Computational Algebra, Computational Number Theory and Applications

Extended Abstract Booklet

University of Kashan

Kashan, Iran
December 17-19, 2014

cacna2014@kashanu.ac.ir

cacna2014@gmail.com

University of Kashan

The University of Kashan's KCMR Kashani Center of Mathematical Researches

انجمن علمی نظریه گروه‌های ایران

Iranian Group Theory Society

The Members of Scientific Committee

The Members of Organizing Committee

Jalal Asgari
Ali Reza Ashrafi
Mojtaba Bahramian
Behnam Bazigaran
Hassan Daghigh
Hossein Eshraghi
Gholamhossein Fathtabar
Elham Ghasemian
Reza Jahaninejad
Rohollah Jahanipoor
Reza Kahkeshani
Rasool Kazemi Najafabadi
Ruholla Khodakaramian
Hassan Khodashenas
Fatemeh Koorepazan-Moftakhar
Majid Mazrooei
Akbar Mohebbi
Seyed Seyfollah Mosazadeh
Marzieh Pourbabaee
Asiyeh Rafieipour
Ghodratallah Rahmanimehr
Ali Asghar Rezaei
Abbas Saadatmandi
Mohammad Ali Salahshour
Mohammad Hadi Seiiedinezhaad
Fatemeh Seifi Shahpar
Maryam Sheikhi-Garjan
Zeynab Soltani
Hamid Reza Tabrizi-Doz

Message from the Conference Chairs

It is a pleasure to welcome you to CACNA 2014, the first conference on “Computational Algebra, Computational Group Theory and Applications” at the University of Kashan, IRAN. Over the past 20 years, the Computational Algebra and Computational Number Theory have grown to be one of the main topics of research in our country. The conference is organized as a set of tracks in Computational Group Theory, Computational Number Theory, Cryptography, Coding Theory, Algebraic Combinatorics and Computer Algebra.

There will be also a workshop on Computational Group Theory, Coding Theory and Computational Number Theory for graduate students and those who are working in computational aspects of algebra, number theory and cryptography. Finally, we are honored to have Professors Francesco Belardo, Bijan Davvaz and Saeed Kayvanfar as our keynote speakers and professors Modjtaba Bahramian, Hassan Daghigh, Somayeh Didari, Mohammad Gholami Babadegani, Reza Kahkeshani, Hamid Mousavi and Reza Orfi as workshop speakers.

The successful organization of this conference has required the talents, dedication and time of many volunteers and strong support from the University of Kashan. We hope that you will find the conference both enjoyable and valuable, and also enjoy the architectural, cultural and natural beauty of Kashan, a city with 7000 years history.

CHAIR OF ORGANIZING COMMITTEE: HASSAN DAGHIGH

CHAIR OF ACADEMIC COMMITTEE: ALI REZA ASHRAFI

Content

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), p. 1.

Keynote Speaker

Spectral Theory of Signed Graphs

Francesco Belardo
Department of Mathematics, University of Primorska, Slovenia

Abstract

A signed graph is pair (G,s) where G is a graph and s, the signature, is a function on the edges of G assigning values in $\{1,-1\}$. Similarly to unsigned graphs, it is possible to associate several graph matrices and to study the signed graphs from a spectral viewpoint. Hence, we will show that the spectral theory of signed graphs naturally extend that of unsigned graphs. In particular, we consider the relation between the least eigenvalue of the Laplacian and the frustration of the signed graph; we establish the relation between the Laplacian characteristic polynomial of a signed graph with adjacency characteristic polynomials of its opportunely defined signed line graph and signed subdivision graph; we express the coefficient of the Laplacian characteristic polynomial of (G,s), based on the signed TU-subgraphs. Finally we outline some problems that are a generalization of those considered in spectral (unsigned) graph theory.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 3-5.

Keynote Speaker

On some Old and New Problems in Algebraic Hyperstructures

Bijan Davvaz
Department of Mathematics, Yazd University, Yazd, Iran
davvaz@yazd.ac.ir

Abstract

The overall aim of this paper is to present an introduction to some of the old and new subjects and problems in algebraic hyperstructures.

Keywords: Hypergroup, polygroup, H_v-group, n-ary hypergroup.

MSC(2010): Primary: 20N20.

1 Introduction

The concept of a hypergroup which is a generalization of the concept of a group, first was introduced by Marty. Indeed, hypergroups represent a natural extension of groups. In a group, the composition of two elements is an element, while in a hypergroup, the composition of two elements is a set. Application of hypergroups have mainly appeared in special subclasses. For example, polygroups which are certain subclass of hypergroups are used to study color algebra and combinatorics. Moreover, there exist two generalization of hypergroups. The concept of an H_v-group as an extension of hypergroups was introduce by Vougiouklis. Recently, research about n-ary hypergroups has been initiated by Davvaz and Vougiouklis, who introduced these structures. The concept of n-ary hypergroups is a generalization of hypergroups in the sense of Marty. Also, we can consider n-ary hypergroups as a nice generalization of n-ary groups. Many papers and several books have been written till now on algebraic hyperstructures [2, 3, 4, 15, 22]. Many of them are dedicated to the applications of hyperstructures in other disciplines. The overall aim of this paper is to present an introduction to some of the old and new subjects and problems in algebraic hyperstructures.

2 Main Subjects

In this section, we review:

(1) Hypergroups [2, 3, 4, 15];

(2) Polygroups [4];

(3) H_v-groups [5, 22];

(4) n-ary hypergroups [16, 13, 13, 20];

(5) Enumeration of hyperstructures on small sets [1, 21];

(6) Ordered semihypergroups [6];

(7) Examples of hyperstructures associated with Chemistry, Biology and Physics [7, 8, 9, 10, 11, 12, 17, 18].

References

[1] H. Aghabozorgi, M. Jafarpour and B. Davvaz, *Enumeration of Varlet and Comer hypergroups*, The Electronic Journal of Combinatorics **18** (2011), #P131.

[2] P. Corsini, Prolegomena of Hypergroup Theory, Second edition, Aviani Editore, (1993).

[3] P. Corsini and V. Leoreanu, Applications of Hyperstructures Theory, Advances in Mathematics, Kluwer Academic Publisher, (2003).

[4] B. Davvaz, Polygroup Theory and Related Systems, World Scientific, (2013).

[5] B. Davvaz, *A brief survey of the theory of H_v-structures*, Proc. 8^{th} International Congress on Algebraic Hyperstructures and Applications, 1-9 Sep., 2002, Samothraki, Greece, Spanidis Press, (2003) 39-70.

[6] B. Davvaz, P. Corsini and T. Changphas, *Relationship between ordered semihypergroups and ordered semigroups by using pseuoorders*, European J. Combinatorics **44** (2015), 208-217.

[7] B. Davvaz, A. Dehghan Nezhad and A. Benvidi, *Chemical hyperalgebra: Dismutation reactions*, MATCH Communications in Mathematical and in Computer Chemistry **67** (2012), 55-63.

[8] B. Davvaz, A. Dehghan Nezad and A. Benvidi, *Chain reactions as experimental examples of ternary algebraic hyperstructures*, MATCH Communications in Mathematical and in Computer Chemistry **65** (2011), 491-499.

[9] B. Davvaz and A. Dehghan Nezhad, *Dismutation reactions as experimental verifications of ternary algebraic hyperstructures*, MATCH Communications in Mathematical and in Computer Chemistry **68** (2012), 551-559.

[10] B. Davvaz, A. Dehghan Nezad and M. M. Heidari, *Inheritance examples of algebraic hyperstructures*, Information Sciences **224** (2013), 180-187.

[11] B. Davvaz, A. Dehghan Nezad and M. Mazloum-Ardakani, *Chemical hyperalgebra: Redox reactions*, MATCH Communications in Mathematical and in Computer Chemistry **71** (2014), 323-331.

[12] B. Davvaz, A. Dehghan Nezad and M. Mazloum-Ardakani, *Describing the algebraic hyperstructure of all elements in radiolytic processes in cement medium*, MATCH Commun. Math. Comput. Chem. **72(2)** (2014), 375-388.

[13] B. Davvaz, W.A. Dudek and S. Mirvakili, *Neutral elements, fundamental relations and n-ary hypersemigroups*, International Journal of Algebra and Computation **19** (2009), 567583.

[14] B. Davvaz, W.A. Dudek and T. Vougiouklis, *A Generalization of n-ary algebraic systems*, Communications in Algebra **37** (2009), 1248-1263.

[15] B. Davvaz and V. Leoreanu-Fotea, *Hyperring Theory and Applications*, International Academic Press, USA, (2007).

[16] B. Davvaz and T. Vougiouklis, *n-Ary hypergroups*, Iranian Journal of Science and Technology, Transaction A **30 (A2)** (2006), 165-174.

[17] A. Dehghan Nezhad, S.M. Moosavi Nejad, M. Nadjafikhah and B. Davvaz, *A physical example of algebraic hyperstructures: Leptons*, Indian Journal of Physics **86(11)** (2012), 1027-1032.

[18] M. Ghadiri, B. Davvaz and R. Nekouian, *H_v-Semigroup structure on F_2-offspring of a gene pool*, International Journal of Biomathematics **5(4)** (2012) 1250011 (13 pages).

[19] D. Heidari and B. Davvaz, *On ordered hyperstructures*, UPB Scientific Bulletin, Series A: Applied Mathematics and Physics **73(2)** (2011), 85-96.

[20] S. Mirvakili and B. Davvaz, *Application of fundamental relations on n-ary Polygroups*, Bulletin of the Iranian Mathematical Society **38** (2012), 169-184.

[21] M. B. Safari, B. Davvaz and V. Leoreanu-Fotea, *Enumeration of 3- and 4-hypergroups on sets with two elements*, European J. Combinatorics **44** (2015), 298-306.

[22] T. Vougiouklis, Hyperstructures and Their Representations, Hadronic Press, Inc, 115, Palm Harber, USA, (1994).

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp:7-8.

Keynote Speaker

Can Pairs of Groups Help the Classification of Groups?

Saeed Kayvanfar
Department of Pure Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran
skayvanf@math.um.ac.ir & skayvanf@yahoo.com

Abstract

P. Hall introduced the notion of isoclinism in order to classify groups of prime power order. The notion of isoclinism can be simulated for pairs (G,N) of groups, in which G is a group and N is a normal subgroup. This talk verifies the classification of some pairs of groups, when N is to be chosen a suitable subgroup. Then using this, we explain how this classification can be considered as the first step of screening for classification of some classes of groups.

Keywords: Pairs of groups, isoclinism, classification of groups.

MSC(2010): Primary: 20D15; Secondary: 20E99, 20D60.

References

[1] G. Ellis, *Capability, homology, and central series of a pair of groups*, J. Algebra **179** (1996), 31–46.

[2] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141.

[3] M. Hassanzadeh, A. Pourmirzaei, S. Kayvanfar, *On the nilpotency of a pair of groups*, Southeast Asian Bulletin of Mathematics **37** (2013), 67–77.

[4] N.S. Hekster, *On the structure of n-isoclinism classes of groups*, J. Pure and Applied Algebra **40** (1986), 63–85.

[5] A. Kaheni, *On the classification of some pairs of p-groups (By an analytical approach in Philip Hall's classification)*, Ph.D. Thesis, Ferdowsi Univ. of Mashhad, 2012.

[6] A. Pourmirzaei, A. Hokmabadi, S. Kayvanfar, *On the capability of a pair of groups*, Bull. Malays. Math. Sci. Soc. **2** (2011), 205-213.

[7] A.R. Salemkar, F. Saeedi, T. Karimi, *The structure of isoclinism classes of pair of groups*, Southeast Asian Bulletin of Math. **31** (2007), 1173–1181.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp:9-10.

Oral Presentation

Finite Semi-Rational Groups: Solvable and non-Solvable

Seyed Hassan Alavi
Department of Mathematics, Bu-Ali Sina University, Hamedan, Iran
alavi.s.hassan@gmail.com

Abstract

In this talk, we give a survey of some recent advances on the problem of studying semi-rational finite groups.

Keywords: Semi-rational groups, solvable groups, non-solvable groups.

MSC(2010): Primary 20E45; Secondary 20E34.

Let G be a finite group. An element x of a finite group G is called *rational* if all generators of the group $\langle x\rangle$ are conjugate in G. If all elements of G are rational, then G itself is called *rational*. It was proved by Gow [6] that if G is a rational solvable group then $\pi(|G|)\subseteq\{2,3,5\}$.

The notion of rational elements and rational groups has been generalised by Chillag and Dolfi [3]. An element $x\in G$ is called *k-semi-rational* if the generators of $\langle x\rangle$ belongs to at most k conjugacy classes of G. The group G is said to be *k-semi-rational* if all its elements are k-semi-rational in G. In particular, a 2-semi-rational group is called *semi-rational* and its elements are called *semi-rational*. Chillag and Dolfi extended Gow's result to semi-rational groups and proved that $\pi(G)\subseteq\{2,3,5,7,13,17\}$ when G is a semi-rational solvable group. They also posed the following problem:

Problem 1. [3, Problem 2] *Let G be a solvable group, and let k be a positive integer. If G is a k-semi-rational, then is $\pi(|G|)$ bounded in terms of k?*

Motivated by [4], we studied semi-rational Frobenius groups in [1]. We indeed answered Problem 1 for Frobenius groups G and showed that $|\pi(G)|\leqslant 4$. In the case where G is a non-solvable Frobenius group, we have proved that $|\pi(G)|\leqslant 11$.

In general, composition factors of rational group studied by Feit and Seitz [5], in particular, they determined all simple rational groups. In this direction, for semi-rational groups, Alavi, Burness and Daneshkhah [2] studied semi-rational almost simple groups.

References

[1] S. H. Alavi, A. Daneshkhah, M. R. Darafsheh, *On Frobenius semi-rational groups*, Submitted.

[2] S. H. Alavi, T. Burness, A. Daneshkhah, *On composition factors of semi-rational groups*, In preparation.

[3] D. Chillag, S. Dolfi, *Semi-rational solvable groups*, J. Group Theory, **13** n. 4 (2010), pp. 535–548.

[4] M. R. Darafsheh, H. Sharifi, *Frobenius $\mathbb{Q}$-groups*, Arch. Math. (Basel), **83** n.2 (2004), pp. 102–105.

[5] W. Feit and G. M. Seitz. On finite rational groups and related topics. *Illinois J. Math.*, 33(1):103–131, 1989.

[6] R. Gow. *Groups whose characters are rational-valued*, J. Algebra **40** (1976), 280-299.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 11-15.

Oral Presentation

On the Randić Characteristic Polynomial of Specific Graphs

Saeid Alikhani
Department of Mathematics, Yazd University, 89195-741, Yazd, Iran
alikhani@yazd.ac.ir

Nima Ghanbari
Department of Mathematics, Yazd University, 89195-741, Yazd, Iran
n.ghanbari@stu.yazd.ac.ir

Abstract

Let G be a simple graph with vertex set $V(G) = \{v_1, v_2, \ldots, v_n\}$. The Randić matrix of G, denoted by $R(G)$, is defined as the $n \times n$ matrix whose (i, j)-entry is $(d_i d_j)^{\frac{-1}{2}}$ if v_i and v_j are adjacent and 0 for another cases. Let the eigenvalues of the Randić matrix $R(G)$ be $\rho_1 \geq \rho_2 \geq \ldots \geq \rho_n$ which are the roots of the Randić characteristic polynomial $\prod_{i=1}^{n}(\rho - \rho_i)$. The Randić energy RE of G is the sum of absolute values of the eigenvalues of $R(G)$. In this paper we compute the Randić characteristic polynomial and the Randić energy for specific graphs G.

Keywords: Randić matrix; Randić energy; Randić characteristic polynomial; eigenvalues.

MSC(2010): Primary: 15A18.

1 Introduction

In this paper we are concerned with simple finite graphs, without directed, multiple, or weighted edges, and without self-loops. Let G be such a graph, with vertex set $V(G) = \{v_1, v_2, \ldots, v_n\}$. If two vertices v_i and v_j of G are adjacent, then we use the notation $v_i \sim v_j$. For $v_i \in V(G)$, the degree of the vertex v_i, denoted by d_i, is the number of the vertices adjacent to v_i.

Let $A(G)$ be adjacency matrix of G and $\lambda_1, \lambda_2, \ldots, \lambda_n$ its eigenvalues. These are said to be the eigenvalues of the graph G and to form its spectrum [1]. The energy $E(G)$ of the graph G is defined as the sum of the absolute values of its eigenvalues

$$E(G) = \sum_{i=1}^{n} |\lambda_i|.$$

Details and more information on graph energy can be found in [3, 4, 5, 6].
In 1975 Milan Randić invented a molecular structure descriptor defined as [7]

$$R(G) = \sum_{v_i \sim v_j} \frac{1}{\sqrt{d_i d_j}}.$$

The Randić-index-concept suggests that it is purposeful to associate to the graph G a symmetric square matrix $R(G)$. The Randić matrix $R(G) = (r_{ij})_{n\times n}$ is defined as [8, 9, 10]

$$r_{ij} = \begin{cases} \frac{1}{\sqrt{d_i d_j}} & \text{if } v_i \sim v_j \\ 0 & \text{otherwise.} \end{cases}$$

Denote the eigenvalues of the Randić matrix $R(G)$ by $\rho_1, \rho_2, \ldots, \rho_n$ and label them in non-increasing order. Similar to characteristic polynomial of a matrix, we consider the Randić characteristic polynomial of $R(G)$ (or a graph G), as $det(\rho I - R(G))$ which is equal to $\prod_{i=1}^{n}(\rho - \rho_i)$. The Randić energy [8, 9, 10] of G is defined as

$$RE(G) = \sum_{i=1}^{n} |\rho_i|.$$

For several lower and upper bounds on Randić energy, see [8, 9, 10].
In this paper, we obtain the Randić characteristic polynomial and energy of specific graphs. As a result, we show that for every natural number $m \geq 2$, there exists a graph G such that $RE(G) = m$.

2 Main Results

In this section we study the Randić characteristic polynomial and the Randić energy for certain graphs. The following theorem gives a relationship between the Randić energy and energy of path P_n.

Lemma 2.1. [10] Let P_n be the path on n vertices. Then

$$RE(P_n) = 2 + \frac{1}{2}E(P_{n-2}).$$

The following theorem gives the Randić energy of even cycles.

Lemma 2.2. [11] Let C_{2n} be the cycle on $2n$ vertices for $n \geq 2$. Then

$$RE(C_{2n}) = \frac{2sin((\lfloor \frac{n}{2} \rfloor + \frac{1}{2})\frac{\pi}{n})}{sin\frac{\pi}{2n}}.$$

Here we shall compute the Randić characteristic polynomial of paths and cycles.

Theorem 2.1. *For $n \geq 5$, the Randić characteristic polynomial of the path graph P_n satisfy*

$$RP(P_n,\lambda) = (\lambda^2 - 1)(\lambda\Lambda_{n-3} - \frac{1}{4}\Lambda_{n-4}),$$

where for every $k \geq 3$, $\Lambda_k = \lambda\Lambda_{k-1} - \frac{1}{4}\Lambda_{k-2}$ with $\Lambda_1 = \lambda$ and $\Lambda_2 = \lambda^2 - \frac{1}{4}$.

Theorem 2.2. *For $n \geq 3$, the Randić characteristic polynomial of the cycle graph C_n is*

$$RP(C_n,\lambda) = \lambda\Lambda_{n-1} - \frac{1}{2}\Lambda_{n-2} - (\frac{1}{2})^{n-1},$$

where for every $k \geq 3$, $\Lambda_k = \lambda\Lambda_{k-1} - \frac{1}{4}\Lambda_{k-2}$ with $\Lambda_1 = \lambda$ and $\Lambda_2 = \lambda^2 - \frac{1}{4}$.

Theorem 2.3. *For $n \geq 2$,*

(i) The Randić characteristic polynomial of the star graph $S_n = K_{1,n-1}$ is

$$RP(S_n,\lambda) = \lambda^{n-2}(\lambda^2 - 1).$$

(ii) The Randić energy of S_n is

$$RE(S_n) = 2.$$

Theorem 2.4. *For $n \geq 2$,*

(i) the Randić characteristic polynomial of complete graph K_n is

$$RP(K_n,\lambda) = (\lambda - 1)(\lambda + \frac{1}{n-1})^{n-1}.$$

(ii) the Randić energy of K_n is

$$RE(K_n) = 2.$$

Theorem 2.5. *For natural number $m,n \neq 1$,*

(i) The Randić characteristic polynomial of complete bipartite graph $K_{m,n}$ is

$$RP(K_{m,n},\lambda) = \lambda^{m+n-2}(\lambda^2 - 1).$$

(ii) The Randić energy of $K_{m,n}$ is

$$RE(K_{m,n}) = 2.$$

Let n be any positive integer and F_n be friendship graph with $2n+1$ vertices and $3n$ edges. In other words, the friendship graph F_n is a graph that can be constructed by coalescence n copies of the cycle graph C_3 of length 3 with a common vertex. The Friendship Theorem of Erdős, Rényi and Sós [2], states that graphs with the property that every two vertices have exactly one neighbour in common are exactly the friendship graphs. The Figure 1 shows some examples of friendship graphs. Here we shall investigate the Randić energy of friendship graphs.

Theorem 2.6. *For $n \geq 2$,*

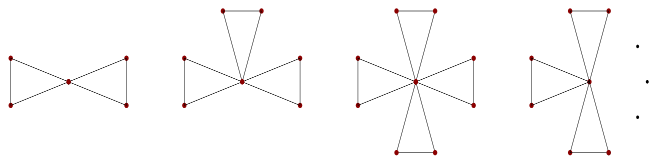


Figure 1: Friendship graphs F_2, F_3, F_4 and F_n, respectively.

(i) The Randić characteristic polynomial of friendship graph F_n is

$$RP(F_n, \lambda) = (\lambda^2 - \frac{1}{4})^{n-1}(\lambda - 1)(\lambda + \frac{1}{2})^2.$$

(ii) The Randić energy of F_n is

$$RE(F_n) = n+1.$$

Remark. In [12] has shown that the energy of a graph cannot be an odd integer. Since $RE(F_n) = n+1$ for $n \geq 2$, the Randić energy can be odd or even integer. More precisely we have:

Corollary 2.1. *For every natural number $m \geq 2$, there exists a graph G such that $RE(G) = m$.*

Let n be any positive integer and D_4^n be Dutch Windmill graph with $3n+1$ vertices and $4n$ edges. In other words, the graph D_4^n is a graph that can be constructed by coalescence n copies of the cycle graph C_4 of length 4 with a common vertex. The Figure 2 shows some examples of Dutch Windmill graphs. Here we shall investigate the Randić energy of Dutch Windmill graphs.

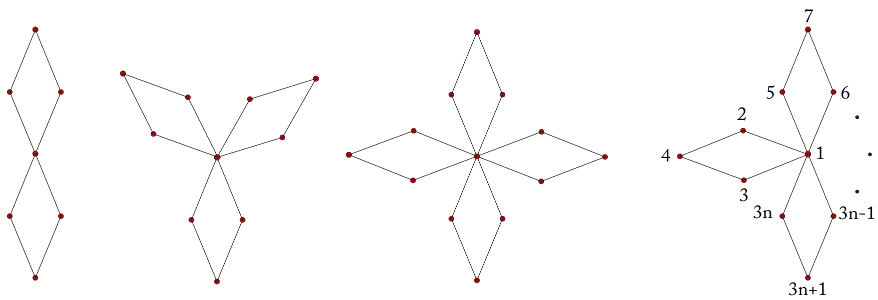


Figure 2: Dutch Windmill Graph D_4^2, D_4^3, D_4^4 and D_4^n, respectively.

Theorem 2.7. *For $n \geq 2$,*

(i) The Randić characteristic polynomial of friendship graph D_4^n is

$$RP(D_4^n, \lambda) = \lambda^{n+1}(\lambda^2 - \frac{1}{2})^{n-1}(\lambda^2 - 1).$$

(ii) The Randić energy of F_n is

$$RE(D_4^n) = 2 + (n-1)\sqrt{2}.$$

References

[1] D. Cvetković, M. Doob, H. sachs, *Spectra of graphs* - Theory and Aplication, Academic Press, New York, 1980.

[2] P. Erdös, A. Rényi, V.T. Sós, *On a problem of graph theory*, Studia Sci. Math. Hungar., 1, 215–235 (1966).

[3] I. Gutman, The energy of a graph: Old and new results, in: A. Betten, A.Kohnert, R. Laue, A. Wassermannn (Eds.), *Algebraic Combinatorics and Applications*, Springer-Verlag, Berlin, 2001, pp. 196–211.

[4] I. Gutman, Topology and stability of conjugated hydrocarbons. The dependence of total π-electron energy on molecular topology, *J. Serb. Chem. Soc.* 70 (2005) 441–456.

[5] I. Gutman, X. Li, J. Zhang, Graph energy, in: M. Dehmer, F. Emmert-Streib (Eds.), *Analysis of Complex Networks. From Biology to Linguistics*, Wiley-VCH, Weinheim, 2009, pp. 145–174.

[6] S. Majstorović, A. Klobucar, I. Gutman, Selected topics from the theory of graph energy: hypoenergetic graphs, in: D. Cvetković, I. Gutman (Eds.), *Applications of Graph Spectra*, Math. Inst., Belgrade, 2009, pp. 65–105.

[7] M. Randić, On characterization of molecular branching, *J. Amer. Chem. Soc*. 97 (1975) 6609–6615.

[8] Ş. B. Bozkurt, A. D. Güngör, I. Gutman, A. S. Çevik, Randić matrix and Randić energy, *MATCH Commum. Math. Comput. Chem*. 64 (2010) 239–250.

[9] Ş. B. Bozkurt, A. D. Güngör, I. Gutman, Randić spectral radius and Randić energy, *MATCH Commum. Math. Comput. Chem*. 64 (2010) 321–334.

[10] I. Gutman, B. Furtula, Ş. B. Bozkurt, On Randić energy, *Lin. Algebra Appl.*, 442 (2014) 50–57.

[11] O. Rojo, L. Medina, Construction of bipartite graphs having the same Randić energy, *MATCH Commun. Math. Comput. Chem.* 68 (2012) 805–814.

[12] R. B. Bapat, S. Pati, Energy of a graph is never an odd integer, *Bull. Kerala Math. Assoc.*, 1 (2004), 129–132.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 17-18.

Poster Presentation

Distance Magic and Barycentric Magic Graphs

Saeid Alikhani
Department of Mathematics, Yazd University, 89195-741, Yazd, Iran
alikhani@yazd.ac.ir

Abstract

In this talk we consider and study properties of two kind of magic graphs. The first kind is distance magic graphs and the second one is barycentric magic graphs.

Keywords: Distance magic, Barycentric magic, labeling.

MSC(2010): Primary: 05C15; Secondary: 05C78.

1 Introduction

Let $G = (V,E)$ be a finite, simple and undirected graph. A labeling for a graph is a map that takes graph elements to numbers (usually positive or non-negative integers).
The concept of distance magic labeling of a graph has been motivated by the construction of magic squares. A magic square of side n is an $n \times n$ array whose entries are an arrangement of the integers $\{1,2,...,n^2\}$ in which all elements in any row, any column, or either the main diagonal or main back-diagonal, add to the same sum r. Now if we take a complete n partite graph with parts $V_1,V_2,...,V_n$ with $|V_i| = n$, $1 \leq i \leq n$ and label the vertices of V_i with the integers in the ith row of the magic square, we find that the sum of the labels of all the vertices in the neighborhood of each vertex is the same and is equal to $r(n-1)$. Motivated by this observation in 1994 Vilfred [7] in his doctoral thesis introduced the concept of sigma labelings. The same concept was introduced by Miller et al. [5] under the name 1-vertex magic vertex labeling. Sugeng et al. [6] introduced the term distance magic labeling for this concept. We use the term distance magic labeling.

Distance magic labeling of G of order n is a bijection $f : V \to \{1,2,...,n\}$ with the property that there is a positive integer k such that $\sum_{y\in N(x)} f(y) = k$ for every $x \in V$. The constant k is called the magic constant of the labeling f. The sum $\sum_{y\in N(x)} f(y)$ is called the weight of the vertex x and is denoted by $w(x)$.

Now we consider another kind of magic graphs.
Let A be an abelian group (written additively). The graph G is called A-magic if there exists a labeling $l : E(G) \to A \setminus \{0\}$ such that for each vertex v, the sum of values of all edges incident with v, denoted by $l^+(v)$, is a constant, that is, $l^+(v) = c$, for some $c \in A$. When this constant is 0, G is said to be A-zero-sum magic. The integer-magic spectrum of a graph G is the set $IM(G) = \{k \in \mathbb{N}$: G is $\mathbb{Z}_k$-magic$\}$.
If there exists a labeling l for a graph G, whose induced vertex set labeling is a constant map and for all $v \in V(G)$ the sum $l^+(v)$ also satisfies $l^+(v) = deg(v)l(u_v v)$ for some vertex u_v adjacent to v, G is said to be A-barycentric-magic [1].
Note that the motivation of this definition is the following definition of k-barycentric sequence which was introduced in [2] and has already been used in graph labeling problems, specially in Ramsey theory [2, 3, 4].

Definition 1.1. *Let $x_1, x_2, \ldots, x_k$ be k elements of an abelian group A. This sequence is k-barycentric if there exists j such that $x_1 + x_2 + \ldots + x_j + \ldots + x_k = kx_j$. The element x_j is called a barycenter.*

In this paper we study the properties of graphs which are distance magic. Also for some graphs G, we characterize all $m \in \mathbb{N}$ for which G is $\mathbb{Z}_m$-barycentric-magic.

References

[1] S. Alikhani and Z. Amirzadeh, *On the barycentric labeling of certain graphs*, J. Discrete Math. Volume 2014, Article ID 482635, 4 pages.

[2] C. Delorme, S. González, O. Ordaz, M.T. Varela, *Barycentric sequences and barycentric ramsey numbers stars*, Discrete Math., 277 (2004), 45-56.

[3] C. Delorme, I. Marquez, O. Ordaz, A. Ortuño, *Existence conditions for barycentric sequences*, Discrete Math., 281 (2004), 163-172.

[4] S. González, L. González, O. Ordaz, *Barycentric Ramsey numbers for small graphs*, Bull. Malay. Math. Sci. Soc., (2)32(1) (2009), 1-17.

[5] M. Miller, C. Rodger and R. Simanjuntak, *Distance magic labelings of graphs*, Australas. J. Combin., 28(2003), 305–315.

[6] K.A. Sugeng, D. Froncek, M. Miller, J. Ryan and J. Walker, *On distance magic labeling of graphs*, J. Combin. Math. Combin. Comput., 71(2009), 39–48.

[7] V. Vilfred, $\sum$-labelled graph and Circulant Graphs, Ph.D. Thesis, University of Kerala, Trivandrum, India, 1994.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 19-22.

Oral Presentation

Recognition of some Symmetric Groups by nse

B. Asadian
Faculty of Mathematical Sciences, University of Shahrekord
asadian.bahare@gmail.com

S. Heydari
Faculty of Mathematical Sciences, University of Shahrekord
heydarisomaye@yahoo.com

N. Ahanjideh
Faculty of Mathematical Sciences, University of Shahrekord
ahanjideh.neda@sci.sku.ac.ir

Abstract

For a finite group G, let $\pi_e(G)$ be the set of element orders of G and $m_i(G)$ be the set of elements of G of order i. Let $\mathrm{nse}(G) = \{m_i(G) : i \in \pi_e(G)\}$. In this paper, we prove that if G is a finite group and $p \geq 5$ is a prime number such that $p \mid |G|$ but $p^2 \nmid |G|$, $n \in \{p, p+1\}$ and $\mathrm{nse}(G) = \mathrm{nse}(S_n)$, then $G \cong S_n$.

Keywords: Set of elements of the same order, prime graph.

MSC(2010): Primary: 20D06; Secondary: 20D15.

1 Introduction

If n is a natural number, then we denote by $\pi(n)$, the set of prime divisors of n. For a finite group G, let $\pi(G)$ be $\pi(|G|)$. Also, we use the notation $\pi_e(G)$ for the set of element orders of G. Suppose that $m_i = m_i(G) = |\{g \in G|$ the order of G is $i\}|$ and $nse(G) = \{m_i | i \in \pi_e(G)\}$. It is clear that if

$n \in \pi_e(G)$, then $m_n = \phi(n)k$, where k is the number of cyclic subgroups of order n in G and ϕ is the Euler's function, Also $\phi(n)|m_n$. The prime graph $GK(G)$ of G is the graph with vertex set $\pi(G)$, where two distinct primes r and s are joined by an edge, if G contains an element of order rs. The set of connected components of $GK(G)$ is denoted by $\pi_1(G), \pi_2(G), ..., \pi_{t(G)}(G)$, which $t(G)$ is the number of connected components of $GK(G)$. If $2 \in \pi(G)$, we always assume that $2 \in \pi_1(G)$. If $\{k_1, ..., k_{t(G)}\}$ is the coprime factors set of $|G|$, where $\pi(k_i) = \pi_i$, then this set is called the set of order components of G and is denoted by $OC(G)$. The sets of order components of finite simple groups with disconnected prime graph can be obtained using [7]. We show every p-Sylow subgroup of G by $S_p(G)$ and set $n_p(G) = |\mathrm{Syl}_p(G)|$. In 1987, J. G. Thompson posed a very interesting problem related to algebraic number fields as follows:
Thompson's Problem. Let $T(G) = \{(n, m_n) \mid n \in \pi_e(G) \text{ and } m_n \in nse(G)\}$. Suppose that for some (finite) group H, $T(G) = T(H)$. If G is a finite solvable group, is it true that H is also necessarily solvable?
This question in some case is answered, but the perfect answer to it has not ever seen. In [1, 5], the authors showed that some alternating groups are characterizable by the set nse in the class of finite groups. Also, in [3], the author proved that $PGL_2(p)$ is characterizable by the set nse in the class of finite groups which their orders are divisible by p but p^2 does not divide their orders. The goal of this paper is to prove the following theorem:
Main Theorem. Let G be a finite group and $p \in \pi(G)$, where $p \geq 5$ and $n \in \{p, p+1\}$. If $p^2 \nmid |G|$ and $\mathrm{nse}(G) = \mathrm{nse}(S_n)$, then $G \cong S_n$.

In the following, we bring some lemmas, which is used in the proof of the main theorem.

Lemma 1.1. [2] *Let G be a finite group and m be a positive integer dividing $|G|$. Also, $L_m(G) = \{g \in G | g^m = 1\}$. Then $m||L_m(G)|$.*

Lemma 1.2. (1)[4, Lemma 1] *If $n \geq 6$ is a natural number, then there are at least $s(n)$ prime numbers p_i such that $(n+1)/2 < p_i < n$ such that*
$s(n) = 6$, for $n \geq 48$;
$s(n) = 5$, for $42 \leq n \leq 47$;
$s(n) = 4$, for $38 \leq n \leq 41$;
$s(n) = 3$, for $18 \leq n \leq 37$;
$s(n) = 2$, for $14 \leq n \leq 17$;
$s(n) = 1$, for $6 \leq n \leq 13$.
(2)[4, Lemma 6(c)] *Let S be a finite simple group of Lie type with $t(S) \geq 2$ and there exist $2 \leq i \leq t(S)$ such that $k_i(S) = p$. If $S \ncong {}^2G_2(q)$, then for every $1 \leq j \leq t(S)$ $(j \neq i)$, there exists at most one prime number $s \in \pi_j(S)$ such that $(p+1)/2 < s < p$. If $S \cong {}^2G_2(q)$, then there exist at most three prime numbers $s \in \pi(G)$ such that $(p+1)/2 < s < p$.*

Lemma 1.3. [6] *The number of Sylow subgroups of order p^m in the Symmetric group of degree n is $\frac{n!}{a_0!a_1!...a_k!p^m(p-1)^m}$, where $n = a_0 + a_1 p + a_2 p^2 + ... + a_k p^k$.*

Corollary 1.1. *If $n \in \{p, p+1\}$, then*

$$m_p(S_n) = \begin{cases} (p-1)! & \text{if } n = p \\ (p+1)(p-1)! & \text{if } n = p+1 \end{cases}$$

2 Main Results

In this section, by applying the method in [1] for S_n, we complete the proof of the main theorem. First note that if σ is a permutation, which its product to disjoint cycles is composed of t_1 cycle of length 1, t_2 cycle of length 2,...,t_l cycle of length l, then $|cl_{S_n}(\sigma)| = \frac{n!}{2^{t_2}3^{t_3}\ldots l^{t_l}t_1!t_2!\ldots t_l!}$. Thus by the fact that for every $s \in \pi_e(S_n)$, $m_s(S_n) = \sum_{O(x_k)=s} |cl_{S_n}(x_k)|$, where x_ks are selected from dintict conjugacy classes. Note that G is a finite group, $p \geq 5$ is a prime number such that $p \mid |G|$ but $p^2 \nmid |G|$, $n \in \{p, p+1\}$ and $\mathrm{nse}(G) = \mathrm{nse}(S_n)$. We emphasize that the proof of Lemmas 2.1 to 2.11 are same with those of given in [1].

Lemma 2.1. *For every $s \in \pi_e(S_n) - \{1\}$, $p \nmid m_s(S_n)$ if and only if $s = p$. In particular, if $s \neq p$, then $p \parallel m_s(S_n)$.*

Lemma 2.2. $m_p(G) = m_p(S_n)$.

Lemma 2.3. *If $s \in \pi_e(G)$ such that $p \nmid m_s(G)$, then $m_s(G) = m_p(G)$.*

Lemma 2.4. *For every $s \in \pi(G) - \{2\}$, $2 \mid m_s(G)$. Also, $2 \in \pi(G)$ and $m_2(G) = m_2(S_n)$.*

Lemma 2.5. $|S_p(G)| = p$.

Lemma 2.6. *For every $s \in \pi(G) - \{p\}$, $sp \notin \pi_e(G)$.*
From the previous lemma, we can conclude that $t(G) \geq 2$ and there exists $2 \leq j \leq t(G)$ such that $k_j(G) = p$.

Lemma 2.7. *$\pi(G) = \pi(S_n)$ and $|G| \mid |S_n|$. In particular, $n_p(S_n) \mid |G|$.*

Lemma 2.8. *G is neither a Frobenius group nor a 2-Frobenius group.*
As was stated before, $t(G) \geq 2$ and there exists $2 \leq j \leq t(G)$ such that $k_j(G) = p$.

