The Scientific Temper (2024) Vol. 15 (spl-2): 212-217

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl-2.33

https://scientifictemper.com/

ORIGINAL RESEARCH PAPER

An encryption and decryption of phonetic alphabets using signed graphs

Vijay Sharma[1*], Nishu[2], Anshu Malhotra[3]

Abstract

Indeed, in signed graphs, the weights on the edges can be both positive and negative; this will provide a solid representation and manipulation framework for complicated relationships among phonetic symbols. Encryption and decryption of phonetic alphabets pose a number of special challenges and opportunities. This paper introduces a novel approach utilizing the eigenvalues and eigenvectors of signed graphs to develop more secure and efficient methods of encoding phonetic alphabets. Presented is a new cryptographic scheme; consider a mapping from phonetic alphabets onto a signed graph. Encryption should be carried out by means of structure-changing transformations of the latter, which leave intact the integrity of the information encoded. This approach allows for secure, invertible transformations to resist typical cryptographic attacks. Here, the decryption algorithm restores the encrypted graph back to the original phonetic symbols by systematically going through steps opposite to that taken during encryption. The proposal of signed graphs in the processes of phonetic alphabet encryption and decryption opens new frontiers of cryptographic practices, which have useful implications for secure communication systems and data protection.

Keywords: Encryption, Decryption, Signed Graph, Eigenvalues, Eigenvectors.

Introduction

Throughout this paper, the basic terms of graph theory (Harary, F., 1969) and (West, D.B., 1996) have been referred to, and for the signed graph (Zaslavsky, T., 1998 & Zaslavsky, T., 2009) and (Cormen, T. *et al*., 2013). Communication system security has become highly critical nowadays during this digital age. Cryptography itself, the science behind securing communication, has undergone a radical change with the discovery of new mathematical techniques. Examples include innovations related to the encryption and decryption of phonetic alphabets, which play a vital role in any secure voice communication, whether in military or diplomatic communications. While several conventional cryptographic techniques have been developed, they are usually not very effective in application to phonetic alphabets since these alphabets possess special characteristics, such as non-linearity and variability between languages.

Take signed graphs, whose edges bear positive or negative weights, as the basis for encrypting and decrypting phonetic alphabets. Signed graphs have been considered in many different parts of graph theory, being particularly useful in representing structures of complex relational entities (Harary, F., 1969). The novelty of this approach is that not only eigenvalues but also their corresponding eigenvectors of the adjacency matrix from a signed graph are used for encoding and decoding phonetic information.

The basis of signed graphs in cryptography is unique and borrowed from times to come, which may improve the security features of encrypted data by further complicating the process of encryption (Gutin G. *et al*., 2014). Mapping phonetic alphabets to signed graphs shall provide a system whereby the phonetic code will be encrypted in a manner that affects their structural properties.

[1]Department of Applied Sciences, The NorthCap University, Gurugram, India.

[2] Department of Computer Science and Engineering, The NorthCap University, Gurugram, India.

[3] Department of Computer Science and Engineering, K.R. Mangalam University, Gurugram, India.

***Corresponding Author:** Vijay Sharma, Department of Applied Sciences, The NorthCap University, Gurugram, India, E-Mail: vijay19asd005@ncuindia.edu

How to cite this article: Sharma, V., Nishu, Malhotra, A. (2024). An encryption and decryption of phonetic alphabets using signed graphs. The Scientific Temper, **15**(spl-2):212-217.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl-2.33

Source of support: Nil

Conflict of interest: None.

Received: 01/11/2024 **Accepted:** 24/11/2024 **Published** : 30/11/2024

The application of eigenvalues and eigenvectors in cryptography is not new; they find their place in several different cryptographic algorithms due to their ability to summarize information compactly and the inherent properties of secure encryption (Niven I. *et al.* 1980). In the case of a signed graph, its structural information can be encapsulated by its eigenvalues, while its eigenvectors can serve to modify this structure in a predictable and controlled manner. This makes them notably appropriate for cryptographic transformations (Biggs N. 1993).

