RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Graph Labelling and Chaldean Numerology in Cryptography

By

Dr. A. Uma Maheswari
Associate Professor & Head PG & Research Department of Mathematics Quaid – E–Millath Government College For Women
Chennai – 600 002.
Email: umashiva2000@yahoo.com

A.S.Purnalakshimi
Research Scholar
Email: aspurnalakshmi@gmail.com

Abstract

Graph labelling, an interesting and developing branch in mathematics has wide range of applications including cryptography. Chaldean numerology, the oldest form of calculation developed by the Babylonians is employed for encoding and decoding messages. In this paper, graph theory with Chaldean numerology and arithmetic number labelling is used for the encryption of text. Python program coding link to decode the message is given.

Keywords: Arithmetic number labelling, Chaldean numerology

Introduction

Graph labelling is assigning of labels represented by integers to vertices[1][2][12] [13],edges[14] [15],faces[3] and blocks[13][14][18][19][21] of a graph. Graph theory finds its applications in many fields like cryptography[4][5][6][9][10][26], medical[17],etc. Cryptography has become the need of the hour since secured transformation of information has become very important. Chaldean numerology [7][8] is an oldest form of calculation used for predicting the future. Arithmetic number labelling was introduced by Uma maheswari and Purnalakshimi in 2022[13]. In this paper, arithmetic number labelling and Chaldean numerology is used for encrypting and decrypting the message.

Definition1: Arithmetic number[1]

A number 'n' is called an Arithmetic number if the arithmetic mean of its divisors is an integer. For example, 6 is an arithmetic number since the arithmetic mean of its divisors 1,2,3,6 is 3, an integer. Some of the arithmetic numbers are 1,3,5,6,7,11,13 .

Definition 2: Arithmetic number labelling [13]

An Arithmetic number labelling of a graph G is a one - to – one function.$f: v(G) \rightarrow W$, where W is the set of whole Numbers.) that induces a bijection $f^*: E(G) \rightarrow (A_1, A_2, A_3, \dots, A_n)$, defined by $f^*(u,v) = |f(u) - f(v)|, \forall\, e = uv \in E(G)$. The graph which admits Arithmetic number labelling is called Arithmetic number graph.

Definition 2: Cartesian product of graph [3]

Let G_1 and G_2 be two simple connected graphs with vertex sets as V_1 and V_2. Then the cartesian product of these two graphs G_1 and G_2 is G_1 x G_2 with vertex set V = V_1 x V_2 and for which two vertices (u_1,u_2) and (v_1,v_2) of G are adjacent if and only if either $u_1 = v_1$ and u_2v_2 belongs to E (G_2), or $u_2 = v_2$ and u_1v_1 belongs to E(G_1) .

Definition 3[20]: Ciphertext is the required version of plain text.
Definition 4[20]: Encryption is the process of transforming plain text into ciphertext.
Definition 5[20]: Decryption is the process of transforming cipher text into plain text.
Definition 6[20]: Key is the most essential tool which encodes the plain text and decodes the ciphertext.

Chaldean numerology

Table 1

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	8	3	5	1	1
K	L	M	N	O	P	Q	R	S	T
2	3	4	5	7	8	1	2	3	4
U	V	W	X	Y	Z				
6	6	6	5	1	7				

Main results

In this section, Arithmetic number labelling and Chaldean numbers are used for encryption of cipher text. New algorithm is developed to secure transmission of codes. The following is the list of instructions involved in the process of encryption.

The Chaldean numbers associated with alphabets are shown in table 2.

Table 2

1	2	3	4	5	6	7	8
A, I, J, Q, Y	B, K, R	C, G, L, S	D, M, T	E, H, N, X	U, V, W	O, Z	F, P

To enable uniqueness in vertex labelling, the numbers are associated with the alphabets in the following manner shown in table 3.