Lemma 2.9. *$t(G) \geq 2$ and G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that*
(1) *H is nilpotent;*
(2) *$\pi(H) \cup \pi(G/K) \subseteq \pi_1$;*
(3) *K/H is a non-abelian simple group;*
(4) *$G/K \leq \mathrm{Out}(K/H)$;*
(5) *the odd order components of G are the odd order components of K/H. In particular, $p \in OC(K/H) - \{k_1\}$.*

Lemma 2.10. *Let $t \in \pi(G) - \{p\}$. If $|H|_t = t^i$, then $p | t^i - 1$.*

Lemma 2.11. *If $t \in \pi(G) \cup \pi(G/K)$, then $t < (p+1)/2$. Forthermore, $\{t \mid (p+1)/2 \leq t \leq p$ and t is prime$\} \subseteq \pi(K/H)$.*
Now Lemma 2.7 and the above lemma show that p is a maximal prime divisor of K/H.

Lemma 2.12. *K/H is not isomorphic to any sporadic simple group.*
Sketch of the proof. *On the contrary, suppose that K/H is isomorphic to a sporadic simple group. As was stated before, p is a maximal prime divisor of K/H. First let $K/H \cong M_{22}$. Then $p = 11$. By applying Lemma 2.7 and Lemma 2.9(4), we can see $|H|_3 = 3^2$. Hence, Lemma 2.10 yields $11 \mid 3^2 - 1$, which is impossible. In other cases, we can get a contradiction with Lemmas 2.7, 2.9 or 2.11.*

Lemma 2.13. *K/H is not isomorphic to any finite simple group of Lie type.*
Sketch of the proof. *On the contrary, suppose that K/H is isomorphic to a finite simple group of Lie type. Frist define two sets that during our proof are used. For a finite group T, define $\alpha_p(T) = \{t \in \pi(T) \mid (p+1)/2 < t < p\}$ and for a natural number m, $\beta(m) = |\{t \mid t \text{ is prime and } (m+1)/2 < t < m\}|$. Let $K/H \cong {}^2G_2(q)$, where $q = 3^{2m+1} > 3$, then by Lemmas 1.2 and 2.9(5), we have $\alpha_p(K/H) \leq 3$. Also, Lemmas 2.7 and 2.11 imply that $\beta(p) = \alpha_p(K/H)$ and hence, $\beta(p) \leq 3$. Hence, Lemma 1.2(1) forces $p \leq 37$. Lemma 2.9(5) shows either $q+\sqrt{3q}+1 = p$ or $q-\sqrt{3q}+1 = p$ and hence, $q = 27$ or $p = 37$. Since $29 \notin \pi(G)$, we get a contradiction with Lemma 2.11. In other cases, we can get a contradiction with Lemma 2.7 or Lemma 2.11.*
Main Theorem. *Let G be a finite group and $p \in \pi(G)$, where $p \geq 5$ and $n \in \{p, p+1\}$. If $p^2 \nmid |G|$ and $\mathrm{nse}(G) = \mathrm{nse}(S_n)$, then $G \cong S_n$.*
Sketch of the proof. *Applying Lemma 2.7 leads us to see that, there exists a natural number m so that $p \leq m \leq n$ and $K/H \cong A_m$. In the following, we examine the values of n:*
(1) Let $n = p$. Thus $m = p$ and $K/H \cong A_n$. But since $|G| \mid |S_n|$, then $|G| = |A_n|$ or $|G| = |S_n|$. If $|G| = |A_n|$, then $|H| = 1$ and $|G/K| = 1$ and hence, $G = K = A_n$. But since $m_2(S_n) > m_2(A_n)$, we get a contradiction with Lemma 2.4. Therefore, $|G| = |S_n|$ and hence, $|G/K|$ is either 2 or $|H| = 2$. According to Lemma 2.10, $|H| \neq 2$ and hence, $G = A_n : Z_2 \cong S_n$, as claimed.
(2) If $n = p+1$, then either $m = p$ or $m = p+1$. When $m = p+1$, with the same argument as (1) is concluded $G \cong S_n$. Let $m = p$. Thus $K/H \cong A_p$. Applying Lemma 2.7 and Corollary 1.1, we get $p(p+1)(p-2)! \mid |G|$ and hence, $(p+1)!/(4, p-1) \mid |G|$. Since $|H| \mid 2(p+1)$, $|H| \neq 1$ and $p+1$ is a power of 2 or not. If $p+1 = 2^{\alpha}$, then H is a nilpotent 2-group and hence, $C_K(H)/H = \{1, K/H\}$ which in every case we can get a contradiction. Finally suppose that $p+1$ is not a power of 2. Thus there exists a prime divisor $t \neq 2$ of $p+1$. Hence $|H|_t = ((p+1)/2)_t$. Now, Lemma 2.10 implies that $p \mid ((p+1)/2)_t - 1$, which is impossible.
Thus we prove that $G \cong S_n$.

References

[1] *N. Ahanjideh and B. Asadian,* NSE characterization of some alternating groups*, J. Algebra Appl.* **14(2)** *(2015).*

[2] *G. Frobenius, Verallgemeinerung des sylowschen satze, Berliner sitz (1985), 981-993.*

[3] *A. Khalili Asboei,* A new characterization of *$PGL(2, p)$, J. Algebra and Its Applications,* ***12 (7)*** *(2013):1350040 (5 pages).*

[4] *A.S. Kondrat´ev and V.D. Mazurove,* Recognition of Alternating groups of prime degree from their element orders*, Sibrian Math. J.,* ***41 (2)*** *(2000), 294-302.*

[5] *R. Shen, C. Shao, Q. Jiang , W. Shi and V. Mazurov,* A new characterization of A_5*, Monatsh. Math.,* ***160 (3)*** *(2010), 337-341.*

[6] *L. Weisner,* On the sylow subgroups of the Symmetric and Alternating Groups*, American Journal of Mathematics,* ***47 (2)*** *(1925), 121-124.*

[7] *J.S. Williams,* Prime graph components of finite groups*, J. Algebra,* ***69 (2)*** *(1981), 487-513.*

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 23-26.

Oral Presentation

On the Groups with the same nse

Soleyman Asgary
Faculty of Mathematic Sciences, University of Shahrekord
soleyman.asgary@stu.sku.ac.ir

Neda Ahanjideh
Faculty of Mathematic Sciences, University of Shahrekord
ahanjideh.neda@sci.sku.ac.ir

Abstract

Let G be a finite group and $\pi_e(G)$ be the set of element orders of G. Suppose that $k \in \pi_e(G)$ and m_k is the number of elements of order k in G. Set $\mathrm{nse(G)} := \{m_k : k \in \pi_e(G)\}$. In this paper, we prove that if G is a group with $\mathrm{nse(PSL(3,9))} = \mathrm{nse(G)}$, then $G \cong PSL(3,9)$.

Keywords: Set of the numbers of elements with the same order, simple K_n-groups, Thompson's problem.

MSC(2010): Primary: 20D05; Secondary: 20D06.

1 Introduction

Let G be a finite group. Denote by $\pi(G)$ the set of prime divisors of the order of G and the set of element orders of G is denoted by $\pi_e(G)$. A finite group G is called a simple K_n-group, if G is a simple group with $|\pi(\mathrm{G})| = \mathrm{n}$. For a group G and $i \in \pi_e(G)$, set $m_i(G) = |\{g \in G :$ the order of g is $i\}|$. In fact, $m_i(G)$ is the number of elements of order i in G and $\mathrm{nse}(G) := \{m_i(G) : i \in \pi_e(G)\}$, the set of the number of elements with the same order. If there is no ambiguity, we write m_i instead of $m_i(G)$. Throughout this paper, we denote by ϕ the Euler's function. If G is a finite group, then we denote by $P_q(G)$ a Sylow q-subgroup of G, by $\mathrm{Syl}_q(G)$ the set of Sylow q-subgroups of G and $n_q(G)$ is the number of Sylow q-subgroups of G, that is, $n_q(G) = |\mathrm{Syl_q(G)}|$.

We say that the group G is characterizable by the set of nse if every group H with $\mathrm{nse}(G) = \mathrm{nse}(H)$ is isomorphic to G. In 1987, J. G. Thompson posed a very interesting problem related to algebraic number fields as follows :

Thompson's Problem. Let $T(G) = \{(k, m_k) : k \in \pi_e(G),\ m_k \in \mathrm{nse}(G)\}$, where m_k is the number of elements of G with order k. Suppose that H is a group with $T(G) = T(H)$. If G is solvable, then is it true that H is also necessarily solvable?

Thompson's Problem is still open, but some authors have tried to deal with the analogous problem which asks whether the finite simple groups can be characterized by nse. In [6], it has been shown that the finite simple groups PSL(2,q), where $q \in \{7, 8, 11, 13\}$ are characterizable by their nse.

In this paper, we show that the finite simple group $PSL(3,9)$, which is a simple K_5-group, can be characterized by nse. The main result of this paper is the following theorem:

Main theorem. If G is a group such that $\mathrm{nse}(G) = \mathrm{nse}(PSL(3,9)) = \{1, 7371, 531440, 678132, 1061424, 589680, 933120, 4009824, 1179360, 1866240, 2122848, 2358720, 4245696, 8491392, 11197440\}$, then $G \cong PSL(3,9)$.

Lemma 1.1. [2] *Let G be a finite group and m be a positive integer dividing $|G|$. If $L_m(G) = \{g \in G \mid g^m = 1\}$, then $m \mid |L_m(G)|$.*

Lemma 1.2. [7] *Let G be a group containing more than two elements. If the maximal number s of elements of the same order in G is finite, then G is finite and $|G| \leq s(s^2 - 1)$.*

Lemma 1.3. [5] *Let G be a finite solvable group and $|G| = mn$, where $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ and $(m,n) = 1$. Let $\pi = \{p_1, \ldots, p_r\}$ and h_m be the number of Hall π-subgroups of G. Then $h_m = q_1^{\beta_1} \ldots q_s^{\beta_s}$ satisfies the following conditions for all $i \in \{1, 2, \ldots s\}$:*

(1) $q_i^{\beta_i} \equiv 1 \pmod{p_j}$ *for some p_j;*

(2) *the order of some chief factor of G is divided by $q_i^{\beta_i}$.*

Lemma 1.4. [4] *If G is a simple K_3-group, then G is isomorphic to one of the following groups:* $A_5, A_6, PSL(2,7), PSL(2,8), PSL(2,17), PSL(3,3), PSU(3,3)$ *or* $PSU(4,2)$.

Lemma 1.5. [8] *Let G be a simple K_4-group. Then G is isomorphic to one of the following groups:*

(1) A_7, A_8, A_9, A_{10};

(2) M_{11}, M_{12}, J_2;

(3) *on of the following simple groups:*

(a) *$PSL(2,r)$, where r is a prime and satisfies $r^2 - 1 = 2^a.3^b.v^c$ with $a,b,c \geq 1$ and $v > 3$ is a prime;*

(b) *$PSL(2,2^m)$, where $m \geq 2$ satisfies $2^m - 1 = u$ and $2^m + 1 = 3t^b$, with u,t are primes, $t > 3$ and $b \geq 1$;*

(c) *$PSL(2,3^m)$, where $m \geq 2$ satisfies either $3^m + 1 = 4t$ and $3^m - 1 = 2u^c$ or $3^m + 1 = 4t^b$ and $3^m - 1 = 2u$, with u,t are odd primes and $b,c \geq 1$;*

(4) *one of the following* 28 *simple groups:*
$PSL(2,16)$, $PSL(2,25)$, $PSL(2,49)$, $PSL(2,81)$, $PSL(3,4)$, $PSL(3,5)$, $PSL(3,7)$, $PSL(3,8)$, $PSL(3,17)$, $PSL(4,3)$, $PSp(4,4)$, $PSp(4,5)$, $PSp(4,7)$, $PSp(4,9)$, $PSp(6,2)$, $O_8^+(2)$, $G_2(3)$, $PSU(3,4)$, $PSU(3,5)$, $PSU(3,7)$, $PSU(3,8)$, $PSU(3,9)$, $PSU(4,3)$, $PSU(5,2)$, $Sz(8)$, $Sz(32)$, ${}^3D_4(2)$, ${}^2F_4(2)'$.

Lemma 1.6. [1] Let G be a simple K_5-group. Then G is isomorphic to one of the following groups:

(1) $PSL(2,q)$ with $|\pi(q^2-1)| = 4$;

(2) $PSL(3,q)$ with $|\pi((q^2-1)(q^3-1))| = 4$;

(3) $PSU(3,q)$ with $|\pi((q^2-1)(q^3+1))| = 4$;

(4) $O_5(q)$ with $|\pi(q^4-1)| = 4$;

(5) $Sz(2^{2m+1})$ with $|\pi((2^{2m+1}-1)(2^{4m+2}+1))| = 4$;

(6) $R(q)$ where q is an odd power of 3, $|\pi(q^2-1)| = 3$ and $|\pi(q^2-q+1)| = 1$;

(7) one of the following 30 simple groups:
$A_{11}, A_{12}, M_{22}, J_3, HS, He, McL, PSL(4,4), PSL(4,5), PSL(4,7), PSL(5,2), PSL(5,3), PSL(6,2)$, $O_7(3)$, $O_9(2)$, $PSp(6,3)$, $PSp(8,2)$, $PSU(4,4)$, $PSU(4,5)$, $PSU(4,7)$, $PSU(4,9)$, $PSU(5,3)$, $PSU(6,2)$, $O_8^+(3)$, $O_8^-(2)$, ${}^3D_4(3)$, $G_2(4)$, $G_2(5)$, $G_2(7)$, or $G_2(9)$.

Remark 1.1. Let G be a group with $\mathrm{nse}(G) = \mathrm{nse}(PSL(3,9))$. By Lemma 1.2, we can see that G is finite. It is known that $m_n = k\phi(n)$, where k is the number of cyclic subgroups of order n in G and if $n > 2$, then $\phi(n)$ is even, so m_n is even. If $n \in \pi_e(G)$, then by Lemma 1.1 and the above notation, we have:

$$\begin{cases} \phi(n) \mid m_n \\ n \mid \sum\limits_{d|n} m_d \end{cases} \tag{1.1}$$

2 Main Results

Lemma 2.1. (i) Let t be the number of cyclic subgroups of order n in G, namely $H_1, \ldots, H_t$ and let for $1 \le i \le t$, β_i be the number of cyclic subgroups of $C_G(H_i)$ of order r, where $\gcd(r,n) = 1$. If $\beta = \min\{\beta_i : 1 \le i \le t\}$, then $m_n\phi(r)\beta = \phi(nr)\beta t \le m_{nr}$.

(ii) If $P \in \mathrm{Syl}_p(G)$ is cyclic of prime order p and $r \in \pi(G) - \{p\}$, then $m_{rp} = n_p(G)(p-1)(r-1)k = m_p(G)(r-1)k$, where k is the number of cyclic subgroups of order r in $C_G(P)$.

Lemma 2.2. Let G be a finite simple K_n-group such that $3^6 \mid |G|$ and $|G| \mid 2^8.3^6.5.7.13$, where $n = 4,5$, then $G \cong PSL(3,9)$.
We will prove the Lemma by the following two steps:
Step 1. G is a simple K_4-group.
From Lemma 1.5, we can conclude that G is not a simple K_4-group.
Step 2. G is a simple K_5-group.
In view of Lemma 1.6 (2), $G \cong PSL(3,9)$.

Theorem 2.1. If G is a group such that $\mathrm{nse}(G) = \mathrm{nse}(PSL(3,9)) = \{1, 7371, 531440, 678132, 1061424, 589680, 933120, 4009824, 1179360, 1866240, 2122848, 2358720, 4245696, 8491392, 11197440\}$, then $G \cong PSL(3,9)$.
We will prove the theorem by the following three steps:
Step 1. By Remark 1.1, G be a finite group and by [3], we can see that $\mathrm{nse}(G) = \mathrm{nse}(PSL(3,9))$= $\{$1,7371,531440,678132, 1061424, 589680, 933120, 4009824, 1179360, 1866240, 2122848, 2358720, 4245696, 8491392, 11197440$\}$.
Step 2. Since $7371 \in$ nse(G), by Remark 1.1, $2 \in \pi(G)$ and $m_2 = 7371$. Let $2 \neq p \in \pi(G)$. Then by (1.1), $p \mid (1+m_p)$ and $(p-1) \mid m_p$, so checking the elements of nse(G) implies that $p \in \{3,5,7,13,17,19,31,43,47,79,241,589681,678133,2358721\}$. Again by (1.1) and Lemma 2.1 we can see that $\pi(G) \subseteq \{2,3,5,7,13\}$. Also by Euler's function and checking the elements of nse(G), we can conclude that $\pi(G) = \{2,3,5,7,13\}$.
Step 3. G is a non-solvable group and hence, G has a normal series $1 \trianglelefteq N \trianglelefteq M \trianglelefteq G$ such that M/N is a simple K_i-group with $i = 3,4,5$. It is easy to prove that M/N is not a simple K_3-group. Therefore M/N is a simple K_i-group with $i = 4,5$, thus by Lemma 2.2, $M/N \cong PSL(3,9)$. By Step 2 and Lemma 2.2, we can conclude that $|G| = 2^7 \times 3^6 \times 5 \times 7 \times 13 = |\mathrm{PSL}(3,9)|$ and by applying the above argument, $G \cong \mathrm{PSL}(3,9)$. This completes the proof of the theorem.

References

[1] A. Jafarzadeh and A. Iranmanesh, *On simple K_n- group for $n = 5,6$*, London Math. Soc. Cambridge University Press (2007), 517-526.

[2] G. Frobenius, *Verallgemeinerung des Sylowschen Satze*, Berliner Sitz, (1985), 981-993.

[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups*, Clarendon Press, New York, 1985.

[4] M. Herzog, *Finite simple groups divisible by only three primes*, J. Algebra, **10.** (1968), 383-388.

[5] M. Hall, The theory of groups, Macmilan, 1959.

[6] M. Khatami, B. Khosravi and Z. Akhlaghi, *A new characterization for some linear groups*, Monatsh Math., **163.** (2011), 39-50.

[7] R. Shen, C.G. Shao, Q.H. Jiang, W.J. Shi and V. Mazurov, *A new characterization of A_5*, Monatsh Math., **160.** (2010), 337-341.

[8] W.J. Shi, *On simple K_4-group*, Chin. Sci. Bul., **36.** (1991), 1281-1283.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 27-30.

Poster Presentation

Symmetric Designs and Projective Special Linear Groups of small Rank

Mohsen Bayat
Department of Mathematics, Faculty of Science
Bu-Ali Sina University, Hamedan, Iran
mohsen0sayex24@gmail.com
(Joint work with Seyed Hassan Alavi and Ashraf Daneshkhah)

Abstract

The main aim of this poster is to present some recent studies on symmetric (v,k,λ) designs admitting a flag-transitive and point-primitive automorphism group G whose socle is a projective special linear group of small rank.

Keywords: Symmetric designs, flag-transitive, point-primitive.

MSC(2010): Primary 20B25, Secondary 05B05.

1 Introduction

A t-(v,k,λ) *design* $\mathscr{D}=(\mathscr{V},\mathscr{B})$ is an incidence structure consisting of a set $\mathscr{V}$ of v *points*, and a set $\mathscr{B}$ of k-element subsets of $\mathscr{V}$, called *blocks*, such that every t-element subset of points lies in exactly λ blocks. The design is *nontrivial* if $t<k<v-t$, and is *symmetric* if $|\mathscr{B}|=v$. If $\mathscr{D}$ is symmetric and nontrivial, then $t\leqslant 2$ (see [3, Theorem 1.1]or [7, Theorem 1.27])). This motivates to study nontrivial symmetric 2-(v,k,λ) designs which we simply call *symmetric* (v,k,λ) *designs*. A *flag* of $\mathscr{D}$ is an incident pair (α,B) where α and B are a point and a block of $\mathscr{D}$, respectively. An *automorphism* of a symmetric design $\mathscr{D}$ is a permutation of the points permuting the blocks and preserving the incidence relation. An automorphism group G of $\mathscr{D}$ is called *flag-transitive* if it is transitive on the set of flags of $\mathscr{D}$. If G is primitive on the point set $\mathscr{V}$, then G is said to be *point-primitive*. A group

G is said to be *almost simple* with socle X if $X \trianglelefteq G \leqslant \mathrm{Aut}(X)$ where X is a (nonabelian) simple group. Further notation and definitions in both design theory and group theory are standard and can be found, for example, in [4, 7, 9].

Symmetric designs with λ small have been of most interest. Kantor [8] classified flag-transitive symmetric $(v,k,1)$ designs (projective planes) of order n and showed that either $\mathscr{D}$ is a Desarguesian projective plane and $\mathrm{PSL}(3,n) \trianglelefteq G$, or G is a sharply flag-transitive Frobenius group of odd order $(n^2+n+1)(n+1)$, where n is even and n^2+n+1 is prime. Regueiro [11] gave a complete classification of biplanes ($\lambda = 2$) with flag-transitive automorphism groups apart from those admitting a 1-dimensional affine group (see also [12, 13, 14, 15]). Zhou and Dong studied nontrivial symmetric $(v,k,3)$ designs (triplanes) and proved that if $\mathscr{D}$ is a nontrivial symmetric $(v,k,3)$ design with a flag-transitive and point-primitive automorphism group G, then $\mathscr{D}$ has parameters $(11,6,3)$, $(15,7,3)$, $(45,12,3)$ or G is a subgroup of $\mathrm{A\Gamma L}(1,q)$ where $q = p^m$ with $p \geqslant 5$ prime [6, 20, 21, 22, 23]. Nontrivial symmetric $(v,k,4)$ designs admitting flag-transitive and point-primitive almost simple automorphism group whose socle is an alternating group or $\mathrm{PSL}(2,q)$ have also been investigated [5, 24]. It is known [18] that if a nontrivial (v,k,λ)-symmetric design $\mathscr{D}$ with $\lambda \leqslant 100$ admitting a flag-transitive, point-primitive automorphism group G, then G must be an affine or almost simple type. Therefore, it is interesting to study such designs whose socle is of almost simple type or affine type.

In this poster, however, we are interested in large λ. In this direction, it is recently shown in [1] that there are only four possible symmetric (v,k,λ) designs admitting a flag-transitive and point-primitive automorphism group G satisfying $X \trianglelefteq G \leqslant \mathrm{Aut}(X)$ where $X = \mathrm{PSL}(2,q)$. In the case where an almost simple group G with socle $X = \mathrm{PSL}(3,q)$ acts flag-transitively and point-primitively on $\mathscr{D}$, we have shown that $\mathscr{D}$ must be a Desarguesian projective plane $\mathrm{PG}(2,q)$ (see [2]). Note in passing that when X is a sporadic simple group, there exist only four possible parameters (see [19]).

In the case where G is imprimitive, Praeger and Zhou [16] studied point-imprimitive symmetric (v,k,λ) designs, and determined all such possible designs for $\lambda \leqslant 10$. This motivates Praeger and Reichard [10] to classify flag-transitive symmetric $(96,20,4)$ designs. As a result of their work, the only examples for flag-transitive, point-imprimitive symmetric $(v,k,4)$ designs are $(15,8,4)$ and $(96,20,4)$ designs. In a recent study of imprimitive flag-transitive designs [17], Cameron and Praeger gave a construction of a family of designs with a specified point-partition, and determine the subgroup of automorphisms leaving invariant the point-partition. They gave necessary and sufficient conditions for a design in the family to possess a flag-transitive group of automorphisms preserving the specified point-partition. Consequently, they gave examples of flag-transitive designs in the family, including a new symmetric 2-$(1408,336,80)$ design with automorphism group $2^{12} : ((3 \cdot \mathrm{M}_{22}) : 2)$, and a construction of one of the families of the symplectic designs exhibiting a flag-transitive, point-imprimitive automorphism group.

References

[1] S. H. Alavi, M. Bayat, and A. Daneshkhah. Symmetric designs admitting flag-transitive and point-primitive automorphism groups associated to two dimensional projective special groups. *submitted*.

[2] S. H. Alavi, and M. Bayat. Symmetric designs admitting flag-transitive and point-primitive automorphism groups associated to three dimensional projective special groups. *submitted*.

[3] A. R. Camina. A survey of the automorphism groups of block designs. *J. Combin. Des.*, 2(2):79–100, 1994.

[4] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[5] H. Dong and S. Zhou. Alternating groups and flag-transitive 2-$(v,k,4)$ symmetric designs. *J. Combin. Des.*, 19(6):475–483, 2011.

[6] H. Dong and S. Zhou. Affine groups and flag-transitive triplanes. *Sci. China Math.*, 55(12):2557–2578, 2012.

[7] D. R. Hughes and F. C. Piper. *Design theory*. Cambridge University Press, Cambridge, 1985.

[8] W. M. Kantor. Primitive permutation groups of odd degree, and an application to finite projective planes. *J. Algebra*, 106(1):15–45, 1987.

[9] E. S. Lander. *Symmetric designs: an algebraic approach*, volume 74 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[10] M. Law, C. E. Praeger, and S. Reichard. Flag-transitive symmetric 2-$(96,20,4)$-designs. *J. Combin. Theory Ser. A*, 116(5):1009–1022, 2009.

[11] E. O'Reilly-Regueiro. *Flag-transitive symmetric designs*. PhD thesis, University of London, 2003.

[12] E. O'Reilly-Regueiro. Biplanes with flag-transitive automorphism groups of almost simple type, with alternating or sporadic socle. *European J. Combin.*, 26(5):577–584, 2005.

[13] E. O'Reilly-Regueiro. On primitivity and reduction for flag-transitive symmetric designs. *J. Combin. Theory Ser. A*, 109(1):135–148, 2005.

[14] E. O'Reilly-Regueiro. Biplanes with flag-transitive automorphism groups of almost simple type, with classical socle. *J. Algebraic Combin.*, 26(4):529–552, 2007.

[15] E. O'Reilly-Regueiro. Biplanes with flag-transitive automorphism groups of almost simple type, with exceptional socle of Lie type. *J. Algebraic Combin.*, 27(4):479–491, 2008.

[16] C. E. Praeger and S. Zhou. Imprimitive flag-transitive symmetric designs. *J. Combin. Theory Ser. A*, 113(7):1381–1395, 2006.

[17] P. J. Cameron and C. E. Praeger. Constructing flag-transitive, point-imprimitive designs. *ArXiv e-prints 1408.6598*, 2014.

[18] D. Tian and S. Zhou. Flag-transitive point-primitive symmetric (v,k,λ) designs with λ at most 100. *J. Combin. Des.*, 21(4):127–141, 2013.

[19] D. Tian and S. Zhou. Flag-transitive 2-(v,k,λ) symmetric designs with sporadic socle. *Journal of Combinatorial Designs*, 2014.

[20] S. Zhou and H. Dong. Sporadic groups and flag-transitive triplanes. *Sci. China Ser. A*, 52(2):394–400, 2009.

[21] S. Zhou and H. Dong. Alternating groups and flag-transitive triplanes. *Des. Codes Cryptogr.*, 57(2):117–126, 2010.

[22] S. Zhou and H. Dong. Exceptional groups of Lie type and flag-transitive triplanes. *Sci. China Math.*, 53(2):447–456, 2010.

[23] S. Zhou, H. Dong, and W. Fang. Finite classical groups and flag-transitive triplanes. *Discrete Math.*, 309(16):5183–5195, 2009.

[24] S. Zhou and D. Tian. Flag-transitive point-primitive 2-$(v,k,4)$ symmetric designs and two dimensional classical groups. *Appl. Math. J. Chinese Univ. Ser. B*, 26(3):334–341, 2011.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 31-37.

Oral Presentation

Constructing Elliptic Curves with Prescribed Torsion using Halving

Hassan Daghigh
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
hassan@kashanu.ac.ir

Fatemeh Seifi Shahpar
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
fatemeh.seifishahpar@gmail.com

Ruhollah Khodakaramian
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
rkhodakaramian@gmail.com

Abstract

In this paper we generalize the algorithm of constructing elliptic curve with a prescribed $N-$torsion point to the efficiently generating an elliptic curve with a point of order 2^sN, with the method of successive halving. In this method we search among the curves generated with the modular curves $Y_1(2^iN)$ for $i = 1,...,s-1$, to find the equation of a curve with a point of order 2^sN- which is cryptographically more efficient than using $Y_1(2^sN)$.

Keywords: Modular curve, elliptic curve, torsion point, halving.

MSC(2010): Primary: 11G05; Secondary:11G07.

1 Introduction

Let $N \geqslant 2$ be an integer. The modular curve $X_1(N)$ (with cusps removed) parametrizes isomorphism classes of pairs (E,P) where E is an elliptic curve and P, is a torsion point of order N on E.
We are trying to find a curve with a prescribed order. We may be able to do this work by reducing a curve defined over a quadratic field $Q(\sqrt{d})$ with a point of order N to a curve defined over F_q, but only when d is a quadratic residue.
Alternatively, we can use an F_q-rational point on $Y_1(N)$, the affine part of $X_1(N)$, to directly construct the Tate normal form

$$E(b,c)/F_q \ : \ y^2+(1-c)xy-by = x^3-bx^2.$$

containing a point of order N, for any sufficiently large q prime to N. Any elliptic curve with a point of order greater than 3 can be put in this form [1]. Provided $E(b,c)$ is nonsingular, we obtain an elliptic curve on which the point $P=(0,0)$ has order N.
To apply this method we require a defining equation for $Y_1(N)$. Then by choosing the point (x,y) on $Y_1(N)$ and applying suitable transformations, we construct $E(b,c)$ and if it is singular, we simply look for a different point on the curve.

2 Computing $Y_1(N)$

Following [4], we give a method to compute a defining equation $F_N(r,s)=0$ for $Y_1(N)$. For the curve $E(b,c)$, if $P=(0,0)$ then $2P=(b,bc)$ and if $nP=(x_n,y_n)$ then

$$x_{n+1} = by_n/x_n^2 \ \ , \ \ \ y_{n+1} = b^2(x_n^2-y_n)/x_n^3$$

If P is an $N-$torsion point and $m+n=N$, then for $m=\lceil \frac{N+1}{2} \rceil$ and $n=\lfloor \frac{N-1}{2} \rfloor$ we have

$$NP = \mathscr{O} \iff x_m = x_n$$

The algorithm to compute $F_N(r,s)=0$ for $N>5$ is as follows [6]:
Assume that the polynomials F_M have already been computed, for $5<M<N$, and that the rational function $x_n(r,s)$ is in the form $x_n = v_n/w_n$, where v_n and w_n are relatively prime polynomials in $\mathbf{Z}[r,s]$.

Algorithm 1. Given an integer $N>5$, compute $F_N(r,s)$ as follows:
1. Compute $G_N = v_m w_n - v_n w_m$, where $m=\lceil \frac{N+1}{2} \rceil$ and $n=\lfloor \frac{N-1}{2} \rfloor$.
2. Remove any powers of $r,s,(r-1)$ or F_M that divide G_N, for all $M>5$ properly dividing N.
3. Make the remaining polynomial square-free and output the result as $F_N(r,s)$.

The following theorem shows that the polynomial $F_N(r,s)$ gives us a curve with a point of exact order N.

Theorem 2.1. *Let $F_N(r,s)$ be the polynomial output by Algorithm 1 on input $N>5$. Let $b=r_0s_0(r_0-1)$ and $c=s_0(r_0-1)$ with $\Delta(b,c)\neq 0$, where r_0 and s_0 lie in a field whose characteristic does not divide N. Then $P=(0,0)$ is a point of order N on $E(b,c)$ if and only if $F_N(r_0,s_0)=0$.*

3 Prescribing 2^kN-torsion

Let N be an odd number. Our contribution is to generalize the method of Sutherland [6] to find a curve with prescribed 2^sN-torsion point by the method of successive halving in [5]. We can use this method to efficiently search for an elliptic curve with a point of order 2^sN using curves generated with $Y_1(2^iN)$, where $1 \leq i < s$. We also use the form of

$$y^2 = x(x^2 + \alpha x + \beta)$$

of an elliptic curve in which $\rho = \alpha^2 - 4\beta$ determines the number of points of order 2.
A curve with a point of order N has a point of order 2^sN if and only if it has a point of order 2^s. Now assume that a given curve E has point Q of order 2^k, with $k \geq 1$. If $Q = 2P$, we say that Q has a half point $P = (x,y)$ of order $2^(k+1)$. Such a condition is equivalent to

$$\xi = x(2P) = \frac{(x^2-\beta)^2}{4y^2} \tag{3.1}$$

$$y^2 = x(x^2 + \alpha x + \beta)$$

So one follows that

Lemma 1. Let $E(F_q)\ : y^2 = x(x^2 + \alpha x + \beta)$ and $Q = (\xi,\zeta) \in E(F_q) \setminus \{\mathcal{O}\}$. A necessary condition for the existence of a half point of Q is that ξ is a square in F_q. Furthermore, since $\zeta^2 = \xi\delta_\xi$ with $\delta_\xi = \xi^2 + \alpha\xi + \beta$, it follows that δ_ξ should also be a square in F_q.
On the other hand, from equations 3.1, we get the quartic equation over F_q

$$f_\xi : x^4 - 4\xi x^3 - 2(2\alpha\xi + \beta)x^2 - 4\beta\xi x + \beta^2 = 0 \tag{3.2}$$

3.1 Halving Process

The main strategy for efficiently searching an elliptic curve with a point of order 2^sN between modular curves $Y_1(2^iN)$, is to determin the points of order 2 of the curve $Y_1(2^iN)$ by starting from $i = 1$ and checking the existence of their half points. We have two cyclic and noncyclic cases for the structure of the group of two torsion points depending on the existence of one or three points of order 2.

A) Cyclic Case:

Lemma 2. A curve $E(F_q)$: $y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = -1$ has a point of order 4 if and only if $\chi(\beta) = 1$.

The inductive step is completed with the following proposition:

proposition 1. Let $y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = -1$. Let us assume that $Q = (\xi,\zeta)$ is a point of $E(F_q)$ of order 2^k with $k > 1$. Then there exists a half point of Q if and only if $\chi(\xi) = 1$.

B) Noncyclic Case:

Lemma 3. Let $E(F_q) : y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = 1$ and $\{(0,0),(\xi_1,0),(\xi_2,0)\}$ its rational points of order 2. Then, E has rational points of order 4 if and only if one of the following conditions holds:
(1) $\chi(\beta) = 1$ and $\chi(\alpha - 2\sqrt{\beta}) = 1$;

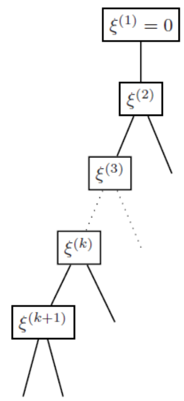


Figure 1: Tree of abscissas in the cyclic case

(2) $\chi(\xi_1) = \chi(2\xi_1 + \alpha) = 1$;
(3) $\chi(\xi_2) = \chi(2\xi_2 + \alpha) = 1$.

As before, in order to continue the halving process, first we need the characterization of the image of multiplication by 2.

Proposition 2. Let $E(F_q) : y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = 1$. Let us assume that $Q = (\xi, \zeta)$ is a point of $E(F_q)$ of order 2^k, with $k > 1$. Then, there exists a half point of Q if and only if

$$\chi(\xi) = 1 \quad , \quad \chi(2\xi + \alpha + 2\sqrt{\delta_\xi}) = 1$$

where $\delta_\xi = \xi^2 + \alpha\xi + \beta$.

In the noncyclic case, as same as the cyclic case, if the process of halving continued untill the step $k = s$, the coresponding curve has at least one point of order 2^s and we are done, otherwise we discard the curve and do the process for the next i.

Remark. Let us assume that the condition in Proposition 2 holds. If a root x of $f_{i,\xi}$ is the abscissa of a point $P \in E(F_q)$, then the other root of $f_{i,\xi}$, namely β/x is the abscissa of $P + (0,0)$. If a root x of one of the polynomials $f_{i,\xi}$ is the abscissa of $P \in E(F_q)$, then the abscissa of $P + (\xi_1, 0)$, namely $\xi_1(x - \xi_2)/(x - \xi_1)$ is a root of the other polynomial. Let us denote by $\{Q_0 = (0,0)\ ,\ Q_1 = (\xi_1, 0)\ ,\ Q_2 = (\xi_2, 0)\}$ the points of order 2, and

$$T_j = \{P \in E(F_q) \mid \exists \ell \geq 0 \ \ such\ that\ \ 2^\ell P = Q_j\}$$

for $j = \{0,1,2\}$. In these trees T_j, if a vertex Q has children, then it has four, which are $\{P, P + Q_0, P + Q_1, P + Q_2\}$. So if all the points Q_0, Q_1, Q_2, have half point, then either the four points can be halved or none of them can. So in each step we need at most three checkings, one in each tree. Therefore, in $E[2^k](F_q) \cong \mathbf{Z}/2^k\mathbf{Z} \times \mathbf{Z}/2^k\mathbf{Z}$, we have 3.4^{k-1} points of order 2^k, but three checkings of condition of proposition 2 and therefore three computations of a root of a quadratic polynomial are enough to continue the process and the algorithm is efficient.

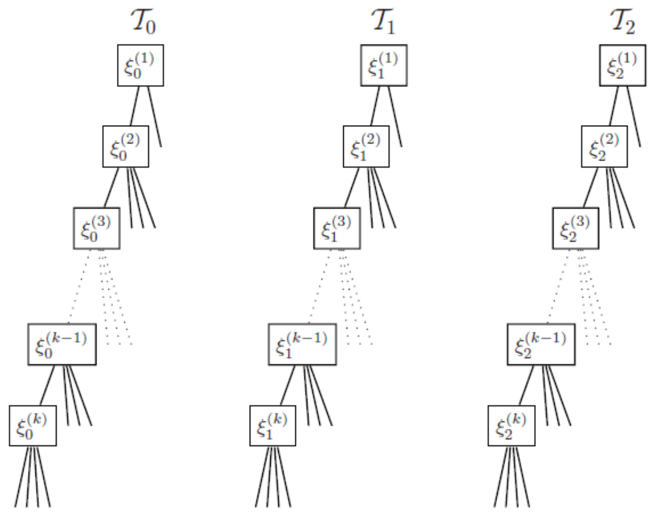


Figure 2: Tree of abscissas in the noncyclic case

At last we implement the procedure using the softwares MAPLE and PARI and find all the curves generated by $Y_1(2N)$ for $N = 17$ with their 2-Sylow subgroup over the prime field F_{43}. We can see that in this family of curves, there is no curve with the rational point of order grater than 2^4 in the group of points of the curve.

4 Main Results

In this paper we generalize the algorithm of constructing elliptic curve with a prescribed $N-$torsion point to the efficiently generating an elliptic curve with a point of order 2^sN, with the method of successive halving. In this method we search among the curves generated with the modular curves $Y_1(2^iN)$ for $i = 1,...,s-1$, to find the equation of a curve with a point of order 2^sN- which is cryptographically more efficient than using $Y_1(2^sN)$.
We also implement the procedure using the softwares MAPLE and PARI and find all the curves generated by $Y_1(2N)$ for $N = 17$ with their 2-Sylow subgroup over the prime field F_{43}. We can see that in this family of curves, there is no curve with the pational point of order grater than 2^4 in the group of points of the curve.