In this paper, each phonetic alphabet is represented in a signed graph with vertices, while their edges are weighted based on the phonetic similarities or differences. During encryption, a transformation matrix is constructed out of eigenvalues and eigenvectors of the adjacency matrix corresponding to the graph. The transformation matrix will allow the encoding of phonetic data in such a way as to guarantee security and efficiency in the resulting cipher text. It does the decryption by applying the inverse of the transformation matrix to the encrypted data, returning the original phonetic sequence.

The use of eigenvalues and eigenvectors in the proposed approach gives it several advantages over other traditional techniques of encryption. Because the space of cryptographic keys is inherently related to the spectral properties of the signed graph, it is quite hard for unauthorized parties to make any sense out of the encrypted data (Cvetkovic D. *et al.* 1980). On the other hand, due to the use of efficient algorithms of linear algebra, the method is computationally fast; hence real-time encryption and decryption are possible, which may be quite important for practical applications in secure voice communications.

This approach is based on basic research related to both graph theory and linear algebra. The spectral characteristics of graphs, which are presented in the work "Algebraic Graph Theory" (Godsil C. *et al.* 2001), and its application in cryptography (Liu S. *et al.* 2018) give a theoretical background to the present study. In combination, these allow this article to introduce an advanced and secure method of phonetic alphabet encoding-decoding and continue developing the field of cryptographic methods in special systems of communication.

Literature Review

(Shannon, C.E., 1949) Came up with the concept of "unicity distance," the least length of ciphertext that might reasonably be expected to yield a unique solution by the cryptanalyst for the key or plaintext. Since then, this has been the basis for any essential assessment of the security of a cryptographic system. The paper has discussed various ways of cryptanalysis, which detail how an attacker may attempt to break a cryptographic system. This paper is a cornerstone in cryptography studies, influencing both theoretical research and practical application in secure communication.

Signed graphs, often called sigraph, were first introduced by (Harary F. 1953) to handle a problem in social psychology (Cartwright D. *et al.* 1956). Sigraphs have been rediscovered often because they come up naturally in many unrelated areas.

(Rosen K.H. 2005) presented the underlying mathematical concepts of encryption algorithms, such as the RSA algorithm, and shared in the application of number theory to the safety of digital communication, computer science, coding theory, and cryptography.

Some classes of signed graphs, known as Common-Edge Sigraphs, have been studied by (Acharya M. *et al.* 2006). A common-edge sigraph is a sigraph for which a given way of assigning a sign to every edge consistently is applied so that a certain kind of combinatorial property in the resultant structure may be gained. Such a study of graphs is considered an extension of classical graph theory, with more structure added to the graphs that can model real-world phenomena-such as social networks with both positive and negative interactions. This work extends the general understanding of Signed Graph Theory by shedding light on many facts relevant to the structure and characteristics of these graphs.

In general, the study on the properties and characterizations of signed graphs was done by (Sinha D. *et al.* 2013), and in particular, that of common-edge signed graphs. The results obtained in the paper are related to network theory, where relations could be in a positive or negative nature-for example, social networks, biological networks, and communication networks.

(Sinha, D. *et al.* 2014) Identified the determination of balancing in common-edge sigraphs by introducing an optimal algorithm that is at once efficient and practical. This work will have important implications for the analysis of networks where the sign of relationships is crucial. The authors showed that this approach reduces the computational complexity, making it faster and more scalable for large datasets.

(Sinha, D., *et al.* 2015) came up with an algorithm to obtain iterated line sigraph $L^k(S) = L(L^{k-1}(S)), k \in N$, where $S = L^0(S)$ and detected for which value of 'k' it is balanced & determined its complexity. Further, the paper proposed an application of line signed graph in encrypting a network and transmitting the data in the form of a balanced $L^k(S)$ and decrypting it by applying inverse matrix operations.

(Sinha, D., *et al.* 2016) Developed a scheme whereby the nodes and edges in the network have been used - which has been modeled by a signed graph to create encryption keys. The structure of the network, such as dependency among nodes and signs of edges, plays an important role in encryption. The various steps involved in this algorithm include generating a signed graph from the plain text, constructing a proper matrix corresponding to that, and then transforming the plain text into cipher text with the use of that matrix.