Table 3

1	2	3	4	5	6	7	8
A -11	B -21	C - 31	D – 41	E -51	U -61	O -71	F -81
I -12	K -22	G - 32	M – 42	H -52	V -62	Z -72	P -82
J -13	R – 23	L - 33	T – 43	N -53	W -63		
Q -14		S - 34		X -54			
Y -15							

Encryption algorithm

1. The text message intended for the receiver is sent as cartesian product of 2 graphs. One is a path graph with arithmetic number labelling, and another is a closed graph with Chaldean numbers associated with the alphabets of the text message. The text message should contain alphabets which do not repeat.
2. This graph is converted into a 5 x 5 matrix if the text has 5 letters. Name this matrix as A
3. The key of encoding is a 5 x 5 matrix named B. Here we use the upper triangular matrix with even numbers. B as

$$\begin{pmatrix} 2 & 4 & 6 & 8 & 10 \\ 0 & 12 & 14 & 16 & 18 \\ 0 & 0 & 20 & 22 & 24 \\ 0 & 0 & 0 & 26 & 28 \\ 0 & 0 & 0 & 0 & 30 \end{pmatrix}$$

4. M = AB which is a 5 x 5 matrix.
5. The elements of this 5 x 5 matrix is assigned as vertices to the cartesian product of graphs G_1 x G_2
6. The graph G_1 x G_2 is the encrypted message.

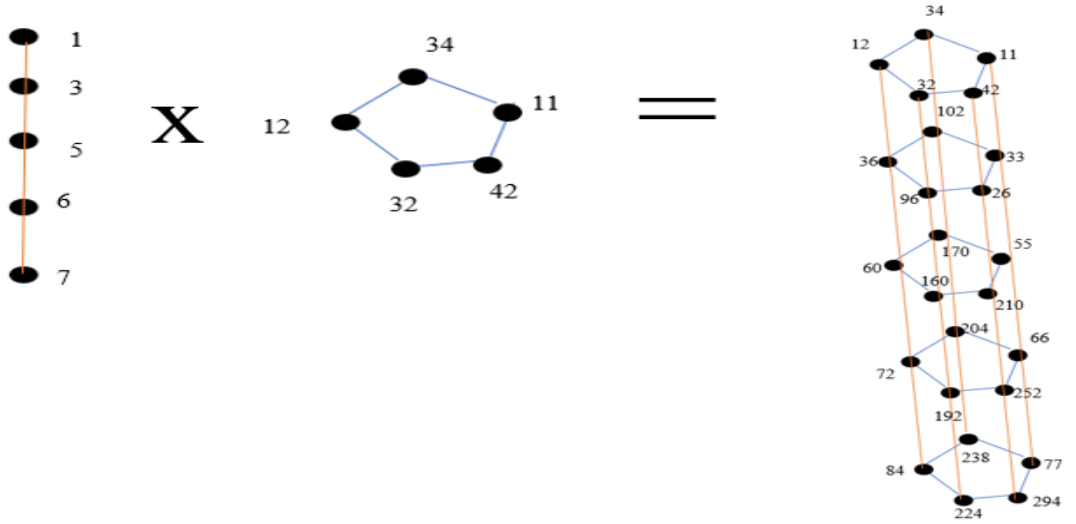
Decryption algorithm

1. The vertices of the received graph H_1 x H_2 is converted into a 5 x 5 matrix with the vertices as elements of a matrix.
2. This is matrix M.
3. This matrix M is multiplied with the inverse of Key matrix B (i.e) $A = MB^{-1}$
4. Once we get the matrix A ,we do the following
5. $CN_{11} = a_{11}/ A_1$, $CN_{12} = a_{12}/ A_2$, $CN_{13} = a_{13}/ A_3$, $CN_{14} = a_{14}/ A_4$, $CN_{15} = a_{15}/ A_5$.
6. Note CN_{11} denotes the alphabet used in table 3 associated with the Chaldean numerology.

ustration

Let us assume that the message sent to the receiver is SIGMA
SIGMA
The numbers associated with the alphabets from table 3 is as follows
S – 34, I -12, G -32, M – 42, A -11.