References

[1] Anthony W. Knapp, Elliptic curves, Princeton University Press, 1992.

[2] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proceedings of the London Mathematical Society, **vol. 33**, (1976), pages 193-237.

[3] Barry Mazur, *Rational points on modular curves*, Lecture Notes in Mathematics, **vol. 601** (Springer-Verlag, 1977), pages 107148.

2-Sylow subgroup $\frac{\mathbb{Z}}{2^n\mathbb{Z}} \times \frac{\mathbb{Z}}{2^r\mathbb{Z}}$	$E: \ y^2 = x(x^2 + \alpha x + \beta) \ over \ \mathbb{F}_{43}$
$\frac{\mathbb{Z}}{2^3\mathbb{Z}}$	$y^2 = x(x^2 + 41x + 7)$
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 20x + 40)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 9x)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 41x)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}}$	$y^2 = x(x^2 + 22x + 7)$
$\frac{\mathbb{Z}}{2^3\mathbb{Z}}$	$y^2 = x(x^2 + 40x + 29)$
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 20x + 6)$
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 4x + 1)$
$\frac{\mathbb{Z}}{2^4\mathbb{Z}}$	$y^2 = x(x^2 + 23x + 12)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 30x + 11)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}}$	$y^2 = x(x^2 + 9x + 30)$
$\frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 18x + 31)$
$\frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$	$y^2 = x(x^2 + 6x + 7)$
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}}$	$y^2 = x(x^2 + 33x + 40)$

Figure 3: 2-Sylow subgroups of $Y_1(2N)$ over F_{43}

[4] Markus A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Mathematics of Computation, **vol. 46**, (1986), pages 637658.

[5] J. Miret, R. Moreno, A. Rio, and M. Valls, *Determining the 2-sylow subgroup of an elliptic curve over a finite field*, Mathematics of Computation, **vol. 74**, (2005), pages 411427.

[6] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Mathematics of Computation, **vol. 81**, (2012), pages 1131-1147.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 39-.

Oral Presentation

On Lattice Basis Ideals of Digraphs

Hamid Damadi
Faculty of Mathematics and Computer science, university of Amirkabir Tehran
hamid.damadi@aut.ac.ir

Farhad Rahmati
Faculty of Mathematics and Computer science, university of Amirkabir Tehran
frahmati@aut.ac.ir

Abstract

Let G be a directed graph with n vertices and m edges, and I(B) a binomial ideal corresponded to the incidence matrix B of the graph G. Also by removing the i'th row of B, a new matrix is made and is called B_i. In this paper it is shown that the heights of $I(B)$ and $I(B_i)$ are equal to n-1 and the dimensions of $I(B)$ and $I(B_i)$ are equal to m-n+1. Then a sufficient and necessary condition is given for $I(B_i)$ to be prime. A sufficient combinatorial condition is given for $I(B)$ and $I(B_i)$ to be complete intersections. Finally a free complex for $I(B)$ will be presented and, for specific graphs, a free resolution will be stated for $I(B)$.

Keywords: Directed graph, binomial ideal, matrix ideals.
MSC(2010): 05E99, 13C99.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 41-47.

Oral Presentation

A Sharp Height Estimate for a Specific Family of Elliptic Curves

Somayeh Didari
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, Iran
somayeh.didari@gmail.com

Abstract

In this paper we find a sharp bound on the canonical height of non-torsion points on elliptic curves of the form $y^2 = x^3 - nx$, where n is a square- free integer. By an example we will show that our bound is the sharpest possible bound.

Keywords: Elliptic curve, height function, root number.

MSC(2010): Primary: 11G05; Secondary: 14H52.

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and $P = (x,y) = (\frac{a}{d^2}, \frac{b}{d^3}) \in E(\mathbb{Q})$. If $gcd(a,d) = 1$, we define the naive height of P by $h(P) = max\{\log|a|, \log|d^2|\}$ and the canonical height of P by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}. \tag{1.1}$$

The canonical height measures the size of points on elliptic curves. It plays fundamental roles in many theoretical and practical problems such as proving the Mordell- Weil theorem. There is a well-known conjecture about this function.

Conjecture 1.1 (Lang's Conjecture)**.** *Let $E/\mathbb{K}$ be an elliptic curve with minimal discriminant $\Delta_{E/\mathbb{K}}$. There exist constants $C_1 > 0$ and C_2, depending only on $[\mathbb{K} : \mathbb{Q}]$, such that for all nontorsion points $P \in E(\mathbb{K})$ we have*

$$\widehat{h}(P) > C_1 \log\left(\mathscr{N}_{\mathbb{K}/\mathbb{Q}}\left(\Delta_{E/\mathbb{K}}\right)\right) + C_2.$$

Silverman [4] showed that Lang's conjecture holds for any elliptic curve with integral j-invariant over any number field.

Let n be a positive square- free integer and E_{-n^2} denotes the elliptic curve $y^2 = x^3 - n^2 x$, Bremner, Silverman and Tzanakis [1, Proposition 2.1] proved that for any non torsion point $P \in E_{-n^2}(\mathbb{Q})$,

$$\widehat{h}(P) \geq \frac{1}{8} \log\left(2n^2\right).$$

Fujita [3] considered elliptic curves of the form $E_{-n} : y^2 = x^3 - nx$ and showed that for any positive forth- power- free integer $n \not\equiv 4 \pmod{16}$, and for every $P \in E_{-n}(\mathbb{Q})$,

$$\hat{h}(P) \geq \tfrac{1}{8} \log n + 0.3917.$$

Later Voutier and Yabuta [7, Theorem 1.2] showed that for any fourth-power-free integer $-n$, and $P \in E_{-n}(\mathbb{Q})$,

$$\widehat{h}(P) > \tfrac{1}{8} \log n + \begin{cases} (9/8)\log(2) & \text{if } n \equiv 1,5,7,9,13,15 \text{ mod } 16 \\ (5/8)\log(2) & \text{if } n \equiv 20,36 \text{ mod } 64 \\ & \text{or } n \equiv 2,3,6,8,10,11,12,14 \text{ mod } 16 \\ -(1/8)\log(2) & \text{if } n \equiv 4,52 \text{ mod } 64. \end{cases}$$

Remark 1.2. *Indeed [7] use a definition of height which is half of our definition.*

In this paper we consider elliptic curves of the form $E_{-n} : y^2 = x^3 - nx$ for which n is a positive square- free integer. we will show that

Theorem 1.3. *Let n be a positive square-free integer and E_n denotes the elliptic curve $y^2 = x^3 - nx$. For every $P \in E_{-n}(\mathbb{Q})$, we have*

$$\hat{h}(P) \geq \frac{1}{8} \log n + 0.4331.$$

Our bound is the best known method, we will show this is the best possible bound.

2 Estimating canonical height

Let E be an elliptic curve and $P \in E(\mathbb{Q})$, computing $\hat{h}(P)$ by (1.1) is difficult. To compute $\hat{h}(P)$ one can use local height of P, indeed The value $\hat{h}(P)$ can be expressed as

$$\hat{h}(P) = \sum_{p \ prime} \hat{\lambda}_p(P) + \hat{\lambda}_\infty(P),$$

where $\hat{\lambda}_p(P)$ is the local height at prime p and $\hat{\lambda}_\infty(P)$ is the local height at infinity. Let

$$\hat{h}_{fin}(P) = \textstyle\sum_{p \ prime} \hat{\lambda}_p(P).$$

Remark 2.1. *Let E_{-n} be an elliptic curve of the form $y^2 = x^3 - nx$, where n is a rational number. It is easy to see that every rational point $P \neq \mathcal{O}$ on E_n has the form $P = (b_1r^2/s^2, b_1rt/s^3)$ for integers $r,s,t \in \mathbb{Z}$ such that $(r,s) = (t,s) = 1$ and*

$$\mathcal{T}(b_1):\ t^2 = b_1r^4 + b_2s^4, \qquad b_1b_2 = -n \tag{2.1}$$

Conversely, if (r,s,t) is a nontrivial primitive solution of $\mathcal{T}(b_1)$, then $(b_1r^2/s^2, b_1rt/s^3)$ is a rational point on E_n.

Lamma 2.2. *Let n be a positive square-free integer and E_n be the elliptic curve given by $y^2 = x^3 - nx$. For every $P = (b_1r^2/s^2, b_1rt/s^3)$, $\hat{h}_{fin}(P)$ can be computed as*

$$\hat{h}_{fin}(P) = 2\log s - \frac{1}{2}\log b_1' + \hat{h}_2(P),$$

where b_1' is the odd part of b_1 and $\hat{h}_2(P)$ is a real number satisfying $-(\log 2)/2 \leq \hat{h}_2(P) \leq 0$.

Proof. By [3, Lemma3.2], we know that

$$\hat{h}_{fin}(P) = 2\log s - \frac{1}{2}\log\Big(\prod_{p|(a,n),p\neq 2} p^{e_p}\Big) + \hat{h}_2(P) \tag{2.2}$$

If $(b_2,r) \neq 1$ then there exists prime p which $p|(b_2,r)$ so $p|b_1r^4 + b_2s^4 = t^2$, hence $p^2|b_2s^4$, thus $p^2|b_2$ which is a contradiction, so $(b_2,r) = 1$. To deal with local height at 2, we consider the possible cases:

1. If s is even, then $\hat{h}_2(P) = 0$.
2. If s is odd, n is odd and r is odd, then $\hat{h}_2(P) = -log(2)/2$.
3. If s is odd, n is odd and r is even, then $\hat{h}_2(P) = 0$.
4. If s is odd, b_1 is even, then $\hat{h}_2(P) = -log(2)/2$.
5. If s is odd, b_2 is even and r is even, then $\hat{h}_2(P) = -log(2)/2$.
6. If s is odd, b_2 is even and r is odd, then $\hat{h}_2(P) = 0$.

□

Lamma 2.3. *Let n be a positive square-free integer and E_{-n} be the elliptic curve given by $y^2 = x^3 - nx$. For every $P = (b_1r^2/s^2, b_1rt/s^3)$, we have*

$$\hat{h}_\infty(P) \geq \frac{1}{8}\log n + \frac{1}{8}\log 2 + \frac{1}{2}\log\frac{b_1rt}{s^3} + 0.3465.$$

Proof. Using algorithm [2, Algorithm 7.5.7], we see that

$$\hat{h}_\infty(P) = \frac{1}{16}\log\frac{64n^3}{q} + \frac{1}{4}\log\omega_1 - \frac{1}{4}\log 2\pi + \frac{1}{2}\log\frac{b_1rt}{s^3} - \frac{1}{2}\log\theta, \tag{2.3}$$

where ω_1 is a real period of E_2 and $q = e^{2\pi\omega_1/\omega_2}$ and $\theta = \sum_{n=0}^{\infty}(-1)^n q^{\frac{n(n+1)}{2}} sin((2n+1)\lambda Re(z(P))$.
Using algorithm [2, Algorithm 7.4.7], we have

$$\omega_1 = \frac{\pi}{AGM(\sqrt[4]{4n}\,\sqrt[4]{n})} = \frac{\pi}{\sqrt[4]{n}AGM(\sqrt{2},1)}$$

and $\omega_2 = i\omega_1$, hence $q = e^{2\pi\omega_1/\omega_2} = e^{-2*\pi}$. On the other hand

$$|\theta| \leq \frac{1}{1-|q|} = \frac{1}{1-e^{-2\pi}}.$$

Combining these results yields the inequality. □

Theorem 2.4. *Let n be a positive square-free integer and E_n be the elliptic curve given by $y^2 = x^3 - nx$. For every $P \in E_{-n}(\mathbb{Q})$, we have*

$$\hat{h}(P) \geq \frac{1}{8}\log n + 0.4331.$$

Proof. Let $P = (b_1r^2/s^2, b_1rt/s^3)$, by Lemma 2.2 and Lemma 2.3, we have

$$\hat{h}(P) = \hat{h}_{fin} + \hat{h}_\infty \geq 2\log s - \tfrac{1}{2}\log b_1' + \hat{h}_2(P) + \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log\tfrac{b_1rt}{s^3} + 0.3465.$$

So we have to consider two cases:

- If b_1 is even then $b_1' = b_1/2$ and by [4] in proof of Lemma 2.2, $\hat{h}_2(P) = -log(2)/2$ so in this case

$$\hat{h}(P) \geq \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log rts + 0.3465 \geq \tfrac{1}{8}\log n + 0.4331.$$

- If b_1 is odd then $b_1' = b_1$, in this case we have four cases:
  - if b_2 is odd and r is odd then t is even so $t \geq 2$, on the other hand by item [2] in Lemma 2.2, $\hat{h}_2(P) = -log(2)/2$ so in this case
  $$\hat{h}(P) \geq \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log rs + 0.3465 \geq \tfrac{1}{8}\log n + 0.4331.$$
  - If b_2 is odd and r is even by [3] in proof of Lemma 2.2, $\hat{h}_2(P) = 0$ so in this case
  $$\hat{h}(P) \geq \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log rst + 0.3465 \geq \tfrac{1}{8}\log n + 0.4331.$$
  - If b_2 is even and r is odd then by [6] in proof of Lemma 2.2, $\hat{h}_2(P) = 0$ so in this case
  $$\hat{h}(P) \geq \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log rst + 0.3465 \geq \tfrac{1}{8}\log n + 0.4331.$$
  - If b_2 is even and r is even then $r \geq 2$, on the other hand by [5] in proof of Lemma 2.2, $\hat{h}_2(P) = -log(2)/2$ so in this case
  $$\hat{h}(P) \geq \tfrac{1}{8}\log n + \tfrac{1}{8}\log 2 + \tfrac{1}{2}\log ts + 0.3465 \geq \tfrac{1}{8}\log n + 0.4331.$$

As we saw, in any case we have $\hat{h}(P) \geq \frac{1}{8}\log n + 0.4331$. □

Now, we give an example which shows that this is the sharpest bound.

Example 2.5. *Let E be the elliptic curve $y^2 = x^3 - 5x$ and $P = [-1, 2]$, then by our result*

$$\hat{h}(P) \geq \tfrac{1}{8}\log 5 + 0.4331 = 0.634279739054262546825094916 7,$$

On the other hand, using PARI/GP, we see that

$$\hat{h}(P) = 0.635528714444549781146168191 3.$$

3 Family of Rank one Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$ and $E(\mathbb{Q})$ be its Mordell-Weil group over $\mathbb{Q}$ which is a finitely generated abelian group. The rank of the free part of $E(\mathbb{Q})$ as a $\mathbb{Z}$-module is called the rank of E over $\mathbb{Q}$. In this section, first we recall the concept of the root number and then using Parity conjecture we find a family of rank one elliptic curves, finally using height function we determine a generator for the family.

Definition 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ and n_p denotes the number of points in the reduction of curve modulo p. Also let $a_p = p+1-n_p$. The local part of the L-series of E at p is defined as*

$$L_p(T) = \begin{cases} 1-a_pT+pT^2 & \textit{if } E \textit{ has good reduction at } p, \\ 1-T & \textit{if } E \textit{ has split multiplicative reduction at } p, \\ 1+T & \textit{if } E \textit{ has non- split multiplicative reduction at } p, \\ 1 & \textit{if } E \textit{ has additive reduction at } p. \end{cases}$$

The L- series of E is defined to be

$$L(E,s) = \prod_p \frac{1}{L_p(p^{-s})},$$

where the product is over all primes.

Theorem 3.2. *The L- series $L(E,s)$ has an analytic continuation to the entire complex plane, and it satisfies the functional equation*

$$\Lambda(E,s) = \varepsilon(E)\Lambda(E,2-s),$$

where

$$\Lambda(E,s) = (N_{E/\mathbb{Q}})^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

$N_{E/\mathbb{Q}}$is the conductor of E and Γ is the Gamma function. Here $\varepsilon(E) = \pm 1$ is called the global root number of E.

The Parity conjecture states that

$$\varepsilon(E) = (-1)^{r_E}, \tag{3.1}$$

where r_E denotes the rank of Mordell- Weil group of E.

Proposition 3.3. *([8])For elliptic curve $E : y^2 = x^3 - dx$, such that $d \not\equiv 0 \ (mod\ 4)$, the sign of the global root number of the elliptic curve $E_d : y^2 = x^3 - dx$, has the following formula*

$$\varepsilon(E_d) = \begin{cases} -1 & \textit{if } d \equiv 2,5,6,7,9,10,14,15 \ (mod\ 16) \\ +1 & \textit{if } d \equiv 1,3,11,13 \ (mod\ 16) \end{cases}$$

Proposition 3.4. *Under the Parity conjecture, for every prime number $p \equiv 2,5,6,7,9,10,14,15 \ (mod\ 16)$, the rank of elliptic curve $E_{-p} : y^2 = x^3 - px$ is exactly one.*

Proof. By [5, Section X.6], for every prime number p, $rank(E_p) \leq 2$. On the other hand by Parity conjecture and 3.3, we know that the rank is odd, so $rank(E_{-p}) = 1$. □

Theorem 3.5. *For any prime number p of the form $p = 4r^2 + (n_1)^4$, where r is odd, the point $P = [-n_1, -n_1 r]$ is a generator of $E_p : y^2 = x^3 - px$.*

Proof. By Lemma 2.2, we know

$$\hat{h}_{fin}(P) = 2\log s - \frac{1}{2}\log n_1 + \hat{h}_2(P) \leq -\frac{1}{2}\log n_1$$

on the other hand

$$\hat{h}_\infty(P) \leq \frac{1}{8}\log p + \frac{1}{2}\log r + \frac{\pi}{8} + \frac{3}{8}\log 2 + \frac{1}{2}\log n_1,$$

Thus

$$\hat{h}(P) \leq \tfrac{1}{8}\log p + \tfrac{1}{2}\log r + 0.4794.$$

By Proposition 3.3, we know that $Rank(E_p) = 1$, Let Q be a generator of E_p, then there exists an integer $k \in \mathbb{Z}$ such that $P = kQ + n_1 T$, where T is a torsion point. Hence $\hat{h}(P) = k^2\hat{h}(Q)$, if $k \neq \pm 1$ then we have

$$\tfrac{1}{8}\log p + \tfrac{1}{2}\log r + 0.4794 \geq \hat{h}(P) = k^2\hat{h}(P) \geq k^2(\tfrac{1}{8}\log p + 0.4331) \geq 4(\tfrac{1}{8}\log p + 0.4331)$$

Thus

$$\tfrac{1}{2}\log r \geq \tfrac{3}{8}\log p \Longrightarrow r^2 \geq p$$

Which is a contradiction. So $k = \pm 1$ and hence P is a generator of the free part of $E_p(\mathbb{Q})$. □

4 Main Results

We show that for any positive square-free integer n, and for every non-torsion point $P \in E_{-n} : y^2 = x^3 - nx$, we have

$$\hat{h}(P) \geq \frac{1}{8}\log n + 0.4331.$$

Also we showed that this is the sharpest possible lower bound. Using this estimation, we showed that for every prime number p of the form $p = 4(2k+1)^2 + (n_1)^4$, the point $P = [-n_1, -n_1(2k+1)]$ is a generator of $E_p : y^2 = x^3 - px$.

References

[1] A. Bremner, J.H. Silverman, N. Tzanakis, *Integral points in arithmetic progression on $y^2 = x\left(x^2 - n^2\right)$*, J. Number Theory. **80(2)** (2000), 187–208.

[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, (1993).

[3] Y. Fujita, N. Terai, *Generators for the elliptic curve $y^2 = x^3 - nx$,* J. Theor. Nombres Bordeaux. **23** (2011) 403–416.

[4] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), 633–648.

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer-Verlag, New York, (1986).

[6] J. H. Silverman. *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.

[7] P. Voutier and M. Yabuta, *Lang's Conjecture and Sharp Height Estimates for the Elliptic Curves* $y^2 = x^3 + ax$, Int. J. Number Theory. **9(5)** (2013), 1141–1170.

[8] Birch B J, Stephens N M. *The parity of the rank of the Mordell-Weil group.* Topology, **5**(1966), 295–299.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 49-53.

Poster Presentation

The Relation between Chromatic Number of non-Commuting Graph and the Structure of $G/Z(G)$

H. R. Dorbidi
Department of Basic Sciences, University of Jiroft, Jiroft, Kerman, Iran
hr_dorbidi@ujiroft.ac.ir

Abstract

In this talk we study the relation between chromatic number of non-commuting graph and the structure of $G/Z(G)$. For small values of $\chi(G)$ we determine the structure of $G/Z(G)$.

Keywords: Non-commuting graph, chromatic number , clique number.

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1 Introduction

The non-commuting graph of a group is one of the first graphs that is associated to a group. In [1] the authors define the non-commuting graph and studied some properties of it. The non-commuting graph of a non-abelian group G denoted by Γ_G is a graph whose vertices are the elements of $G\backslash Z(G)$ and two distinct vertices x, y are adjacent iff $xy \neq yx$. In [1] the following conjecture was stated:

If $\Gamma_G \cong \Gamma_H$ then $|G| = |H|$.

This conjecture was answered negatively in [12]. The affirmative answer for simple groups and $p-$groups appeared in [6] and [2]. Another question that appeared in the subsequent papers is the following:

When the non-commuting graph determines the structure of group?

For simple groups this question answered in many papers. This is related to Thompson's conjecture about simple groups and prime graph of a group.

The chromatic number of a graph is the minimum number k such that the vertices of the graph can be colored by $\{1,\cdots,k\}$ such that adjacent vertices have different colours. The chromatic number of a graph is denoted by $\chi(G)$. A complete subgraphs of a graph is called a clique. The suprimum of the size of the cliques is called clique number and denoted by $\omega(G)$.

Let $\sigma(G)$ be the minimum number n such that G is union of n proper subgroups. If $\Phi(G)$ denotes the frattini subgroup of G then there is a relation between $\sigma(G)$ and the structure $G/\Phi(G)$. The relation between $\chi(G)$ and the structure of $G/Z(G)$ is a similar problem. It is proved that if G has at most 20 maximal subgroup then G is solvable. The similar problem states if $\omega(G)\leq 20$ then G is solvable.

2 Main Results

Theorem 1. *$\chi(G)$ is the minimum number of abelian groups which cover G.*

Theorem 2. *(Isaacs) $\chi(G)<\infty$ iff $\omega(G)<\infty$ iff $|G/Z(G)|<\infty$.*

Remark 1.

1. If $G=\bigcup_{i\in I}H_i$ and $S\subseteq I$ then $\bigcap_{i\in S}H_i=Z(G)$ or $\bigcap_{i\in S'}H_i=Z(G)$.
2. If $G=\bigcup_{i\in I}H_i$ and $S\subseteq I\backslash\{j\}$ then $\bigcap_{i\in S}H_i=Z(G)$ or $\bigcap_{i\in S'}H_i=Z(G)$ or $[G:H_j]=2$.
3. If $|G/Z(G)|=n$ and $|H_i/Z(G)|=a_i$ and $k_i=\frac{n}{a_i}$ then for $n=2m, 1<\sum_{i=1}^{m}(\frac{1}{k_{2i}}+\frac{1}{k_{2i-1}}-\frac{1}{k_{2i}k_{2i-1}})$ and for $n=2m+1, 1<\frac{1}{k_n}+\sum_{i=1}^{m}(\frac{1}{k_{2i}}+\frac{1}{k_{2i-1}}-\frac{1}{k_{2i}k_{2i-1}})$

Definition 1. A group G is called an $AC-$group if the centralizer of any non-central element is an abelian group.

The $AC-$groups are studied in [13] and [14].

Definition 2. The minimum number t such that $G=\bigcup_{i=1}^{t}C_G(g_i)$ where $g_1,\cdots,g_t\in G\backslash Z(G)$ denoted by $c(G)$.

Definition 3. A group G is called a $C-$group if $c(G)=\chi(G)$.

Lemma 3. $c(G)\leq\omega(G)\leq\chi(G)$.

Lemma 4. *If G is an $AC-$group then G is a $C-$group.*

Lemma 5. *If G is a $C-$group and $G = \cup_{i=1}^{t} H_i$ where $\chi(G) = t$ then $H_i \cap H_j = Z(G)$.*

Theorem 6. *If $|G/Z(G)| = pqr$ then G is an $AC-$group.*

Theorem 7. *If $|G/Z(G)|$ is a cube free number and every element has prime power order then G is an $AC-$group.*

Corollary 8. *If $G/Z(G) \cong A_5$ then G is an $AC-$group.*

Theorem 9.*[4] If G is a non-solvable finite group and $\omega(G) \leq 21$ then $G \cong Z(G) \times A_5$ and $\omega(G) = \chi(G) = 21$.*

Corollary 10. *If $\omega(G) \leq 20$ then G is a solvable group.*

Theorem 11. *If G is a finite group and $G/Z(G) \cong A_5$ then $G \cong Z(G) \times A_5$ and $\chi(G) = 21$.*

Theorem 12. *([11]) If $|G| = n$ then $\omega(G) \leq \chi(G) \leq \frac{n}{2} + 1$.*

Theorem 13. *If $G/Z(G)$ has an element of order n with k prime factors and $c(G) \geq k+1$ then $\omega(G) \geq n+1$. If G is a $C-$group or $k \leq 2$ then $c(G) \geq k+1$.*

Theorem 14. *If G is a $C-$group and $\chi(G) = t$ then $|G/Z(G)| \leq (t-1)^2$.*

Theorem 15. *$\chi(G) = 3$ iff $\omega(G) = 3$.*

Theorem 16. *$\omega(G) = 4$ then every element of $G/Z(G)$ has order two or three.*

Theorem 17. *$\omega(G) = 5$ then every element of $G/Z(G)$ has order $2, 3, 4$.*

The following Theorem of *G. Higman* classifies all the solvable groups G in which every element has prime power order[8][p 213].

Theorem 18. *Let G be a solvable group in which every element has prime power order. Then G is one of the following groups:*

1. *A Frobenius group $G = FH$, where F is an abelian $p-$group $(p > 2)$ and H is a generalized quaternion group.*

2. *G has a normal series $P \trianglelefteq PQ \trianglelefteq G$ where G/P and PQ are Frobenius groups, P and G/PQ are $p-$groups, PQ/P is a $q-$group, PQ/P and G/PQ are cyclic(Here $p|q-1$).*

Theorem 19. *If $G/Z(G)$ has a normal cyclic subgroup K of index p then $\chi(G) = |K| + 1$.*

Theorem 20. *If $G/Z(G) \cong D_n$ then $\chi(G) = n+1$. In particular, $\chi(D_{2n-2}) = n$.*

Corollary 21. *If $|G/Z(G)| = pq$ where $p \leq q$ then $G/Z(G) \cong D_4, \chi(G) = 5$ or $G/Z(G) \cong \bigoplus_{i=1}^{3} \mathbb{Z}_2$, $\chi(G) = 5, 7$.*

Corollary 22. *If $|G/Z(G)| = pqr$ where $p < q < r$ and $q \nmid r-1$ then $\chi(G) = qr + 1$.*

Corollary 23. *If* $|G/Z(G)| = 30$ *then* $\chi(G) = 16$.

Theorem 24.*[1]*

1. $\chi(GL_2(q)) = \omega(GL_2(q)) = q^2 + q + 1$.
2. $\chi(SL_2(q)) = \omega(SL_2(q)) = q^2 + q + 1$.
3. $\chi(PSL_2(q)) = \omega(PSL_2(q)) = q^2 + q + 1$.

Theorem 25. $\chi(G) = 3$ *iff* $G/Z(G) \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

Theorem 26. $\chi(G) = 4$ *iff* $G/Z(G) \cong \mathbb{Z}_3 \bigoplus \mathbb{Z}_3, S_3$.

Theorem 27. *If* $\chi(G) = 5$ *then* $G/Z(G) \cong \bigoplus_{i=1}^{3} \mathbb{Z}_2, A_4, D_4$ *or* $|G/Z(G)| = 16$.

Theorem 28. *If* $|G_1| = 20$ *and* G_1 *has no element of order* 10 *then* $G_1 \cong \langle a, b : a^4 = b^5 = 1, ab = b^2 a \rangle$.

Theorem 29. *If* $\chi(G) = 6$ *then* $G/Z(G) \cong G_1, D_5, \bigoplus_{i=1}^{2} \mathbb{Z}_5$ *or* $|G/Z(G)|\,|64$.

References

[1] A. Abdollahi, A. Akbari and H.R. Maimani, *Non-commuting graph of a group* J. Algebra,**298** (2006), 468-492.

[2] A. Abdollahi, S. Akbari, H. R. Dorbidi, H. Shahverdi, *Commutativity pattern of finite non-abelian p-groups determine their orders*, Comm Algebra, **41**, (2013), 451-461.

[3] A. Abdollahi, A. Azad,A. Mohammadi Hassanabadi, M. Zarrin,*On the Clique Numbers of Non-commuting Graphs of Certain Groups*, Algebra Colloquium,**17** no. 4 (2010), 611-620.

[4] A. Abdollahi, A. Mohammadi Hassanabadi, *Finite groups with a certain number of elements pairwise generating a non-nilpotent subgroup*, Bull. Iranian Math. Soc.**30** (2) (2004), 1-20.

[5] E. A. Bertram, *Some applications of graph theory to finite groups*, Discrete Math. **44** (1983) 31-43.

[6] M.R. Darafsheh, *Groups with the same non-commuting graph*, Discrete Appl. Math.**157** (2009) no. 4, 833-837.

[7] P. Erdös and E. G. Straus, *How abelian is a finite group?*, Linear and Multilinear Algebra, **3** (1976), 307-312.

[8] B. Huppert, Character Theory of Finite Groups, De Gruyter Expositions in Mathematics, New York (1998).

[9] I. M. Isaacs, *Equally partition groups*, Pacific Journal of Math.**49**, No.1 (1973).

[10] N. Ito, *On finite groups with given conjugate types*, Nagoya Math. J.**6**,(1953), 17-28.

[11] D. R. Mason, *On coverings of a finite group by abelian subgroups*, Math. Proc. Cambridge. Phil. Soc. **83** (1978), 205-209.

[12] A.R. Moghaddamfar, *About Noncommuting graphs*, Siberian Math. J.**47**, No.5, (2005), 1112-1116.

[13] D. M. Rocke, *p-groups with abelian centralizers*, Proc. London Math. Soc.**30** (1975), no 3, 55-75.

[14] R. Schmidt, *Zentralisatorverbands endlicher gruppen*, rend. Sem. Mat. Univ. Padova,**44** (1970), 97-131.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 55-58.

Oral Presentation

The Groups with few End Vertices in their Coprime Graphs

H. R. Dorbidi
Department of Basic Sciences, University of Jiroft, Jiroft, Kerman, Iran
hr_ dorbidi@ujiroft.ac.ir

Abstract

In this talk we classify the groups whose coprime graphs has at most seven end vertices.

Keywords: Coprime graph, end vertex.

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1 Introduction

In this paper we study the coprime graph of a group is defined in [4]. The coprime graph of a group G, denoted by Γ_G, is a graph whose vertices are elements of G and two elements $x \neq y$ are adjacent iff $(|x|,|y|) = 1$. The following question were posed in [4]:

Classify groups with three end vertices.

Wse classify groups with at most seven end vertices. First we recall some facts and notations related to this paper. Throughout this paper G denotes a nontrivial finite group. The centralizer of $a \in G$ is denoted by $C_G(a)$. If $H \leq G$ the normalizer of H is denoted by $N_G(H)$. Also $Z(G)$ denotes the center of G. The symmetric group on n letters is denoted by S_n.

Let $\pi(n)$ be the set of prime divisors of n. For a natural number $n = p_1^{n_1} \cdots p_k^{n_k}$ set $r(n) = p_1 \cdots p_k$.

Let Γ be a simple graph. The *degree* of $v \in V(\Gamma)$ denoted by $d(v)$. The set of vertices which are adjacent to v is denoted by $N_\Gamma(v)$. A vertex of degree one is called an end vertex.

2 Main Results

In this section we classify groups with at most seven end vertices.

Lemma 1. *Set $f(n)=\sum\phi(d)$, where $r(n)|d|n$. If $n=p_1^{n_1}\cdots p_k^{n_k}$ then $f(n)=(p_1^{n_1}-1)\cdots(p_k^{n_k}-1)$.*

Lemma 2. *Let $a\in G$ be an element of order n. Then $deg(a)=1$ i.e a is an end vertex iff $r(n)=r(G)$. Also G contains at least $f(n)$ end vertices.*

Theorem 3. *Assume Γ_G has at most seven end vertices. If a is an end vertex with maximal order then $o(a)\in\{2,3,4,5,6,7,8,10,12,14\}$. Also $\pi(G)\leq 2$ and $\pi(G)\subseteq\{2,3,5,7\}$.*

The following Theorem is a part of a Frobenius theorem in [3][Theorem 9.9,p 119-120].

Theorem 4. *If $m||G|$ then $|\{g\in G: g^m=1\}|$ is divisible by m.*

Theorem 5. *Let G be a group of order 18 which has an element of order six. Then one of the following occurs:*

1. *G is an abelian group and $G\cong\mathbb{Z}_2\bigoplus\mathbb{Z}_3\bigoplus\mathbb{Z}_3,\mathbb{Z}_2\bigoplus\mathbb{Z}_9$. In this case Γ_G has $f(18)=8$ end vertices.*
2. *$G\cong\left\langle b,c,d: b^2=c^3=d^3=1, cd=dc, cb=bc, bdb^{-1}=d^{-1}\right\rangle$. Also G has three element of order two, eight elements of order three and six elements of order six.*

Theorem 6. *Let G be a group such that $\pi(G)=\{2,p\}$ and $p^2\nmid|G|$. Let a be an element of order n. Assume every end vertex of Γ_G be in $\langle a\rangle$. Then $\langle a\rangle$ is a characteristic subgroup of G. Also its $p-$Sylow subgroup is the unique subgroup of order p. Also every element in $G\backslash\langle a\rangle$ is a $2-$power element.*

Theorem 7. *Assume Γ_G has at most seven end vertices. Let a be an end vertex of maximal order. If $o(a)\in\{2,3,4,5,7,8\}$ then $G\cong\mathbb{Z}_2,\mathbb{Z}_3,\mathbb{Z}_4,\mathbb{Z}_2\bigoplus\mathbb{Z}_2,\mathbb{Z}_5,\mathbb{Z}_7,\mathbb{Z}_2\bigoplus\mathbb{Z}_2\bigoplus\mathbb{Z}_2,\mathbb{Z}_2\bigoplus\mathbb{Z}_4,\mathbb{Z}_8,Q_4,D_4$.*

Theorem 8. *Assume Γ_G has at most seven end vertices. Let a be an end vertex of maximal order. If $o(a)=6$ then G is one the following groups:*

1. *$G\cong\mathbb{Z}_6$ and Γ_G has two end vertices.*
2. *$G\cong\left\langle a,b: a^6=b^2=1, bab^{-1}=a^{-1}\right\rangle\cong D_6$ and Γ_G has two end vertices.*
3. *$G\cong\left\langle a,b: a^6=1, b^2=a^3, bab^{-1}=a^{-1}\right\rangle=Q_6$ and Γ_G has two end vertices.*
4. *$G\cong\mathbb{Z}_2\bigoplus\mathbb{Z}_2\bigoplus\mathbb{Z}_3$ and Γ_G has six end vertices.*
5. *$G\cong\left\langle b,c,d: b^2=c^3=d^3=1, cd=dc, cb=bc, bdb^{-1}=d^{-1}\right\rangle$ and Γ_G has six end vertices.*
6. *$|G|=24,36,72$.*

Theorem 9. *Assume Γ_G has at most seven end vertices. Let a be an end vertex of maximal order. If $o(a)=10$ then G is one the following groups:*

1. *$G\cong\mathbb{Z}_{10}$ and Γ_G has four end vertices.*
2. *$G\cong\left\langle a,b: a^{10}=b^2=1, bab^{-1}=a^{-1}\right\rangle\cong D_{10}$ and Γ_G has four end vertices.*

3. $G \cong \langle a,b : a^{10} = 1, b^2 = a^5, bab^{-1} = a^{-1} \rangle$ *and* Γ_G *has four end vertices.*

4. $G \cong \langle a,b : a^{10} = 1, b^4 = a^5, bab^{-1} = a^{-1} \rangle$ *and* Γ_G *has four end vertices.*

Theorem 10. *Assume Γ_G has at most seven end vertices. Let a be an end vertex of maximal order. If $o(a) = 12$ then G is one of the following groups:*

1. $G \cong \mathbb{Z}_{12}$ *and* Γ_G *has six end vertices.*

2. $G \cong \langle a,b : a^{12} = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{12}$ *and* Γ_G *has six end vertices.*

3. $G \cong \langle a,b : a^{12} = b^2 = 1, bab^{-1} = a^5 \rangle$ *and* Γ_G *has six end vertices.*

4. $G \cong \langle a,b : a^{12} = 1, b^2 = a^6, bab^{-1} = a^{-1} \rangle$ *and* Γ_G *has six end vertices.*

5. $G \cong \langle a,b : a^{12} = 1, b^2 = a^6, bab^{-1} = a^5 \rangle$ *and* Γ_G *has six end vertices.*

6. $G \cong \langle a,b : a^{12} = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle \cong \langle a,b : a^{12} = 1, b^2 = a^{-3}, bab^{-1} = a^{-1} \rangle$ *and* Γ_G *has six end vertices.*

7. $G \cong \langle a,b : a^{12} = 1, b^2 = a^3, bab^{-1} = a^5 \rangle \cong \langle a,b : a^{12} = 1, b^2 = a^{-3}, bab^{-1} = a^5 \rangle$ *and* Γ_G *has six end vertices.*

Theorem 11. *Assume Γ_G has at most seven end vertices. Let a be an end vertex of maximal order. If $o(a) = 14$ then G is one of the following groups:*

1. $G \cong \mathbb{Z}_{14}$ *and* Γ_G *has six end vertices.*

2. $G \cong \langle a,b : a^{14} = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{14}$ *and* Γ_G *has six end vertices.*

3. $G \cong \langle a,b : a^{14} = 1, b^2 = a^7, bab^{-1} = a^{-1} \rangle$ *and* Γ_G *has six end vertices.*

Corollary 12.

1. Γ_G *has two end vertices iff* $G \cong \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_6$,
   $\langle a,b : a^6 = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_6$,
   $\langle a,b : a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle = Q_6$.

2. Γ_G *has three end vertices iff* $G \cong \mathbb{Z}_4, \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

3. Γ_G *has four end vertices iff* $G \cong \mathbb{Z}_5, \mathbb{Z}_{10}$,
   $\langle c,d,e : c^2 = d^4 = e^3 = 1, cd = dc, ce = ec, ded^{-1} = e^{-1} \rangle$,
   $\langle a,b : a^{10} = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{10}$,
   $\langle a,b : a^{10} = 1, b^2 = a^5, bab^{-1} = a^{-1} \rangle$,
   $\langle a,b : a^{10} = b^4 = 1, bab^{-1} = a^{-1} \rangle$,
   $\langle a,b : a^{10} = 1, b^4 = a^5, bab^{-1} = a^{-1} \rangle$.