(Nisha, S., *et al.* 2017) comprehensively reviewed the RSA public key cryptography algorithm. RSA, in full, represents Rivest-Shamir-Adleman; it's one of the most prevalent algorithms in use today to keep digital communication and data safe. The paper covered the basic principles behind RSA, its implementation, and its contemporary relevance in cryptographic systems. RSA represents a type of public key cryptosystem that relies on the mathematical properties of large prime numbers and their products.

A product of this, together with a derived value e, called the public exponent, and d as the private exponent, forms the public and private keys, respectively, used in encryption and decryption. Key generation, encryption, and decryption processes are designed to be performed securely under this algorithm. RSA finds its application not just in encryption but also in digital signatures, which give verification about the authenticity and integrity of messages.

(Stinson, D.R., 2018) Gave a comprehensive review of symmetric key cryptography, where the encryption and decryption use the same key. He also described some common hash functions including SHA-2 and SHA-3 and MACs for providing message authenticity.

Detailed methods for constructing graphs suitable for encryption were given by (Ni B. *et al.* 2021). Such constructions are based on some mathematical properties, which ensure that the constructed graph is sufficiently complicated to be resistant to cryptanalysis. The authors have shown that schemes devised with those are resistant to some common cryptographic attacks, such as brute force and differential cryptanalysis. The discussed computational complexity of breaking these schemes further highlights their strength. Proposed schemes will be shown secure and efficient, possibly applicable in several domains, where graph representations will be highly relevant.

(Yang, K., *et al.* 2021) Explored a new matrix-based encryption method by eigenvalues and eigenvectors. The authors presented such an encryption algorithm, where the plaintext would be transformed by matrices extracted from its eigenvalue decompositions. They presented the security and efficiency analyses of their scheme and compared those against classic encryption techniques.

(Liu, J., *et al.* 2022) Introduced an encryption method designed for image data using the eigenvalue decomposition of the image matrix. Such a method transforms image data for encryption by eigenvectors. It contains a thorough security analysis and is very effective for several image datasets.

(Gupta, S. *et al.* 2022) proposed a scheme for a secure communication protocol that employed an eigenvector-based transformation for the encryption and decryption of messages. In this protocol, the inherent nature of the eigenvectors is utilized for enhanced security and better efficiency. The paper also discussed experimental results and a comparison with the standard technique of encryption.

(Zaslavsky, T., 2022) Proposed a generalized form of signed graphs: gain graphs. In such a graph, each edge was assigned an element from a group, also known as a "gain." The author introduced an enormous class of mathematical terms and expressions in graph theory, combinatorics, and algebra related to all the concepts regarding the study of signed and gain graphs. This paper covered various terminologies employed to define the properties of signed graphs, such as balance, switching, and sign function.

More recently, (Sinha D. *et al.* 2023) proposed an alternative encryption and decryption approach using signed graph matrices combined with the RSA algorithm. Merging graph theory with cryptography increases the level of security (Sinha, D. *et al.* 2016) and also opens up new methods of encrypting complicated data structures, hence making this contribution valuable in the area of secure communications. The authors explained that a matrix representation of a signed graph could be encrypted with the RSA algorithm (Sinha, D. *et al.* 2015), and such a matrix would generate a secure ciphertext that can only be decrypted with the appropriate RSA private key. This method can be further extended to other types of signed graphs (Sinha D. *et al.* 2013 & Sinha D. *et al.* 2014); similarly, the RSA algorithm can be extended to image security through signed graphs.

(Patel A. *et al.* 2023) Reviewed some cryptographic algorithms that use eigenvalue decomposition. The authors have presented a comparative study of various algorithms utilizing matrix diagonalization for encryption and decryption besides discussing the relative strengths and weaknesses of each. Further, the paper has suggested the scope for improvements along with its applications in secure communication.

(Chen, M., *et al.*, 2023) explored the eigenvalue decomposition-based public key encryption schemes. The authors then proposed a new public-key encryption scheme and discussed its security against several cryptographic attacks. They gave the theoretical proof of its security and also the practical implementation details.

Methodology

The implementation of eigenvalues and eigenvectors of signed graphs for encryption and decryption for security purposes through Python programming.

