How to Cite:
Deepika, K., & Meenakshi, S. (2022). An application of distance degree sequence of graphs in message encryption and decryption. *International Journal of Health Sciences*, *6*(S4), 7046–7052. https://doi.org/10.53730/ijhs.v6nS4.10373

An application of distance degree sequence of graphs in message encryption and decryption

Deepika K
Department of Mathematics, Research Scholar, Vels Institute of Science Technology and Advanced Studies

S Meenakshi
Department of Mathematics, Associate Professor, Vels Institute of Science Technology and Advanced Studies
Corresponding author email: meenakshikarthikeyan@yahoo.co.in

***Abstract*---**Encryption of a message has always been a concern as far as the communication area is concerned. There are various methods that have been proposed to encrypt or decrypt a message some of which are practically applied. In particular, many properties of graphs are applied for encryption of message. In this paper, I have proposed message encryption and decryption based on the concept of distance degree sequence of graphs. Also, I have proposed a program based on Python version for the same.

***Keywords*---**graph, encryption, decryption, distance degree sequence graphs.

Introduction

The major concern in encryption is the safe transmission of messages. The first form of encrypting a message was by replacing symbols. This method was not a standard one as the symbols need a key to understand. This key can also be called the cipher. Later, Arb mathematician Al- Kindi studied the method of frequency analysis, in the attempt to crack Caesae ciphers. This method observes the frequency of letters in the encrypted message and determines the possible shift. This method was later proved to be ineffective. To provide a safer way of military or army communication, Thomas Jefferson studied a key to encrypt and decrypt messages. The key or the cipher is known as the Wheel Cipher or the Jefferson Disk. This key was not built, although was only in theory that could jumble an English message upto 36 characters. The jumbled message must be plugged into a receiver with an identical cipher from which the message can be decrypted. This technique also proved to be ineffective after the finding of Enigma machine by the Axis powers during the II world war.

In modern days. Encryption plays a vital role in the transfer of communication for security and trade which is done through internet. Graph theory, in particular, is now used for transferring of messages[4]. For example, planar graphs are used in data encryption. Rigid, very excellent graphs are used to encrypt binary string[5]. Also, Degree Sequence of graphs is used in transferring message[6], [7]. As a continuation, I have proposed a method or process of encrypting a message based on distance degree sequence of graphs.

Analyzing and studying of sequences plays a very major role in the field of graph theory. This study of sequences is comparatively easier and more comfortable than a single invariant as sequence offers more information about graphs and their properties. Degree sequence of a graph was the first sequence to be studied and developed. Given a graph, to find its degree sequence is very easy. It only requires to find the number of vertices adjacent to every vertex of the graph and framing it as a sequence. But, given a degree sequence, to find if there exists a graph accepting the given sequence is not easy. The Erdos Gallai theorem gives an approach to solve the graph realization problem i.e. it gives a necessary and sufficient condition for a finite sequence of numbers to be a degree sequence of a graph[1]. A sequence obeying these conditions is called a "graphic sequence". Later, V Havel studied the existence of finite graphs based on the Degree sequence of graphs[2]. S L Hakimi studied on the realizability of degree sequences for a graph[3]. Realization theorems were given for various graphs to realize a given degree sequence. Further, the study of sequences were extended to distance based sequences namely the distance degree sequence, path degree sequence, eccentric sequence etc. Eccentric sequences were the first distance based sequences to be studied. Later, Distance Degree Sequences were studied to differentiate chemical isomers based on its molecular structure. The molecular structure is defined based on the distance degree sequence[9]. Further, Embedding trees in lattice graphs and other spaces were studied by Kennedy and Quintas[8]. Also, embedding of distance degree regular graphs and distance degree injective graphs were also studied later by Medha Itagi Huilgol, M. Rajeshwari and S. Syed Asif Ulla[10].

Here, I have proposed an encryption and decryption process based on the distance degree sequence where I have used the concept of cartesian product of graphs and finding the distance degree sequence of the vertices of the graphs. The encryption is done from the distance degree sequence obtained.

Preliminaries

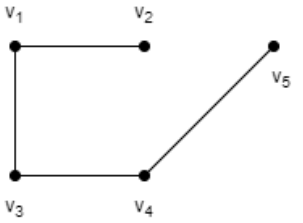
Some prerequisites are given below for better understanding of the article.

Definition 2.1

A graph G is a set of points called nodes or vertices that are linked by a set of lines called edges. Usually, a graph is denoted as G=(V, E) where V is the set of vertices and E is the set of edges.

Definition 2.2

An enumeration of the number of nodes or vertices at a distance 1, 2, 3, …e(v) is defined as the Distance Degree Sequence of a vertex v in a graph G . Here, e(v) is the eccentricity of v in G. The distance degree sequence of vertex v in G is considered as a sequence $\{d_{i0}, d_{i1}, d_{i2}, \ldots d_{ij}, \ldots\}$ where dij is the number of nodes at distance j from v.