4. *If* Γ_G *has six end vertices then* $|G| = 24, 36, 72$ *or* $G \cong \mathbb{Z}_7, \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_3, \mathbb{Z}_{12}, \mathbb{Z}_{14}$,
   $\langle b, c, d : b^2 = c^3 = d^3 = 1, cd = dc, cb = bc, bdb^{-1} = d^{-1} \rangle$,
   $v\langle a, b : a^{12} = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{12}$,
   $\langle a, b : a^{12} = b^2 = 1, bab^{-1} = a^5 \rangle$,
   $\langle a, b : a^{12} = 1, b^2 = a^6, bab^{-1} = a^{-1} \rangle$,
   $\langle a, b : a^{12} = 1, b^2 = a^6, bab^{-1} = a^5 \rangle$,
   $\langle a, b : a^{12} = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle \cong \langle a, b : a^{12} = 1, b^2 = a^{-3}, bab^{-1} = a^{-1} \rangle$,
   $\langle a, b : a^{12} = 1, b^2 = a^3, bab^{-1} = a^5 \rangle \cong \langle a, b : a^{12} = 1, b^2 = a^{-3}, bab^{-1} = a^5 \rangle$,
   $\langle a, b : a^{14} = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_{14}$,
   $\langle a, b : a^{14} = 1, b^2 = a^7, bab^{-1} = a^{-1} \rangle$.

5. Γ_G *has seven end vertices iff* $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_2, \mathbb{Z}_2 \bigoplus \mathbb{Z}_4, \mathbb{Z}_8, Q_4, D_4$.

References

[1] J. A. Bondi, J. S. Murty, Graph theory with applications, American Elsevier Publishing Co, INC, 1997.

[2] J. A. Gallian, Contemporary Abstract Algebra, D. C. Heath and company, 1994.

[3] B. Huppert, Character Theory of Finite Groups, DE Gruyter Expositions in Mathematics, New York 1998.

[4] X. Ma, H. Wei, L. Yang,The Coprime Graph of a Group, Int. J. Group Theory, Vol 3(no 3) (2014) 13-23.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 59-60.

Poster Presentation

Energy of Infinite Class of (3,6)-Fullerene Graphs

M. Faghani
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran
mo_faghan@yahoo.com

S. Firouzian
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran
siamfirouzian@pnu.ac.ir

M. Nouri Jouybari
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran
mostafa_umz@yahoo.com

Abstract

Suppose F be a (3,6)-Fullerene graph with n vertices, namely a planar 3-regular graph have triagonal and hexagonal faces. If A be adjacency matrix of F and $\lambda_1, \ldots, \lambda_n$ be eigenvalue of A we know the energy of a graph is:$E(G) = \sum_{i=1}^{n} |\lambda_i|$. In this paper we consider an infinie class of fullerene graph with $8n$ vertices and find suitable labeling that be centrosymmetric. Finally with suitable blocking and by properties of centrosymmetric matrix, find a upper bound of energy of infinite class of this fullerene.

Keywords: Centrosymmetric matrix, labeling, fullerene graph, energy.

MSC(2010): Primary: 05C35; Secondary: 05C50; 92E10.

References

[1] M. Ghorbani, M. Faghani, A. R. Ashrafi, S. Heidari Rad, A. Graovac, *Upper Bound for Energy of Matrices Associated to an Infinite Class of Fullerenes,* MATCH Commun. Math. Comput. Chem. **Vol.71** (2014), 341-354.

[2] G. Y. Katona , M. Faghani, A. R. Ashrafi, *Centrosymmetric graphs and a lower bound for graph energy of fullerenes,* Discussion Mathematicae, (2014), 1-18.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 61-62.

Poster Presention

Average Distance of Infinite Class of (3,6)-Fullerene Graphs

M. Faghani
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran
mo_faghan@yahoo.com

S. Firouzian
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran
siamfirouzian@pnu.ac.ir

P. Ziyabakhsh
Department of Mathematics, Payame Noor University (PNU), P.O. Box 19395-3697 Tehran, Iran

Abstract

Suppose F be a (3,6)-Fullerene graph with n vertices, namely a planar 3-regular graph have triagonal and hexagonal faces. We know from Euler's formula, number of triangle in these graphs be four. Diastance between two x and y vertices be length of shortest path between x and y, and has been shown $d(x,y)$. Consider $W(F)$ be half sum of distances between vertices exclusively and Define average of distance of F be $\mu(G) = \frac{W(F)}{\binom{n}{2}}$. Generally this invariant problem in fullerene graphs be unsolved. In this paper we consider an infiinite class of (3,6)-fullerene graph with $8n$ vertices and compute average distance of them. By this value, we present some bound of invariant of this graphs.

Keywords: Fullerene graph, Wiener index, average distance.

MSC(2010): Primary: 05C35; Secondary: 05C50; 92E10.

References

[1] Simon Mukwembi, *Average Distance, Independence Number and Spanning Trees,* Journal of Graph Theory, **Vol.76** (2012), 194-199.

[2] Rao Li, *A note on the Average Distance of a Graph,* Discussion Mathematicae, **Vol.14** (2011), 531-536.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 63-67.

Poster Presentation

Considering the Information Criteria

Masume Ghahramani
Department of Mathematics, Gilan-E-Gharb Branch, Islamic Azad University, Gilan-E- Gharb, Iran
mghdatagilan@gmail.com

Mehdi Shams
Department of Statistics, School of Mathematical Sciences, University of Kashan, Kashan, Iran
mehdishams@kashanu.ac.ir

Abstract

Statistical modeling is a crucial issue in scientific data analysis. Models are used to represent stochastic structures, predict future behaviour, and extract usful information from data. Many researchers in medicine, engineering, social sciences and economics, planning, management, geography, physics, mathematics, statistics and other sciences to conduct an investigation, according to the data available for the test under consideration requires notice to the selection criteria models are suitable. When the correct model is unknown, the researchers proposed a family of models to find the closest model is the correct model, it is necessary to define a criterion for unbiased information. This paper examines the information criteria AIC and AICc deals.

Keywords: Bias, information criterion, Kullback-Leibler risk.

MSC(2010): Primary: 94A15; Secondary: 65F05, 46L05, 11Y50.

1 Introduction

Statistical modeling is used for investigating a random phenomenon that is not completely predictable. One of the criteria that have usage of the frequency in model selection is Kullback-Leibler (KL) information criterion (see Kullback and Leibler 1951). This information criterion was introduced as one risk in model selection. Akaike (1973) introduced information criterion, AIC as asymptotically the unbiased of an estimator for the second term the KL risk and to form penalty likelihood function. Akaike stated modeling is not only finding a model which describes the behavior of the observed data, but it is main aim is predicted as a possible good, the future of the process under investigation. The during these years has been made the corrections on penalty term, and criteria such as AIC (Akaike 1973), TIC (Takeuchi 1976), are introduced. In section 2, is stated the Kullbake-Liebler risk and a consistent information criterion is proposed instead of the AIC. In section 3, information criterion $A'ICc$ is proposed instead of the AICc. In section 4, we present the main results.

2 Kullback-Leibler (KL)

Let $X = (X_1, ..., X_n)$ is a i.i.d random sample from true model and unknown, $h(.)$ and the family $F_{\theta_k} = \{f(.;\theta_k) = f_{\theta_k}; \theta_k \in \Theta \subseteq R^k\}$ from offered models has been considered for approximate true model. The family F_{θ_k} is well specified, if there is a $\theta_0 \in \Theta$ such that $h(.) = f(.;\theta_0)$; otherwise it is mis specified. The KL risk definds for generate model and unknown $h(.)$, and offered model, f_{θ_k} as:

$$KL(h, f_{\theta_k}) = E_h[log(\frac{h(.)}{f(.;\theta_k)})] = E_h[logh(.)] - E_h[logf(.;\theta_k)] \quad (1)$$

The expectation is taken with respect to the unknown model $h(.)$. The first term in the right hand side of (1) is called irrelevant part, because it does not depend on θ_k , and the second term is called relevant part. Based on the properties of the KL risk, the smaller value showed the closeness of the offered model to the unknown and true model. Therefore the problem reduces to obtain a good estimate of the expected log-likelihood. Since the expectation is with respect to the model with unknown parameters, one estimator is $E_h\{logf(.;\hat{\theta}_n)\} = \frac{1}{n}\sum_{i=1}^{n} logf(X_i;\hat{\theta}_n)$. So that $\hat{\theta}_n$ is the maximum likelihood estimator of θ_k and $f(.;\hat{\theta}_n)$ is the maximum likelihood function.
The general form of the information criterion that has been shown by IC, as:

IC = -2 (log-likelihood of statistical model - bias estimator)=$-2l_f(\hat{\theta}_n)$ +2 bias estimator.

Akaike, when offered family is well specified, size of bias is estimated with dimensional parameter $\hat{\theta}_n$, means k, and Akaike information criterion, is stated as: $AIC = -2l_f\hat{\theta}_n + 2k$.
With attention to form the AIC by increasing the number of parameters in the offered model the penalty term, 2k will be increased and the term -2$\sum_{i=1}^{n} logf(X_i;\hat{\theta}_n)$ will be decrease. Penalty term is constant to chance of size sample in the information criterion AIC, and by increasing the size sample, AIC can not distinguish the true model with the probability one. Therefore this problem is the same concept of inconsistency for an information criterion. Following the inconsistency of information criterion AIC, based on the definition similar to the definition of AIC, a consistent of information criterion which called $A'IC$ has presented. Akaike information criterion, by Akaike for model selection is introduced, but this useful criterion is inconsistent (see Akaike 1973). In this selection the bias term has used in the general form information criterion is considered from another perspective. We obtain the information criterion that furthermore has nice specials the information criterion AIC, it is also consistent. In the beginning the bais of the log-likelihood function as follows:

$$b = E_h\{logf(.;\hat{\theta}_n) - nE_h\{logf(Z;\hat{\theta}_n)\},$$

so that Z is a random variable i.i.d with $X_i's$. In the second term of the right hand side the inner expectation is calculated with respect to h(z) and the outer expectation is calculated with respect to h(x). By evaluating the bias it is composed as follows:

$$b = E_h\{logf(.;\hat{\theta}_n) - logf(.;\theta_0)\} + E_h\{logf(.;\theta_0) - nE_h\{logf(Z;\theta_0)\}\}$$
$$+nE_h\{E_h\{logf(Z;\theta_0) - E_h\{logf(Z;\hat{\theta}_n)\}\} = b_1 + b_2 + b_3.$$

We calculate the three expectations separately b_1, b_2 and b_3.
a) For calculation of b_1 by writing $l_f(\theta_0) = logf(.;\theta_0)$ and by applying a Taylor series expansion around the maximum likelihood estimator $\hat{\theta}_n$, we have

$$l_f(\theta_0) = l_f(\hat{\theta}_n) + (\theta_0 - \hat{\theta}_n)^T \frac{\partial l_f(\theta)}{\partial \theta} \mid_{\theta=\hat{\theta}_n} + \frac{1}{2}(\theta_0 - \hat{\theta}_n)^T \frac{\partial^2 l_f(\theta)}{\partial \theta \partial \theta^T} \mid_{\theta=\hat{\theta}_n} (\theta_0 - \hat{\theta}_n) + o_p(1) \quad (2)$$

$o_p(1)$ is expression of quantity that in the probability tends to zero. With attention to, the $\frac{\partial l_f(\theta)}{\partial \theta} \mid_{\theta=\hat{\theta}_n} = 0$ and $\frac{1}{n}\frac{\partial^2 l_f(\theta)}{\partial \theta \partial \theta^T} \mid_{\theta=\hat{\theta}_n}$ is converge to $J(\theta_0)$. (for more study see Akaike 1973).
So, $J(\theta_0) = -E_h[\frac{\partial^2 l_f(\theta)}{\partial \theta \partial \theta^T}] \mid_{\theta=\theta_0}$ Thus, the relation above can be approximated, as:

$$l_f(\hat{\theta}_n) - l_f(\theta_0) \approx \frac{n}{2}(\theta_0 - \hat{\theta}_n)^T J(\theta_0)(\theta_0 - \hat{\theta}_n) + o_p(1)$$

This based on the b_1 can be written as follow:

$$b_1 \approx E_h\{\frac{n}{2}(\theta_0 - \hat{\theta}_n)^T J(\theta_0)(\theta_0 - \hat{\theta}_n)\} \quad (3)$$

b) The b_2 does not contain an estimator and it can easily be written as;

$$b_2 = E_h\{logf(.;\theta_0) - nE_h\{logf(Z;\theta_0)\}\} = 0 \quad (4)$$

c) For calculation of value the b_3 first, the phrase $E_h\{logf(Z;\theta_0)\}$ be definded equally of $\Omega(\hat{\theta}_n)$. By using from Taylor expectation $\Omega(\hat{\theta}_n)$ around θ_0 we have:

$$\Omega(\hat{\theta}_n) = \Omega(\theta_0) + (\hat{\theta}_n - \theta_0)^T \frac{\partial \Omega(\theta)}{\partial \theta} \mid_{\theta=\theta_0} + \frac{1}{2}(\hat{\theta}_n - \theta_0)^T \frac{\partial^2 \Omega(\theta)}{\partial \theta \partial \theta^T} \mid_{\theta=\theta_0} (\hat{\theta}_n - \theta_0) + o_p(1)$$

with attention to the $\frac{\partial \Omega(\theta)}{\partial \theta} \mid_{\theta=\theta_0} = 0$. Thus when n tends to infinity, the relation above can be approximated as:

$$\Omega(\hat{\theta}_n) \approx \Omega(\theta_0) + \frac{1}{2}(\hat{\theta}_n - \theta_0)^T J(\theta_0)(\hat{\theta}_n - \theta_0) + o_p(1)$$

Thus the b_3 can be written as:

$$b_3 \approx \frac{n}{2} E_h\{(\hat{\theta}_n - \theta_0)^T J(\theta_0)(\hat{\theta}_n - \theta_0)\} \quad (5)$$

If the family of F_{θ_k} is well specified, with attention to quadratic forms in relations (3) and (5), that converge to centrally distributed chi-square with k degrees of freedom. Therefore b_1 and b_3 can be written as:

$$b_1 = b_3 = \frac{n}{2}k \quad (6)$$

So by combining of b_1 and b_3 , in relation (6) and , in relation (4), bias the b is as follow: $b = b_1 + b_2 + b_3 = nk$. With replacing the value of b in the general form of the information criterion, the

offered information criterion called, $A'IC$ is obtained as: $A'IC = -2l_f(\hat{\theta}_n)$+2nk.
In the offered information criterion $A'IC$, penalty term 2nk changes will change with sample size changes. So, if sample size will be very large, information criterion $A'IC$, with the probability of one, find the true model data. In other words information criterion $A'IC$, is the only consistent information criterion, that has been obtained based on Kullback-Leibler risk. (For further study about the consistency of an information criterion, see Hu and Shao 2008).

3 Information criterion AICc

The AIC penalizes for the addition of parameters, and thus selects a model that fits well but has a minimum number of parameters (i.e., simplicity and parsimony). For small sample sizes (i.e. $\frac{n}{k} < 40$), the second-order Akaike Information Criterion($AICc$) should be used instead:

$$AICc = -2(log - likelihood) + 2k + \frac{2k(k+1)}{n-k-1} = AIC + \frac{2k(k+1)}{n-k-1}$$

where n is the sample size. As sample size increases, the last term of the AICc approaches zero, and the AICc tends to yield the same conclusions as the AIC (Burnham and Anderson 2002). By attention to information criterion $A'IC$, information criterion $A'ICc$ is proposed instead of the AICc.

$$A'ICc = -2(log - likelihood) + 2nk + \frac{2k(k+1)}{n-k-1} + 2k - 2k = A'IC + \frac{2k(k+1)}{n-k-1}.$$

4 Main Results

The Akaike information criterion (AIC) is a measure of the relative quality of a statistical model, for a given set of data. As such, AIC provides a means for model selection. The AIC can not distinguish the true model with the probability one. Therefore this paper a consistent information criterion is proposed instead of the AIC, and also information criterion $A'ICc$ is proposed instead of the AICc. for future research to further explore the information criteria AIC, $A'IC$, AICc and $A'ICc$ in different models to be compared, and the principle of parsimony and goodness of fit can be examined.

References

[1] Akaike, H, *Information theory and an extension of maximum likelihood principle*, In Second Intention Symposium on Information Theory,. (1973), 267-281.

[2] Akaike, H, *A new look at the statistical model identification*, ,IEEE Transactions on Automatic Control (1974), 19 (6): 716 723.

[3] Burnham, K. P.; Anderson, D. R. , *Multimodel inference: understanding AIC and BIC in Model Selection* , Sociological Methods and Research (2002), 33: 261304.

[4] Hu, B. Shao, J, *Generalized linear model selection using r*, journal of statistical planning and information (2008), 138, 3705-3712.

[5] Konishi, S. and Kitagawa, G, *Generalized information criteria in model selection*, Biometrika (1996), 83, 875-890.

[6] Kullback, S., Leibler, R.A., *On information and sufficiency*. Ann. Math. Statist, (1951), 22, 1,76-86.

[7] Takeuchi, K., *Distribution of information statistics and criteria for adequacy of models*, mathematical sciences in japan (1976), 153, 12-18 .

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 69-72.

Poster Presentation

Information Theory in Statistics

Masume Ghahramani
Department of Mathematics, Gilan-E-Gharb Branch, Islamic Azad University, Gilan-E- Gharb, Iran
mghdatagilan@gmail.com

Mehdi Shams
Department of Statistics, Faculty of Mathematical Sciences, University of Kashan , Kashan, Iran
mehdishams@kashanu.ac.ir

Abstract

Information theory is a branch of applied mathematics, electrical engineering, and computer science involving the quantification of information. Information theory was developed by Claude E. Shannon to find fundamental limits on signal processing operations such as compressing data and on reliably storing and communicating data. Since its inception it has broadened to find applications in many other areas, including statistical inference, natural language processing, cryptography, neurobiology, the evolution and function of molecular codes, model selection in ecology, thermal physics, quantum computing, linguistics, plagiarism detection, pattern recognition, anomaly detection and other forms of data analysis. Theory of information in all applications. This article briefly describe some of the information theory Deals.

Keywords: Entropy, estimation theory, Kullback-Leibler.

MSC(2010): Primary: 94A15; Secondary: 65F05, 46L05, 11Y50.

1 Introduction

A key measure of information is entropy, which is usually expressed by the average number of bits needed to store or communicate one symbol in a message. Entropy quantifies the uncertainty involved in predicting the value of a random variable. For example, specifying the outcome of a fair coin flip (two equally likely outcomes) provides less information (lower entropy) than specifying the outcome from a roll of a die (six equally likely outcomes). Applications of fundamental topics of information theory include lossless data compression (e.g. ZIP files), lossy data compression (e.g. MP3s and JPEGs), and channel coding (e.g. for Digital Subscriber Line (DSL)). The field is at the intersection of mathematics, statistics, computer science, physics, neurobiology, and electrical engineering. Its impact has been crucial to the success of the Voyager missions to deep space, the invention of the compact disc, the feasibility of mobile phones, the development of the Internet, the study of linguistics and of human perception, the understanding of black holes, and numerous other fields. Important sub-fields of information theory are source coding, channel coding, algorithmic complexity theory, algorithmic information theory, information-theoretic security, and measures of information. Information theory to include, Coding theory [1], Detection theory [2], Estimation theory [3] , Fisher information [4], Information theory and measure theory [5], deals. In this article, we briefly review the information theory. In section 2, is stated quantities of informations, In section 3, is presented Kullback- Leibler (KL) divergence, In section 4, is stated estimation theory, In section 5, we present the main results.

2 Quantities of Information

Information theory is based on probability theory and statistics. The most important quantities of information are entropy, the information in a random variable, and mutual information, the amount of information in common between two random variables. The former quantity indicates how easily message data can be compressed while the latter can be used to find the communication rate across a channel. The choice of logarithmic base in the following formulae determines the unit of information entropy that is used. The most common unit of information is the bit, based on the binary logarithm. Other units include the nat, which is based on the natural logarithm, and the hartley, which is based on the common logarithm. In what follows, an expression of the form $p \log p$ is considered by convention to be equal to zero whenever $p = 0$. This is justified because $\lim_{p \to 0^+} p \log p = 0$ for any logarithmic base.

Entropy of a Bernoulli trial as a function of success probability, often called the binary entropy function $H_b(p)$. The entropy is maximized at 1 bit per trial when the two possible outcomes are equally probable, as in an unbiased coin toss. The entropy H, of a discrete random variable X is a measure of the amount of uncertainty associated with the value of X. Suppose one transmits 1000 bits (0s and 1s). If these bits are known ahead of transmission (to be a certain value with absolute probability), logic dictates that no information has been transmitted. If, however, each is equally and independently likely to be 0 or 1, 1000 bits (in the information theoretic sense) have been transmitted. Between these two extremes, information can be quantified as follows. If $\mathbb{X}$ is the set of all messages $\{x_1, \ldots, x_n\}$, that X could be, and $p(x)$ is the probability of some $x \in \mathbb{X}$, then the entropy H, of X is defined: $H(X) = E_X[I(x)] = -\sum_{x \in \mathbb{X}} p(x) log p(x)$. (Here $I(x)$ is the self-information, which is the entropy contribution of an individual message, and E_X is the expected value.) An important property of entropy is that it is maximized when all the messages in the message space are equiprobable $p(x) = \frac{1}{n}$ most unpredictablein which case $H(X) = \log n$. The special case of information entropy for a random variable with two outcomes is the binary entropy function, usually taken to the logarithmic base 2: $H_b(p) = -p \log p - (1-p) \log(1-p)$.

2.1 Joint Entropy

The joint entropy of two discrete random variables X and Y is merely the entropy of their pairing: (X,Y). This implies that if X, and Y, are independent, then their joint entropy is the sum of their individual entropies. For example, if (X,Y) represents the position of a chess piece X the row and Y the column, then the joint entropy of the row of the piece and the column of the piece will be the entropy of the position of the piece:

$$H(X,Y) = E_{X,Y}[-\log p(X,Y)] = -\sum_{x,y} p(x,y)\log p(x,y).$$

Despite similar notation, joint entropy should not be confused with cross entropy [6].

2.2 Conditional entropy (equivocation)

The conditional entropy or conditional uncertainty of X given random variable Y (also called the equivocation of X about Y) is the average conditional entropy over Y :

Because entropy can be conditioned on a random variable or on that random variable being a certain value, care should be taken not to confuse these two definitions of conditional entropy, the former of which is in more common use [7]. A basic property of this form of conditional entropy is that:

$$H(X \mid Y) = H(X,Y) - H(Y).$$

3 Kullback- Leibler (KL) divergence

Another interpretation of KL divergence is this: suppose a number X is about to be drawn randomly from a discrete set with probability distribution p(x). If Alice knows the true distribution p(x), while Bob believes (has a prior) that the distribution is q(x), then Bob will be more surprised than Alice, on average, upon seeing the value of X. The KL divergence is the (objective) expected value of Bob's (subjective) surprisal minus Alice's surprisal, measured in bits if the log is in base 2. In this way, the extent to which Bob's prior is "wrong" can be quantified in terms of how "unnecessarily surprised" it's expected to make him. Other important information theoretic quantities include Renyi entropy (a generalization of entropy), differential entropy (a generalization of quantities of information to continuous distributions), and the conditional mutual information.

The Kullback-Leibler divergence (or information divergence, information gain, or relative entropy) is a way of comparing two distributions: a "true" probability distribution p(X), and an arbitrary probability distribution q(X). If we compress data in a manner that assumes q(X) is the distribution underlying some data, when, in reality, p(X) is the correct distribution, the Kullback-Leibler divergence is the number of average additional bits per datum necessary for compression. It is thus defined

$$D_{KL}(P(X) \mid\mid q(X)) = \sum_{x\in\mathbb{X}} -p(x)\log q(x) - \sum_{x\in\mathbb{X}} -p(x)\log p(x) = \sum_{x\in\mathbb{X}} p(x)\log\frac{p(x)}{q(x)}.$$

Although it is sometimes used as a 'distance metric', KL divergence is not a true metric since it is not symmetric and does not satisfy the triangle inequality (making it a semi-quasimetric) [8].

4 Estimation theory

Estimation theory is a branch of statistics that deals with estimating the values of parameters based on measured/empirical data that has a random component. The parameters describe an underlying physical setting in such a way that their value affects the distribution of the measured data. An estimator attempts to approximate the unknown parameters using the measurements. For example, it is desired to estimate the proportion of a population of voters who will vote for a particular candidate. That proportion is the parameter sought; the estimate is based on a small random sample of voters. In estimation theory, two approaches are generally considered. The probabilistic approach (described in this article) assumes that the measured data is random with probability distribution dependent on the parameters of interest. The set-membership approach assumes that the measured data vector belongs to a set which depends on the parameter vector. For example, in electrical communication theory, the measurements which contain information regarding the parameters of interest are often associated with a noisy signal. Without randomness, or noise, the problem would be deterministic and estimation would not be needed.

5 Main Results

Information theory is known as the mathematical theory of communication, with great features such as domain general, and basic principles to deal with the problems that brought the simplicity and robustness of results, are described. The whole idea is so that it can be written in the language, musical notes, spoken words, pictures and many other related marks are used. In this paper, some applications of the theory of knowledge is expressed in statistics.

References

[1] Terras. A, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press (1999). ISBN 0-521-45718-1.

[2] Marcum, J. I. *A Statistical Theory of Target Detection by Pulsed Radar*. The Research Memorandum: (1947), Retrieved 2009-06-28.

[3] Lehmann,E.L and Casella, G. *Theory of Point Estimation*, (1983), (ISBN 0387985026).

[4] Roy Frieden, B. *Science from Fisher Information*: A Unification. Cambridge Univ. Press. (2004), ISBN 0-521-00911-1.

[5] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*, second edition, New Jersey: Wiley and Sons. (2006), ISBN 978-0-471-24195-9.

[6] Fazlollah, M. *An Introduction to Information Theory*. Dover Publications, Inc., New York. (1994), ISBN 0-486-68210-2.

[7] Robert, B. Ash. *Information Theory*. Dover Publications, Inc. (1990) ISBN 0-486-66521-6.

[8] Kullback, S., Leibler, R.A., *On information and sufficiency*. Ann. Math. Statist, (1951), 22, 1,76-86.

The First Conference on Computational Group Theory, Computational Number Theory and Applications**,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 73-75.

Oral Presentation

Some Lower Bounds for Summation of Absolute Value of Skew-Eigenvalues of some Graphs

Elham Ghasemian
Department of Pure Mathematics, Faculty of Mathematical Sciences,University of Kashan, Kashan, I. R. Iran
e.ghasemian@yahoo.com

Fatemeh Taghvaee
Department of Pure Mathematics, Faculty of Mathematical Sciences,University of Kashan, Kashan, I. R. Iran
taghvaei19@yahoo.com

Gholam Hossein Fath-Tabar
Department of Pure Mathematics, Faculty of Mathematical Sciences,University of Kashan, Kashan, I. R. Iran
fathtabar@kashanu.ac.ir

Abstract

The spectra of the skew-adjacency matrices of a graph are concidered as a possible way to distinguish adjacency cospectral graphs. In this paper we obtain some lower bounds for summation of absolute value of skew-eigenvalues of some graphs.

Keywords: Graph spectra, skew-adjacency matrices.

(2010) AMS classification Number: 05C50, 15A18.

1 Introduction

In this section we recall some definitions that will be used in the paper. An orientation of a simple graph G is a sign-valued function σ on the set of ordered pairs $\{(i,j),(j,i)|ij \in E(G)\}$ that specifies an orientation to each edge ij of G. If $ij \in E(G)$, we take $\sigma(i,j)=1$ when $i \to j$ and $\sigma(i,j)=-1$ when $j \to i$. The resulting oriented graph is denoted by G^{σ}. Both σ and G^{σ} are called orientations of G.

The skew-adjacency matrix $S^{\sigma}=S(G^{\sigma})$ of G^{σ} is the $\{0,1,-1\}$-matrix with (i,j)-entry equal to $\sigma(i,j)$ if $ij \in E(G)$ and 0 otherwise. Thus $S_{i,j}=1$ if $(i,j) \in E(G^{\sigma})$, -1 if $(j,i) \in E(G^{\sigma})$ and 0 otherwise. Let $\overrightarrow{U_k}$ denote the set of all collections $\overrightarrow{u}$ of vertex disjoint dicycles in $\overrightarrow{G(A)}$ (including loops and digons) that cover precisely k vertices of $\overrightarrow{G(A)}$. For $\overrightarrow{u} \in \overrightarrow{U_k}$, let $\prod_{\overrightarrow{u}}(A) = \prod_{(i,j)\in E(\overrightarrow{u})} a_{i,j}$, then

$$det(A)=(-1)^n \sum_{\overrightarrow{u}\in\overrightarrow{U_n}}(-1)^{|\overrightarrow{u}|}\prod_{\overrightarrow{u}}(A),$$

where $|\overrightarrow{u}|$ denotes the number of dicycles in $\overrightarrow{u}$.

Recall that U_k denotes the set of all collections u of (undirected) vertex disjoint edges and cycles (of length 3 or more) in G that cover k vertices, and that a routing $\overrightarrow{u}$ of $u \in u_k$ is obtained by replacing each edge in u by a digon(dicycles of length 2) and each cycle in u by a dicycle. If σ is an orientation of a simple graph G and $\overrightarrow{u}$ is a routing of $u \in U_k$, let $\sigma(\overrightarrow{u}) = \prod_{(i,j)\in E(\overrightarrow{u})}\sigma(i,j)$.

We say that $\overrightarrow{u}$ is positively oriented (resp. negatively oriented) relative to σ if $\sigma(\overrightarrow{u})$ equel 1 (resp. -1), or, equivalently, if an even (resp. odd) number of arcs in $\overrightarrow{u}$ have an orientation that is opposite to that in G^{σ}. If $S=S(G^{\sigma})$ is the skew-adjacency matrix of G^{σ}, then

$$\prod_{\overrightarrow{u}}(S)=\prod_{(i,j)\in\overrightarrow{u}} s_{i,j}=\prod_{(i,j)\in\overrightarrow{u}}\sigma(i,j)=\sigma(\overrightarrow{u}).$$

Also, if the dicycle components (including digons) of $\overrightarrow{u}$ are $\overrightarrow{u_i}$, $i\in[k]$, then $\sigma(\overrightarrow{u})=\prod_{i=1}^{n}\sigma(\overrightarrow{u_i})$. Now suppose that U_k^e be the set of all members of U_k with no odd cycles. If σ is an orientation of G and $u \in U_k^e$, let $C^+(u)$ (resp. $C^-(u)$) denote the number of cycles in u that are positively (resp. negatively) oriented relative to σ when u is given a routing $\overrightarrow{u}$. Then $C(u)=C^+(u)+C^-(u)$ is the total number of cycles in u. If $m(u)$ is the number of single edge components of u, then $|u|=C(u)+m(u)$ is the number of components of u.

Definition 1.(see[2]) Given a graph $G=(V,E)$, a matching M in G is a set of pairwise non-adjancent edges; that is, no two edges share a common vertext. A perfect matching is a matching which matches all vertices of the graph. That is, every vertex of the graph is incident to exactly one edge of the matching.

Definition 2. Let G be a simple graph with n vertices and A be the adjacent matrix of G and let λ_i $(i=1,2...n)$ be the eigenvalues of A. Then the energy of the graph is defined as:

$$E(G)=\sum_{i=1}^{n}|\lambda_i|.$$

The skew-energy of G^{σ} is the energy of matrix $S(G^{\sigma})$, that is, $E(G^{\sigma})=\sum_{\lambda\in Sp(G^{\sigma})}|\lambda|$ (see [3]).

2 Main Results

In this section we abtain some lower bounds for summation of absolute of skew-eigenvalue of some graphs with conditions are considered. Let $P_S(x)=det(xI-S)=x^n+s_1x^{n-1}+...+s_n$ be the characteristic polynomial of a skew-adjacency matrix S associated with an orientation G^{σ} of G.

Lemma 3.(see [1]) If $S(G^{\sigma})$ is an $n \times n$ skew-adjacency matrix of the orientation G^{σ} of a graph G. Then

1) $\det S = s_n = m_n(G) + \sum_{u \in U_n^e, C(u)>0} (-1)^{C^+(u)} 2^{C(u)}$, if n is even, in particular, $\det S = -s_n = 0$ if n is odd

2) $s_n \leqslant m_n(G)^2$, (when n is even), with equality if and only if each nice even cycle in G is negatively to σ,

where $m_n(G)$ is the number of perfect matchings in G, $c^+(U)$ is the number of cycles in U that are positively orinted relative to σ and $c(U)$ is the number of cycles in U.

Definition 4. A subgraph H of G is termed nice [2, p. 125] if $G - V(H)$ has a perfect matching. Note that if $u \in U_n^e$ and C is a cycle in u, then C must be nice because each of the remaining cycles in u may be replaced by matchings.

Let G is a graph with exactly one perfect matching such that the number vertex of G is even and each nice even cycle in G is negatively oriented relative to σ. Thus $\det S = m_n(G)^2$ and so we have the following resulte.

Theorem 5. Let G is a graph of order n with conditions saied in above. Then: $E(G^{\sigma}) \geqslant n$

Theorem 6. Let G be graph with n vertices,(n is even), and m edges such that each nice even cycle in G is negatively oriented relative to σ. Then:

$$E(G^{\sigma}) \geqslant \sqrt{2m + n(n-1)\det(s^{\sigma})^{\frac{2}{n}}}$$

Corollary 7. Let T is a tree with n vertices such that it has exactly one perfect matching, then

1) $E(T) \geq n$

2) $E(T) \geq \sqrt{(n+2)(n-1)}$

Acknowledgments

The authors are partially supported by the University of Kashan under grant number 159021/11.

References

[1] M.Cavers, S.M.Cioaba, S. Fallat, D. A. Gregory, W. H. Haemers, S.J. Kirkland, J. J. McDonald and M. Tsatsomeros, Skew-adjacency matrices of graphs, *Linear Algebra Appl.*, **436** (2012) 927-934.

[2] L. Lovasz, M.D. Plummer, Matching Theory, North-Holland, New York, 1986

[3] H. Yaoping, L. Tiangang, Characteristic polynomials of skew-adjacency matrices of oriented graphs, 2011.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 77-80.

Oral Presentation

Security of Dual Generalized Rebalanced-RSA

Mohammad Gholami
Faculty of Mathematics, University of Shahrekord
gholami-m@sci.sku.ac.ir

Somayeh Moradi
Faculty of Mathematics, University of Shahrekord
s.nazari60@gmail.com

Abstract

Dual RSA cryptosystem is essentially two distinct instances of RSA that share the same public and private exponents. Dual RSA can be used in scenarios that requires two instances of RSA. Dual RSA includes three variants: Dual RSA Small public key, Dual RSA Small private key and Dual Generalized Rebalanced (DGR)-RSA. In this paper, we present a new attack on DGR-RSA based on continued fractions and lattices to break the system.

Keywords: Cryptography, dual RSA, continued fraction, lattice.

MSC(2010): Primary: 94A60; Secondary: 11T71, 14G50.

1 Introduction

RSA cryptosystem is one of the public-key cryptography with a modulus N, such that N is product of two large unknown primes. This system [1] was introduced by Rivest, Shamir, and Adleman in 1977. Let $N = pq$ be the product of two large primes p, q of the same size. Let e, d be two integers satisfying $ed = 1 \bmod \phi(N)$ where $\phi(N) = (p-1)(q-1)$ is the number of integers a, $0 < a < N$, such that $(a, N) = 1$. We call N the RSA modulus, e the encryption exponent, and d the decryption exponent. The pairs $< e, N >$ and $< d, N >$ are called the public and private keys, respectively. A message is an integer M, $0 < M < N$. To encrypt M, one computes $C = M^e \bmod N$. To decrypt the cipher text, the receiver computes $C^d \bmod N$. Indeed, $C^d = M^{ed} = M \bmod N$. In order to decrease the computational costs of decryption in practice, the RSA decryption computations are performed in modulus of p and q and then combined via the Chinese Remainder Theorem (CRT) to obtain the desired solution in modulus of N, instead of directly computing the exponentiation in N.

Both encryption and decryption in RSA require only one modular exponentiation. However, computing an exponentiation modulo N is very costly. In order to solve this problem, Dual RSA [2, 3] was introduced by Sun, Wu, Ting and Hinek in 2007. In fact, whenever two RSA key pairs are required, Dual RSA can be used to decrease the storage requirements. In Dual RSA, the private exponent d is replaced by CRT-exponents $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$, which reduce the cost for each exponentiation when d is larger than the primes. As a result, the storage requirements is to reduce. The security of RSA is based on the integer factorization problem, because if we can factor N, then RSA can be broken.

Dual Generalized Rebalanced-RSA (DGR-RSA) [2] is a Dual RSA with small public exponent and small CRT-exponents. In this paper, we are interested in reviewing a new attack on DGR-RSA. In section II, we review the Dual RSA and present three variants of Dual RSA: Dual RSA small-e (small public exponent), Dual RSA small-d (small private exponent) and DGR-RSA. In section III, we present the key generation algorithm for DGR-RSA. Finally, in section IV, we consider the security of DGR-RSA.

2 Dual RSA

The following two remarks can be seen easily from the number theory [4].

Remark 2.1. Let $|x|$ be the bit-length of any $x \in \mathbb{N}$. Thus, we have $2^{|x|-1} \leq x < 2^{|x|}$.

Remark 2.2. For $s = p+q-1$, we have $N - \phi(N) = s$.