Encryption

Define vertex set consisting of individual letters of a word. By using the encoding table, calculate the difference in weight between two letters that are adjacent to one another. Whenever the weight between two consecutive letters (vertices) is positive, we connect those vertices with the positive edge (edge will have a value of +1); otherwise, it will have a value of -1. Include node 0 as a reference at the very beginning of the graph.

Table 1: Encoding table letters

Letter	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
No. of representation	65	66	67	68	69	70	71	72	73	74	75	76	77
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
No. of representation	78	79	80	81	82	83	84	85	86	87	88	89	90

Encryption Algorithm

- Determine the weight between two adjacent letters using the encoding Table 1.
- If the weight of two adjacent letters is positive, then positive edge otherwise negative edge.
- Include reference node 0 at the top of the graph.
- Find the weight of this reference node with the first letter using the encoding table.
- Calculate the adjacency matrix (M) of the graph.
- Put weights calculated in step 2 on the diagonal of the adjacency matrix (M) to get a matrix A_1.
- Determine the eigenvalues and eigenvectors of A_1.
- Encrypt data using the matrix (Eigenvectors of A_1) K_1.
- Convert encrypted data into a 1-dimensional array.

Decryption

Convert a one-dimensional array into a matrix. Calculations of weights are based on the original, unaltered text. Let's imagine that there is a need to use a hidden key (matrix of eigenvectors) to send the word "ASHU" to the receiver. Calculate the weight differences between letters that are adjacent to one another by using the encoding table. Carry out the transformation of weights into edges with a positive or negative value.

Decryption Algorithm

- Convert the 1-dimensional array into the matrix.
- Compute *M* using K_1^{-1}.
- Compute weights from the diagonal of *M*.
- Get plain text.

Implementation of Encryption–Decryption Algorithm

To encrypt the word "ASHU" and send it to the receiver

Encryption phase

- Calculate weights between two adjacent characters using the encoding table 1. For example, weight between 0A=0-65=-65, AS=65-83=-18, SH=83-72=11, HU=72-85=-13, U0=85-0=85.
- Convert weights into +ve and –ve edges. The edge between A and S will be -ve, while the edge between S and H will be +ve as shown in Figure 1.
- Adjacency matrix (M) calculation

$$M = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

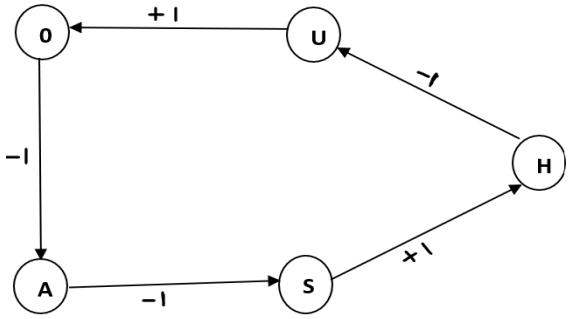

Figure 1: Signed graph

Where the first row corresponds to 0, the second row corresponds to A, and so on.

- Fill the diagonal of the adjacency matrix A with the calculated weights to get W.

$$A_1 = \begin{bmatrix} -65 & -1 & 0 & 0 & 0 \\ 0 & -18 & -1 & 0 & 0 \\ 0 & 0 & 11 & 1 & 0 \\ 0 & 0 & 0 & -13 & -1 \\ 1 & 0 & 0 & 0 & 85 \end{bmatrix}$$

- Determine the eigenvalues and eigenvectors of the matrix 'A_1' and consider it as a secret Key K_1.

$$Spectrum\ of\ A_1 = \{-65, 85, 11, -13, -18\}$$

$$K_1 = \begin{bmatrix} -1.0000 & -0.0000 & 0.0005 & -0.0002 & 0.0213 \\ -0.0000 & 0.0000 & -0.0345 & 0.0083 & -0.9998 \\ -0.0000 & -0.0001 & 0.9994 & -0.0416 & 0.0000 \\ 0.0001 & -0.0102 & 0.0000 & 0.9991 & -0.0000 \\ 0.0067 & 0.9999 & -0.0000 & 0.0000 & -0.0002 \end{bmatrix}$$

- Now encrypt A using this key (K_1)

$$K_1 * M = \begin{bmatrix} 0.0213 & 1.0000 & 0.0000 & 0.0005 & 0.0002 \\ -0.9998 & 0.0000 & -0.0000 & -0.0345 & -0.0083 \\ 0.0000 & 0.0000 & 0.0001 & 0.9994 & 0.0416 \\ -0.0000 & -0.0001 & 0.0102 & 0.0000 & -0.9991 \\ -0.0002 & -0.0067 & -0.9999 & -0.0000 & -0.0000 \end{bmatrix}$$

- Convert this matrix into a one-dimensional array to get encrypted data.

