide the graph into three cliques: $\{1, 2\}$, $\{3, 4\}$, $\{5, 6, 7, 8\}$ so the $\{1, 3, 5\}$ is the maximum independent set.

Definition 3.3 (Coloring). A coloring is map $f : V \to \{1, 2, \dots, k\}$ which satisfies the condition $\forall (u, v) \in E, f(u) \neq f(v)$. The chromatic number is the minimum k needed to color G. $\diamondsuit$

The chromatic number is the minimum k needed to color G. It is clear that the chromatic number cannot be smaller than the size of maximum clique, however it is not always the critical discrimination.

How do we convince ourselves there exists no reduction from Hamiltonian to Eulerian?

- It turns out that Hamiltonian can be reduced to the maximum clique, maximum independent set and the chromatic problem.
- The reverse is also true.

So the problems are equivalent in this sense, there are thousands of mysteries that are equivalent to Hamiltonian problem, but none of them have been solved.

It turns out that we can reduce these thousands of problems to each other and how do we characterize the class of problems?

They can be characterized:

- They are all in NP (problems whose solution is easy to verify), so the extremely lucky person can always solve the problem
- These are the hardest problem in NP, any problem in NP can be reduced the problem.

So with a high probability, we cannot find an easy solution for these problems, which means that we do not believe Hamiltonian graphs can be reduced to Eulerian.

We do not have a very efficient way to find the clique number of the graph G.