Dual RSA is essentially two distinct instances of RSA that share the same public and private exponents. Combining one instance of RSA with public key (e, N_1) and private key (d, p_1, q_1) with other instance public key (e, N_2) and private key (d, p_2, q_2), results one Dual RSA instance with public key (e, N_1, N_2) and private key (d, p_1, q_1, p_2, q_2), where e and d satisfy $ed \equiv 1 \bmod \phi(N_1)$ and $ed \equiv 1 \bmod \phi(N_2)$. By these two relations, it follows that there exists two positive integer k_1 and k_2 such that

$$\begin{cases} ed &= 1 + k_1\phi(N_1) = 1 + k_1(N_1 - s_1) \\ ed &= 1 + k_2\phi(N_2) = 1 + k_2(N_2 - s_2) \end{cases} \tag{2.1}$$

The equations 2.1 are called *the Dual RSA key equations* or simply *the key equations*. We can replace the private exponent d with $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$, where d_p and d_q are called the CRT-exponents. Whenever small CRT-exponents are used, the Dual version has public key (e, N_1, N_2) and private key $(d_p, d_q, p_1, q_1, p_2, q_2)$, where e, d_p and d_q satisfy $ed_p \equiv 1 \bmod p_i - 1$ and $ed_q \equiv 1 \bmod q_i - 1$ for $i = 1, 2$. By these relations, it follows that there exists positive integers k_{p_1}, k_{q_1}, k_{p_2} and k_{q_2} such that

$$\begin{cases} ed_p &= 1 + k_{p_1}(p_1 - 1) = 1 + k_{p_2}(p_2 - 1) \\ ed_q &= 1 + k_{q_1}(q_1 - 1) = 1 + k_{q_2}(q_2 - 1) \end{cases} \tag{2.2}$$

The equations 2.2 are called *the Dual RSA-CRT equations* or simply *the CRT equations*. Dual RSA includes three variants: Dual RSA small-e, Dual RSA small-d and DGR-RSA that each consists of three algorithms: key generation, encryption and description. Encryption for each scheme follows by the standard method. That is, a plain text massage M, $0 < M < N$, is encrypted by $C = M^e \bmod N$, and decrypted by using the CRT.

3 Dual Generalized Rebalanced-RSA

In this section, we consider a Dual RSA with a small public exponent and small CRT-exponents, which is called a DGR-RSA. We present key generation algorithm that takes (n_e, n_d, n_k, n) as input (with $n_e < \frac{n}{2}$ and $n_e + n_d = \frac{n}{2} + n_k$) and outputs a valid public/private key pair with an n_e-bit public exponent, an n_d-bit private exponent and n-bit modulo. The value n_k is a security parameter which is the bit-length of the constants k_{p_i} and k_{q_i} (for $i = 1,2$) in 2.2. The following result from number theory will be used in the key generation algorithm.

Theorem 3.1. Let a and b be two coprime integers, i.e. $(a,b) = 1$. For every integer h there exists a unique pair of integers (u_h, v_h) satisfying $au_h - bv_h = 1$, where $(h-1)b < u_h < hb$ and $(h-1)a < v_h < ha$.

The DGR-RSA key generation algorithm, with (n_e, n_d, n_k, n) as input, is as follows.

1. Randomly select an n_e-bit integer e and let k be the smallest integer larger than $(n/2 - n_e)/n_k$, i.e $k = \lceil (n/2 - n_e)/n_k \rceil$.
2. Randomly select $k-1$ n_k-bit integers $p_{a_1}, \ldots, p_{a_{(k-1)}}$ and an even integer p_{a_k} such that $p_a = p_{a_1} \ldots p_{a_{(k-1)}} p_{a_k}$ has bit-length $(n/2 - n_e)$ and $(e, p_a) = 1$.
3. Randomly select an n_k-bit integer k_{p_1} such that $(e, k_{p_1}) = 1$.
4. Based on theorem 3.1, compute d_p and p_b such that $ed_p = (k_{p_1} p_a) p_b + 1$, where $e < p_b < 2e$ and $k_{p_1} p_a < d_p < 2k_{p_1} p_a$. If $p_1 = p_a p_b + 1$ not be prime then go to step 3.
5. If $(k_{p_1} p_a p_b / p_{a_{i'}}) + 1$ be prime for some $1 \leq i' \leq k-1$ then let $p_2 = (k_{p_1} p_a p_b / p_{a_{i'}}) + 1$. Otherwise, go to step 3.
6. Randomly select $k-1$ n_k-bit integers $q_{a_1}, \ldots, q_{a_{(k-1)}}$ and an even integer q_{a_k} such that $q_a = q_{a_1} \ldots q_{a_{(k-1)}} q_{a_k}$ has bit-length $n/2 - n_e$ and $(e, q_a) = 1$.
7. Randomly select an n_k-bit integer k_{q_1} such that $(e, k_{q_1}) = 1$.
8. Based on theorem 3.1, compute d_q and q_b such that $ed_q = (k_{q_1} q_a) q_b + 1$, where $e < q_b < 2e$ and $k_{q_1} q_a < d_q < 2k_{q_1} q_a$. If $q_1 = q_a q_b + 1$ not be prime then go to step 7.
9. If $(k_{q_1} q_a q_b / q_{a_{j'}}) + 1$ be prime for some $1 \leq j' \leq k-1$ then let $q_2 = (k_{q_1} q_a q_b / q_{a_{j'}}) + 1$. Otherwise, go to step 7.
10. Let $N_1 = p_1 q_1$, $N_2 = p_2 q_2$, $k_{p_2} = p_{a_{i'}}$ and $k_{q_2} = q_{a_{j'}}$.

The relations in the above algorithm are logical, because:

$$\begin{aligned} ed_p &= 1 + k_{p_1}(p_1 - 1) = 1 + k_{p_1}(p_a p_b) = 1 + k_{p_1}(p_{a_1} \ldots p_{a_{i'}} \ldots p_{a_k} p_b) \\ &= 1 + p_{a_{i'}}(p_{a_1} \ldots k_{p_1} \ldots p_{a_k} p_b) = 1 + k_{p_2}(p_2 - 1) \end{aligned}$$

for some $i' \in \{1, \ldots, k-1\}$. Similarly $ed_q = 1 + k_{q_1}(q_1 - 1) = 1 + k_{q_2}(q_2 - 1)$ for some $j' \in \{1, \ldots, k-1\}$, where $k_{q_2} = q_{a_{j'}}$.

4 Security of Dual Generalized Rebalanced-RSA

In this section, we present an attack when the security parameter in the key generation algorithm is small (i.e., n_k is small). In this attack, the following theorems will be used.

Theorem 4.1. Let a, b, c and d be some integers satisfying $|\frac{a}{b} - \frac{c}{d}| < \frac{1}{2d^2}$. Then $\frac{c}{d}$ is one of the convergents in the continued fraction expansion of $\frac{a}{b}$.

Theorem 4.2. Let $f(x_1, \ldots, x_r)$ be a linear polynomial with integer coefficients. Let $X_1, \ldots, X_r$ be positive integers, $W = \|f(x_1X_1, \ldots, x_rX_r)\|_2$ and N be a sufficiently large integer with unknown factorization. Given $(y_1, \ldots, y_r) \in \mathbb{Z}^r$ satisfying $|y_1| < X_1, \ldots, |y_r| < X_r$, if $(y_1, \ldots, y_r)$ is a root of f and $\prod_{i=1}^r X_i < W$, or if $(y_1, \ldots, y_r)$ is a root of f modulo N and $\prod_{i=1}^r X_i < N$ then for sufficiently large W or N, respectively, we can compute $(y_1, \ldots, y_r)$ in polynomial time, provided a common assumption about the algebraic independence of reduced vectors holds.

In key generation algorithm, the following relations hold.

$$\begin{array}{rclrcl} N_1 & = & p_1q_1 & N_2 & = & p_2q_2 \\ p_1 & = & p_ap_b+1 & p_2 & = & p_{a'}p_b+1 \\ q_1 & = & q_aq_b+1 & q_2 & = & q_{a'}q_b+1 \\ p_a & = & p_{a_1}p_{a_2}\cdots p_{a_{(k-1)}}p_{a_k} & p_{a'} & = & \frac{p_ak_{p_1}}{p_{a_{i'}}} \\ q_a & = & q_{a_1}q_{a_2}\cdots q_{a_{(k-1)}}q_{a_k} & q_{a'} & = & \frac{q_ak_{q_1}}{q_{a_{j'}}} \end{array}$$

for some $i', j' \in \{1, 2, \ldots, k-1\}$, where $k = \lceil (n/2 - n_e)/n_k \rceil$, $k_{p_2} = p_{a_{i'}}$ and $k_{q_2} = q_{a_{j'}}$. Further, the maximum size of each parameter is shown in the following table.

parameters	bitlength	max size
p_1, q_1, p_2, q_2	$\frac{n}{2}$	$2^{\frac{n}{2}}$
$p_{a_i}, q_{a_i}, k_{p_1}, k_{q_1}$	n_k	$2^{n_e+n_d-\frac{n}{2}}$
$p_a, p_{a'}, q_a, q_{a'}$	$\frac{n}{2} - n_e$	$2^{\frac{n}{2}-n_e}$
p_b, q_b	n_e	2^{n_e}

Table 1: bit-length and max size

In continue, by Theorem 4.2, it is verified that for large enough N_1, we will be able to recover some factor N_1 and N_2.

References

[1] R. Rivest, A. Shamir, and L. Aldeman, *a method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, **vol.** 21 (1978), 120-126.

[2] H. M. Sun, M. E. Wu, W. C. Ting, M. J. Hinek, *dual RSA and its security analysis*, IEEE Trans. on Inf. Theory, **vol.** 53 (2007), 2922–2933.

[3] M. J. Hinek, *on the security of some variants of RSA*, Waterloo, Ontario, canada, 2007.

[4] G. H. Hardy and E. M. Wright, *an Introduction to the theory of numbers*, 4th ed. Cambridge, U.K.: Oxford Univ. Press, 1960.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 81-86.

Poster Peresentation

On Computing of Fundamental Groups

M. Hamidi
Faculty of Mathematical Sciences , University of Payame Noor
m.hamidi20@gmail.com

Abstract

The purpose of this paper is to computing of fundamental relations of (general)hypergroups. In this regards first we study some basic properties of fundamental relation of hypergroups, then we show that any given group is isomorphism to the fundamental group of a nontrivial hypergroup. Especially any abelian group is isomorphic to a fundamental group of a commutative hypergroup. Finally we study the connections between categories of hypergroups and groups via the fundamental relation.

Keywords: Hypergroup, fundamental relation, group, category.

MSC(2010): Primary: 20N20, 20B05, 20J15; Secondary: 20N20, 20B05, 20J15.

1 Introduction

The theory of hyperstructures has been introduced by Marty in 1934 at the $8th$ Congress of the Scandinavian Mathematicians [9]. Marty introduced hypergroups as a generalization of groups. He published some notes on hypergroups, using them in different contexts as algebraic functions, rational fractions, non commutative groups and then many researchers have been worked on this new field of modern algebra and developed it. A short review of the theory of hypergroups appears in [2]. The relation β (resp. β^*) was introduced on hypergroups by Koskas [8] and was studied mainly by Corsini [2] and Vougiouklis [12]. Freni in [4] proved that in hypergroups the relation β is transitive. Recently, Freni in [5] introduced the relation Γ as a generalization of the relation β and proved that in hypergroups, the relation Γ is transitive. In [1], Davvaz, et.al are introduced the smallest equivalence relation ν^* on a hypergroup H such that the quotient $\frac{H}{\nu^*}$, the set of all equivalence classes, is a nilpotent group and in this paper the characterization of nilpotent groups via strongly regular relations is investigated and several results on the topic are presented.

In this paper, we compute the fundamental groups via the fundamental relations and work on commutative hypergroups and try to show that any abelian group is a fundamental group of a commutative hyper group with underling abelian group.

2 Preliminaries

In this section we recall some definition and results from [2, 12], which we need to development of our paper. Suppose G be a nonempty set and $P^*(G)$ be the family of all nonempty subset of G, every function $\circ_i : G \times G \longrightarrow P^*(G)$ where $i \in \{1,2,\ldots,n\}$ and $n \in \mathbb{N}$ are called hyperoperation. For all x, y of G, $\circ_i(x,y)$ is called the hyperproduct of x, y. An algebraic system $(G, \circ_1, \circ_2, \ldots, \circ_n)$ is called a hyperstructure and binary structure $(G, \circ)$ endowed with only hyperoperation is called a *hypergroupoid*. For any two nonempty subsets A and B of G and $x \in G$:

$$A \circ B = \bigcup_{a \in A, b \in B} a \circ b, \qquad A \circ x = \bigcup_{a \in A} a \circ x \qquad \textit{and} \qquad x \circ B = \bigcup_{b \in B} x \circ b$$

Recall that a hypergroupoid $(G, \circ)$ is called a *semihypergroup* if for any $x,y,z \in G, (x \circ y) \circ z = x \circ (y \circ z)$ and semihypergroup $(G, \circ)$ is a *hypergroup* if satisfies in *reproduction axiom*, i.e. for any $x \in G, x \circ G = G \circ x = G$. If G is *commutative* with respect to $(\circ)$, then we call it is a commutative hypergroup. Let G_1 and G_2 be two hypergroups. The map $f : G_1 \to G_2$ is called an *inclusion* homomorphism if for all $x, y \in G, f(x \circ y) \subseteq f(x) \circ f(y)$ and $f(x.y) \subseteq f(x).f(y)$ and is called a *strong* homomorphism if for all $x, y \in G$, we have $f(x \circ y) = f(x) \circ f(y)$.

3 Fundamental Groups

Let $(G, \circ)$ be a hypergroup and ρ is an equivalence relation on G. Letting $\frac{G}{\rho} = \{\rho(g) \mid g \in G\}$, be the set of all equivalence classes of G with respect ρ. Define a hyperoperation $\otimes$ as follows:

$$\rho(a) \otimes \rho(b) = \{\rho(c) \mid c \in \rho(a) \circ \rho(b)\}$$

In [2] it was proved that $(\frac{G}{\rho}, \otimes)$ is a hypergroup if and only if ρ is regular. Moreover, $(\frac{G}{\rho}, \otimes)$ is a group if and if only ρ is strongly regular ([2]). The smallest equivalence relation, β^* on G such that $(\frac{G}{\beta^*}, \otimes)$ is a group is called *fundamental relation*. Let $\mathscr{U}$ denote the set of all finite product of elements of G. Define relation β on G by

$$a \beta b \Longleftrightarrow \exists u \in \mathscr{U} : \{a,b\} \in u$$

In [2] it was proved that β^* is the *transitive closure* of β, and $(\frac{G}{\beta^*}, \otimes)$ is called the *fundamental group* of $(G, \circ)$. In [2] it was rewrited the definition of β^* on G as follows:

$$a \beta^* b \Longleftrightarrow \exists z_1 = a, z_2, ..., z_n = b \in G; \text{ and } u_1, u_2.., u_n \in U \text{ such that} \{z_i, z_{i.1}\} \in u_i \text{ for any } \ 1 \leq i \leq n$$

Fundamental relation plays an important role in theory of algebraic hyperstructure.(for more see [2, 6, 7, 10, 11]). Let us first survey some simple results on hypergroups such that we will apply in

the next sections. Now, briefly introduce the category of hypergroup. Category H-gr, consists of the following data:
Objects: $(G,\circ),(H,\circ),\dots$ that are hypergroups.
Arrows: $f,g,\dots$ that are good homomorphisms.
For each arrow $f:(G,\circ)\longrightarrow(H,\circ)$ there are given objects $dom(f)=G$ and $cod(f)=H$ and called domain and codomain.
Given arrows $f:(G,\circ)\longrightarrow(H,\circ)$ and $g:(H,\circ)\longrightarrow(T,\circ)$, that with $cod(f)=dom(g)$, there is an arrow $g\circ f:G\longrightarrow T$ called the composite of f and g and for any arrows $h:(G,\circ)\longrightarrow(H,\circ),g:(H,\circ)\longrightarrow(T,\circ),f:(T,\circ)\longrightarrow(M,\circ)$ have $(f\circ g)\circ h=f\circ(g\circ h)$.
For object G there is given an arrow $1:G\longrightarrow G$ and called *identity* arrow of G and for any arrow $f:G\longrightarrow G$ have $f\circ 1=1\circ f=f$.

Let $G\times H$ denote the cartesian product of G and H. If $(G,\circ_G)$ and $(H,\circ_H)$ are two hypergroups. Then, we define hyperoperation "$\circ$" on $G\times H$ by $(r,s)\circ(r',s')=\{(a,b)\mid a\in r\circ_G r',b\in s\circ_H s'\}$. Let $(G,\circ_G)$ and $(H,\circ_H)$ be two hypergroups. Then $(G\times H,\circ)$ is a hypergroup.

Theorem 3.1. [3] Let $(G,\circ)$ and $(H,\circ)$ be two hypergroups. For fundamental relations β^*_G, β^*_H and $\beta^*_{G\times H}$, we have $\frac{(G\times H,\circ)}{\beta^*_{G\times H}}\cong\frac{(G,\circ)}{\beta^*_G}\times\frac{(H,\circ)}{\beta^*_H}$.

Corollary 3.2. *Let for $1\leq i\leq n$, $(G_i,\circ)$ be hypergroups, and β^*_i's be fundamental relations on G_i's. Then,*

$$\frac{(G_1\times G_2\times\ldots\times G_n,\circ)}{\beta^*_{G_1\times G_2\times\ldots\times G_n}}\cong\frac{(G_1,\circ,)}{\beta^*_1}\times\frac{(G_2,\circ,)}{\beta^*_2}\times\ldots\times\frac{(G_n,\circ,)}{\beta^*_n}$$

4 Computing of Fundamental Groups

Theorem 4.1. *In H-gr there exists product and for two object G and H triple $((G\times H,\circ),\pi_G,\pi_H)$ is a product.*

Lemma 4.2. *Let $(G,\odot)$, $(H,\odot')$ be hypergroups and $f:(G,\odot)\to(H,\odot')$ be a homomorphism. Then the following statements are satisfied:*
(i) For any $x,y\in G$, $x\beta^*y$ implies that $f(x)\beta^*f(y)$;
(ii) If f is an injection, then for any $x,y\in G$, $f(x)\beta^*f(y)$ implies that $x\beta^*y$;
(iii) If f is a bijection, then for any $x,y\in G$, $x\beta^*y$ if and only if $f(x)\beta^*f(y)$;
(iv) If f is a bijection. Then for any $x\in G$, $f(\beta^*(x))=\beta^*(f(x))$.

Corollary 4.3. *Let $(G_1,\odot_1)$ and $(G_2,\odot_2)$ be isomorphic hypergroups. Then $(\frac{(G_1,\odot_1)}{\beta^*},\otimes)\cong(\frac{(G_2,\odot_2)}{\beta^*},\otimes)$.*

Definition 4.4. A group $(G,.)$ is said to be a *fundamental group* if there exists a nontrivial hypergroup say, $(H,\odot)$ such that $(\frac{(H,\odot)}{\beta^*},\otimes)\cong(G,.)$. In other words, it is equal to the fundamental of nontrivial hypergroup up to isomorphic.

Remark 4.5. We know that on any group $(G,.)$, if define a binary hyperoperation "$\odot$" as $x\odot y=\{x.y\}$ such that is singleton, then $(G,\odot)$ is a *trivial hypergroup*. Therefore, its fundamental group is isomorphic with to $(G,.)$. In the following, we define a nontrivial hypergroup such that its fundamental group, be isomorphic with to given group $(G,.)$.

Lemma 4.6. *Let $(G,.)$ be a group. Then for any group $(H,.)$, there exist a binary hyperoperation "$\odot$" on group $G\times H$ such that $(G\times H,\odot)$ is a hypergroup.*

Remark 4.7. (i) The hypergroup $(G\times H,\odot)$ is called the *associated hypergroup* to G via H (or shortly associated hypergroup) and denote by G_H.
(ii) The mapping $\varphi : G \longrightarrow G_H$ by $\varphi(g) = (g,1)$ is an embedding.
(iii) G_H is a hypergroup with identity.
(iv) $H = \mathbb{Z}$ and we denote G_H by $\overline{G}$.
(vi) For $H = \mathbb{Z}_2, G_H$ is the smallest associated hypergroup.

Theorem 4.8. *Let $(G_1,.)$ and $(G_2,.)$ be isomorphic groups. Then, for any group $(H,.)$, ${G_1}_H$ and ${G_2}_H$ are isomorphic hypergroups.*

Theorem 4.9. *Every group is a fundamental group.*

Theorem 4.10. *Let G and H be two sets such that $|G| = |H|$. If $(G,\odot)$ is a hypergroup, then there exist a hyperoperation "$\odot'$" on H , such that $(G,\odot)$ and $(H,\odot')$, are isomorphic hypergroups.*

Corollary 4.11. *Let $(G,.)$ be a group of infinite order ($|G| = \infty$). Then there exists a hyperoperation "$\odot$" on G such that $(G,.)$ is fundamental group of itself.($\frac{(G,\odot)}{\beta^*} \cong (G,.)$)*

Theorem 4.12. *Every finite group is not its fundamental group.*

Lemma 4.13. *Let $(n,k) = d$, where $n,k \in \mathbb{Z}$. Then in cyclic group $(\mathbb{Z}_n,+)$, $o(\overline{k}) = \frac{n}{d}$.*

Theorem 4.14. *Let $n \in \mathbb{N}$. For any $k < n$, there exists hyperoperation $\circ_k$ on $\mathbb{Z}_n$ such that $(\mathbb{Z}_n,\circ_k)$ is a hypergroup.*

Corollary 4.15. *Let $n,k \in \mathbb{N}$. Then for any $m \leq n, (\mathbb{Z}_m,\circ_k)$ is a subhypergroup of $(\mathbb{Z}_n,\circ_k)$.*

Theorem 4.16. *Let $n \in \mathbb{N}$. For any $k < n$, there exists a hyperoperation "$\circ_k$" on $\mathbb{Z}_n$, such that $(\frac{(\mathbb{Z}_n,\circ_k)}{\beta^*},\oplus) \cong (\mathbb{Z}_{(n,k)},+)$.*

Theorem 4.17. *Let $n \in \mathbb{Z}$. Then, there exist hyperoperation $\circ_n$ on $\mathbb{Z}$ such that $(\mathbb{Z},\circ_n)$ is a hypergroup.*

Theorem 4.18. *Let $n \in \mathbb{N}$. Then there exists a hyperoperation "$\circ_n$" on $\mathbb{Z}$, such that $(\frac{(\mathbb{Z},\circ_n)}{\beta^*},\oplus) \cong (\mathbb{Z}_n,+)$.*

Theorem 4.19. *Any finite abelian group is a fundamental group.*

Proposition 4.20. $(\mathbb{Z},+)$ *is a fundamental group.*

Theorem 4.21. *Every finitely generated abelian group is a fundamental group.*

5 On Fundamental Functor of Category of Hypergroups

In this section we apply the results obtained of previous sections and define a functor of category H-gr (category of hypergroups) to category Grp(category of groups) as *fundamental functor* and investigate some properties of fundamental functor. In last we show that H-gr and Grp are not isomorphic.

Theorem 5.1. *Let $(H,\circ)$ be a hypergroup. If $(K,\circ)$ is a subhypergroup of $(H,\circ)$, then $\frac{(K,\circ)}{\beta^*}$ is a subgroup of $\frac{(H,\circ)}{\beta^*}$.*

Lemma 5.2. (i) : *Every singleton can be an object in Grp.*
(ii) : *Every nonempty set can be an object in H-gr.*

Theorem 5.3. (i) *In Grp, the singletons are zero objects.*
(ii) *In H-gr, the singletons are terminal objects.*
(iii) *H-gr has not zero object.*

Corollary 5.4. *The categories H-gr and Grp are not isomorphic.*

Definition 5.5. For categories H-gr and Grp, define a categorical morphism as follows:

$$F : H\text{-}gr \longrightarrow Grp \text{ by } F(G) = (\frac{G}{\beta^*}, \otimes) \tag{5.1}$$

where, $(G, \circ)$ is a hypergroup and for any homomorphism $f : (G_1, \circ) \longrightarrow (G_2, \circ)$, we define

$$F(f) : (\frac{G_1}{\beta^*}, \otimes) \longrightarrow (\frac{G_2}{\beta^*}, \otimes) \text{ by } F(f) = \beta^*(f) \tag{5.2}$$

we show that F is fundamental and call *fundamental functor* .

Theorem 5.6. *F is a functor of H-gr to Grp.*

Theorem 5.7. *The fundamental functor preserves terminal object.*

Theorem 5.8. *The fundamental functor preserves binary products.*

Theorem 5.9. *The fundamental functor is not faithful.*

Theorem 5.10. *The fundamental functor is surjective on objects.*

Theorem 5.11. *The fundamental functor is not injective on objects.*

References

[1] H. Aghabozorgi, B. Davvaz, M. Jafarpour *Nilpotent groups derived from hypergroups*, J. Algebra **382** (2013), 177184.

[2] P. Corsini, *Prolegomena of Hypergroup theory* , Second Edition, Aviani Editor (1993).

[3] B. Davvaz and V. Leoreanu-Fotea, *Hyperring Theory and Applications* , International Academic Press, USA, 2007.

[4] D. Freni, *Une note sur le coeur dun hypergroupe et sur la cloture transitive de* , Riv. diMat. Pura. Appl. **8** (1991)153156.

[5] D. Freni, *A new characterization of the derived hypergroup via strongly regular equivalences*. Comm. Algebra, **30**, No. **8**, 3977-3989 (2002).

[6] D. Freni, *On a Strongly Regular Relation in Hypergroupoids*, Pure Math. Appl., Her. A, **3-4** (1992) 191-198.

[7] D. Freni, *Hypergroupoids and fundamental relations*, 5th AHA, ed. M. Stefanescu, Hadronic Press. Palm Harbor, USA, (1994), 81-92.

[8] M. Koskas , *Groupoides, demi-hypergroupes et hypergroupes* , J.Math. Pures Appl. **49** **(9)**(1970), 155-192.

[9] F. Marty, *Sur une generalization de la notion de groupe 8th Congres Math*. Scandinaves, Stockholm (1934), 45-49.

[10] R. Migliorato, *Fundamental relation on non-associative hypergroupoids*, Ital. J. pure. appl. Math. No.**6** , (1999), 147-160.

[11] H. Spartalis, *On the number of Hv-groups with P-hyperoperation*, Discrete Math. **155**(1996), 225-231.

[12] T. Vougiouklis, *Hyperstructures and their representations,* Hadronic Press Inc, (1994).

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 87-92.

Oral Presentation

Computation of Fundamental TM-algebras

M. Hamidi
Faculty of Mathematical Sciences , University of Payame Noor
m.hamidi20@gmail.com

Abstract

In this paper, we consider the notions of TM-algebras and Quasi hyper TCK-algebras, give some related results, introduce the relation β on hyper BCK-algebras and let β^* be the transitive closure of β. Then by considering the concept of strongly regular equivalence relation (fundamental relation) β^* on quasi hyper BCK-algebras, we define the notion of fundamental TM-algebra and we prove that any countable TM-algebra is a fundamental TM-algebra and infinite countable TM-algebra is a fundamental TM-algebra of itself.

Keywords: TM-algebra, fundamental TM-algebra, quasi hyper BCK-algebra.

MSC(2010): Primary: 06F35, 03G25; Secondary: 06F35, 03G25.

1 Introduction

The study of BCK-algebras was initiated by Y. Imai and K. Iseki [11] in 1966 as a generalization of the concept of set-theoretic difference and propositional calculi. Since a great deal of literature has been produced on the theory of BCK-algebras. In [13] Borzooei, et al. applied the hyperstructures to BCK-algebras, and introduced the concept of a hyper BCK-algebras which is a generalization of a BCK-algebra and investigated some related properties. They introduced the notions of hyper BCK-ideals and weak hyper BCK-ideals and gave relations between theorem. Y.B. Jun et al, [12] gave a condition for a hyper BCK-algebra to be a BCK-algebra and introduced the notion of strong hyper BCK-ideal and reflexive hyper BCK-ideal. It is known that the class of BCK-algebras is a proper subclass of the class of BCI-algebras. In [1, 2] Q. P. Huand X. Li introduced a wide class of abstract algebras as BCH-algebras.They have shown that the class of BCI-algebras is a proper subclass of the class of BCH-algebras. J. Neggers and H. S. Kim [6] introduced the notion of d-algebras which is another generalization of BCK-algebras, and also they introduced the notion of B-algebras [7, 8]. Moreover, Y. B. Jun, E. H. Roh and H. S. Kim [3] introduced a new notion, called a BH-algebra, which is a generalization of $BCH/BCI/BCK$-algebras. Walendziak obtained the another equivalent axioms for B-algebra [9]. H. S. Kim, Y. H. Kim and J. Neggers [5] introduced the notion a (pre-) Coxeter algebra and showed that a Coxeter algebra is equivalent to an abelian group all of whose elements have order 2, i.e., a Boolean group. C. B. Kim and H. S. Kim [4] introduced the notion of a BM-algebra which is a specialization of B-algebras. Tamilarasi [17] introduced a class of abstract algebras as TM-algebras , which is a generalisation of $Q/BCK/BCI/BCH$-algebras.

Now, in this paper, we consider a nonempty set and construct a quasi hyper BCK-algebra and $TM-algebra$ with given set and via the fundamental relation prove that any TM-algebra is a fundamental TM-algebra. Moreover, show that any infinite countable set convert to a TM-algebra such that is fundamental TM-algebra of itself, but any finite TM-algebra is not a fundamental TM-algebra of itself.

2 Preliminaries

Definition 2.1. [11] Let X be a set with a binary operation "$*$" and a constant "0". Then, $(X,*,0)$ is called a *BCK-algebra* if it satisfies the following conditions:
(BCI-1) $((x*y)*(x*z))*(z*y)=0$,
(BCI-2) $(x*(x*y))*y=0$,
(BCI-3) $x*x=0$,
(BCI-4) $x*y=0$ and $y*x=0$ imply $x=y$,
(BCK-5) $0*x=0$.
We define a binary relation "$\leq$" on X by $x\leq y$ if and only if $x*y=0$. Then, $(X,*,0)$ is a BCK-algebra if and only if it satisfies the following conditions:
(BCI-1′) $((x*y)*(x*z))\leq(z*y)$,
(BCI-2′) $(x*(x*y))\leq y$,
(BCI-3′) $x\leq x$,
(BCI-4′) $x\leq y$ and $y\leq x$ imply $x=y$,
(BCK-5′) $0\leq x$.

Definition 2.2. [4] Let X be a set with a binary operation "$*$" and a constant "0". Then, $(X,*,0)$ is called a *TM-algebra* if it satisfies the following conditions:
(TM-1) $x*0=x$,
(TM-2) $(z*x)*(z*y)=y*x$.

We define a binary relation "$\leq$" on X by $x\leq y$ if and only if $x*y=0$.

Theorem 2.3. [17] Let $(X,*,0)$ be a TM-algebra. Then for any x,y and $z\in X$, the following hold:
1) $x*x=0$,
2) $(x*y)*x=0*y$,
3) $x*(x*y)=y$,
4) $(x*z)*(y*z)\leq x*y$,
5) $(x*y)*z=(x*z)*y$,
6) $x*0=0\Rightarrow x=0$,

7) $x \leq y \Rightarrow x*z \leq y*z$ and $z*y \leq z*x$,
8) $x*(x*(x*y)) = x*y$.

Definition 2.4. [4] Let $(X,*,0)$ and $(X',*',0')$ be two TM-algebras. A mapping $f: X \to X'$ is called a *homomorphism* from X into X', if for any $x,y \in X$, $f(x*y) = f(x)*' f(y)$. The homomorphism f, is called an *isomorphism*, if it is onto and one to one.

Definition 2.5. [10] Let H be a nonempty set and $P^*(H)$ be the family of all nonempty subsets of H. Functions $\circ_{i_H} : H \times H \longrightarrow P^*(H)$, where $i \in \{1,2,\ldots,n\}$ and $n \in \mathbb{N}$, are called binary hyperoperations. For all x, y of H, $\circ_{i_H}(x,y)$ is called the hyperproduct of x and y. An algebraic system $(H, \circ_{1_H}, \circ_{2_H}, \ldots, \circ_{n_H})$ is called an n-algebraic hyperstructure and structure $(H, \circ_H)$ endowed with only one hyperoperation is called a hypergroupoid. For any two nonempty subsets A and B of hypergropoid H and $x \in H$, we define

$$A \circ_H B = \bigcup_{a \in A, b \in B} a \circ_H b, \qquad A \circ_H x = \bigcup_{a \in A} a \circ_H x \qquad \textit{and} \qquad x \circ_H B = \bigcup_{b \in B} x \circ_H b$$

Definition 2.6. [14] Let H be a non-empty set, endowed with a binary hyperoperation "$\circ$" and a constant "0". Then, $(H,\circ,0)$ is called a *quasi hyper BCK-algebra* if satisfies the following axioms:
(H1) $(x \circ z) \circ (y \circ z) \ll x \circ y$,
(H2) $(x \circ y) \circ z = (x \circ z) \circ y$,
(H3) $x \circ H \ll x$.
and a quasi hyper BCK-algebra is called a *hyper BCK-algebra*, if
(H4) $x \ll y$ and $y \ll x$ imply $x = y$,
for all x,y,z in H, where $x \ll y$ is defined by $0 \in x \circ y$ and for every $A,B \subseteq H$, $A \ll B$ is defined by $\forall a \in A, \exists b \in B$ such that $a \ll b$. Nontrivial hyper quasi hyper BCK-algebra means that the hyperoperation "$\circ$" is not singleton.

Nontrivial quasi hyper BCK-algebra means that the hyperoperation "$\circ$" is not singleton.

3 Construct of TM-algebras and Quasi Hyper BCK-algebras

Definition 3.1. Let $(X,\circ)$ be a quasi hyper BCK-algebra and R be an equivalence relation on X. If A and B are nonempty subsets of X, then
(i) $A\overline{R}B$ means that for all $a \in A$, there exists $b \in B$ such that aRb and for all $b' \in B$, there exists $a' \in A$ such that $b'Ra'$.
(ii) $A\overline{\overline{R}}B$ means that for all $a \in A$, and $b \in B$, we have aRb.
(iii) R is called regular on the right (on the left) if for all x of X, from aRb, it follows that $(a\circ x)\overline{R}(b \circ x)$ $((x \circ a)\overline{R}(x \circ b)$ respectively).
(iv) R is called strongly regular on the right (on the left) if for all x of X, from aRb, it follows that $(a\circ x)\overline{\overline{R}}(b\circ x)$ $((x\circ a)\overline{\overline{R}}(x\circ b)$ respectively).
(v) R is called regular (strongly regular) if it is regular (strongly regular) on the right and on the left.
(vi) R is called good, if $(a \circ b)R0$ and $(b \circ a)R0$ imply aRb, for all $a,b \in X$.

Theorem 3.2. *In any quasi hyper BCK-algebra H, the following hold:*
$(a1)$ $x \circ y \ll \{x\}$,
$(a2)$ $x \circ 0 \ll \{x\}$,
$(a3)$ $0 \circ x \ll \{0\}$,
$(a4)$ $0 \circ 0 \ll \{0\}$,

$(a5)$ $(A \circ B) \circ C = A \circ (B \circ C)$,
$(a6)$ $A \circ B \ll A$ *and* $0 \circ A \ll \{0\}$.
for all $x, y, z \in H$ *and* $A, B, C \subseteq H$.

Lemma 3.3. *Let* $(X, \leq, 0)$ *be a well-ordered set. Then, there exists a binary operation* "$*$" *on* X*, such that* $(X, *, 0)$ *is a* TM*-algebra.*

Corollary 3.4. *Every countable set can be a* TM*-algebra.*

Theorem 3.5. *Let* X *be an infinite countable set. Then there exist* $x_0 \in X$ *and a binary operation* "$*$" *on* X *and* $\mathbb{W}$*, such that* $(X, *, x_0)$ *and* $(\mathbb{W}, *, 0)$ *are* TM*-algebras and* $(X, *, x_0) \cong (\mathbb{W}, *, 0)$.

Theorem 3.6. *Every set can be a* TM*-algebra.*

Theorem 3.7. *Every nonempty set can be a quasi hyper BCK-algebra.*

Theorem 3.8. *Let* X *and* Y *be two nonempty sets and* $|X| = |Y|$*. Then for* $x_0 \in X$ *and* $y_0 \in Y$*, there exists a binary hyperoperation* "$\circ$" *on* X *and* Y*, such that* $(X, \circ, x_0)$ *and* $(Y, \circ, y_0)$ *are two isomorphic quasi hyper BCK-algebras.*

Theorem 3.9. *Let* $(A, *_A, 0_A)$ *and* $(B, *_B, 0_B)$ *be two TM-algebras. Then there exists a hyperoperation* "$\circ$" *on* $A \times B$*, such that* $(A \times B, \circ, (0_A, 0_B))$ *is a quasi hyper BCK-algebra.*

4 Fundamental Relation on Quasi Hyper *BCK*-algebras

In this section, by define the notion of fundamental relation (strongly regular equivalence relation) on quasi hyper *BCK*-algebras, we define the concept of fundamental TM-algebra and we prove that any countable TM-algebra is a fundamental TM-algebra.

Let $(X, \circ)$ be a quasi hyper *BCK*-algebra and A a subset of X. Then we let $\mathscr{L}(A)$, denote the set of all finite combinations of elements A with $\circ$. Now, in the following, the well-known idea of β^* relation on hyperstructure [10, 15, 16] is transferred and applied to hyper *BCK*-algebras.

Definition 4.1. Let $(X, \circ)$ be a quasi hyper BCK-algebra. Then we set:

$$\beta_1 = \{(x, x) \mid x \in X\}$$

and, for every integer $n \geq 1$, β_n is the relation defined as follows:

$$x \beta_n y \Longleftrightarrow \exists (a_1, a_2, \ldots, a_n) \in X^n,\ \exists u \in \mathscr{L}(a_1, a_2, \ldots, a_n) \text{ such that } \{x, y\} \subseteq u$$

Obviously, for every $n \geq 1$, the relations β_n are symmetric and the relation $\beta = \bigcup_{n \geq 1} \beta_n$ is reflexive and symmetric. Let β^* be the *transitive closure* of β. Then in the following theorem we show that β^* is a strongly regular relation.

Theorem 4.2. *Let* $(X, \circ)$ *be a quasi hyper BCK-algebra. Then* β^* *is a strongly regular relation on* X.

Theorem 4.3. *Let* $(X, \circ)$ *be a weak commutative quasi hyper BCK-algebra. Then,* β^* *is a good strongly regular relation on X.*

Theorem 4.4. *Let* $(X,\circ)$ *be a quasi hyper BCK-algebra. Then,* $(\frac{X}{\beta^*},\overline{\circ})$ *is a TM-algebra, such that*

$$\beta^*(x)\overline{\circ}\beta^*(y) = \{\beta^*(z) \mid z \in x\circ y\} \text{ for all } x,y \in X.$$

Theorem 4.5. *Let* $(A,\circ_A)$ *and* $(B,\circ_B)$ *be two quasi hyper BCK-algebras. Then,*

$$\frac{(A\times B,\circ_{A\times B})}{\beta^*_{A\times B}} \cong \frac{(A,\circ_A)}{\beta^*_A} \times \frac{(B,\circ_B)}{\beta^*_B}$$

.

