INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Cryptosystem using double vertex graph

C Beaula[1]*, **P Venugopal**[1]

1 Sri Siva Subramaniya Nadar, Kalavakkam, 603 110, Tamilnadu, India. Tel.: 91 9841797926

OPEN ACCESS

Received: 28.09.2020

Accepted: 04.11.2020

Published: 15.12.2020

Citation: Beaula C, Venugopal P (2020) Cryptosystem using double vertex graph. Indian Journal of Science and Technology 13(44): 4483-4489. https://doi.org/10.17485/IJST/v13i44.1699

* **Corresponding author**.

Tel: 91 9841797926
beaula_charles@yahoo.co.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/Objective: The Coronavirus Covid-19 has affected almost all the countries and millions of people got infected and more deaths have been reported everywhere. The uncertainty and fear created by the pandemic can be used by hackers to steal the data from both private and public systems. Hence, there is an urgent need to improve the security of the systems. This can be done only by building a strong cryptosystem. So many researchers started embedding different topics of mathematics like algebra, number theory, and so on in cryptography to keep the system, safe and secure. In this study, a cryptosystem using graph theory has been attempted, to strengthen the security of the system. **Method:** A new graph is constructed from the given graph, known as a double vertex graph. The edge labeling of this double vertex graph is used in encryption and decryption. **Findings:** A new cryptosystem using the amalgamation of the path, its double vertex graph and edge labeling has been proposed. From the double vertex graph of a path, we have given a method to find the original path. To hack such an encrypted key, the knowledge of graph theory is important, which makes the system stronger. **Applications:** The one-word encryption method will be useful in every security system that needs a password for secure communication or storage or authentication.

Keywords: Double vertex graphs; path; adjacency matrix; encryption; cryptography

1 Introduction

All the communications, whether it is social, business, or any other networking are done using digital technology. The world is getting more and more digitalized to make the life easy. The technology is compact in our hands and any work can be done with just a click. As everything is getting digitalized, it is the responsibility of the service provider, to make their system as safe and secure for their clients. Hence, updating security in a system becomes essential and a continuous process.

The coronavirus Covid-19 has affected almost all the countries and lakhs and lakhs of people got infected and millions of deaths have been reported globally. This pandemic forced the countries to shut down all their businesses. The governments are completely engaged in keeping the death rate of their countries under control. They are continuously motivating researchers to find vaccines for this virulent disease. The hackers have started using this unprecedented opportunity of chaos and panic to wield social, economic, and financial crises for their gain[(1)]. Hence, whether it is a private or public system, there is an urgent need to protect the data from these hackers, by improving the security of the systems. This can be done by cryptography. Cryptography is a technique used for protecting information and communications by using some secret codes so that the information is known only to the receiver and the sender. It plays an important role in updating and making a system more secure. It is used to provide secrecy and integrity to our data, and both authentication and anonymity to our communications.

The cryptography[(2)] is of two kinds (i) Symmetric key cryptography - the decryption key can be calculated from the encryption key and vice versa and (ii) Non-Symmetric key cryptography - encryption and decryption keys are different and it cannot be calculated from one another. The key used for encryption is called the *public key* and the key used for decryption is known as a *private key*. Cryptosystem is a combined process of encryption and decryption. The sender should be very careful in handling the encryption of plaintext and should not give a single clue to the third party. The receiver also needs to be careful in decrypting the ciphertext without any error. However, in this digital era, any cryptosystem is valid only for a limited period, as it is cracked by hackers in a short period. Hence, there is a great demand to adopt different techniques to strengthen the cryptosystem. This necessity motivated many researchers to look into various techniques and subjects to make cryptosystem stronger. In this paper, cryptography using graph theory has been considered, as the knowledge of graph theory is important for hackers, to hack the secret key.

Graph theory is a field having a lot of applications; any real-life problem is simplified using graphs and can be solved using graph theory properties and techniques. The flexibility of graph properties strengthens the cryptosystem. The graph structures play an important role in the encryption and decryption process. The literature survey given in[(3–5)] helps to understand the use of graph theory in cryptography. The graph theory technique is used in cryptography to strengthen the security of data transmission, as the knowledge of graph theory is very important for the decryption of any ciphertext[(2,6)]. Dawn Song et al.[(7)] used an expander graph in authenticating long digital streams over lossy networks as the constant degree of the graph makes the authentication more efficient. Cusack and Chapman[(8)] gives a method using the Cayley graph constructed from groups, to construct cryptosystems.

Any important secret document which has to be shared among people will be encrypted by a password. This encrypted document and the secret key to decrypt the document will be sent separately to the receiver. Mostly a single word is used as a password.