We co



= nstruct a graph G_1 x G_2

$$\begin{bmatrix} 34 & 12 & 32 & 42 & 11 \\ 102 & 36 & 96 & 26 & 33 \\ 170 & 60 & 160 & 210 & 55 \\ 204 & 72 & 192 & 252 & 66 \\ 238 & 84 & 224 & 294 & 77 \end{bmatrix}$$

Vertices of this graph is converted to a matrix. A =

$$\begin{bmatrix} 2 & 4 & 6 & 8 & 10 \\ 0 & 12 & 14 & 16 & 18 \\ 0 & 0 & 20 & 22 & 24 \\ 0 & 0 & 0 & 26 & 28 \\ 0 & 0 & 0 & 0 & 30 \end{bmatrix}$$

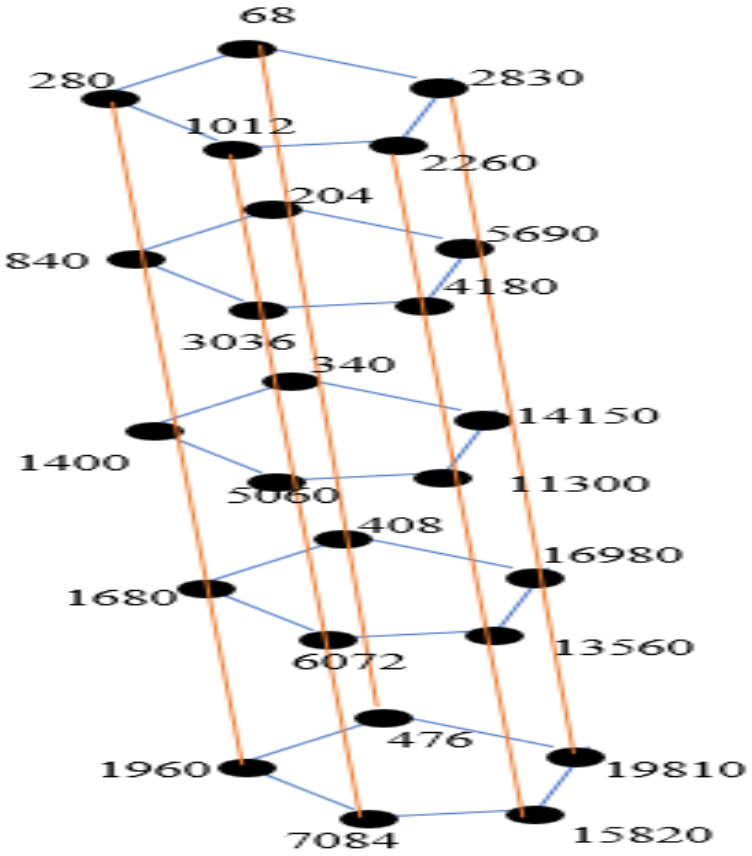
Consider the key for encoding matrix B =

$$\begin{bmatrix} 34 & 12 & 32 & 42 & 11 \\ 102 & 36 & 96 & 26 & 33 \\ 170 & 60 & 160 & 210 & 55 \\ 204 & 72 & 192 & 252 & 66 \\ 238 & 84 & 224 & 294 & 77 \end{bmatrix} \times \begin{bmatrix} 2 & 4 & 6 & 8 & 10 \\ 0 & 12 & 14 & 16 & 18 \\ 0 & 0 & 20 & 22 & 24 \\ 0 & 0 & 0 & 26 & 28 \\ 0 & 0 & 0 & 0 & 30 \end{bmatrix}$$

Compute M = AB

$$\begin{bmatrix} 68 & 280 & 1012 & 2260 & 2830 \\ 204 & 840 & 3036 & 4180 & 5690 \\ 340 & 1400 & 5060 & 11300 & 14150 \\ 408 & 1680 & 6072 & 13560 & 16980 \\ 476 & 1960 & 7084 & 15820 & 19810 \end{bmatrix}$$

The matrix M when converted to a graph is



M =

Now we will decode the graph

The vertices of the graph are converted to a matrix.

$$\begin{bmatrix} 68 & 280 & 1012 & 2260 & 2830 \\ 204 & 840 & 3036 & 4180 & 5690 \\ 340 & 1400 & 5060 & 11300 & 14150 \\ 408 & 1680 & 6072 & 13560 & 16980 \\ 476 & 1960 & 7084 & 15820 & 19810 \end{bmatrix}$$