Definition 4.6. A TM-algebra $(X,*,0)$, is called a fundamental TM-algebra, if there exists a non-trivial quasi hyper BCK-algebra $(H,\circ)$, such that $(\frac{(H,\circ)}{\beta^*},\overline{\circ}) \cong (X,*)$.

Theorem 4.7. *Every TM-algebra is a fundamental BCK-algebra.*

Corollary 4.8. *Every nonempty set can be a fundamental* TM*-algebra.*

Theorem 4.9. *Let* $(X,*,0)$ *be any finite* TM*-algebra. Then for any hyperoperation "*$\circ$*" on X, such that* $(X,\circ,0)$ *is a quasi hyper BCK-algebra, there is not any isomorphic between* $(X,*,0)$ *and* $(\frac{(X,\circ)}{\beta^*},\overline{\circ})$*, that is* $(X,*,0) \ncong (\frac{(X,\circ,0)}{\beta^*},\overline{\circ})$.

Theorem 4.10. *Let X be an infinite countable set. Then there exist an operation "*$*$*" and a hyperoperation "*$\circ$*" on X, such that* $(\frac{(X,\circ,0)}{\beta^*},\overline{\circ}) \cong (X,*,0)$*. That is X is a fundamental* TM*-algebra of itself.*

Open Problem: If $(X,*,0)$ be an infinite non-countable TM-algebra, then is it X as a fundamental BCK-algebra of itself?

References

[1] Q. P. Hu and X. Li, *O*n BCH-algebras, Math. Seminar Notes **11** (1983), 313-320.

[2] Q. P. Hu and X. Li, *O*n proper BCH-algebras, Math. Japonica **30** (1985), 659-661.

[3] Y. B. Jun, E. H. Roh and H. S. Kim, *On BH-algebras*, Sci. Math. Japonica Online **1** (1998), 347-354.

[4] C. B. Kim and H. S. Kim, *On BM-algebras*, Sci. Math. Japo. Online e-2006 (2006), 215-221.

[5] H. S. Kim, Y. H. Kim and J. Neggers, *C*oxeters and pre-Coxeter algebras in Smarandache setting, Honam Math. J. **26(4)** (2004), 471-481.

[6] J. Neggers and H. S. Kim, *O*n d-algebras, Math. Slovaca **49** (1999), 19-26.

[7] J. Neggers and H. S. Kim, *O*n B-algebras, Mate. Vesnik **54** (2002), 21-29.

[8] J. Neggers and H. S. Kim, *A* fundamental theorem of B-homomorphism for B-algebras, Int. Math. J. **2** (2002), 215-219.

[9] A. Walendziak, *S*ome axiomatizations of B-algebras, Math. Slovaca **56**, No. **3** (2006),301-306.

[10] P. Corsini, *P*rolegomena of Hypergroup Theory, Second Edition, Aviani Editor (1993).

[11] Y. Imai and K. Iseki, *O*n Axiom Systems of Propositional Calculi, XIV, Proc. Japan Acad. **42** (1966), 19-22.

[12] Y. B. Jun, X. L. Xin, M. M. Zahedi, E. H. Roh, *S*trong Hyper *BCK*-ideals of Hyper *BCK*-algebras, Sci. Math. Jpn. **51 (3)**, (2000), 493-498.

[13] Y. B. Jun, M. M. Zahedi, X. L. Xin, R. A. Borzooei, *O*n Hyper *BCK*-algebras, Ital. J. Pure Appl. Math. **8** (2000), 127-136.

[14] S. Rasouli, D. Heidari, B. Davvaz, β*- Relations on Implicative Bounded Hyper BCK-algebras*, Hacet. J. Math. Stat. **39(4)** (2010), 461-469.

[15] S. Spartalis, T. Vougioklis, *T*he fundamental relation on H_v-rings, Riv. Math. Univ. pura Appl. **14**, (1994), 7-20.

[16] T. Vougiouklis, *H*yperstructures and Their Representations, Hadronic Press Inc, (1994).

[17] K. Megalai, A. Tamilarasi, *T*M-algebra-An Introduction, Int. J. Comput. App., Special Issue on Computer Aided soft Computing Techniques for imaging and Biomedical Application , (2010), 17-23

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 93-97.

Oral Presentation

Zeros of the Riemann Zeta Function and Explicit Approximations of the Prime Numbers

Mehdi Hassani
Department of Mathematics, University of Zanjan, University Blvd., 45371-38791, Zanjan, Iran
mehdi.hassani@znu.ac.ir

Abstract

We study the method of Rosser and Schoenfeld for explicit approximation of Chebychev functions in the theory of distribution of prime numbers. This method based on some computations over the zeros of the Riemann zeta function and ends in some sharp explicit bounds for the primes counting function $\pi(x) = \sum_{p \leq x} 1$ and the $n$the prime number p_n. We utilize such bounds to study some problems concerning distribution of prime numbers.

Keywords: The Riemann zeta function, zero-free region, distribution of the prime numbers.

MSC(2010): Primary: 11M26; Secondary: 11N05, 11Y35.

1 Introduction

The Riemann zeta function is defined for $\Re(s) > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. In his only paper about prime numbers, B. Riemann extended $\zeta(s)$ by analytic continuation to the complex plan with a simple pole at $s = 1$ with residue 1, and obtained a functional equation concerning it. The Riemann zeta function has trivial (real) zeros at the double negative points $s = -2n$ for all $n \in \mathbb{N}$, and has infinitely many nontrivial (nonreal) zeros inside the region $0 \leq \Re(s) \leq 1$ (critical strip), which are symmetric about both the vertical line $\Re(s) = \frac{1}{2}$ (critical line) and the real axis $\Im(s) = 0$. The Riemann Hypothesis (RH) asserts that all nontrivial zeros of $\zeta(s)$ lie on the critical line $\Re(s) = \frac{1}{2}$. RH is one of the Riemann's wonderful conjectures about $\zeta(s)$, and the only one which still is waiting for a proof or disproof. Riemann guessed an explicit relation between distribution of primes and zeros of the Riemann zeta function. This relation is known as the Riemann's explicit formula, and can be formulate as follows

$$\frac{\psi(x^+)+\psi(x^-)}{2}=x-\log(2\pi)-\frac{1}{2}\log\left(1-\frac{1}{x^2}\right)-\lim_{T\to\infty}\sum_{|\gamma|\le T}\frac{x^\rho}{\rho}. \tag{1.1}$$

Here the summation is over all nontrivial zeros $\rho=\beta+i\gamma$ of the Riemann zeta function and $\psi(x)=\sum_{p^m\le x}\log p$. The relation (1.1) suggests that if we obtain some approximations for the sum

$$\sum_{|\gamma|\le T}\frac{x^\rho}{\rho}, \tag{1.2}$$

then we may obtain some approximations for $\psi(x)$. We recall the function $\theta(x)=\sum_{p\le x}\log p$ and the elementary relations $\psi(x)=\sum_{m=1}^{\infty}\theta\left(x^{\frac{1}{m}}\right)$ and

$$\pi(x)=\frac{\theta(x)}{\log x}+\int_2^x\frac{\theta(t)}{t\log^2 t}\mathrm{d}t, \tag{1.3}$$

where $\pi(x)=$ the number of primes $\le x$.

The above relations describe how we can transfer approximations concerning the sum (1.2) to approximations concerning the function $\pi(x)$, and hence primes. This observation is the starting point of a method due to J.B. Rosser and L. Schoenfeld for approximating the sum (1.2), based one several numerical and analytic information about the nontrivial zeros of the Riemann zeta function. Numerical information consists of computational justification of RH for $|\Im(s)|\le T_0$. Rosser and Schoenfeld used the value $T_0=1‘894‘438.51224$. Thanks to the project ZetaGrid, we may take $T_0=29‘538‘618‘432.236$. Analytic information consists of explicit zero free regions (regions with no zero) for $\zeta(s)$ of the form $\sigma\ge 1-B(\gamma)$, in which B is a positive (and preferably differentiable) function. The classical zero free regions are originally due to de la vallée Poussin with $B(t)\ll(\log t)^{-1}$ and the best known explicit region of this form is due to H. Kadiri with $B(t)=\frac{1}{5.69693}(\log t)^{-1}$. Rosser and Schoenfeld used a classic region with $B(t)=\frac{1}{9.6459908801}(\log(\frac{t}{17}))^{-1}$. The best known zero free regions is originally due to Korobov and Vinogradov with $B(t)\ll(\log t)^{-\frac{2}{3}}(\log\log t)^{-\frac{1}{3}}$, and the best known explicit region of this type, and in fact the best know zero free region for the Rimemann zeta function up to now, is due to K. Ford with $B(t)=\frac{1}{57.54}(\log t)^{-\frac{2}{3}}(\log\log t)^{-\frac{1}{3}}$.

The method of Rosser and Schoenfeld [1] ends in several explicit sharp bounds for the functions related by primes. The best known bounds for the primes counting function $\pi(x)$ and the $n$the prime number p_n is due to P. Dusart [2]. He applied the method of Rosser and Schoenfeld to prove that

$$\frac{x}{\log x}\left(1+\frac{1}{\log x}+\frac{1.8}{\log^2 x}\right)\le\pi(x)\le\frac{x}{\log x}\left(1+\frac{1}{\log x}+\frac{2.51}{\log^2 x}\right), \tag{1.4}$$

where the left inequality holds for $x\ge 32‘299$, and the right inequality holds for $x\ge 355‘991$. Also, he proved that

$$n\left(\log n+\log\log n-1+\frac{\log\log n-2.25}{\log n}\right)\le p_n\le n\left(\log n+\log\log n-1+\frac{\log\log n-1.8}{\log n}\right), \tag{1.5}$$

where the left hand side inequality holds for $n\ge 2$ and the right hand side one holds for $x\ge 27‘076$. While we have the above unconditional bounds, it is very important to obtain conditional bounds under assumption RH. Among several conditional results, Rosser and Schoenfeld [1] proved that if we assume RH is true, then for $x \geq 2`657$ we have

$$|\pi(x) - \mathrm{li}(x)| < \frac{\sqrt{x}\log x}{8\pi} \quad \text{where} \quad \mathrm{li}(x) = \lim_{\varepsilon \to 0^+} \left(\int_0^{1-\varepsilon} + \int_{1+\varepsilon}^{x} \right) \frac{\mathrm{d}t}{\log t}. \tag{1.6}$$

Explicit approximations of the above type has wide applications in problems concerning primes. In the next section we explain some recent results.

2 Main Results

2.1 Means of prime numbers and Mandl's inequality

Stirling's approximation for $n!$ implies that $\lim_{n\to\infty} \frac{A'_n}{G'_n} = \frac{\mathrm{e}}{2}$, where A'_n and G'_n are the arithmetic and geometric means of the integers $1, 2, \ldots, n$, respectively. Motivated by the above fact, we study the behaviour of the similar sequence consisting of the ratio A_n by G_n, the arithmetic and geometric means of the prime numbers $p_1, p_2, \ldots, p_n$. Indeed, by using the inequalities (1.4) and (1.5) we prove the following result.

Theorem 2.1. *For $n \geq 2$ we have*

$$\frac{\mathrm{e}}{2} - \frac{14.951}{\log n} < \frac{A_n}{G_n} < \frac{\mathrm{e}}{2} + \frac{9.514}{\log n}.$$

Regarding to the above theorem more computational evidences support the following conjectures concerning the ratio $\frac{A_n}{G_n}$.

Conjecture 1. For $n \geq 226$ we have $\frac{A_{n+1}}{G_{n+1}} < \frac{A_n}{G_n}$.

Conjecture 2. There exists a real number α with $0 < \alpha < 9.514$, and there exists a positive integer n_0 such that for $n \geq n_0$ we have

$$\frac{\mathrm{e}}{2} + \frac{\alpha}{\log n} < \frac{A_n}{G_n}.$$

The so-called Robert Mandl's inequality asserts that $A_n < \frac{p_n}{2}$ for $n \geq 10$. By using the inequalities (1.4) and (1.5) we prove a refinement and a reverse of Mandl's inequality as follows.

Theorem 2.2. *We have*

$$\frac{p_n}{2} - \frac{9}{4}n < A_n < \frac{p_n}{2} - \frac{1}{12}n,$$

where the left hand side inequality is valid for any integer $n \geqslant 2$, and the right hand side inequality is valid for any integer $n \geqslant 10$.

2.2 On an inequality of S. Ramanujan

Among his various conjectures and results on the theory of prime numbers, Ramanujan asserts that the inequality

$$\pi(x)^2 < \frac{ex}{\log x} \pi\left(\frac{x}{e}\right), \tag{2.1}$$

holds for x sufficiently large. Originally, this inequality can be found on page 310 in Ramanujan's second notebook. As a fast proof, the prime number theorem with error term gives the expansion

$$\pi(x) = x \sum_{k=0}^{n} \frac{k!}{\log^{k+1} x} + O\left(\frac{x}{\log^{n+2} x}\right), \tag{2.2}$$

for any integer $n \geq 0$. Considering this expansion with $n = 4$, implies

$$\pi(x)^2 - \frac{ex}{\log x}\pi\left(\frac{x}{e}\right) = -\frac{x^2}{\log^6 x} + O\left(\frac{x^2}{\log^7 x}\right) \quad \text{as } x \to \infty,$$

and this proves (2.1) for x sufficiently large. By utilizing the conditional approximation (1.6) we obtain the following result.

Theorem 2.3. *Assume that the Riemann hypothesis is true. Then the inequality (2.1) is valid for* $x \geq 138‘766‘146‘692‘471‘228$.

Under assumption of the existence some "very good" upper bounds for the function $\pi(x)$, we prove the following.

Theorem 2.4. *Assume that* $\pi(x)/x = \sum_{k=0}^{4} k!/\log^{k+1} x + E$ *where* $E < b\log^{-6} x$ *for some real number* b *with* $b > 120$*, and for* $x \geq x_0$*. Also, let* $\varepsilon \in (0, 1/25)$ *is a fixed real number. Then, the inequality (2.1) is valid for any* $x > \mathrm{e}^N$*, where* $N = \max\{2b(1+\varepsilon) + 73 + \varepsilon, 2.2 + 132/\varepsilon, \log x_0\}$*. Moreover, we have* $N > 530.2$*.*

2.3 A very sharp bound concerning $\psi(x)$

While the classical zero free regions give approximations like (1.4), we except that regions of Korobov–Vinogradov type give sharper approximations. In a recent joint investigation, which is under refereeing, Y. Cheng, G.J. Fox and the author of present note prove the following result.

Theorem 2.5. *We have* $|\psi(x) - x| \leq E(x)$*, where*

$$E(x) \leq \begin{cases} 7.65 x^{\frac{1}{2}} (\log x)^2 & 28.99 \leq x \leq 6.647 \times 10^{13}, \\ 4.87 x (\log x)^2 \mathrm{e}^{-\frac{1}{97}(\log x)^{\frac{3}{5}} (\log\log x)^{-\frac{1}{3}}} & x \geq 6.647 \times 10^{13}. \end{cases}$$

One may transfer the above bound in terms of $\pi(x)$ by using the relation (1.3) and the known inequalities $0.998684 x^{\frac{1}{2}} < \psi(x) - \theta(x) < 1.001102 x^{\frac{1}{2}} + 3x^{\frac{1}{3}}$, which are valid for $x \geq 121$ and $x > 0$ respectively, and then determine the constant of O-term in (2.2) in order to obtain sharp bounds with satisfactory terms. As the above examples show, such bounds have several applications and allow us to improve many known results.

References

[1] J. Barkley Rosser, L. Schoenfeld, *Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$*, Math. Comp. **29** (1975), 243–269.

[2] P. Dusart, Autour de la fonction qui compte le nombre de nombres premiers, Thése de Doctorat de l'Université de Limoges, (1998).

[3] M. Hassani, *On an inequality of Ramanujan concerning prime counting function*, Ramanujan J. **28** (2012), 435–442.

[4] M. Hassani, *On the ratio of the arithmetic and geometric means of the prime numbers and the number* e, Int. J. Number Theory **9** (2013), 1593–1603.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 99-103.

Poster Presentation

A Visual Study of Weyl Sums over nontrivial Zeros of the Riemann Zeta Function

Mehdi Hassani
Department of Mathematics, University of Zanjan, University Blvd., 45371-38791, Zanjan, Iran
mehdi.hassani@znu.ac.ir

Abstract

We generate several graphs of the Weyl sums involving the several sequences concerning the values of γ_n, where γ_n runs over the imaginary parts of the zeros of $\zeta(s)$. Such graphs lead us to several conjectures about uniform distribution of sequences involving values of γ_n.

Keywords: The Riemann zeta function, uniform distribution modulo 1.

MSC(2010): Primary: 11M26; Secondary: 11K06.

1 Introduction

The Riemann zeta function is defined for $\Re(s) > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, and extended by analytic continuation to the complex plan with a simple pole at $s = 1$. It has trivial (real) zeros at $s = -2n$ for all $n \in \mathbb{N}$, and has infinitely many nontrivial (nonreal) zeros inside the region $0 \leq \Re(s) \leq 1$ (critical strip), which are symmetric about both the vertical line $\Re(s) = \frac{1}{2}$ (critical line) and the real axis $\Im(s) = 0$.

An arbitrary real sequence $(a_n)_{n\geq 1}$ is uniformly distributed modulo 1, if for all real numbers a, b with $0 \leq a < b \leq 1$ one has $\#\{n \leq N : \{a_n\} \in [a,b]\} \sim (b-a)N$ as $N \to \infty$. Here, $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of the real number x. An efficient criterion to determine uniform distribution modulo 1 of a given sequence, due to H. Weyl asserts that the sequence $(a_n)_{n\geq 1}$ is uniformly distributed modulo 1 if and only if $\sum_{n\leq N} e(ha_n) = o(N)$ as $N \to \infty$, for every positive integer h. Here, and in what follows, we let $e(x) = \mathrm{e}^{2\pi i x}$. It is known that the sequence $(\alpha\gamma_n)_{n\geq 1}$ is uniformly distributed modulo 1, where $\alpha \neq 0$ is a fixed real number and γ_n runs over the imaginary parts of the zeros of $\zeta(s)$. Dekking and Mendès France introduced an idea to make visible the Weyl sums $\sum_{n\le N} e(ha_n)$ for a given real sequence $(a_n)_{n\ge 1}$ and given positive integers h and N, by drawing a plane curve generated by successively connected lines segment, which joins the point V_n to V_{n+1}, where $V_n = (S_1(n), S_2(n))$ with $S_1(n) = \sum_{k\le n} \cos(2\pi h a_k)$ and $S_2(n) = \sum_{k\le n} \sin(2\pi h a_k)$, for $1 \le n < N$.

In this note, we generate several graphs of the Weyl sums involving the several sequences concerning the values of γ_n. Since it is not possible to consider all positive integer values of h, hence we will take $h = 1$ in all graphs. To generate figures appeared on this paper, we used Maple software to do several computations running over the numbers $(\gamma_n)_{1\le n\le 20000}$, all of which are based on the tables of zeros of the Riemann zeta function due to A. Odlyzko. The present note is a concise version of [1].

2 Visual observations and some conjectures

2.1 Sequences concerning polynomial values

Figure 1 shows the graphs of the Weyl sums $\sum_{n\le 5000} e(\gamma_n^k)$ with $k = 2, 3, 10$. Small size of frames lead us to the following conjecture.

Conjecture 1. For any non-constant polynomial $P(x)$ with real coefficients, the sequence $(P(\gamma_n))_{n\ge 1}$ is uniformly distributed modulo 1.

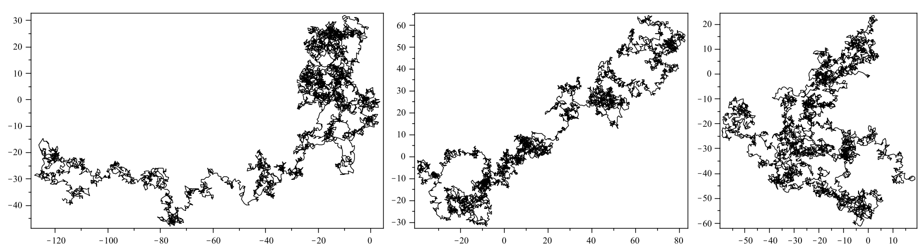


Figure 1: Graphs of the Weyl sums $\sum_{n\le 5000} e(\gamma_n^k)$ with $k = 2, 3, 10$ respectively from left to right

2.2 Sequences concerning rational powers

Figure 2 shows the graphs of the Weyl sums $\sum_{n\le 5000} e(\gamma_n^r)$ for several rational values of r. A. Fujii developed a method to obtain uniform distribution modulo 1 of a family of sequences $(f(\gamma_n))_{n\ge 1}$ for a wide class of smooth functions f. In particular, his method implies that sequences of the form $(\gamma_n^r)_{n\ge 1}$ for any fixed real $r \in (0, 1)$ are uniformly distributed modulo 1.

2.3 Sequences concerning $\log \gamma_n$

The above mentioned family of smooth functions f due to Fujii for which the sequences $(f(\gamma_n))_{n\ge 1}$ are uniformly distributed modulo 1 includes a number of logarithmic functions. More precisely, he asserts that for any fixed arbitrary real number $t > 0$ the sequences with general terms

$$(\log \gamma_n)(\log_k \gamma_n), \qquad (\log \gamma_n)^{1+t}, \qquad \frac{\gamma_n}{(\log \gamma_n)^{t-1}}, \qquad \frac{\gamma_n \log \gamma_n}{\log_k \gamma_n},$$

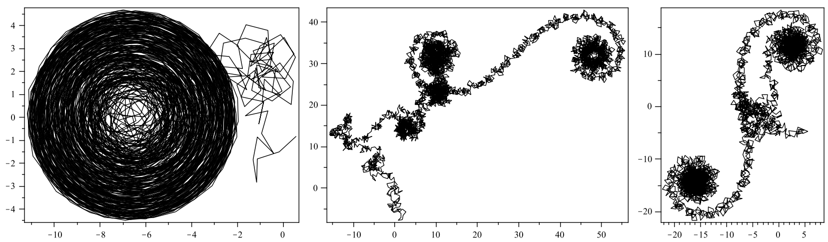


Figure 2: Graphs of the Weyl sums $\sum_{n\leq 5000} e(\gamma_n^r)$ with $r = 2/3, 7/8, 17/20$ respectively from left to right

all are uniformly distributed modulo 1. Here, $k \geq 1$ is an integer, and $\log_k$ denotes the k-fold iterative logarithm function. Also, he remarks that the sequence with general term $\log \gamma_n$ is not uniformly distributed modulo 1. Figure 3 shows the graphs of the Weyl sums $\sum_{n\leq 5000} e(a_n)$ with $a_n = \log \gamma_n$, $a_n = \gamma_n \log \gamma_n$, $a_n = \gamma_n / \log \gamma_n$ and $a_n = n \log \gamma_n$. The sizes of the frames in these graphs led us to the following conjecture.
Conjecture 2. Sequences with general terms $a_n = \gamma_n \log \gamma_n$, and $a_n = n \log \gamma_n$ are uniformly distributed modulo 1.

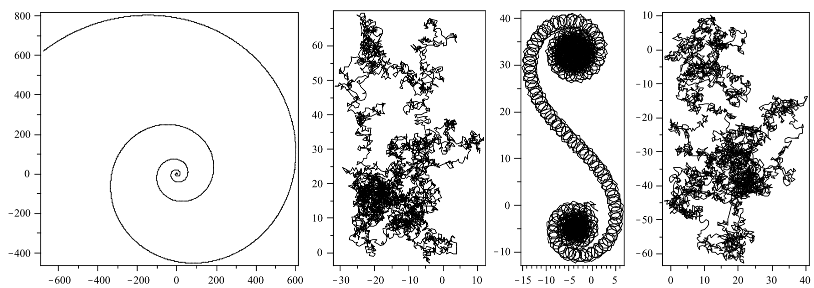


Figure 3: Graphs of the Weyl sums $\sum_{n\leq 5000} e(a_n)$ with $a_n = \log \gamma_n$, $a_n = \gamma_n \log \gamma_n$, $a_n = \gamma_n / \log \gamma_n$ and $a_n = n \log \gamma_n$, respectively from left to right

2.4 Tornado patterns in space curves

As we mentioned in the above sections, by a theorem of Fujii, sequences with general terms $a_n = \gamma_n^r$ where $r \in (0,1)$, and $a_n = \gamma_n / \log \gamma_n$ are uniformly distributed modulo 1. Some of the graphs of their corresponding Weyl sums in Figure 2, and Figure 3, consist of "S" shape, where many of lines segment snuggle around two holes and generate S-shape graphs. To detect exactly for which values of N the graphs of the Weyl sums $\sum_{n\leq N} e(a_n)$ generate such S-shapes, we study the space curve form of the graphs of the Weyl sums $\sum_{n\leq N} e(ha_n)$ for a given real sequence $(a_n)_{n\geq 1}$ and given positive integers h and N, by drawing a space curve generated by successively connected lines segment, which joins the point V_n to V_{n+1}, where $V_n = (S_1(n), S_2(n), n/1000)$.

In Figure 4, we generate the space curves of the Weyl sums $\sum_{n\leq 20000} e(a_n)$ with $a_n = \gamma_n^{10/11}$, $a_n = \gamma_n^{17/20}$, and $a_n = \gamma_n / \log \gamma_n$. These curves show more detains of the related S-shape graphs. They contain some "tornado" patterns, and it seems that as N growths in the related Weyl sums $\sum_{n\leq N} e(a_n)$, we expect some more "tornado" patterns around several holes. There are also some spiral and tornado patterns in the classical examples, pictured in Figure 5. Studying the mathematical justification for the patterns in these classical examples will help us in understanding of the patterns appeared in the case of the Riemann zeta function. We note that the most simple tornado pattern is the space curve of the Weyl sum $\sum_{n\leq N} e(a_n)$ with $a_n = \alpha n$ where α is an irrational coefficient. The leftmost graph pictured in Figure 5 shows the space curve of the Weyl sum $\sum_{n\leq 1000} e(n/\mathrm{e})$, as an example. The fundamental fact here is that for the linear sequence $a_n = \alpha n$ with irrational coefficient α, the generating vertices V_n of the related plane curve lie on a circle with radii $1/(2|\sin(\pi\alpha)|)$ and the center located at the point $(-1/2, \cot(\pi\alpha)/2)$.

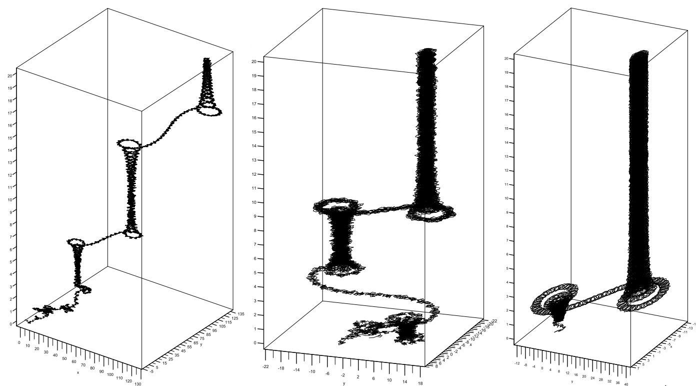


Figure 4: The space curves of the Weyl sums $\sum_{n\leq 20000} e(a_n)$ with $a_n = \gamma_n^{10/11}$, $a_n = \gamma_n^{17/20}$, and $a_n = \gamma_n/\log\gamma_n$, respectively from left to right

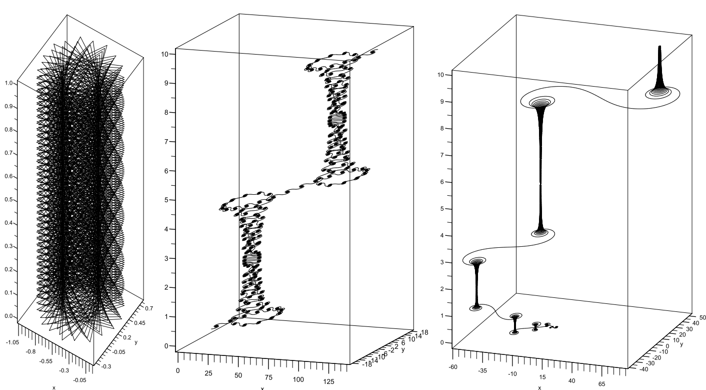


Figure 5: The space curves of the Weyl sums $\sum_{n\leq 1000} e(n/\mathrm{e})$ (leftmost graph), and $\sum_{n\leq 10000} e(a_n)$ with $a_n = (50/5001)n^2$ (mid graph), and $a_n = n\log n$ (rightmost graph)

To justify the pattern in the rightmost graph of Figure 5, Tenenbaum and Mendès France remark that because of the weak growth of $\log n$, the curve behaves locally like the curve associated with the linear sequence $a_n = c_H n$ where c_H is a local constant with $c_H \approx \{\log H\}$ for $n \approx H$. Thus, the graph of the Weyl sum of the sequence $a_n = n\log n$ appears as a succession of annuli, joined by almost straight lines, corresponding to the values of H such that $\{\log H\} \approx 0$.

References

[1] M. Hassani, *Geometric patterns in uniform distribution of zeros of the Riemann zeta function*, 245–258, Chapter 9 of Mathematics Without Boundaries, T. M. Rassias, P. M. Pardalos (eds.), Springer, (2014).

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 105-107.

Oral Presentation

On the Absolute Center and Autocommutator Subgroup of a Group

Rasoul Hatamian
Department of Pure Mathematics, Payam Noor University, Tehran, Iran
hatamianr@yahoo.com

Marzieh Chakaneh
Department of Pure Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran
m.chakaneh@stu.um.ac.ir

Saeed Kayvanfar
Department of Pure Mathematics, Ferdowsi University of Mashhad, Mashhad, Iran
skayvanf@math.um.ac.ir & skayvanf@yahoo.com

Abstract

The purpose of this paper is to give a new and shorter proof of the Hegarty's result on the absolute center and autocommutator subgroup of a group and to improve the bound attained by Hegarty for autocommutator subgroup. Furthermore, we prove an analogous statement for π-groups.

Keywords: Absolute center, autocommutator subgroup.

MSC(2010): Primary: 20D45; Secondary: 20E36, 20K30.

1 Introduction

Let G be a group and g_1, g_2 be elements of G, then $g_1^{g_2} = g_2^{-1} g_1 g_2$ and $[g_1, g_2] = g_1^{-1} g_1^{g_2} = g_1^{-1} g_1^{\varphi_{g_2}}$ denote the *conjugate* of g_1 by g_2 and the *commutator* of g_1 and g_2, respectively, where φ_{g_2} is the inner automorphism of G. Following Hegarty [2], if $\alpha \in Aut(G)$ and $g \in G$, then the *autocommutator* of g and α is defined to be $[g,\alpha] = g^{-1}g^{\alpha} = g^{-1}\alpha(g)$.

Now, using the above notation one may define

$$L(G) = \{g \in G|\ [g,\alpha] = 1,\ for\ all\ \alpha \in Aut(G)\},$$

$$K(G) = \langle\ [g,\alpha]|\ g \in G\ ,\ \alpha \in Aut(G)\ \rangle,$$

which are called the *absolute center* and the *autocommutator subgroup* of G, respectively. It is clear that the absolute center is a subgroup contained in the center of G and $K(G)$ is a subgroup of G containing the deriver subgroup.

Now, the following general question can be arisen. For which classes χ of groups, if $G/L(G) \in \chi$, then $K(G) \in \chi$?

In 1904, Schur [5] proved his famous result that for any group G, if $G/Z(G)$ is finite, then so is G'. Also in [6], Wiegold showed that if $|G/Z(G)| = n$, then $|G'| \leq n^{\frac{1}{2}\log_2 n}$.

In 1994, Hegarty [2] by a complicated technique proved the analogous of Schur's result for $G/L(G)$, which states if $G/L(G)$ is finite, then so is $K(G)$. That is, the answer to the above question is affirmative if χ is the class of finite groups. Furthermore, He showed that if $|G/L(G)| = n$, then $|K(G)| \leq n^{n((n-1)^2+[n/2])[\log_2 n]}$.

In the present paper, we prove both the Hegarty's result by a different and very simple technique and present a smaller bound for the order of $K(G)$ in terms of $|G/L(G)|$.

Furthermore, we also give an affirmative answer to the stated question when χ is the class of π-groups (π is a set of primes).

2 Main Results

(I) $\chi =$ the class of finite groups.

The following theorem is the first main theorem of the paper which is proved by a different method of Hegarty's. It also improves the bound attained by Hegarty[2].

Theorem 2.1. *If G is a group whose absolute center has finite index n, then $K(G)$ is finite and*

$$|K(G)| \leq n^{(\frac{1}{2}\log_2 n + [\log_2 n])}.$$

Hegarty in [3] by an example pointed out the converse of Theorem 2.1 does not hold in general, but if G is to be chosen finitely generated, then the converse is true. In the following theorem, we prove that the assumption of being finitely generated for G can be substituted by a weaker assumption. That is, $G/L(G)$ is considered to be finitely generated.

Theorem 2.2. *Let G be a group such that $d(G/L(G))$ and $K(G)$ are finite. Then $G/L(G)$ is finite and its order is bounded by some function of $|K(G)|$ and $d(G/L(G))$, where $d(G/L(G))$ is the minimal number of generators of $G/L(G)$.*

(II) $\chi =$ the class of π-groups (π is a set of primes).

For proving the main theorem of this part, we need the following lemmas.

Lemma 2.3. *Let G be a group such that $G/L(G)$ is torsion. Then $K(G)/G'$ is also a torsion group.*

Lemma 2.4. *Let $G = \langle X \rangle$ be an abelian torsion group. If the prime q does not divide the order of x, for every $x \in X$, then q does not divide the order of g, for every element $g \in G$.*

Now, the following theorem gives the second affirmative answer to the above general question.

Theorem 2.5. *If G is a group whose absolute central factor is a π-group, then $K(G)$ is also a π-group.*

References

[1] R. Hatamian, M. Hassanzadeh and S. Kayvanfar, *A converse of Baer's theorem*, Ricerche di Matematica., DOI 10.1007/s11587-013-0172-6.

[2] P. V. Hegarty, *The absolute centre of a group*, J. Algebra **169** (1994), 929-935.

[3] P. V. Hegarty, *Autocommutator subgroup of finite groups*, J. Algebra **190** (1997), 556-562.

[4] N. S. Hekster, *On the structure of n-isoclinism classes of groups*, J. Pure Appl. Algebra **40** (1986), 63-85.

[5] I. Schur, *Über die darstellung der endlichen gruppen durch gebrochene lineare substitutionen*, J. Für Math. **127** (1904), 20-50.

[6] J. Wiegold, *Multiplicators and groups with finite central factor-groups*, Math. Z. **89** (1965), 345-347.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 109-111.

Oral Presentation

Products of Conjugacy Classes in Finite Groups

Maryam Jalali-Rad
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan
87317-51167, I. R. Iran
jalali6834@gmail.com

Ali Reza Ashrafi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan
87317-51167, I. R. Iran
ashrafi@kashanu.ac.ir

Abstract

Suppose G is a finite group, A and B are conjugacy classes of G and $\eta(AB)$ denotes the number of conjugacy classes contained in AB. The aim of this paper is to compute $\eta(AB)$, where A and B are conjugacy classes of G and $G \in \{D_{2n}, T_{4n}, U_{6n}, V_{8n}, SD_{8n}\}$ or G is a group of orders $2pq, p^3, p^4$ such that p and q are prime numbers.

Keywords: Conjugacy class, normal subset, $p-$group.

MSC(2010): Primary: 65F05; Secondary: $20E45$, $20C15$.

1 Introduction

Throughout this paper all groups are assumed to be finite. If G is such a group and A, B are conjugacy classes of G then it is an elementary fact that AB is a normal subset of G. So, AB can be written as a union of conjugacy classes of G. The number of conjugacy classes of G contained in AB is denoted by $\eta(AB)$.

The most important works on the problem of computing the number of $G-$conjugacy classes in the product of conjugacy classes were done by Adan$-$Bante. Here, we report some of his nice results in this topic. Suppose $SL(2,q)$ is the group of 2×2 matrices with determinant one over a finite field of size q. Adan$-$Bante and Harris [1] proved that if q is even, then the product of any two noncentral conjugacy classes of $SL(2,q)$ is the union of at least $q-1$ distinct conjugacy classes of $SL(2,q)$, and if $q>3$ is odd, then the product of any two noncentral conjugacy classes of $SL(2,q)$ is the union of at least $\frac{q+3}{2}$ distinct conjugacy classes of $SL(2,q)$. Adan$-$Bante [2], proved that for any finite supersolvable group G and any conjugacy class A of G, $dl(\frac{G}{C_G(A)})\leq 2\eta(AA^{-1})-1$, where $C_G(A)$ denotes the centralizer of A in G and $dl(H)$ is the derived length of a group H. In [3], he also proved that if p is an odd prime number, G is a finite $p-$group and a^G, b^G are conjugacy classes of G of size p. Then either $a^Gb^G=(ab)^G$ or a^Gb^G is the union of at least $\frac{p+1}{2}$ distinct conjugacy classes. If G is nilpotent and a^G is again a conjugacy class of G of size p then either $a^Ga^G=(a^2)^G$ or a^Ga^G is the union of exactly $\frac{p+1}{2}$ distinct conjugacy classes of G of size p.

Darafsheh and Robati [6] continued the works of Adan$-$Bante and proved that if $[a,G]=\{[a,x]\mid x\in G\}$ then we have:

i. $\eta(a^Gb^G)=|a^G||b^G|/|[a,G]\cap(b^{-1})^Gb^G||(ab)^G|$;

ii. If $a^Gb^G\cap Z(G)\neq\emptyset$, then $\eta(a^Gb^G)=|a^G|$;

iii. If $|a^G|$ is an odd number, then $\eta(a^Ga^G)=1$;

iv. If $|a^G|$ is an even number, then $\eta(a^Ga^G)=2n$, where n is the number of cyclic direct factors in the decomposition of the Sylow $2-$subgroup of $[a,G]$.

We encourage to the interested readers to consult also papers by Arad and his co-workers [4, 5] and references therein for more information on this topic. Our notation is standard and can be taken from [9, 10].

2 Main Results

The aim of this section is to compute $\eta(AB)$, where A and B are conjugacy classes of G and $G\in\{D_{2n},T_{4n},U_{6n},V_{8n},SD_{8n}\}$ or G is a group of orders $2pq,p^3,p^4$ such that p and q are prime numbers. The semi-dihedral group SD_{8n}, dicyclic group T_{4n} and the groups U_{6n} and V_{8n} have the following presentations, respectively:

$$\begin{aligned}
SD_{8n} &= \langle a,b \mid a^{4n}=b^2=e,\ bab=a^{2n-1}, \\
T_{4n} &= \langle a,b \mid a^{2n}=1, a^n=b^2, b^{-1}ab=a^{-1}\rangle, \\
U_{6n} &= \langle a,b \mid a^{2n}=b^3=e,\ bab=a\rangle, \\
V_{8n} &= \langle a,b \mid a^{2n}=b^4=e,\ aba=b^{-1},\ ab^{-1}a=b\rangle.
\end{aligned}$$

It is easy to see the dicyclic group T_{4n} has order $4n$ and the cyclic subgroup $\langle a\rangle$ of T_{4n} has index 2 [10]. The conjugacy classes of u_{6n} and V_{8n}, n is odd, computed in the famous book of James and Liebeck [10]. The groups V_{8n}, n is even, and SD_{8n} have order $8n$ and their cconjugacy classes computed in [7, 8], respectively.