In this paper, a new cryptosystem using the amalgamation of paths, its double vertex graph and edge labelling has been proposed.

2 Preliminaries

Graph theory[(9,10)], a branch of mathematics has a lot of applications in Chemistry, Operations Research, Social Science, Computer Science, etc. It is obvious that hiding small information using a big network structure strengthens the encryption. Based on requirements, many new big networks can be constructed from a given graph or a set of graphs using different techniques like Cartesian product, union, join, double vertex graphs, and so on.

Alavi et al.[11] introduced a double vertex graph. It is defined as follows:

Definition[1]. Let $G = (V,E)$ be a graph of order $n \geq 2$. The double vertex graph $U_2(G)$ is the graph whose vertex set consists of all $\binom{n}{2}$ unordered pairs from V such that two vertices $\{x,y\}$ and $\{u,v\}$ are adjacent if and only if $|\{x,y\} \cap \{u,v\}| = 1$ and if $x = u$ then y *and* v are adjacent in G. See Figure 1 for the path P_7 and Figure 2 for its corresponding double vertex graph $U_2(P_7)$.

Comparing to the original graph, the distance between any two vertices is increased in its double vertex graph[12], which gives more efficiency and collision resistance for the encryption. The encrypted text using double vertex graph cannot be traced back without the knowledge of how the double vertex graphs were constructed. This makes the system more secure.

In general, graphs can be represented in two ways namely adjacency list and adjacency matrix[9]. The adjacency list representation of graph $G = (V,E)$ consists of an array of lists $|V|$, representing each row by a vertex in V.

The adjacency matrix

$A = (a_{ij})_{n\times n}$ of a graph $G = (V,E)$ is a $|V| \times |V|$ matrix such that

(i) For unweighted graph

$$a_{ij} = \begin{cases} 1 & if\ (v_i,\ v_j) \in E \\ 0 & otherwise \end{cases} \quad and$$

(ii) For weighted graph

$$a_{ij} = \begin{cases} w_{ij} & if\ (v_i,\ v_j) \in E \\ 0 & otherwise \end{cases}$$

3 Main Results

In this section, we first introduce an encryption algorithm based on a double vertex graph of a path. This path is constructed from the given password. An illustration is given for this encryption algorithm by considering a password. Then a decryption algorithm is introduced to decrypt the encrypted word. We use the encoding table[2] given in Table 1 to convert any word to a number string.

Table 1. Encoding table

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Coding Number	1	2	3	4	5	6	7	8	9	10	11	12	13
Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Coding Number	14	15	16	17	18	19	20	21	22	23	24	25	26

Theorem 3. 1: Every edge of a path P_n contributes $(n-2)$ edges in double vertex graph $U_2(P_n)$.

Proof: Consider a path P_n of length n. It has $n-1$ edges and $n$vertices.

The double vertex graph $U_2(P_n)$ of a path has nC_2 number of vertices, and is given by

$$V\left(U_2\left(P_n\right)\right) = \{12,\ 13,\ldots 1n,\ 23,\ 24,\ldots .2n,\ 34,\ 35,\ldots .3n,\ldots,\ (n-2)\,(n-1)\,,(n-1)\,n\}$$

Consider an edge $(l, l+1)$ of the path.

By the definition of double vertex graph, the corresponding edges in double vertex graph $U_2(P_n)$ are $(il,\ i(l+1));\ 1 \le i < l$ and $(lj,\ (l+1)j);\ l+1 < j \le n$.

Number of horizontal edges in $U_2(P_n) = l-1$

Number of vertical edges in $U_2(P_n) = n-(l+1)$

Therefore, the number of edges for $(l, l+1)$ in $U_2(P_n) = l-1+n-(l+1) = n-2$.

Hence the proof.

Remark 3.1: By Theorem 1, every edge in the path P_n contributes $(n-2)$ edges in double vertex graph $U_2(P_n)$. Let $a_{l(l+1)}$ be the weight of an edge $(l, l+1)$ in the path P_n. This weight $a_{l(l+1)}$ is partitioned into $(n-2)$ numbers to assign a weight to all $(n-2)$ edges constructed from $(l, l+1)$ in $U_2(P_n)$ using the following method.

Let the first edge be labelled as, $x_1 = \left\lceil \frac{a_{l(l+1)}}{n-2} \right\rceil$.