M =

Since M =A B^{-1} we multiply M with B^{-1} which is

$$\begin{bmatrix} 1/2 & -1/6 & -\frac{1}{30} & -\frac{3}{30} & -\frac{6}{325} \\ 0 & \frac{1}{12} & -\frac{7}{120} & -\frac{1}{520} & -\frac{1}{650} \\ 0 & 0 & 1/20 & \frac{-11}{260} & -\frac{1}{1950} \\ 0 & 0 & 0 & \frac{1}{26} & -\frac{7}{195} \\ 0 & 0 & 0 & 0 & \frac{1}{30} \end{bmatrix}$$

Hence, we get

$$\begin{bmatrix} 68 & 280 & 1012 & 2260 & 2830 \\ 204 & 840 & 3036 & 4180 & 5690 \\ 340 & 1400 & 5060 & 11300 & 14150 \\ 408 & 1680 & 6072 & 13560 & 16980 \\ 476 & 1960 & 7084 & 15820 & 19810 \end{bmatrix} \text{ x } \begin{bmatrix} 1/2 & -1/6 & -\frac{1}{30} & -\frac{3}{30} & -\frac{6}{325} \\ 0 & \frac{1}{12} & -\frac{7}{120} & -\frac{1}{520} & -\frac{1}{650} \\ 0 & 0 & 1/20 & \frac{-11}{260} & -\frac{1}{1950} \\ 0 & 0 & 0 & \frac{1}{26} & -\frac{7}{195} \\ 0 & 0 & 0 & 0 & \frac{1}{30} \end{bmatrix}$$

$$\begin{bmatrix} 34 & 12 & 32 & 42 & 11 \\ 102 & 36 & 96 & 26 & 33 \\ 170 & 60 & 160 & 210 & 55 \\ 204 & 72 & 192 & 252 & 66 \\ 238 & 84 & 224 & 294 & 77 \end{bmatrix}$$

So, we got the original matrix A. We can use any row to decode. We now consider the elements in the first row which are 34,12,32,42,11.

Alphabets associated to this Chaldean numerology (CN) is as follows:

$CN_1 = \frac{34}{A_1} = \frac{34}{1} =$ **34** which is associated to S from Table 3

Similarly

$CN_2 = \frac{12}{1} = \frac{12}{1} =$ **12** which is associated to I from Table 3

$CN_3 = \frac{32}{1} = \frac{32}{1} =$ **32** which is associated to G from Table 3

$CN_4 = \frac{42}{11} = \frac{42}{11} =$ **42** which is associated to M from Table 3.

$CN_5 = \frac{11}{A_1} = \frac{11}{1} =$ **11** which is associated to A from Table 3.

We use the elements in the third row to decode.

$CN_1 = \frac{170}{A_3} = \frac{170}{5} =$ **34** which is associated to S from Table 3.

$CN_2 = \frac{60}{A_3} = \frac{60}{5} =$ **12** which is associated to I from Table 3.

$CN_3 = \frac{160}{A_3} = \frac{160}{5} =$ **32** which is associated to G from Table 3.

$CN_4 = \frac{210}{A_3} = \frac{210}{5} =$ **42** which is associated to M from Table 3.