For simplicity of our argument, we assume that $\eta(G)$ denotes the set of all $\eta(AB)$, where A and B are conjugacy classes of G.

Proposition 1.

1. $\eta(D_{2n}) = \begin{cases} \{1,[\frac{n}{4}]+2,[\frac{n}{4}],\lceil\frac{n}{4}\rceil+1\} & n \text{ is even} \\ \{1,2,\frac{n+1}{2}\} & n \text{ is odd} \end{cases}$,
2. $\eta(V_{8n}) = \{1,2\}$,
3. $\eta(T_{4n}) = \{1,2\}$,
4. $\eta(U_{6n}) = \{1,2\}$,
5. $\eta(SD_{8n}) = \{1,2\}$.

Proposition 2. Suppose G is a group of order $2pq$, p and q, $p>q$, are odd primes. Then

$$\eta(G) \in \{\{1\},\{1,2\},\{1,2,\frac{p+1}{2}\},\{1,2,\frac{q+1}{2}\},\{1,2,\frac{pq+1}{2}\}\}.$$

References

[1] E. Adan−Bante and J. M. Harris, On conjugacy classes of $SL(2,q)$, *Rev. Colombiana Mat.* **46** (2012) (2) 97–111.

[2] E. Adan−Bante, Derived length and products of conjugacy classes, *Israel J. Math.* **168** (2008) 93–100.

[3] E. Adan−Bante, On nilpotent groups and conjugacy classes, *Houston J. Math.* **36** (2) (2010) 345–356.

[4] Z. Arad, D. Chillag and G. Moran, Groups with a small covering number, In: Products of Conjugacy Classes in Groups, Lecture Notes in Math. 1112, Berlin, Springer−Verlag, pp. 222–244, 1985.

[5] Z. Arad and E. Fisman, An analogy between products of two conjugacy classes and products of two irreducible characters in finite groups, *Proc. Edin. Math. Soc.* **30** (1987) 7–22.

[6] M. R. Darafsheh and S. Mahmood Robati, Products of conjugacy classes and products of irreducible characters in finite groups, *Turkish J. Math.* **37** (2013) (4) 607–616.

[7] M. R. Darafsheh and N. S. Poursalavati, On the existence of the orthogonal basis of the symmetry classes of tensors associated with certain groups, *SUT J. Math.* **37** (1) (2001) 1–17.

[8] M. Hormozi and K. Rodtes, Symmetry classes of tensors associated with the semi−dihedral groups SD_{8n}, *Colloq. Math.* **131** (2013) (1) 59–67.

[9] I. M. Isaacs, Character theory of finite groups, Academic Press, New York, 1976.

[10] G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge Univ. Press, London−New York, 1993.

[11] C. Zhang, J. -X. Zhou and Y. -Q. Feng, Automoprphisms of cubic Cayley graphs of order $2pq$, *Discrete Math.* **309** (2009) 2687–2695.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 113-115.

Poster Presentation

On the Multiplication Module

S. Karimzadeh
Department of Mathematics, Vali-e-Asr University of Rafsanjan, Rafsanjan, Iran
karimzadeh@vru.ac.ir

S. Hadjirezaei
Department of Mathematics, Vali-e-Asr University of Rafsanjan,Rafsanjan, Iran
s.hajirezaei@vru.ac.ir

Abstract

In this paper we assert some properties of finitely generated multiplication modules. Also we charactrize all finitely generated multiplication modules M when $Fitt_0(M)$ is a power of a maximal ideal of R..

Keywords: Multiplication module, Fitting ideals, prime ideal.

MSC(2010): Primary: 13C05; Secondary: 13D05.

1 Introduction

Let R be a commutative ring with identity and M be a finitely generated R-module. For a set $\{x_1,\ldots,x_n\}$ of generators of M there is an exact sequence $0 \longrightarrow N \longrightarrow R^n \xrightarrow{\varphi} M \longrightarrow 0$ where R^n is a free R-module with the set $\{e_1,\ldots,e_n\}$ of basis, the R-homomorphism φ is defined by $\varphi(e_j) = x_j$ and N is the kernel of φ. Let N be generated by $u_i = a_{1i}e_1 + \ldots + a_{ni}e_n$, with i in some index set I. Let $\mathrm{Fitt}_i(M)$ be an ideal of R generated by the minors of size $n-i$ of matrix

$$\begin{pmatrix} a_{11} & \ldots & a_{1i} & \ldots \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \ldots & a_{ni} & \ldots \end{pmatrix}.$$

For $i > n$ $\text{Fitt}_i(M)$ is defined R, and for $t < 0$ $\text{Fitt}_i(M)$ is defined as the zero ideal. It is known that $\text{Fitt}_i(M)$ is the invariant ideal determined by M, that is, it is determined uniquely by M and it does not depend on the choice of the set of generators of M [5]. The ideal $\text{Fitt}_i(M)$ will be called the i-th Fitting ideal of the module M. It follows from the definition of $\text{Fitt}_i(M)$ that $\text{Fitt}_i(M) \subseteq \text{Fitt}_{i+1}(M)$ Moreover, it is shown that $\text{Fitt}_0(M) \subseteq \text{ann}(M)$ and $(ann(\text{M}))^n \subseteq \text{Fitt}_0(M)$. ($M$ is generated by n elements.) The most important Fitting ideal of M is the first of the $Fitt_j(M)$ that is nonzero. We shall denote this Fitting ideal by $I(M)$. Note that if $I(M)$ contains a nonzerodivisor then $I(M_P) = I(M)_P$ for every prime ideal P of R. Fitting ideals are strong tools to identify propreties of modules and sometimes to charactrize modules. For example Buchsbaum and Eisenbud have shown in [3] that for a finitely generated R-module M, $I(M) = R$ if and only if M is a projective of constant rank module.

An R-module M is called a multiplication module if for each submodule N of M, $N = IM$ for some ideal I of R. In this case we can take $I = (N : M)$ [1].

2 Main Results

In this section we study some properties of Fitting ideals.

Proposition 2.1. *Let R be a ring and M be a finitely generated multiplication R-module. Let Q be a maximal ideal of R such that $Fitt_0(M) = Q^n$, for some positive integer n. Then M is a cyclic R-module.*

Proof. By [4, proposition 20-7], $Q^n = Fitt_0(M) \subseteq ann(M)$. Hence $ann(M)$ is contained only in maximal ideal Q. Thus by [1, Lemma 3] M is cyclic. □

Theorem 2.2. *let R be a ring and M be a multiplication R-module generated by two elements. If $Fitt_0(M) = 0$ then M is projective of constant rank one R-module.*

Proof. Let $M =< x_1, x_2 >$ and $0 \longrightarrow N \longrightarrow R^2 \xrightarrow{\varphi} M \longrightarrow 0$ be an exact sequence. Let $N =< \{n_i\}_{i\in I} >$ and $n_i = a_{1i}e_1 + a_{2i}e_2$. Put $A_1 = (Rx_2 : Rx_1)$ and $A_2 = (Rx_1 : Rx_2)$. Thus $a_{1j} \in A_1$ and $a_{2j} \in A_2$, for each $j \in I$. We have $Fitt_1(M) =< a_{ij}, 1 \leq i \leq 2, j \in I > \subseteq A_1 + A_2$. Let $a \in A_1$. So $ax_1 \in Rx_2$. This implies that $ax_1 = bx_2$, for some element b in R. Thus $(a, -b) \in N$. Hence $A_1 \subseteq Fitt_1(M)$. Similarly we have $A_2 \subseteq Fitt_1(M)$. So $A_1 + A_2 \subseteq Fitt_1(M)$. So $A_1 + A_2 = Fitt_1(M)$. On the other hand we have $(A_1 + A_2)M = M$. Hence $A_1 + A_2 = R$. Thus $Fitt_1(M) = R$. So by [3, Lemma 1], M is a projective of constant rank one R-module. □

Lemma 2.3. *Let M be a finitely generated multiplication R-module. Then $Fitt_0(M) = ann(M)$.*

Proof. By [1, Lemma 3 and Propostion 1] , M_Q is cyclic. Thus $\text{Fitt}_0(M_Q) = \text{ann}(M_Q)$, for every prime ideal Q of R. Since M is finitely generated, hence $\text{ann}(M_Q) = \text{ann}(M)_Q$. Thus by [4, Corollary 20.5], $\text{Fitt}_0(M)_Q = \text{ann}(M)_Q$, for every prime ideal Q of R. Therefore $\text{Fitt}_0(M) = \text{ann}(M)$. □

Proposition 2.4. *Let M be a finitely generated multiplication module. Let N be a submodule of M such that $(N : M) =< e >$, where e is an idempotent element of R. Then $M \cong N \oplus M/N$.*

Proof. It is easily seen that M/N is a multiplication module and $ann(M/N) = (N : M) =< e >$. Thus by Lemma 2.3 $Fitt_0(M/N) =< e >$. So M/N is a projective R-module. Now Consider the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

Since M/N is projective, hence $M \cong N \oplus M/N$. □

Theorem 2.5. *Let M be a finitely multiplication R-module. If $Fitt_0(M)$ is a prime ideal then M is indecomposable.*

Proof. Let $M = N \oplus K$ and $\pi_1, \pi_2 : M \longrightarrow M$ be defined by $\pi_1(n+k) = n$ and $\pi_2(n+k) = k$. Since M is a finitely generated multiplication module so there exist $0 \neq r_1$ and $0 \neq r_2$ in R such that $\pi_1(m) = r_1 m$ and $\pi_2(M) = r_2 m$, for every $m \in M$. Since $\pi_1 o \pi_2 = \pi_2 o \pi_1 = 0$, hence $r_1 r_2 M = 0$. So $r_1 r_2 \in ann(M) = Fitt_0(M)$. Since $Fitt_0(M)$ is a prime ideal, hence $r_1 \in ann(M)$ or $r_2 \in ann(M)$. Therefore $N = 0$ or $K = 0$. □

Theorem 2.6. *Let M be a finitely generated multiplication module over a ring R. Let N be a finitely generated nonzero submodule of M and $Fitt_0(M)$ be a prime ideal of R. Then $Fitt_0(N) \subseteq Fitt_0(M)$.*

Proof. Consider the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

By [2]p.174], $Fitt_0(N)Fitt_0(M/N) \subseteq Fitt_0(M)$. Since $Fitt_0(M)$ is a prime ideal of R, hence $Fitt_0(N) \subseteq Fitt_0(M)$ or $Fitt_0(M/N) \subseteq Fitt_0(M)$. If $Fitt_0(M/N) \subseteq Fitt_0(M)$, by Lemma 2.3, We have $Fitt_0(M/N) = (N : M) \subseteq Fitt_0(M) \subseteq ann(M)$. So $N = 0$, a contradiction. Hence $Fitt_0(N) \subseteq Fitt_0(M)$. □

References

[1] A. Barnard, multiplication modules, *J. Algebra* **7**(1981) 174-178.

[2] W. C. Brown, Matrices Over Commutative Rings, Pure Appl. Math., vol. 169, Marcel Dekker Inc., New York (1993).

[3] D. A. Buchsbaum and D. Eisenbud, What makes a complex exact *J. Algebra* **25** (1973) 259-268.

[4] D. Eisenbud, Commutative Algebra with a View toward Algebraic Geometry, Springer-verlag, New York 1995.

[5] H. Fitting, Die Determinantenideale eines Moduls, Jahresbericht d. Deutschen Math.-Vereinigung, 46 (1936), 195-228..

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), p. 117.

Poster Presentation

There is a Distributive Lattice which is not Starrable

Hossain Khass
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
khass@grad.kashanu.ac.ir

Behnam Bazigaran
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
bazigaran@kashanu.ac.ir

Abstract

In this paper we try to prepare a computer program that proves there is a finite distributive lattice which is not starrable.

Keywords: distributivity, starrability

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 119-121.

Oral Presentation

Some Properties of Graph Related to Conjugacy Classes of Special Linear Group $SL_n(F)$

Danial Khoshnevis
School of Mathematics, Iran University of Science and Technology, Tehran, Iran
danyal_ khoshnevis@mathdep.iust.ac.ir

Zohreh Mostaghim
School of Mathematics, Iran University of Science and Technology,Tehran,Iran
mostaghim@iust.ac.ir

Abstract

Suppose that G is a finite group. The graph $\Gamma(G)$ is related to conjugacy classes of G. Its vertices are the non-central conjugacy class sizes of G and there is an edge between two distinct vertices of $\Gamma(G)$, if and only if their class sizes have a common prime divisor.
In this paper, some properties of graph $\Gamma(G)$ such as chromatic polynomial, chromatic number and clique number are discussed for $G \cong SL_n(F)$, where F is a finite field.

Keywords: Conjugacy class, special linear group, chromatic number, clique number.

MSC(2010): Primary: 05C25; Secondary: 20E45.

1 Introduction

The graph related to conjugacy classes is studying widely. For instance in [1], the authors proved that for a finite simple group G , $n(\Gamma(G)) \leqslant 2$. They also showed for a non-abelian finite simple group G, its conjugacy class graph is complete.
Also in [3], Fang and Zhang proved the symmetric group S_3 , the dihedral group D_5, the three pairwise non-isomorphic non-abelian groups of order 12, and the non-abelian group T_{21} of order 21

is the complete list of all G such that $\Gamma(G)$ contains no triangles.
We explain some of notations that will be used later. All groups considered in this paper are finite. Let G be a finite group, x an element of G. x^G denotes the conjugacy class containing x and $|x^G|$ denotes the size of x^G. Let Γ be a graph. A subset C of the vertices of Γ is called a clique if the induced subgraph on C is a complete graph. The maximum size of a clique in a graph Γ is called the clique number and denoted by $\omega(\Gamma)$. The minimum number of colors which can be assigned to the vertices such that every two adjacent vertices have different colors is called the choromatic number of Γ and denoted by $\chi(\Gamma)$. Let Γ be a graph and also $|V(\Gamma)| = n$ and u is a complex number. For any natural number r, let $m_r(\Gamma)$ denotes the number of distinct color-partitions of $V(\Gamma)$ into r color-classes, and define $U_{(r)}$ to be the complex number $U_{(r)} = \Pi_{i=0}^{r-1}(u-i) = u(u-1)\cdots(u-r+1)$. The chromatic polynomial of Γ is the polynomial

$$C(\Gamma;U) = \sum_{r=1}^{|V(\Gamma)|} m_r(\Gamma)U_{(r)}$$

In this paper, we consider graph $\Gamma(G)$ for $G \cong SL_n(F)$, where F is a finite field. We study some properties of this graph.

2 Preliminary Lemmas

We need the following lemmas which will be used later:
Lemma 2.1 [4] Let G be a non-abelian finite simple group. Then $\Gamma(G)$ is a complete graph.
Lemma 2.2 Suppose that Γ is a graph, then:

$$\sum_{\varepsilon=1}^{|V(\Gamma)|} d(v_\varepsilon) = 2|E(\Gamma)|.$$

Lemma 2.3 [2] If G is a finite group and N is a normal subgroup. Then:
i) $|g^N| \Big| |g^G|$; $g \in N$.
ii) $|(gN)^{\frac{G}{N}}| \Big| |g^G|$; $g \in G$.

3 Main Results

Suppose that $F = GF(q)$;q is a prime power. So $SL_n(F)$ is denoted by $SL_n(q)$.

Theorem 3.1 If $G \cong SL_n(q)$, then $|V(\Gamma(G))| = (q-1)^{-1}\sum_{d|(n,q-1)} \varphi_2(d)C_{\frac{n}{d}} - (n,q-1)$.
Theorem 3.2 Let $G \cong SL_n(q)$:

i) If $q = 2$ and $n = 2$, then graph $\Gamma(G)$ is a non-complete graph, $|E(\Gamma(G))| = 0$.

ii) If $q \neq 2$ and $n \geqslant 2$, then graph $\Gamma(G)$ is a complete graph and

$$|E(\Gamma(G))| = 2^{-1}(|V(\Gamma(G))|)(|V(\Gamma(G))|-1).$$

Proposition 3.3 Let $G \cong SL_n(q)$

i) If $q = 2$ and $n = 2$, then $\chi(\Gamma(G)) = 1$ and $\omega(\Gamma(G)) = 0$.

ii) If $q \neq 2$ and $n \geqslant 2$, then $\chi(\Gamma(G)) = \omega(\Gamma(G)) = (q-1)^{-1} \sum_{d|(n,q-1)} \varphi_2(d) C_{\frac{n}{d}} - (n, q-1)$.

Proposition 3.4 Let $G \cong SL_n(q)$

i) If $q = 2$ and $n = 2$, then $C(\Gamma(G); U) = u^2$.

ii) If $q \neq 2$ and $n \geqslant 2$, then the chromatic polynomial of graph $\Gamma(G)$ is as following:

$$C(\Gamma(G); U) = u(u-1)\cdots(u - ((q-1)^{-1} \sum_{d|(n,q-1)} \varphi_2(d) C_{\frac{n}{d}} - (n, q-1)) + 1).$$

References

[1] E. A. Bertram, M. Herzog, A. Mann, *On a graph related to conjugacy classes of groups*, Bull, London Math. Soc **22** (1990), 569-575.

[2] S. Dolfi, *Prime factors of conjugacy-class lengths and irreducible character-degrees in finite soluble groups*, J.Algebra **174** (1995), 749-752.

[3] M. Fang, P. Zhang , *Finite groups with graphs containing no triangles*, J.Algebra **264** (2003), 613-619.

[4] E. Fisman, Z. Arad, *A proof of Szep's conjecture on the non-simplicity of certain finite groups*, J.Algebra **108** (1987), 340-354.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 123-128.

Oral Presentation

Calculation of Modified Wiener and Hyper-Wiener Indices of a Graph by Character Table of its Automorphism Group

Fatemeh Koorepazan-Moftakhar
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317-51167, I. R. Iran
f.moftakhar@grad.kashanu.ac.ir

Ali Reza Ashrafi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317-51167, I. R. Iran
ashrafi@kashanu.ac.ir

Abstract

The modified-−Wiener and modified hyper−Wiener indices of graphs are defiend as follows:

$$\begin{aligned}\hat{W}(G) &= \frac{|V(G)|}{2|\Gamma|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u,g(u)),\\ W\hat{W}(G) &= \frac{1}{2}\hat{W}(G)+\frac{|V(G)|}{4|\Gamma|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u,g(u)^2).\end{aligned}$$

The aim of this talk is to report our recent results in this topic.

Keywords: Modified Wiener, automorphism group, modified hyper−Wiener.

1 Introduction

Suppose G is connected graph and $V(G)$ is its vertex set. The distance between the vertices $u, v \in V(G)$, $d(u,v)$, is defined as the number of edges in a shortest path connecting u and v. The sum of distances between all pairs of vertices in G is called the Wiener index of G [6]. Graovac and Pisanski [3] applied the symmetry group of the graph under consideration to generalize the Wiener index. To the best of our knowledge, this paper is the only published paper in mathematics literature that combines the symmetry and topology of molecules. To explain, we assume that G is a graph with automorphism group $\Gamma = Aut(G)$. Following [3], we define the distance number of an automorphism g, $\delta(g)$, to be the average of $d(u, g(u))$ overall vertices $u \in V(G)$ and $\delta(G) = \frac{1}{|\Gamma||V(G)|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u, g(u))$. The modified Wiener index of G is defined as:

$$\hat{W}(G) = \frac{1}{2}|V(G)|^2\delta(G) = \frac{|V(G)|}{2|\Gamma|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u, g(u)).$$

Throughout this paper we use the standard notations of group theory and graph theory. Suppose G and H are two graphs. The Cartesian product $G\Box H$ is a graph with vertex set $V(G)\times V(H)$ in such a way that vertices (a,b) and (x,y) are adjacent if and only if $a = x$ and $by \in E(H)$ or $b = y$ and $ax \in E(H)$. Our notation is standard and taken from the standard books on these topics. The path, cycle and complete graphs with n vertices are denoted by P_n, C_n and K_n, respectively.

The hyper$-$Wiener index of acyclic graphs was introduced by Milan Randić in 1993. Then Klein et al. [4], generalized Randić's definition for all connected graphs, as a generalization of the Wiener index. It is defined as

$$WW(G) = \frac{1}{2}W(G) + \frac{1}{2}\sum_{\{x,y\}} d(x,y)^2$$

We define in a similar way the modified hyper-Wiener index of G as follows:

$$\hat{WW}(G) = \frac{1}{2}\hat{W}(G) + \frac{|V(G)|}{4|\Gamma|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u, g(u)^2).$$

In this talk we report our recent results in [1, 5]

2 Main Results

A graph G is called asymmetric if its automorphism group is trivial. It is easy to see that the modified Wiener index of a graph G is equal to zero if and only if G is asymmetric. In [2, Corollary 2.3.3], it is proved that the most of finite graphs are having trivial automorphism group. To explain, we assume that α_n and β_n denote the number of $n-$vertex graphs and $n-$vertex graphs with trivial automorphism group, respectively. Then,

$$lim_{n\to\infty}\frac{\alpha_n}{\beta_n} = 1.$$

This means that the modified Wiener index of the most of graphs is zero.

A class function over the complex number $\mathbb{C}$ is a function f on a group H, such that f is constant on the conjugacy classes of H. It is well-known that the set $CF(H,\mathbb{C})$ of all class functions constitutes a vector space over $\mathbb{C}$.

Suppose G is a connected graph and $\Gamma = Aut(G)$. For each automorphism $g \in \Gamma$, we define $\delta(g) = \frac{1}{|V(G)|}\sum_{x\in V(G)} d(x,g(x))$. This defines a mapping $\delta : \Gamma \to \mathbb{C}$. Then,

$$\hat{W}(G) = \frac{|V(G)|^2}{2|\Gamma|}\sum_{g\in\Gamma}\delta(g). \tag{1}$$

Theorem 1. δ is a class function and $\delta(g) = \delta(g^{-1})$, for each automorphism $g \in \Gamma$.

Suppose H is a group, V is a vector space over $\mathbb{C}$ and φ is a homomorphism from H into $GL(V)$, the set of all invertible n by n matrices on $\mathbb{C}$, $n = dimV$. The homomorphism φ is said to be a complex representation of H and the function χ from H into $\mathbb{C}$ given by $\chi(g) = tr\varphi(g)$, $g \in H$, is called the complex character of H afforded by φ. If χ and γ are two complex class functions on H then their scalar product is defined as

$$\langle\chi,\gamma\rangle = \frac{1}{|H|}\sum_{g\in H}\chi(g)\overline{\gamma(g)}.$$

An irreducible complex character is a complex character χ such that $\langle\chi,\chi\rangle = 1$. It is well-known that the set of all irreducible complex characters of H constitute an orthonormal subset of $CF(H,\mathbb{C})$.

In Theorem 1, we proved that δ is a class function. Since $\delta(e) = 0$, δ is not a character of H. In the next theorem, we will prove that if $n > 1$ then the trivial character is a constituent of δ.

Theorem 2. Suppose G is a connected $n-$vertex graph, $\Gamma = Aut(G)$, t_1 denotes the number of orbits of Γ on $V(G)$ and t_2 is the number of orbits of Γ on $V(G)\times V(G)$ under natural actions of Γ on $V(G)$ and $V(G)\times V(G)$, respectively. Then,

1. $\langle\delta,\delta\rangle \geq 1 - \frac{2t_1}{n} + \frac{t_2}{n^2}$,
2. $\langle\delta,1_G\rangle \geq n - \frac{t_1}{n}$, where 1_G denotes the trivial character of G.

Suppose G is a graph with $V(G) = \{v_1,\ldots,v_n\}$ and as usual $\Gamma = Aut(G) = \{g_1,\ldots,g_m\}$. The matrix $\hat{D} = [\hat{d}_{ij}]$ is called the modified distance matrix, where $\hat{d}_{ij} = d(v_i,g_j(v_i))$, $1 \leq i \leq n$ and $1 \leq j \leq m$. Then the modified Wiener index of G is equal to:

$$\frac{n}{2m} \times \text{the summation of all entries in } \hat{D}.$$

Notice that $\delta(g_i)$ is the the average of the row corresponding to g_i. Define $\gamma : G \longrightarrow \mathbb{C}$ given by $\gamma(x) = \frac{1}{|\Gamma|}\sum_{g\in\Gamma} d(x,g(x))$.

Theorem 3. Suppose G is a connected $n-$vertex graph and $\Gamma = Aut(G)$. Then $\hat{W} \geq \frac{n}{2}(n-t_1)$, where t_1 denotes the number of orbits of Γ on $V(G)$. If G is vertex transitive then the equality is satisfied if and only if G is isomorphic to K_n.

In the following example, we calculate the character table of the automorphism group of some graphs together with their associated class functions. Suppose $\mathbb{Z}_n$, S_n and D_{2n} denote the cyclic group of order n, the symmetric group on n letters and the dihedral group of order $2n$. If H and K

are subgroups of a group G such that H is normal, $H \cap K = \{e\}$ and $G = HK$ then we say G is a semidirect product of H by K and in this case we write $G = H : K$.

Example 4. In this example the class function δ together with the modified Wiener index of Petersen graph P_5. It is well-known that the automorphism group of the Petersen graph is isomorphic to the symmetric group S_5. This graph is depicted in Figure 1 and its character table together with class function δ_1 is recorded in Table 1.

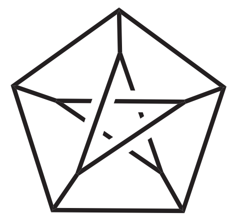


Figure 1: The Petersen Graph.

Table 1: The Character Table of $Aut(P_5) \cong S_5$ and the Class Function δ_1.

	$1a$	$2a$	$2b$	$6a$	$3a$	$4a$	$5a$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	-1	1	-1	1
χ_3	4	-2	0	1	1	0	-1
χ_4	4	2	0	-1	1	0	-1
χ_5	5	1	1	1	-1	-1	0
χ_6	5	-1	1	-1	-1	1	0
χ_7	6	0	-2	0	0	0	1
δ_1	0	$\frac{6}{5}$	$\frac{6}{5}$	$\frac{6}{5}$	$\frac{9}{5}$	$\frac{9}{5}$	$\frac{3}{2}$

From Table 1, one can see that $\delta_1 = \dfrac{3}{2}\chi_1 - \dfrac{3}{10}\chi_5$ and $\hat{W}(P_5) = 75$.

Our calculations given Example 4, and some other calculations with GAP and MAGMA suggest the following conjecture:

Conjecture 5: For each graph G, the class function δ is a rational combination of the trivial character χ_1 and at most two other irreducible characters of $Aut(G)$.

For the sake of completeness, we mention here a result of Graovac and Pisanski [3] about modified Wiener index of the Cartesian product of graphs.

Theorem 6. (Graovac and Pisanski [3, Theorem 5.13]) Suppose G and H are connected graphs such that each orbit of the action of $Aut(G \times H)$ on $V(G) \times V(H)$ has the form $A \times B$, where A is an orbit for the action of $Aut(G)$ on $V(G)$ and B is an orbit for the action of $Aut(H)$ on $V(H)$. Then

$$\hat{W}(G \Box H) = |V(G)|^2 \hat{W}(H) + |V(H)|^2 \hat{W}(G).$$

Example 7. In this example the modified Wiener index of a C_4-grid, C_4-nanotube and C_4-nanotorus are computed. We recall that the symmetry group of a path P_n is a cyclic group of order two with the following non identity element g:

$$g = \begin{cases} (1\ n)(2\ n-1)\cdots(\frac{n-1}{2}\ \frac{n+3}{2}) & n \text{ is odd} \\ (1\ n)(2\ n-1)\cdots(\frac{n}{2}\ \frac{n+2}{2}) & n \text{ is even} \end{cases}$$

On the other hand, the group of all symmetries of a regular polygon, including both rotations and reflections is isomorphic to a dihedral group of order $2n$, denote by D_{2n}. We mention here that there is a typographical error in [3, Example 5.6] for computing $\hat{W}(P_n)$. One can easily prove that:

$$\hat{W}(P_n) = \hat{W}(C_n) = \begin{cases} \frac{n^3}{8} & n \text{ is even} \\ \\ \frac{n^3-n}{8} & n \text{ is odd} \end{cases} \quad (2)$$

Apply (2) and [3, Theorem 5.13] to prove the following equality:

$$\begin{aligned} \hat{W}(C_m \square P_n) &= \hat{W}(P_m \square P_n) = \hat{W}(C_m \square C_n) \\ &= |V(C_m)|^2 \hat{W}(C_n) + |V(C_n)|^2 \hat{W}(C_m) \\ &= \begin{cases} \frac{m^2n^2}{8}(n+m) & m \text{ and } n \text{ are even} \\ \frac{mn}{8}(mn^2 + n(m^2-1)) & m \text{ is odd and } n \text{ is even} \\ \frac{mn}{8}(m(n^2-1) + nm^2) & n \text{ is odd and } m \text{ is even} \\ \frac{mn}{8}(m(n^2-1) + n(m^2-1)) & m \text{ and } n \text{ are odd} \end{cases} \end{aligned}$$

The modified hyper$-$Wiener index of P_n can be calculated in the following form:

$$W\hat{W}(P_n) = \begin{cases} \frac{n^3}{16} + \frac{n^2}{24}(n^2-1) & n \text{ is even} \\ \\ \frac{n^4}{24} + \frac{n^3}{16} - \frac{n^2}{24} - \frac{n}{16} & n \text{ is odd} \end{cases}$$

By a method similar to the case of P_n, we have:

$$W\hat{W}(C_n) = \begin{cases} \frac{1}{48}n^4 + \frac{1}{16}n^3 + \frac{1}{24}n^2 & n \text{ is even} \\ \\ \frac{1}{48}n^4 + \frac{1}{16}n^3 - \frac{1}{48}n^2 - \frac{1}{16}n & n \text{ is odd} \end{cases}$$

It is clear that if $u, v \in K_n$ then $d(u,v) = 1$ and so between graphs with exactly n vertices, the complete graph K_n has the minimum hyperWiener index. Hence for every $n$vertex graph G,

$$WW(G) \geq WW(K_n) = \binom{n}{2}$$

On the other hand, it is easy to see that the symmetry group of K_n is isomorphic to the symmetric group S_n and so

$$\hat{W}(K_n) = W\hat{W}(K_n) = \frac{n^2}{2} - \frac{n}{2}.$$

Since graphs with trivial automorphism group have zero hyper−Wiener index, the complete group K_n does not have the minimum value of hyper−Wiener index in the set of all $n-$vertex graphs. We end this section by calculation of the modified hyper−Wiener index of S_n. It is well-known that the symmetry group of the star graph is isomorphic to Sym_{n-1}. So,

$$\begin{aligned} \hat{W}(S_n) &= n(n-2), \\ W\hat{W}(S_n) &= \frac{3}{2}n(n-2). \end{aligned}$$

References

[1] S. Firouzian, M. Faghani, F. Koorepazan−Moftakhar and A. R. Ashrafi, The hyper−Wiener and modified hyper−Wiener indices of graphs with an application on fullerenes, to appear in *Studia UBB Chemia*.

[2] C. Godsil, G. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics, **207**, Springer-Verlag, New York, 2001.

[3] A. Graovac, T. Pisanski, On the Wiener index of a graph, *J. Math. Chem.* **8** (1991) 53–62.

[4] D. J. Klein, I. Lukovits and I. Gutman, On the definition of the hyper−Wiener index for cycle−containing structures, *J. Chem. Inf. Comput. Sci.*, **35** (1995) 50–52.

[5] F. Koorepazan−Moftakhar and A. R. Ashrafi, Distance under symmetry, to appaer in *MATCH Commun. Math. Comput. Chem.*.

[6] H. Wiener, Structural determination of paraffin boiling points, *J. Am. Chem. Soc.* **69** (1947) 17–20.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*, University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), p. 129.**

Poster Presentation

Replacement Product of Two Cayley Graphs

Amir Loghman
Department of Mathematics, Payame Noor Universtiy, P. O. BOX 19395-3697 Tehran, Iran
amirloghman@gmail.com

Abstract

Let G be a group generated by a finite set S. Assume that S is symmetric, namely $S = S^{-1}$. The Cayley graph $X = C(G,S)$ is defined as follows. Vertices of X are elements in G and two vertices $g_1, g_2 \in G$ are adjacent if $g_1 = g_2 s$ for some $s \in S$. Also let Γ_1 be an (n,k)-graph and let Γ_2 be a (k,k')-graph with $V(\Gamma_2) = [k] = \{1,\ldots,k\}$ and fix a randomly numbering φ_{Γ_1} of Γ_1. The replacement product $\Gamma_1 \circledR_{\varphi_{\Gamma_1}} \Gamma_2$ is the graph whose vertex set is $V(\Gamma_1) \times V(\Gamma_2)$ and there is an edge between vertices (v,k) and (w,l) whenever $v = w$ and $kl \in E(\Gamma_2)$ or $vw \in E(\Gamma_1)$, $\varphi_G^v(w) = k$ and $\varphi_G^w(v) = l$. In this note we study these new product of graphs and compute cayley graph of some nanostructure.

Keywords: Cayley graph, replacement product, fullerene graphs.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 131-132.

Oral Presentation

On a Class of Linear Codes

M. Mazrooei
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
m.mazrooei@kashanu.ac.ir

A. Rafieipour
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
a.rafieepour@gmail.com

Abstract

We study the code parameters of a class of linear codes over the Galois field $\mathbb{Z}_l$, where l is an odd prime. This class is originally introduced by L. Skula as an invariant subspace of a special linear operator on the vector space $(\mathbb{Z}_l)^{\frac{l-1}{2}}$.

Keywords: Dual code, generator matrix, linear code.

MSC(2010): Primary: 68P30; Secondary: 15A03.

1 Introduction

Let q be a prime power and F_q denote the field with q elements. A linear code C of length n and dimension k over F_q (an $[n,k]_q$-code) is a k-dimensional linear subspace of F_q^n. The elemnts of a code are called codewords. A generator matrix G for C is a $k \times n$ matrix whose rows form an F_q-basis of C. By definition,

$$C = \{x^t G \mid x \in F_q^k\},$$

where x^t stands for the transpose of a vector x. For any codeword $c = (c_1, \cdots, c_n)$, the weight $w(c)$ of c is defined as the number of nonzero coordinates of c. The number

$$d(C) := \min\{w(c) \mid 0 \neq c \in C\}$$

is called the minimum distance of C. It is well-known that $k + d(C) \leq n+1$. If the equality holds, then we say that C is an MDS code.

The dual code $C^{\perp}$ of C is the $[n, n-k]_q$-code

$$\{(x_1, \cdots, x_n) \in F_q^n \mid \forall c = (c_1, \cdots, c_n) \in C,\ \sum_{i=1}^{n} x_i c_i = 0\}.$$

Now, assume that l is an odd prime, $n = \frac{l-1}{2}$ and V is the vector space

$$(\mathbb{Z}_l)^n = \{(c_1, \cdots, c_n) \mid c_i \in \mathbb{Z}_l\}.$$

Let $L = \{1, 2, \cdots, n\}$ and for a subset $A \subseteq L$ put

$$C_A = \{(a_1, \cdots, a_n) \in V \mid \forall j \in A,\ \sum_{i=1}^{n} a_i i^{2j-1} = 0\}.$$

It is easy to verify that C_A is a subspace of V for any $A \subseteq L$. The subspaces C_A are defined by L. Skula in [1] as invariant subspaces of a special linear operator on the vector space V. Skula has proven that

1) For $A \subseteq B \subseteq L$, the relation $C_A \supseteq C_B$ holds,

2) $C_\emptyset = V$ and $C_L = 0$,

3) C_A is an $(n - |A|)$-dimensional vector space.

In this paper, we are intrested to study C_A as a linear code over the field $\mathbb{Z}_l$. Specially, we focus on the minimum distance, the dual code and the generator matrix of such codes.

2 Main Results

The following results are obtained for linear codes C_A.

Theorem 2.1. *For any $\emptyset \neq A \subseteq L$, C_A is a linear code of minimum distance $d(C) \leq |A|+1$. Specially, C_A is an MDS code for all 1-elemnt subsetes of L.*

Theorem 2.2. *If $A = \{j\}$, $1 \leq j \leq n$, then $C_A^{\perp} = C_B$ where $B = L \setminus \{n - j + 1\}$. This give us an algorithm to find the dual code $C_A^{\perp}$ for all $A \subseteq L$.*

Theorem 2.3. *The set*

$$\{(1, 2^{2i-1}, \cdots, n^{2i-1}) \mid i \in B\}$$

is a basis of C_A where $B \subseteq L$ is the set in which $C_A^{\perp} = C_B$. This gives us a generator matrix of C_A.

References

[1] Skula L., *Special invariant subspaces of a vector space over $\mathbb{Z}/l\mathbb{Z}$*, Archivum Mathematicum **vol. 25** (1989), 35-46.

[2] Vanstone S. A. and Van Oorschot P. C., An Introduction to Error Correcting Codes with Applications (The Springer International Series in Engineering and Computer Science), Springer, (1989).

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 133-137.

Oral Presentation

A Note on the Power Graph of some Finite Groups and their Automorphism Groups

Z. Mehranian
Department of Mathematics, University of Qom, Qom, I. R. Iran
mehranian.z@gmail.com

A. Gholami
Department of Mathematics, University of Qom, Qom, I. R. Iran
gholami@kashanu.ac.ir

A. R. Ashrafi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan
87317-51116, I. R. Iran
ashrafi@kashanu.ac.ir

Abstract

In this note, we compute the power graph of the cyclic group of order n and some of finite groups with their automorphism groups.

Keywords: power graph, generalized join, automorphism group.

MSC(2010): Primary: 20D45; Secondary: 05C60.