The second edge to $(n-3)^{\text{rd}}$ edges are labelled as

$$x_m = \left\lceil \frac{a_{l(l+1)} - (x_1 + x_2 + \cdots + x_{m-1})}{n-2} \right\rceil;\ 2 \le m \le (n-3)$$

The $(n-2)^{\text{nd}}$ edge is labelled as

$$x_{n-2} = a_{l(l+1)} - (x_1 + x_2 + \cdots + x_{n-3})$$

3.1 Encryption algorithm

The steps in the encryption algorithm using double vertex graph are as follows:

1. Convert the Plaintext to number string $N_k = n_1, n_2, n_3, \ldots\ldots\ldots n_k$, using the coding table (Table 1). Add 26 to each number of N_k so that $n_l + 26 = a_{l(l+1)};\ 1 \le l \le k$.
2. Label the edges $(l, l+1); 1 \le l \le (n-1)$ in the path$P_n (n = k+1)$ with $a_{l(l+1)}$
3. Construct $U_2(P_n)$, each edge weight $a_{l(l+1)}$ of the path is partitioned into $(n-2)$ values and is used to label the $(n-2)$ edges
   $(il,\ i(l+1));\ 1 \le i < l$ and $(lj,\ (l+1)j);\ l+1 < j \le n$.
4. Form an adjacency matrix A for $U_2(P_n)$.
5. Extract the entries of A, which gives the final encrypted message.

Encrypted message

The encrypted message will be of the following form

Encrypted message = (No. of rows of A, extraction of A).

3.1 Illustration

Suppose we want to send a message **STRIKE .**

The plaintext is "STRIKE", which is a six-letter word. Therefore $k = 6$.

Step 1: Replace this plaintext by N_6= 19, 20,18,9,11,5 using the Coding table given in Table 1.

Step 2: Add 26 to each of the digits of N_6 and label these digits in the path P_7. See Figure 1 .

Fig 1. Path P_7

In Figure 1, $a_{12} = 45$, $a_{23} = 46$, $a_{34} = 44$, $a_{45} = 35$,$a_{56} = 37$, $a_{67} = 31$

Partition of edge weights

By Theorem 3.1, each edge in P_n is partitioned into $(n-2)$ edges in $U_2(P_n)$.

Consider the edge $a_{12} = 45$. It is partitioned into $(7-2) = 5$ edges in $U_2(P_7)$. The weights of these 5 edges are calculated using Remark 1.

$$\left\lceil \frac{45}{7-2} \right\rceil = 9, \left\lceil \frac{45-9}{7-2} \right\rceil = 8, \left\lceil \frac{45-(9+8)}{7-2} \right\rceil = 6, \left\lceil \frac{45-(9+8+6)}{7-2} \right\rceil = 5$$

$$45-(9+8+6+5) = 17$$

Therefore, $45 = 9+8+6+5+17$

Similarly, the weights of other edges in the path P_7 are partitioned as follows:

$46 = 10 + 8 + 6 + 5 + 17$

$44 = 9 + 7 + 6 + 5 + 17$

$35 = 7 + 6 + 5 + 4 + 13$

$37 = 8 + 6 + 5 + 4 + 14$

$31 = 7 + 5 + 4 + 3 + 12$

Step 3: Label the edges of the double vertex graph $U_2(P_7)$ with the corresponding partitions.

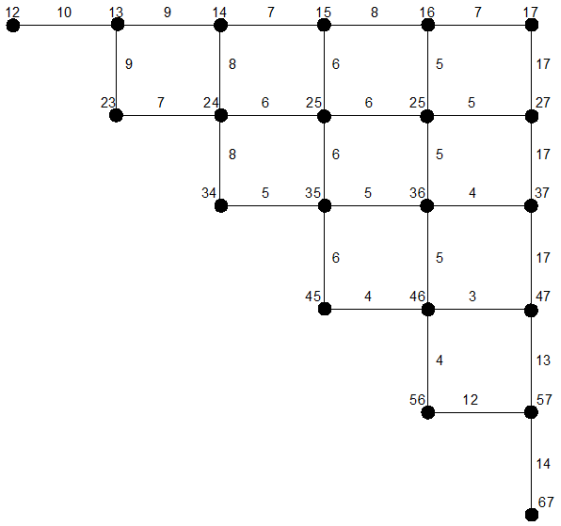

Fig 2. Double vertex graph $U_2(P_7)$

Step 4: The adjacency matrix A of $U_2(P_7)$ is

$$A = \begin{pmatrix}
0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
10 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 9 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 7 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 8 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 17 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 9 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 8 & 0 & 0 & 0 & 7 & 0 & 6 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 6 & 0 & 0 & 0 & 6 & 0 & 6 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 6 & 0 & 5 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 17 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 17 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 5 & 0 & 5 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 5 & 0 & 4 & 0 & 5 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 17 & 0 & 0 & 4 & 0 & 0 & 0 & 17 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 4 & 0 & 3 & 4 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 17 & 0 & 3 & 0 & 0 & 13 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 12 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 13 & 12 & 0 & 14 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 14 & 0
\end{pmatrix}$$

Step 5: Encrypted message: The encrypted message consists of an order of the matrix and all the entries from the adjacency matrix $U_2(P_7)$.