Encrypted Data = [0.0213, -0.9998, 0.0000, -0.0000, -0.0002; -0.9998, 0.0000, -0.0000, -0.0345, -0.0083;0.0000, 0.0000, 0.0001, 0.9994, 0.0416; -0.0000, -0.0001, 0.0102, 0.0000, -0.9991; -0.0002, -0.0067, -0.9999, -0.0000, -0.0000]

- Send encrypted text to the receiver.

Decryption Phase

The receiver receives the encrypted data as well as the key. These are the steps to be followed to decrypt the original text.

- Convert the received data into a matrix. The received array will always form a square matrix.

$$Converted\ Matrix = \begin{bmatrix} 0.0213 & 1.0000 & 0.0000 & 0.0005 & 0.0002 \\ -0.9998 & 0.0000 & -0.0000 & -0.0345 & -0.0083 \\ 0.0000 & 0.0000 & 0.0001 & 0.9994 & 0.0416 \\ -0.0000 & -0.0001 & 0.0102 & 0.0000 & -0.9991 \\ -0.0002 & -0.0067 & -0.9999 & -0.0000 & -0.0000 \end{bmatrix}$$

- Calculate $K^{-1} *$ Converted Mat to get A_1

$$A_1 = \begin{bmatrix} -65 & -1 & 0 & 0 & 0 \\ 0 & -18 & -1 & 0 & 0 \\ 0 & 0 & 11 & 1 & 0 \\ 0 & 0 & 0 & -13 & -1 \\ 1 & 0 & 0 & 0 & 85 \end{bmatrix}$$

- Store diagonal values in D

$$D = [-65, -18, 11, -13, 85]$$

- Fill the diagonal with all 0's to get A

$$M = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- Plotting graph using adjacency matrix

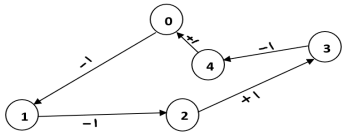

Figure 2: Decrypted graph

- Extract text using the diagonal value *D*.

Since 0 is placed as the reference node, therefore all letters can be retrieved using the formula.

$$v_n = v_{n-1} - D_{n-1}$$

Where $v_0 = 0$ and D_n is the n^{th} diagonal value.

$$v_1 = v_0 - D_0 = 0 - (-65) = 65$$

$$v_2 = v_1 - D_1 = 65 - (-18) = 83$$

$$v_3 = v_2 - D_2 = 83 - (11) = 72$$

$$v_4 = v_3 - D_3 = 72 - (-13) = 85$$

$$v_5 = v_4 - D_4 = 85 - (85) = 0$$

Now convert these values into letters using the encoding table (Table A) and the decrypted text will be 'ASHU'.

Conclusion and Future Scope

In this paper, a word (in upper case) can be encrypted using any programming language like Java and Python. The study of the encryption and decryption of phonetic alphabets using eigenvectors of signed graphs forms a very niche area covering concepts from cryptography, phonetics, linear algebra, and graph theory. Encryption with eigenvectors and signed graphs may open a new security mechanism. The computational difficulty and the resistance of such an approach against common cryptographic attacks, such as brute force and side-channel attacks, may indicate a way to develop robust security algorithms. As the key developed is the matrix with the eigenvectors, the hacker's decoding of the message using the brute force method is practically impossible. Yes, it is. Yet highly improbable. This approach will not work very well if the sentence has many words of comparable meaning.

Acknowledgments

The authors acknowledge The NorthCap University for supporting the conduction of research work.

Conflict of Interest

The authors have no conflict of interest to declare. The authors certify that the submission is the original work and is not under any review for publication.