Fig(i) Graph G

The Distance Degree Sequence DDS(G) of graph G is
((1, 2, 1, 1), (1, 1, 1, 1, 1), (1, 2, 2), (1, 2, 1, 1), (1, 1, 1, 1, 1)).

Definition 2.3

The process of encoding a message or an information is known as Encryption. This is usually done in Cryptography where the original information known as the plain text is converted into an alternative form known as the cipher text.

Definition 2.4

The reverse process of Encryption is known as Decryption. It is the process of converting an encrypted information into its original plain text.

Objective of this paper

The objective or scheme of this paper is to encrypt a message based on the distance degree sequence of graphs. There are various random graphs in graph theory. Such random pairs of graphs are chosen to which Cartesian products are obtained and distance degree sequence is applied to transfer a message to its encrypted form.

Proposed Method

- The first step is to decide the number of characters used in transferring any message.
- Then we choose one or more pairs of random graphs such that the Cartesian Product of graphs is found.
- The obtained Cartesian Product graphs must have vertices whose number equals the number of characters used in the chosen language. In this paper, I am choosing English as the language for message encryption. So, the number of characters are 27 including blank space.

- Each vertex in the Cartesian product graphs is assigned a character from letter A to Z including blank space.
- Then Distance degree sequence of every vertex is found. The message to be encrypted is considered and for every letter its corresponding vertex distance degree sequence is written and thus the message is encrypted.
- Assigning the characters to every vertex of the graph in a particular order is important here. The ordering may be either in horizontal way or vertical way. This can be mentioned in the key such that the person who deciphers the information may alone be able to find it.
- Also, for some vertices, the distance degree sequence may be repeated, that is, two or more vertices may have same distance degree sequence. This can also be mentioned in the key.
- It is always not necessary that all characters should be in a single Cartesian Product graph. There may be two or more Cartesian product graphs such that each graph has a set of vertices assigned to a set of characters. The character that appears in a particular graph can also be hinted in the key.
- We now encrypt a message based on the above proposed concept.
- I have taken 6 random graphs namely, G, H, G', H', G'', H'' for which the Cartesian products are found for the pairs of graphs namely G, H ; G', H' and G'', H'' and are denoted as G_1, G_2 and G_3 respectively.

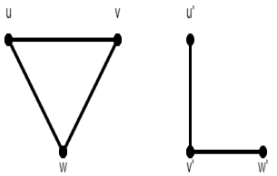


Fig (ii) Graphs G and H

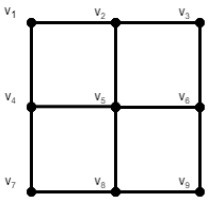
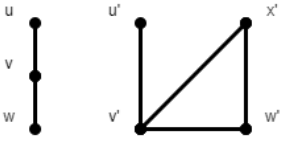
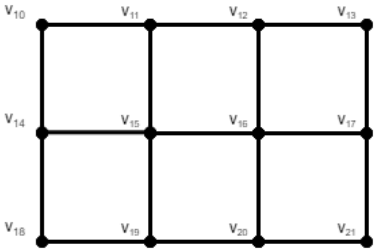


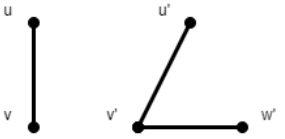
Fig (iii) Graph G_1



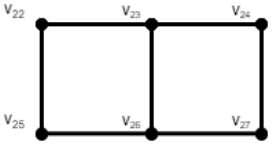
Fig(iv) Graphs $G', and\ H'$



Fig(v) Graph G_2



Fig(vi) Graphs $G'' \text{ and } H''$



Fig(vii) Graph G_3

The cartesian product graphs G_1, G_2 and G_3 have 27 vertices together and every vertex is assigned a character from A to Z including the blank space. The distance degree sequence of every vertex is found out and listed. The encryption is done based on the distance degre sequence of the vertices. The following array gives the distance degree sequence of vertices or characters of the three cartesian product graph. Along with the distance degree sequence, the array also shows the repetitions of a particular distance degree sequence and the graph for the corresponding character.