(21, 0, 10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10, 0, 9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 0, 0, 0, 0, 17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 9, 0, 0, 0, 0, 0, 7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 0, 0, 7, 0, 6, 0, 0, 8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 0, 0, 6, 0, 6, 0, 0, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 0, 0, 6, 0, 5, 0, 0, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 17, 0, 0, 0, 5, 0, 0, 0, 0, 17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 0, 0, 0, 0, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 5, 0, 5, 0, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 0, 5, 0, 4, 0, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 17, 0, 0, 4, 0, 0, 0, 17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 6, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5, 0, 4, 0, 3, 4, 0, 0, 0 , 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 17, 0, 3, 0, 0, 13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0, 12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 13, 12, 0, 14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 14, 0)

Remark 3. 2: The encrypted message can be decrypted by the receiver using the decryption algorithm.

3.2 Decryption algorithm

1. Form a matrix using the encrypted message and name it as A
2. Construct a graph using A, which would be$U_2(P_n)$
3. Extract P_n from $U_2(P_n)$ and label each edge $(l, l+1)$ as follows,
   $(l,\ l+1) = a_{l(l+1)} = (il,\ i(l+1))\ +(lj,\ (l+1)\,j);\ 1 \le i < l\ ,$
   $l+1 < j \le n,\ 1 \le l \le (n-1)$

4. Calculate $n_l = a_{l(l+1)} - 26; 1 \leq l \leq (n-1)$ and form the number string N_k
5. Convert the number string N_k to plaintext using Coding Table.

4 Conclusion

In this study, a double vertex graph to encrypt a word was proposed. First, the given message was encoded using the encoding table. In the second step, the plain text was converted into a path graph. From this path graph, a double vertex graph was constructed. Then an adjacency matrix is formed from this double vertex graph. These four stages make the encryption stronger. Without the knowledge of graph theory, it is very difficult to hack and decrypt the encrypted word. This kind of cryptosystem is used to communicate single word like password securely. This study can be extended to encrypt a sentence. This work can also be extended to other big graph structure to make the password even more secure and strong.

Acknowledgement

The authors wish to thank the management of Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam 603 110 for their continuous support and encouragement for the research work.

References

1) Coronavirus pandemic reminds us that security is important during the zoom boom. . Available from: https://cointelegraph.com/news/coronavirus-pandemic-reminds-us-that-security-is-important-during-the-zoom-boom.
2) Stallings W. Cryptography and Network Security. 6th ed. and others, editor;Pearson Education Inc. 2014.
3) Priyadarsini PLK. A survey on some applications of graph theory in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*. 2015;18(3):209–217. Available from: https://dx.doi.org/10.1080/09720529.2013.878819.
4) Yamuna M, Gogia M. Jazib Hayat khan "Encryption Using Graph Theory and Linear Algebra". *International Journal of Computer Application*. 2012;5:102–107.
5) Yamuna M, Karthika K. Data Transfer using Bipartite Graphs. *International Journal of Advance Research in Science and Engineering*. 2015;4:128–131.
6) Etaiwi W. Encryption algorithm using graph theory. *Journal of Scientific Research and Reports*. 2014;3(19):2519–2527. Available from: https://dx.doi.org/10.9734/jsrr/2014/11804.
7) Song D, Zuckerman D, Tygar JD. Expander Graphs for digital stream authentication and robust overlay networks. In: and others, editor. Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P.02). 2002.
8) Cusack B, Chapman E. Using graphic methods to challenge cryptographic performance. In: Proceedings of 14th Australian Information Security Management Conference, Perth, Western Australia. 2016;p. 30–36. Available from: https://doi.org/10.4225/75/58a6991e71023.
9) Harary F. Graph Theory. and others, editor;Narosa Publishing House. 1988.
10) Deo N. Graph theory with applications to engineering and computer science. and others, editor;Prentice-Hall. 1974.
11) Alavi Y, Behzad M, Erdos P, Lick DR. Double vertex graphs. *Journal of Combinatorics, Information and System Sciences*. 1991;16:37–50. Available from: https://doi.org/10.1007/978-1-4614-7254-4.
12) Beaula C, Venugopal P, Padmapriya N. Graph distance of vertices in double vertex graphs. *International Journal of Pure and Applied Mathematics*. 2018;18:343–351.