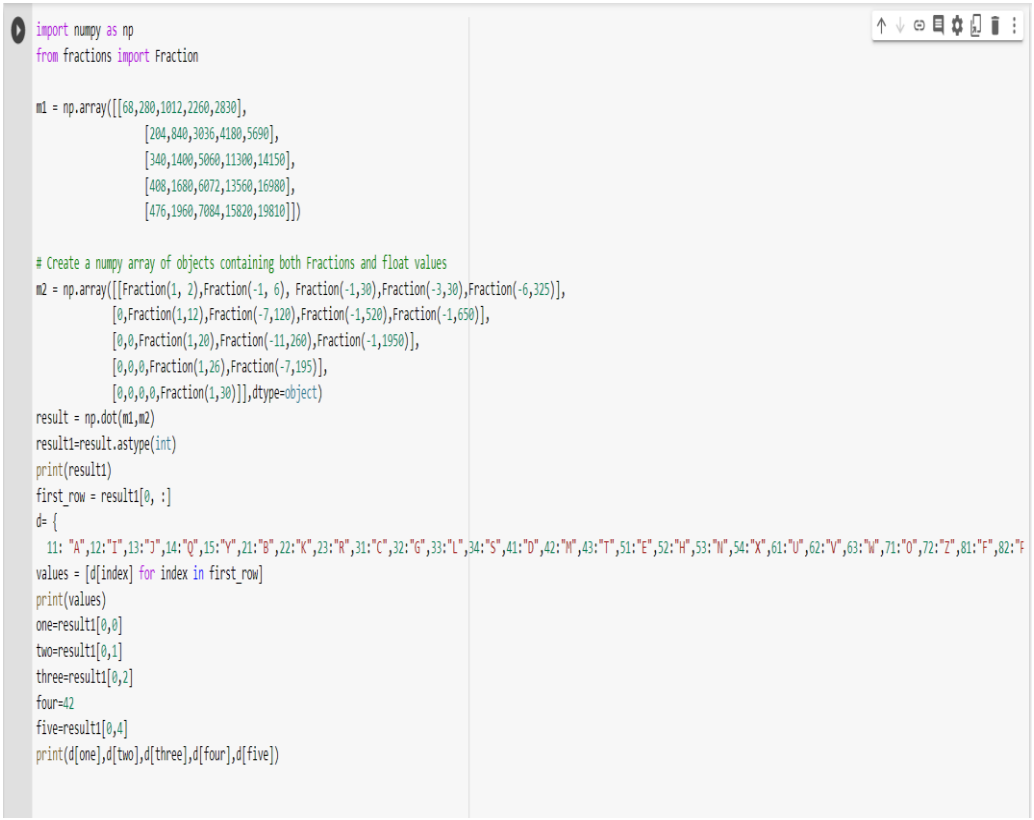
$CN_5 = \frac{55}{A_3} = \frac{55}{5} =$ **11** which is associated to S from Table 3.

Likewise, we can use any row for decoding. For convenience we can use the row which has smaller numbers.

Hence, we have encrypted and decrypted the word ‘SIGMA’. To simplify the process of decoding, we can use Python program. Python program coding link to decode a five letter message is given below.

https://colab.research.google.com/drive/1KVZomOYqL8hbWkW70ITN5ZFxdkyPCCeR?usp=sharing

screenshot of the program.



```
import numpy as np
from fractions import Fraction

m1 = np.array([[68,280,1012,2260,2830],
               [204,840,3036,4180,5690],
               [340,1400,5060,11300,14150],
               [408,1680,6072,13560,16980],
               [476,1960,7084,15820,19810]])

# Create a numpy array of objects containing both Fractions and float values
m2 = np.array([[Fraction(1, 2),Fraction(-1, 6), Fraction(-1,30),Fraction(-3,30),Fraction(-6,325)],
            [0,Fraction(1,12),Fraction(-7,120),Fraction(-1,520),Fraction(-1,650)],
            [0,0,Fraction(1,20),Fraction(-11,260),Fraction(-1,1950)],
            [0,0,0,Fraction(1,26),Fraction(-7,195)],
            [0,0,0,0,Fraction(1,30)]],dtype=object)
result = np.dot(m1,m2)
result1=result.astype(int)
print(result1)
first_row = result1[0, :]
d= {
  11: "A",12:"I",13:"J",14:"Q",15:"Y",21:"B",22:"K",23:"R",31:"C",32:"G",33:"L",34:"S",41:"D",42:"M",43:"T",51:"E",52:"H",53:"N",54:"X",61:"U",62:"V",63:"W",71:"O",72:"Z",81:"F",82:"F
values = [d[index] for index in first_row]
print(values)
one=result1[0,0]
two=result1[0,1]
three=result1[0,2]
four=42
five=result1[0,4]
print(d[one],d[two],d[three],d[four],d[five])
```

Conclusion

In this paper, a new algorithm for coding and decoding is introduced. The algorithm involves arithmetic number labeling and Chaldean numerology. This algorithm for encoding and decoding involving graph labeling is more secure and simple. In this work coding using Python is employed to simplify the process of decoding. There is scope for creating more algorithms using graph operations for encryption and decryption.

References

Antonio M Oller Marcer 'On arithmetic numbers' by arXiv:1206.1823v![Math.NT] 8 june2012.