References

Acharya, M., & Sinha, D. (2006). Common-edge sigraphs. AKCE International Journal of Graphs Combinatorics, 3(2), 115-130.

Biggs, N. (1993). Algebraic Graph Theory. Cambridge University Press.

Cartwright, D. and Harary, F. (1956). Structural balance: a generalization of Heider's theory, Psychological Review, 63(5), 277-293.

Chen, M., & Zheng, F. (2023). A study of eigenvalue-based public key encryption schemes. Journal of Mathematical Cryptography.

Cormen, T., Leiserson C., Rivest R., Stein (2013) Introduction to algorithm, 3rd edn. PHI Learning Private Limited, New Delhi.

Cvetkovic, D., Doob, M., & Sachs, H. (1980). Spectra of Graphs: Theory and Application. Academic Press.

Godsil, C., & Royle, G. (2001). *Algebraic Graph Theory*. Springer.

Gupta, S. & Sharma, T. (2022). Secure communication using eigenvector-based transformations. Computers & Security.

Gutin, G., & Yeo, A. (2014). *Signed Graphs and their Applications*. Springer.

Harary, F. (1953). On the notion of balance of a signed graph. Michigan Mathematical Journal, 2(2), 143-146.

Harary, F. (1969) Graph Theory, Addison-Wesley Publ. Comp, Reading Massachusetts.

Liu, S., Chen, X., & Li, X. (2018). Eigenvalue-based cryptographic schemes for graph-based data. *Journal of Cryptographic Engineering*, 8(1), 1-12.

Liu, J., Wang, X. & Li, L. (2022). Eigenvalue-based encryption for

image data. IEEE Transactions on Image Processing.
Ni, B., Qazi, R., Rehman, S., & Farid, G. (2021). Some graph-based encryption schemes. Journal of Mathematics, 2021(8), Article ID 6614172.
Nisha, S., & Farik, M. (2017). RSA public key cryptography algorithm - A review. International Journal of Scientific and Technology Research, 6(7), 187-191.
Niven, I., & Zuckerman, H.S. (1980). An introduction to the Theory of Numbers. Wiley.
Patel, A., & Kumar, R. (2023). Cryptographic algorithms based on eigenvalue decomposition. International Journal of Cryptography and Security.
Rosen, K. H. (2005). Elementary number theory and its applications. Pearson Addison-Wesley, 5th edition.
Shannon, C.E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656-715.
Sinha, D., Upadhyaya, S., & Kataria, P. (2013). Characterization of common edge signed graphs. Journal Applied Discrete Mathematics, 161, 1275-1285.
Sinha, D., & Sethi, A. (2014). An optimal algorithm to detect balancing in common-edge sigraph. International Journal of Computer Applications, 93(10), 19-25.
Sinha, D. and Sethi, A. (2015). An Optimal Algorithm to Detect Sign Compatibility of a given Sigraph, National Academy of Science Letters, DOI 10.1007/s40009-014-0317-5.
Sinha, D., & Sethi, A. (2016). Encryption using network and matrices through signed graphs. International Journal of Computer Applications, 138(4), 6-13.
Sinha, D., Sethi, A., and Wardak, O. (2023). Encryption and decryption of signed graph matrices through RSA algorithm. Indian Journal of Pure and Applied Mathematics. DOI: 10.1007/s13226-023-00452-9.
Stinson, D. R. (2018). Cryptography: Theory and Practice. Chapman and Hall/CRC, Boca Raton, FL, USA, 4th edition.
West, D.B. (1996) Introduction to graph theory. Prentice-Hall of India Pvt. Ltd, New. Delhi.
Yang, K., & Zhang, H. (2021). Matrix-based encryption using eigenvalues and eigenvectors. Journal of Applied Mathematics and Computing.
Zaslavsky, T. (1998) Glossary of signed and gain graphs and allied areas, II Edition, Electronic J. Combinatorics, #DS9.
Zaslavsky, T. (2009) A mathematical bibliography of signed and gain graphs and allied areas, VIII Edition. Electronic J. Combinatorics, Dynamic Surveys, 233 p, #DS8.
Zaslavsky, T. (2022). Glossary of signed and gain graphs and allied areas. Electronic Journal of Combinatorics.