Solving Graph Isomorphism with Recursive Minimum Bit Strings

Josh Krcadinac 7624406  
Rafael Lastiri  
March 2015

Table of Contents

[Graph Isomorphism 3](#_Toc416214398)

[Applications 3](#_Toc416214399)

[Bibliography 5](#_Toc416214400)

# Graph Isomorphism

The definition of two graphs being isomorphic is being able to find a 1:1 mapping of the vertices in the first graph to the second graph such that adjacency is preserved [1]. In other words, can we take two graphs and move the vertices around so that it’s ordering of edges and vertices make it look like the other graph. In order to do this we require the two graphs that we check for isomorphism to have some similar properties and similar structure. If two graphs do not have the same properties then right away we can conclude that they are not isomorphic. After we determine if two graphs are candidates for being isomorphic there are a number of ways that we can check to see if they are indeed isomorphism’s of each other.

A few of the requirements that must first be met when checking for isomorphism are the number or vertices, the number of edges, vertex degrees, and structure between graphs. It is straight forward why we need the same number of nodes and edges in two graphs, without this consistency isomorphism is impossible. This leads to the next step of counting the nodes of similar degree. We must have the same number of vertices with similar degrees because this is the only way that we can create the 1:1 mapping correctly. After have determined that two graphs have these requirements then we can move on to checking the structure of the graphs and see if one can be mapped to the other.

# Applications

While researching I found that graph isomorphism has some interesting applications to real world problems. This topic has applications chemistry, civil engineering, cryptography and social network pattern analysis. These are a few that I looked into although there are many, many other applications as well.

In chemistry isomorphism can be used to check and see if molecular compounds are similar or not in structure [2]. This is helpful for identifying substances that are unknown to us using subgraph isomorphism. We can detect parts of the structures that we have previous knowledge of and figure out what compounds we are dealing with this way. In civil engineering we can use isomorphism to find geographic locations that have desired qualities. We would want to do this to find a prime location for where we want to construct buildings that have constraints on where they can or can’t be built. Isomorphism can also be applied to cryptography in an interesting way. The idea is to use an isomorphic S-Box instead of using the classical S-Box for AES encryption [3]. We are able to do replacement of the S-Box and still be able to keep the cryptographic properties of AES encryption as well as increase its complexity. Social networks are popular and it is possible to apply isomorphism to pattern analysis of these networks. It is possible to look for patterns in the network [4] that represent known bad behaviour to root out any suspicious activities taking place.

# Bibliography

[1] The Graph Isomorphism Problem, Scott Fortin, 1996

[2] An Efficient Algorithm for Similarity Analysis of Molecules, Johnnie Baker, Chun-che Tsai, Rohit Pasari, Paul Durand, 1999

[3] A New S-Box Structure Based on Graph Isomorphism, Bao Tran, Thuc Nguyen, Thu Tran, 2009

[4] Social Network Analysis: Methods and Applications, Stanley Wasserman, Katherine Faust, 1999