A.Rosa, "Cyclic Steiner triple systems and labellings of triangular cacti", scientia,I (1988) 87-95.

Koh, K. M., & Soh, K. W. (2016). Power domination of the cartesian product of graphs. AKCE International Journal of Graphs and Combinatorics, 13(1), 22-30.

Deepa, V. Maheswari, "*Ciphering and Deciphering Messages by Graph Labeling Techniques Through Multilevel Cryptosystem*", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-4S5, December 2019, Pg.No: 34-39

B. Deepa, V. Maheswari, "*Encoding and Decoding using Graph Labeling*", The International Journal of Analytical and Experimental Modal Analysis, Volume XI, Issue X, October/2019, Page No:8-15

B. Deepa, V. Maheswari, V. Balaji, "*Creating Ciphertext and Decipher using Graph Labeling Techniques*", International Journal of Engineering and Advanced Technology (IJEAT)

ISSN: 2249 – 8958, Volume-9 Issue-1S, October 2019, Pg.No: 206-212

Dudley, U. (1997). *Numerology, or, what Pythagoras wrought*. Cambridge University Press.

A. Gregory, (2015). The Pythagoreans: number and numerology. *Mathematicians and Their Gods: Interactions between Mathematics and Religious Beliefs. Oxford, UK*.

V.N.Jaya Shruthy, Maheswari.V, "*Double Encryption, Decryption Process using Graph Labeling through Enhanced Vigenere Cipher*", Journal of Physics: Conference Series, 1362(2019), Pg.No:1-7 .

V.N. Jaya Shruthy, V.Maheswari, "*A Hybrid Perspective of Symmetric Encryption Through Graph Labeling for Union of Two Star Graphs*", The International journal of analytical and experimental modal analysis Volume XI, Issue X, October/2019, Pg.No:104-114.

Uma Maheswari. A & Purnalakshimi. A. S, "AUM block labelling for friendship, tadpole and cactus graphs''(2022), Neuro Quantology, June 2022,Volume 20,Issue 6,Pp7876-7884.

Uma Maheswari. A & A.S.Purnalakshimi,"Arithmetic number labelling of graphs" in Advances in graph labelling, coloring and power domination theory -Volume 1.

Uma Maheswari. A & Azhagarasi, S, "New Labeling for Graphs-AUM Block Sum Labeling", International Journal of Current Science, Vol.12, No.1, pp.574-584.

Uma Maheswari.A & Azhagarasi, S. "AUM Block Labelling for Cycle Cactus Block Graphs", Compliance Engineering Journal, Vol.13, No.4, pp.84-96.

Uma Mahewari . A, Azhagarasi.S & Bala Samuvel.J, "Some New labelling on cycle C_n with zigzag chords chords", International journal of Mechanical Engineering, Kalahari Journals, Vol 6, No 3 December 2021, ISSN 0974 -5823 Pg: 1616 -1623.

Uma Mahewari. A, Azhagarasi.S & Bala Samuvel.J, "Vertex Even Mean and Vertex Odd Mean Labelling for Path Union and crown on cycle with parallel P_3 chords", Design engineering (2021), Issue 6 Pages 5775 -5792, ISS:0011 -9342.

Uma Maheswari. A & Purnalakshimi. A. S, "Graph Theory in the Analysis of Arithmophobia" International journal of Innovative Technology and Exploring Engineering, ISSN:2278-3075, Vol-X, Issue -X, July 2019.

Uma Maheswari. A & Purnalakshimi. A. S, "AUM Block labelling for star, bistar and sunlet graph" Neuro Quantology, Volume 20,Issue 10.

Uma Maheswari.A & Azhagarasi .S "AUM Block sum labelling for some special graphs", International journal of Mechanical Engineering, Vol 7 Special Issue 5,2022 ISSN 0974-5823.

Uma Maheswari.A & Azhagarasi .S' 'A new algorithm for coding and encoding using AUM Block labelling' Compliance engineering journal.

Uma Maheswari. A & Purnalakshimi. A. S, "AUM block labelling for snake graphs and dutch windmill graph", Neuro Quantology, Aug 2022,Volume 20,Issue 9,Pp 414-421.