['A'] 2, 3, 2, 1, 0, 1, 1,]
['B'], 3, 3, 2, 0, 0, 1, 1],
['C', 2, 3, 2, 1, 0, 1, 2],
['D', 3, 3, 2, 0, 0, 1, 2],
['E', 4, 4, 0, 0, 0, 1, 1],
['F', 3, 3, 2, 0, 0, 1, 3],
['G', 2, 3, 2, 1, 0, 1, 3],
['H', 3, 3, 2, 0, 0, 1, 4],
['I', 2, 3, 2, 1, 0, 1, 4],
['J', 2, 3, 3, 2, 1, 2, 1],
['K', 3, 4, 3, 1, 0, 2, 1],
['L', 3, 4, 3, 1, 0, 2, 2],
['M', 2, 3, 3, 2, 1, 2, 2],
['N', 3, 3, 3, 2, 0, 2, 1],
['O', 4, 5, 2, 0, 0, 2, 1],

['P', 4, 5, 2, 0, 0, 2, 2],
['Q', 3, 3, 3, 2, 0, 2, 2],
['R', 2, 3, 3, 2, 1, 2, 3],
['S', 3, 4, 3, 1, 0, 2, 3],
['T', 3, 4, 3, 1, 0, 2, 4],
['U', 2, 3, 3, 2, 1, 2, 4],
['V', 2, 2, 1, 0, 0, 3, 1],
['W', 3, 2, 0, 0, 0, 3, 1],
['X', 2, 2, 1, 0, 0, 3, 2],
['Y', 2, 2, 1, 0, 0, 3, 3],
['Z', 3, 2, 0, 0, 0, 3, 2],
[' ', 2, 2, 1, 0, 0, 3, 4]]

Now we encrypt any message based on the above table.
Let the message to be encrypted be " I AM SAFE"
The generated encrypted sequence for the input string will be
[2 3 2 1 0 1 4 2 2 1 0 0 3 4 2 3 2 1 0 1 1 2 3 3 2 1 2 2 2 2 1 0 0 3 4 3 4
3 1 0 2 3 2 3 2 1 0 1 1 3 3 2 0 0 1 3 4 4 0 0 0 1 1].
This encrypted string can be decoded as "I AM SAFE" at the other end.

The generated encryption sequence for the given input string is:
[2 3 2 1 0 1 4 2 2 1 0 0 3 4 2 3 2 1 0 1 1 2 3 3 2 1 2 2 2 2 1 0 0 3 4 3 4
3 1 0 2 3 2 3 2 1 0 1 1 3 3 2 0 0 1 3 4 4 0 0 0 1 1]

The decoded string is:
I AM SAFE

Conclusion

The process of encryption is safe in this proposed method as random graphs of any order can be chosen and the number of graphs chosen can also vary. Other than the encrypter and the decrypter, it will be difficult for an unauthorised person to guess these graphs. Also, the encryption is done based on the distance degree sequence of the Cartesian product of pairs of graphs which is again a challenge to make a guess. The characters that are assigned to each vertex in the graph can either be horizontal or vertical. This makes the above proposed method for a safe transmission of messages.

References

1. P. Erdos and T.Gallai, "Graphs with prescribed degrees of vertices," Matematikai Lapok, vol. 11, pp. 264–274, 1960 (Hungarian).
2. V. Havel, "A remark on the existence of finite graphs," Casopis ˇ Pro Pestov ˇ an´ ´ı Matematiky, vol. 80, pp. 477–480, 1955 (Czech).
3. S. L. Hakimi, "On realizability of a set of integers as degrees of the vertices of a linear graph. I," Journal of the Society for Industrial and Applied Mathematics, vol. 10, pp. 496–506, 1962.
4. Yamuna M et al 2013 International Journal of Engineering and Technology5 2920 – 25.

5. Yamuna M and Elakkiya A 2015 International Journal of Advance Research in Science and Engineering 3 1600 – 06 .
6. Yamuna M 2014 The International Journal of Computer Science and Applications 2 11 – 15.
7. Yamuna M 2017 IOP Conf. Series: Materials Science and Engineering 263 (2017) 042117 doi:10.1088/1757-899X/263/4/042117.
8. J. W. Kennedy and L. V. Quintas , "Extremal f-trees and embedding spaces for molecular graphs,"Discrete Applied Mathematics, Vol. 5(2), pp. 191-209, 1983.
9. M. Randic, "Characterizations of atoms, molecules, and classes of molecules based on paths enumerations," MATCH, Vol. 7, pp. 5–64, 1979.
10. 10. Medha Itagi Huilgol, M. Rajeshwari and S. Syed Asif Ulla, "Embedding in
11. distance degree regular and distance degree injective graphs," Malaya Journal of Mathematik,Vol. 4(1), pp. 134–141, 2013.[15] Medha Itagi Huilgol, M. R
12. Rinartha, K., & Suryasa, W. (2017). Comparative study for better result on query suggestion of article searching with MySQL pattern matching and Jaccard similarity. In *2017 5th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-4). IEEE.
13. Rinartha, K., Suryasa, W., & Kartika, L. G. S. (2018). Comparative Analysis of String Similarity on Dynamic Query Suggestions. In *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)* (pp. 399-404). IEEE.
14. Malaka, I. G., Syarif, S., Arsyad, M. A., Baso, Y. S., & Usman, A. N. (2021). Development of women's reproductive health application as android-based learning media of adolescent knowledge. *International Journal of Health & Medical Sciences*, *4*(2), 182-188. https://doi.org/10.31295/ijhms.v4n2.1685