1 Introduction

All groups and graphs in this note are assumed to be finite. Suppose G is a finite group, the **power graph of** G, $\mathscr{P}(G)$, is a graph in which $V(\mathscr{P}(G)) = G$ and two distinct elements x and y are adjacent if and only if one of them is a power of the other. It can be easily investigated that the power graph $\mathscr{P}(G)$ is a connected graph of diameter at most 2. The power graphs are a new representation of groups using graphs. These graphs were first used by Kelarev [3]. Chakrabarty et al. [1] proved that for a finite group G, $\mathscr{P}(G)$ is complete if and only if G is a cyclic group of order 1 or p^m, for some prime number p and positive integer m. They also obtained a formula for the number of edges in a finite power graph. Suppose Γ is a graph with $V(\Gamma) = \{1, 2, \cdots, p\}$ and $\mathscr{F} = \{\Gamma_1, \cdots, \Gamma_p\}$ is a family of graphs such that $n_j = |V(\Gamma_j)|$, $1 \leq j \leq p$. Define $\Lambda = \Gamma[\Gamma_1, \cdots, \Gamma_p]$ to be a graph with vertex set $V(\Lambda) = \bigcup_{j=1}^{p} V(\Gamma_j)$ and edge set $E(\Lambda) = \left(\bigcup_{j=1}^{p} E(\Gamma_j)\right) \cup \left(\bigcup_{ij \in E(\Gamma)} \{uv; u \in V(\Gamma_i), v \in V(\Gamma_j)\}\right)$.

Example 1. Let G be an alternating group of order 12. Then $\mathscr{P}(G)$ consists of 4 triangels and three lines sharing a common vertex (the identity):

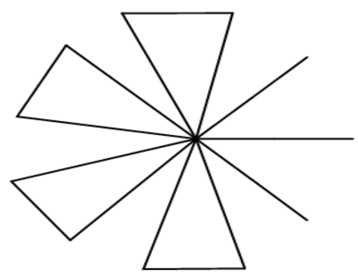


Figure 1: The Power Graph of $\mathbb{A}_4$.

Definition 2. The semi-dihedral group SD_{8n}, dicyclic group T_{4n}, the groups V_{8n} and U_{6n} have the following presentations, respectively:

$$\begin{aligned}
SD_{8n} &=< a, b | a^{4n} = b^2 = e, bab = a^{2n-1} >,\\
T_{4n} &=< a, b | a^{2n} = e, a^n = b^2, b^{-1}ab = a^{-1} >,\\
V_{8n} &=< a, b | a^{2n} = b^4 = e, aba = b^{-1}, ab^{-1}a = b >,\\
U_{6n} &=< a, b | a^{2n} = b^3 = e, a^{-1}ba = b^{-1} > .
\end{aligned}$$

2 The Recent Results

The aim of this section is to compute the power graph of group $\mathbb{Z}_n$ and groups SD_{8n}, T_{4n}, V_{8n} and U_{6n}. We calculate the automorphism groups of the power graph of group $\mathbb{Z}_n$ and mentioned groups.

Theorem 3[4] $\mathscr{P}(\mathbb{Z}_n) = K_{\phi(n)+1} + \Delta_n[K_{\phi(d_1)}, K_{\phi(d_2)}, \cdots, K_{\phi(d_p)}]$, where Δ_n is a graph with vertex and edge sets $V(\Delta_n) = \{d_i \mid 1, n \neq d_i | n, 1 \leq i \leq p\}$ and $E(\Delta_n) = \{d_i d_j \mid d_i | d_j, 1 \leq i < j \leq p\}$, respectively.

In [2] Doostabadi et al. conjectured that the automorphism group of $\mathbb{Z}_n$ is isomorphic to the direct product of some symmetry groups.

Conjecture 4.[2] For every positive integer n,

$$Aut(\mathscr{P}(\mathbb{Z}_n)) \cong S_{\phi(n)+1} \times \prod_{1,n \neq d|n} S_{\phi(d)}.$$

It is clear that the mentioned conjecture is incorrect, when n is prime power. In the next theorem this conjecture is proved for positive integer n, such that n cannot written as a prime power.

Theorem 5.[4] If n is not a prime power, then

$$Aut(\mathscr{P}(\mathbb{Z}_n)) \cong S_{\phi(n)+1} \times \prod_{1,n \neq d|n} S_{\phi(d)}.$$

Corollary 6.[4] The automorphism group of the power graph D_{2n} can be computed as follows:

$$Aut(\mathscr{P}(D_{2n})) \cong \begin{cases} S_{n-1} \times S_n, & n \text{ is a prime power} \\ S_n \times \prod_{d|n} S_{\phi(d)}, & otherwise \end{cases}.$$

Example 7. The power graph of SD_{8n} is a union of $\mathscr{P}(\mathbb{Z}_{4n})$, n copies of $\mathscr{P}(\mathbb{Z}_4)$ that share an edge and $2n$ copies of $\mathscr{P}(\mathbb{Z}_2)$, all of them are connected to each other in the identity element of SD_{8n}, as shown in Figure 2. The power graph of T_{4n} can be constructed in a similar way as a union of $\mathscr{P}(\mathbb{Z}_{2n})$ and n copies of $\mathscr{P}(\mathbb{Z}_4)$ that share an edge, all connected to each other in the identity element of T_{4n}, as shown in Figure 3.

The automorphism group of power graph T_{4n} and SD_{8n} are computed in the following theorems:

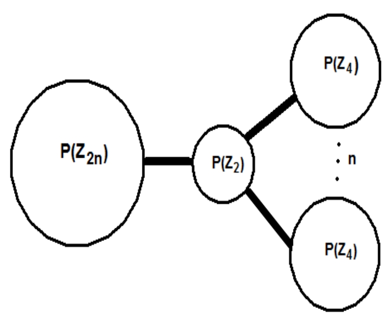


Figure 2: The Power Graph of T_{4n}.

Theorem 8. let $n \geq 3$ be a natural number, then

$$Aut(\mathscr{P}(T_{4n})) \cong \begin{cases} S_{2n-2} \times S_2 \times (S_2 \wr S_n), & n \text{ is a power of } 2, \\ \prod_{d|2n} S_{\phi(d)} \times (S_2 \wr S_n), & otherwise \end{cases}.$$

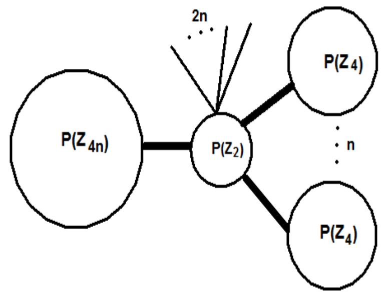


Figure 3: The Power Graph of SD_{8n}.

Theorem 9. let $n \geq 2$ be a natural number, then

$$Aut(\mathscr{P}(SD_{8n})) \cong \begin{cases} S_{4n-2} \times S_{2n} \times (S_2 \wr S_n), & n \text{ is a power of } 2, \\ \prod_{d|4n} S_{\phi(d)} \times S_{2n} \times (S_2 \wr S_n), & otherwise \end{cases}.$$

The automorphism groups of power graphs U_{6n} and V_{8n} are computed in the following theorems:

Theorem 10. let n be a natural number, then

$$Aut(\mathscr{P}(U_{6n})) \cong \begin{cases} \prod_{d|3n} S_{\phi(d)} \times \prod_{d|2n, d\nmid n} S_{\phi(d)} \wr S_3, n \neq 3t, t \geq 1 \\ \prod_{d|2n, d\nmid n} S_{\phi(d)} \wr S_3 \times \prod_{d|n} S_{\phi(d)} \times \prod_{d|n, d\nmid t} S_{\phi(d)} \wr S_3, n = 3t, t \geq 1, 3 \nmid t \\ \prod_{d|2n, d\nmid n} S_{\phi(d)} \wr S_3 \times \prod_{d|n} S_{\phi(d)} \times \prod_{d|3t, d\nmid t} S_{\phi(d)} \wr S_3 \times \prod_{d|n, d\nmid 3t} S_{\phi(d)} \wr S_2, \\ n = 3^k t, k \geq 2, t \geq 1 \end{cases}.$$

Theorem 11 let n be a natural number, then

$$Aut(\mathscr{P}(V_{8n})) \cong \begin{cases} S_{2n} \times S_2 \wr S_n \times \prod_{d|2n, d\nmid n} S_{\phi(d)} \wr S_2 \times \prod_{d|2n} S_{\phi(d)}, n \geq 3, 2 \nmid n \\ S_{2n+1} \times S_2 \wr S_n \times \prod_{t=1}^{k-1} S_{2^t}^2 \times S_{2^k} \wr S_2, n = 2^k, k \geq 2 \\ S_{2n} \times S_2 \wr S_n \times \prod_{d|t} S_{\phi(d)}^4 \times \prod_{s=2}^{k} \prod_{\substack{d|2^s t \\ d\nmid 2^{s-1} t}} S_{\phi(d)}^2 \times \prod_{\substack{d|2^{k+1} t \\ d\nmid 2^k t}} S_{\phi(d)} \wr S_2, \\ n = 2^k t, k \geq 1, 2 \nmid t \end{cases}.$$

References

[1] I. Chakrabarty, S. Ghosh and M. K. Sen, Undirected power graphs of semigroups, Semigroup Forum **78** (2009) 410–426.

[2] A. Doostabadi, A. Erfanian and A. Jafarzadeh, Some results on the power graph of groups, The Extended Abstracts of the 44th Annual Iranian Mathematics Conference, 27–30 August 2013, Ferdowsi University of Mashhad, Iran.

[3] A. V. Kelarev and S. J. Quinn, A combinatorial property and power graphs of groups, Contributions to general algebra, 12 (Vienna, 1999), 229–235, Heyn, Klagenfurt (2000).

[4] Z. Mehranian, A. Gholami and A. R. Ashrafi, A note on the Power graph of a finite group, *Transactions on Combinatorics*, submitted.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 139-142.

Oral Presentation

On Enumeration of M-Polysymmetrical Hypergroups of Order less than 6

Saeed Mirvakili
Department of Mathematics, Payame Noor University, Theran, Iran
saeed_mirvakili@pnu.ac.ir

Raoufeh Manaviyat
Department of Mathematics, Payame Noor University, Theran, Iran
r.manaviyat@pnu.ac.ir

Abstract

In this paper, we enumerate M-polysymmetrical hypergroups of order less than 6. We show that there are 7 isomorphism classes of M-polysymmetrical hypergroups of order 5 and present the Cayley tables of them.

Keywords: Hypergroup, polysymmetrical.

MSC(2010): Primary: 20N20.

1 Introduction

The concept of a hyperstructures first was introduced by Marty at the 8^{th} international Congress of Scandinavian Mathematicians. The hyperstructure theory had applications to several domains of theoretical and applied mathematics[4, 5].

J. Mittas in his paper[6], which has been announced in the French Academy of Sciences, has introduced a special type of hypergroup that he has named polysymmetrical. Also, in the same paper J. Mittas has given certain fundamental properties of this hyperstructure.

Staring from the above paper and having called Mittas structure M-polysymmetrical hypergroup (in order to distinguish this polysymmetrical hypergroup from other types of polysymmetrical hypergroups) we have proceeded to a profound analysis of this hypergroup[7] and its subhypergroups[8].

We recall definition of M-polysymmetrical hypergroup of [8] as follows:

A non-empty set H is called M-polysymmetrical hypergroup (M-P-H.) if it is endowed with a hyperoperation $+: H \times H \to \mathscr{P}^*(H)$, when $\mathscr{P}^*(H)$ is the set of all non-empty subsets of H, that satisfies the following axioms:

(1) $+$ is associative, i. e, for every $x,y,z \in H$ we have $x+(y+z) = (x+y)+z$;

(2) $+$ is commutative, i. e, for every $x,y \in H$, $x+y = y+x$;

(3) there exists $0 \in H$ such that for every $x \in H$ we have $x \in x+0$;

(4) for every $x \in H$ there exists $x' \in H$ such that $0 = x+x'$, (x' is an opposite or symmetrical of x , with regard to considered 0, and the set of all the opposites $S(x) = \{x' | 0 = x+x'\}$ is the symmetrical set of x),

(5) for every $x,y,z \in H, x' \in S(x), y' \in S(y)$ and $z' \in S(z)$, $x \in y+z$ implies that $x' \in y'+z'$.

Theorem 1.1. *[8] Let $(H,+)$ be a M-PH, then for every $x,y,z,w \in H$ we have:*

(1) $S(0) = 0$, that means $0+0 = 0$;

(2) $0 \in 0+x \Rightarrow x = 0$ and hence $y \in y+x \Rightarrow x = 0$;

(3) 0 is unique;

(4) $(x+y) \cap (z+w) \Rightarrow x+y = z+w$;

(5) for all $z' \in S(z)$, $x \in y+z$ implies that $y \in x+z'$;

(6) $0 \in x+y \Rightarrow x+y = 0$.

2 Main Results

In this section we use the results of the papers [8] and [9] and characterize the M-PHs. of order less than 6 up to isomorphism.

Theorem 2.1. *Every M-PH. $(H,+)$ of order 2 is a group and so $H \cong \mathbb{Z}_2$.*

Notice that there are 20 isomorphism classes of H_v-groups of order 2 and 8 isomorphism classes of hypergroups of order 2.

Theorem 2.2. *There are 2 isomorphism classes of M-PHs. of order 3 with the following tables:*

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

+	0	1	2
0	0	12	12
1	12	0	0
2	12	0	0

Bayon and Lygeros [1] show that there are 1.026.462 isomorphism classes of H_v-groups of order 3. Also, Tsitouras and Massouros [9] enumerated 23.192 isomorphism classes of hypergroups of order 3.

Theorem 2.3. *There are 4 isomorphism classes of M-PHs. of order 4 with the following tables:*

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

+	0	1	2	3
0	0	123	123	123
1	123	0	0	0
2	123	0	0	0
3	123	0	0	0

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3
0	0	1	23	23
1	1	23	0	0
2	23	0	1	1
3	23	0	1	1

Bayon and Lygeros [2] show that there are 10.614.362 isomorphism classes of abelian hypergroups of order 4. Bayon and Lygeros [3] enumerated 8.028.299.905 isomorphism classes of abelian H_v-groups of order 4.

Theorem 2.4. *There are 7 isomorphism classes of M-PHs. of order 5 with the following tables:*

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	0	1	2	4
4	0	1	2	3	4

+	0	1	2	3	4
0	0	1234	1234	1234	1234
1	1234	0	0	0	0
2	1234	0	0	0	0
3	1234	0	0	0	0
4	1234	0	0	0	0

+	0	1	2	3	4
0	0	12	12	34	34
1	12	34	34	0	0
2	12	34	34	0	0
3	34	0	0	12	12
4	34	0	0	12	12

+	0	1	2	3	4
0	0	1	2	34	34
1	1	2	34	0	0
2	2	34	0	1	1
3	34	0	1	2	2
4	34	0	1	2	2

+	0	1	2	3	4
0	0	1	234	234	234
1	1	234	0	0	0
2	234	0	1	1	1
3	234	0	1	1	1
4	234	0	1	1	1

+	0	1	2	3	4
0	0	1	23	23	4
1	1	23	4	4	0
2	23	4	0	0	1
3	23	4	0	0	1
4	4	0	1	1	23

+	0	1	2	3	4
0	0	1	2	34	34
1	1	0	34	2	2
2	2	34	0	1	1
3	34	2	1	0	0
4	34	2	1	0	0

References

[1] Bayon, R. and Lygeros, N., *L*es hypergroupes et H_v-groupes dordre 3, submitted to Bulletin of the Greek Mathematical Society.

[2] Bayon, R. and Lygeros, N., *N*umber of abelian H_v-groups of order n, In N. J. A. Sloane, editor, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/projects/OEIS?Anum=A108089, 2005.

[3] Bayon, R. and Lygeros, N., *L*es hypergroupes ab*é*liens dordre 4. In El*é*ments structurels de la th*é*orie des hyperstructures: Colloque de lUniversit*é* de Thrace, mars 2005.

[4] Corsini, P. and Leoreanu, V., *A*pplications of hyperstructures theory, Advanced in Mathematics, Kluwer Academic Publisher, (2003).

[5] Davvaz, B., Polygroup Theory and Related Systems, World Scientific, (2013).

[6] Mittas, J., *H*ypergroupes et hyperanneaux polysymetriques, C.R. Acad. Sci. Paris, **271** (1970), 290-293.

[7] Yatras, C.N., *H*omorphism in the theory of the *M*-polysymmetrical hypergroups and monogene *M*-polysymmetrical hypergroups, Procceedings of the workshop on Global Analysis, Differential Geometry and Lie Algebras, (1995), 155-165.

[8] Yatras, C.N., *M*-polysymmetrical hypergroups, Riv. di Mat. pura ed Appl., **11** (1992), 81-92.

[9] Tsitouras, Ch. and Massouros, Ch. G., *O*n enumeration of hypergroups of order 3, Computers and Mathematics with Applications, **59** (2010) 519-523.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 143-144.

Poster Presentation

A Review on Extension Theorems for Linear Codes

Mohammad Ali Mohammad Ghasemi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
mohammadghasemi1390@yahoo.com

Reza Kahkeshani
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
kahkeshanireza@kashanu.ac.ir

Abstract

In this paper, we review the recent results concerning extension theorems of linear codes.

Keywords: Linear codes, extension, projective geometry.

MSC(2010): 94B27 . 94B05 . 51E20 . 05B25.

1 Introduction

Let $\mathbb{F}_q$ be the field of q elements and let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$. A linear code C of length n, dimension k and minimum distance d over $\mathbb{F}_q^n$ is called an $[n,k,d]_q$-code. A generator matrix for C is a matrix whose rows generate C. For an $[n,k,d]_q$-code C with a generator matrix G, C is called extendable to C' if there exists a vector $h \in \mathbb{F}_q^k$ such that the extended matrix $[G,h^T]$ generates an $[n+1,k,d+1]_q$ code C'. The code C' is an extension of C.

2 Results

Theorem 2.1. ([1]) *Every $[n,k,d]_2$ code with d odd is extendable.*

Hill and Lizak generalized Theorem 2.1 to the following for non-binary codes. The idea of the proof of the next theorems refer to the Projective Geometry.

Theorem 2.2. ([2, 3]) *Every* $[n,k,d]_q$ *code with* $\gcd(d,q)=1$ *whose weights are congruent to* 0 *or* *d (mod q) is extendable.*

For an $[n,k,d]_q$ code C with $\gcd(d,q)=1$, let

$$\Phi_0 = \frac{1}{q-1}\sum_{q|i,i>0} A_i, \qquad \Phi_1 = \frac{1}{q-1}\sum_{i\neq 0,d(mod q)} A_i.$$

The pair of integers (Φ_0,Φ_1) is called the diversity of C. According to Theorem 2.1, C is extendable if $\Phi_1 = 0$. Landjev and Rousseva generalized Theorem 2.1 to the following:

Theorem 2.3. ([4]) *Every* $[n,k,d]_q$ *code with* $\gcd(d,q)=1$ *is extendable if*

$$\Phi_1 \leq q^{k-3}(s(q)-q-1)/(q-1),$$

where $s(q)$ *is the smallest size of a nontrivial blocking set in* $PG(2,q)$.

Maruta and Yoshida gave a further generalization of the previous results and proved the following theorems:

Theorem 2.4. *There exists no* $[n,k,d]_q$ *code with* $\gcd(d,q)=1$ *for* $0<\Phi_1<q^{k-2}$.

Theorem 2.5. *Every* $[n,k,d]_q$ *code with* $\gcd(d,q)=1$ *is extendable if* $\Phi_1<q^{k-2}$.

3 Acknowledgments

The authors are partially supported by the University of Kashan under grant number 364996/3.

References

[1] J. Bierbrauer, *Introduction to Coding Theory*, Chapman and Hall, London (2005).

[2] R. Hill, *An extension theorem for linear codes*, Des. Codes Cryptogr. 17, 151-157 (1999).

[3] R. Hill, P. Lizak, *Extensions of linear codes*, In Proceedings of the IEEE International Symposium on Information Theory, p. 345. Whistler, Canada (1995).

[4] I, Landjev, A. Rousseva, *An extension theorem for arcs and linear codes*, Probl. Inform. Transm. 42, 319-329 (2006).

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), p. 145.

Oral Presentation

Simple Mean-Field Approximations for the Restricted Solid-on-Solid Growth Models

R. Rezaeizade
Science & Research University, Hamedan, Iran
r.rezaeizade@gmail.com

Abstract

We study models for surface growth with a wetting and a roughening transition. Using simple and pair mean-field approximations. The simple mean-field equations are solved exactly and they predict the roughening transition and the correct growth exponents in a region of the phase diagram.

Keywords: Phase transition, rsos model, mean-field approximation.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 147-150.

Poster Presentation

Revised Augmented Eccentric Connectivity Index of Fullerenes

Maryam Safazadeh
Department of Mathematics, Persian Gulf University, Bushehr, Iran

Reza Sharafdini
Department of Mathematics, Persian Gulf University, Bushehr, Iran

Abstract

In theoretical chemistry, molecular structure descriptors are used for modeling physio-chemical, pharmacologic, toxicological, biological and other properties of chemical compound. The augmented eccentric connectivity index of graph G is defined as

$$^{A}\xi(G) = \sum_{u\in V(G)} M(u)\varepsilon(u)^{-1},$$

where $\varepsilon(u)$ is defined as the length of a maximal path connecting u to another vertex of G. Fullerenes are molecules in the form of cage-like polyhedra, consisting solely of carbon atoms bonded in a nearly spherical configuration. In this paper we compute some bounds of the augmented eccentric connectivity index and then we calculate this topological index for two infinite classes of fullerenes.

Keywords: Augmented eccentric connectivity index, fullerenes, topological index, eccentricity.

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1 Introduction

In theoretical chemistry, molecular structure descriptors are used for modeling physico-chemical, pharmacologic, toxicological, biological and other properties of chemical compound.

Let G be any simple connected graph with vertex set $V(G)$ and edge set $E(G)$ and $n = |V(G)|$. For two vertices u and v in $V(G)$ their distance $d_G(u,v)$ is defined as the length of a shortest path connecting u and v in G. For a given vertex u of G its eccentricity $\varepsilon_G(u)$ is the largest distance between u and any other vertices of G, i.e., $\varepsilon_G(u) = \max_{v \in V(G)} d(u,v)$. The maximum eccentricity over all vertices of G is called the diameter of G and is denoted by $D(G)$; the minimum eccentricity among the vertices of G is called radius of G and is denoted by $R(G)$. The set of all vertices of minimum eccentricity is called the center of G.

The eccentric connectivity index of a graph G is defined as

$$\xi^c(G) = \sum_{u \in V(G)} d_G(u)\varepsilon_G(u),$$

where $d_G(u)$ denotes the degree of vertex u, i. e., the number of its neighbors in G. The eccentric connectivity index was introduced by Madan *et al.* and used in a series of papers concerned with QSAR/QSPR studies [8, 7, 5]. This index was successfully used for mathematical models of biological activities of diverse nature. In fact, this index has been shown to give a high degree of predictability of pharmaceutical properties, and may provide leads for the development of safe and potent anti-HIV compounds.

The augmented eccentric connectivity index ${}^{\star}\xi^A(G)$ of a graph G is defined as [2]

$${}^{\star}\xi^A(G) = \sum_{u \in V(G)} \frac{M(u)}{\varepsilon_G(u)},$$

where $M(u)$ denotes the product of degrees of all neighbors of vertex u. From above definition it is clear that, as the degrees are taken over the neighborhoods and then multiplied, so the contribution of a vertex to this index is non-local and again since the reciprocal of eccentricity is considered for a vertex so the contribution of a vertex is also non-linear.

A revised version of augmented eccentric connectivity index, under the name Ediz eccentric connectivity index, has been defined as

$${}^{\star}\xi^A(G) = \sum_{u \in V(G)} \frac{S(u)}{\varepsilon(u)},$$

where $S(u)$ denotes the sum of degrees of all neighbors of vertex u.

Fullerenes, discovered experimentally in 1985, are molecules in the form of cage-like polyhedra, consisting solely of carbon atoms bonded in a nearly spherical configuration. It is well-known fact that fullerenes made entirely of n carbon atoms, have 12 pentagonal and (n/2-10) hexagonal faces, while $n \neq 22$ is a natural number equal or greater than 20 [12,13]. The most important member of the family of fullerenes is C_{60} (See Fig.1). In this paper we aim to compute revised augmented eccentric connectivity index for two infinite classes of fullerene graphs C_{12n+2} and C_{20n+40}. Throughout this paper, our notations are standard and mainly taken from standard books of graph theory such as [19].

2 Main Results

In this section we aim to compute the revised augmented eccentric connectivity index of two infinite classes of fullerenes, namely C_{12n+2} and C_{20n+40}. First consider an infinite class of fullerene with exactly $12n+2$ vertices and $18n+3$ edges, depicted in Fig. 3. In Table 1, the augmented eccentric connectivity index of C_{12n+2} fullerenes is computed for $1 \leq n \leq 9$.

Fullerenes	Exceptional augmented eccentric connectivity index for $1 \leq n \leq 9$
C_{26}	$3 \times 72/5 + 1$
C_{38}	$3 \times 114/7$
C_{50}	$3 \times 36/7 + 3 \times 102/8 + 3 \times 12/9$
C_{62}	$3 \times 72/8 + 3 \times 72/9 + 3 \times 42/10$
C_{74}	$3 \times 36/8 + 3 \times 72/9 + 3 \times 54/10 + 3 \times 36/11 + 3 \times 24/12$
C_{86}	$3 \times 72/9 + 3 \times 54/10 + 3 \times 36/11 + 3 \times 36/12 + 3 \times 36/13 + 24/14$
C_{98}	$3 \times (12/9 + 18/10 + 12/11 + 12/12 + 12/13 + 12/14 + 12/15 + 8/16)$
C_{110}	$3 \times (18/10 + 12/11 + 12/12 + 12/13 + 12/14 + 12/15 + 12/16 + 12/17 + 8/18)$

A general formula for the revised augmented eccentric connectivity index of C_{12n+2}, $n \geq 10$, is obtained as follows:

Theorem 2.1.

$$^{A}\xi(C_{12n+2}) = \frac{90}{n} + 108\sum_{i=1}^{n} \frac{1}{n+i}.$$

Proof. Using GAP [20] software, one can see that there are three types of vertices of fullerene graph C_{12n+2}. These are the vertices of the central and outer pentagons and other vertices of C_{12n+2}. By computing the eccentricity of these vertices we have the following table:

Vertices	$\varepsilon(u)$	Number
The Type 1 Vertices	2	8
The Type 1 Vertices	n	6
Other Vertices	$n+i(1 \leq i \leq n)$	12

Consider now an infinite class of fullerene with exactly $20n+40$ vertices and $30n+60$ edges, depicted in Fig. 4. In Table 2, the eccentricity of vertices of C_{20n+40} fullerenes are computed for $1 \leq n \leq 10$. If $n11$ then a general formula for the augmented eccentric connectivity index of C_{20n+40} is obtained as follows:

Theorem 2.2.

$$^{A}\xi(C_{20n+40}) = 180\sum_{i=0}^{n} \frac{1}{n+4+i} + 90(\frac{1}{2n+5} + \frac{1}{2n+6}).$$

Proof. Similar to proof of Theorem 2.1, one can see that there are three types of vertices in the fullerene graph (See Fig. 4). These are the vertices of the central and outer pentagons and other vertices of C_{20n+40}. Computing the eccentricity of these vertices we have the following table:

Vertices	$\varepsilon(u)$	Number
The Type 1 Vertices	$2n+6$	10
The Type 1 Vertices	$2n+5$	10
Other Vertices	$n+4+i(0 \leq i \leq n+1)$	20

References

[1] A.R. Ashrafi, M. Ghorbani, Eccentric Connectivity Index of Fullerenes, 2008, In: I. Gutman, B. Furtula, Novel Molecular Structure Descriptors Theory and Applications II, pp. 183–192.

[2] H. Dureja and A. K. Madan, Superaugmented eccentric connectivity indices: new-generation highly discriminating topological descriptors for QSAR/QSPR modeling, Med. Chem. Res., vol. 16, pp. 331–341, 2007.

[3] M. R. Farahani, The Ediz Eccentric Connectivity index and the Total Eccentricity Index of a Benzenoid System *Journal of Chemica Acta* **2** (2013) 22–25.

[4] I. Gutman, O. E. Polansky, *Mathematical Concepts in Organic Chemistry*, Springer–Verlag, Berlin, 1986.

[5] S. Gupta, M. Singh, and A. K. Madan, Application of graph theory: relationship of eccentric connectivity index and Wieners index with anti-inflammatory activity, J. Math. Anal. Appl., vol. 266, no. 2, pp. 259–268, 2002.

[6] M. Ghorbani, Connective eccentric index of fullerenes, *J. Math. Nanosci.* 1(2011) 43–50.

[7] S. Sardana and A. K. Madan, Application of graph theory: relationship of molecular connectivity index, Wieners index and eccentric connectivity index with diuretic activity, Match, no. 43, pp. 85–98, 2001.

[8] V. Sharma, R. Goswami, and A. K. Madan, Eccentric connectivity index: A novel highly dis- criminating topological descriptor for structure-property and structure-activity studies, J. Chem. Inf. Comput. Sci., vol. 37, pp. 273–282, 1997.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 151-154.

Oral Presentation

Distance-Regular Graphs and Distance Based Graph Invariants

Reza Sharafdini
Department of Mathematics, Faculty of Sciences, Persian Gulf University, Bushehr, Iran
sharafdini@pgu.ac.ir

Abstract

In this article we aim to obtain an explicit formula for some distance based graph invariants of distance-regular graphs. In fact we obtain formulas for Wiener index and its multiplicative version of a distance-regular graph in terms of its intersection array and its distance partition.

Keywords: Distance-regular, strongly regular, Wiener index, multiplicative Wiener index, distance-balanced, Szeged index.

MSC(2010): Primary: 05C12, 05C31.

1 Introduction

Throughout this paper $G = (V,E)$ denotes a connected, simple and finite graph with vertex set $V = V(G)$ and edge set $E = E(G)$.

The *distance* $d(u,v)$ between two vertices u and v is the minimum of the lengths of paths between u and v. The *diameter* D of a graph G is defined as $D := \max_{u,v\in V(G)} d(u,v)$. For a graph G of diameter D, vertex $v \in V(G)$, and for $0 \leq i \leq D$, define $G_i(v) = \left\{ w \in V \mid d(v,w) = i \right\}$. These cells $G_0(v), G_1(v), \dots, G_D(v)$ form a distance partition (or a level decomposition) of G based on $v \in G$. For each $v \in V(G)$, $G_1(v)$ is called the set of neighbors of v; and the size of $G_1(v)$ is called the degree of v. A graph is said to be *k-regular* if $|G_1(u)| = |G_1(v)| = k \quad$ for all $\quad u,v \in V(G)$. A *distance-regular* graph is a simple connected graph such that for any two vertices u and v, the number of vertices at distance i from u and at distance j from v depends only upon i, j, and $t = d(v,w)$. Equivalently, a distance-regular graph is a simple connected graph of diameter D for which there exist integers $a_i, b_i, c_i, i = 0,\ldots,D$ such that for any two vertices x,y in $V(G)$ at distance $i = d(x,y)$, there are exactly c_i neighbors of y in $G_{i-1}(x)$, b_i neighbors of y in $G_{i+1}(x)$ and a_i neighbors of y in $G_i(x)$. Namely,

$$| G_1(y) \cap G_j(x) | = \begin{cases} a_i & \text{if } j = i; \\ c_i & \text{if } j = i-1; \\ b_i & \text{if } j = i+1. \end{cases}$$

The numbers a_i, b_i, and c_i are often displayed in a three-line array $\begin{Bmatrix} c_0 & c_1 & \cdots & c_{D-1} & c_D \\ a_0 & a_1 & \cdots & a_{D-1} & a_D \\ b_0 & b_1 & \cdots & b_{D-1} & b_D \end{Bmatrix}$, which is known as its intersection array. In particular G is regular of degree $k := b_0$ and $a_0 = c_0 = b_D = 0, \quad ,c_1 = 1, \quad a_i + b_i + c_i = k \quad 0 \le i \le D$. We may represent the intersection arrays of a distance-regular graph as

$$\{b_0 = k, b_1, ..., b_{D-1}; c_1 = 1, c_2, ..., c_D\}.$$

Suppose that G is a distance-regular graph of diameter D with the intersection array $\{b_0 = k, b_1, ..., b_{D-1}; c_1 = 1, c_2, ..., c_D\}$. Fixing $0 \le i \le D$, by the definition of distance-regular graphs, the size of $G_i(u)$ does not depend on the choice of $u \in V(G)$. Let us denote the size of $G_i(u)$ by k_i, i.e., $k_i := |G_i(u)|, 0 \le i \le D$. Note that $k_0 = |G_0(u)| = 1$ and $k_1 = |G_1(u)| = k$ and

$$1 + k + k_2 + \ldots + k_D = |V(G)|. \tag{1.1}$$

Moreover, For any vertex $u \in V(G)$, any vertex of $G_i(u)$ is adjacent to b_i vertices in $G_{i+1}(u)$ and any vertex of $G_{i+1}(u)$ is adjacent to c_i vertices in $G_i(u)$. Thus by two way of counting the number of edges between $G_i(u)$ and $G_{i+1}(u)$ we have:

$$k_i b_i = | G_i(u) | \, b_i = | G_{i+1}(u) | \, c_{i+1} = k_{i+1} c_{i+1}. \tag{1.2}$$

Hence, it follows from (1.2) that the number of vertices at distance i of a vertex u, namely $|G_i(u)|$, is obtained directly from the intersection array ([1, Proposition 20.4])

$$k_i = |G_i(u)| = \frac{\prod_{j=0}^{i-1} b_j}{\prod_{j=2}^{i} c_j} \quad (2 \le i \le D) \quad \text{and} \quad |G_1(u)| = b_0. \tag{1.3}$$

The problem of distances in graph attracts the attention of scientist both as theory and applications. In 1947, H. Wiener [18] has proposed his path number, as the total distance between all carbon atoms for correlating with the thermodynamic properties of alkanes. Numerous of its chemical applications were reported and its mathematical properties are well understood. This index now is called the *Wiener index* $W(G)$ of a graph G, and defined as the sum of distances between all unordered pairs of vertices of G, i.e., $W(G) := \sum_{\{u,v\} \subseteq V} d(u,v)$. In fact, if we denote by $d(G,k)$, $k \ge 0$, the number of unordered vertex pairs at distance k, then $W(G) = \sum_{k=1}^{D} k \cdot d(G,k)$. Note that $d(G,3)$ is called the *Wiener polarity* of G which is some times denoted by $W_p(G)$.

For $u \in V(G)$, the *distance sum* $D(u)$ and its multiplication version $D^*(u)$ of u is defined as $D(u) = \sum_{v \in V(G)} d(u,v), \qquad D^*(u) = \prod_{\substack{v \in V(G) \\ v \ne u}} d(u,v)$. In this case the Wiener index of G and its multiplicative version are represented as follows:

$$W(G) = \frac{1}{2} \sum_{u \in V(G)} D(u), \tag{1.4}$$

$$W^*(G) = \frac{1}{2} \prod_{u \in V(G)} D^*(u). \tag{1.5}$$

The following modification of Wiener index has also been considered:

$$W_\lambda(G) := \sum_{\{u,v\} \subseteq V} d(u,v)^\lambda; \quad \lambda \neq 0.$$

$$W_\lambda(G) := \frac{1}{2} \sum_{\{u,v\} \in V(G)} D_\lambda(u); \quad \lambda \neq 0,$$

where $D_\lambda(u)$ is called λ-*distance sum* of u and defined as follows: $D_\lambda(u) = \sum_{\{u,v\} \in V(G)} d(u,v)^\lambda$ The multiplicative version of Wiener index of G, denoted by $W^*(G)$ is also defined as follows [4]: $W^*(G) := \prod_{\substack{v \in V(G) \\ v \neq u}} d(u,v) = \prod_{k=1}^{D} k \cdot d(G,k)$. Hosoya [5] introduced a distance-based graph polynomial $H(G,x) = \sum_{k \geq 1} d(G,k) x^k$, nowadays called the *Hosoya polynomial*. It is easy to check that it can be written in the following form $H(G,x) = \sum_{\{u,v\} \subseteq V(G)} x^{d(u,v)}$. The first derivative of the Hosoya polynomial at = 1 is equal to the Wiener index.

2 Main Results

Theorem 2.1. *Let G be a distance-regular graph whose intersection array is* $\{b_0, b_1, ..., b_{D-1}; c_1 = 1, c_2, ..., c_D\}$. *Then we have* $W_\lambda(G) = \frac{nb_0}{2}\left(1 + \sum_{i=2}^{D} i^\lambda \frac{\prod_{j=1}^{i-1} b_j}{\prod_{j=2}^{i} c_j}\right)$.

Theorem 2.2. *Let G be a distance-regular graph whose intersection array is* $\{b_0, b_1, ..., b_{D-1}; c_1 = 1, c_2, ..., c_D\}$. *Then we have* $W^*_\lambda(G) = \frac{n^{D-1} b_0^D \prod_{i=1}^{D-1} b_i^{D-i}}{4 \prod_{i=2}^{D} c_i^{D+1-i}} D!^\lambda$.

Theorem 2.3. *Let G be a distance-regular graph of diameter D with n vertices. Then for each* $u \in V(G)$

$$D(u) = \sum_{i=1}^{D} ik_i, \quad D^*(u) = D! \prod_{i=1}^{D} k_i,$$

$$W(G) = \frac{n}{2} \sum_{i=1}^{D} ik_i, \quad W^*(G) = \frac{D!^n}{2} \prod_{i=1}^{D} k_i^n.$$

A general case of the above theorem is formulated in the following statement whose proof is done in the same way of Theorem 2.3.

Theorem 2.4. *Let G be a distance-regular graph of diameter D with n vertices. Then for each* $u \in V(G)$ $D_\lambda(u) = \sum_{i=1}^{D} i^\lambda k_i, \quad W_\lambda(G) = \frac{n}{2} \sum_{i=1}^{D} i^\lambda k_i$.

Theorem 2.5. *Let G be a distance-regular graph of diameter D with n vertices. Then* $H(G,x) = \frac{n}{2} \sum_{i=1}^{D} k_i x^i$.

Theorem 2.6. *Let G be a bipartite distance-regular graph of diameter D with n vertices. Then for each $f = uv \in E(G)$*

$$D(f) = \sum_{i=1}^{D-1} \big(ik_i b_i + (i-1)b_1 b_2 \dots b_i\big), \quad W_e(G) = \frac{nb_0}{4} \sum_{i=1}^{D-1} \big(ik_i b_i + (i-1)b_1 b_2 \dots b_i\big).$$

The line graph $L(G)$ of a graph G is defined as follows: each vertex of $L(G)$ represents an edge of G, and any two vertices of $L(G)$ are adjacent if and only if their corresponding edges share a common endpoint in G. One can also define iterated line graphs by setting $L^0(G) = G, L^1(G) = L(G)$ and generally $L^n(G) = L(L^{n-1}(G))$.

The following observation is due to M.H. Khalifeh *at. el* [6, Theorem 2.4]

Theorem 2.7. *Suppose G is a connected graph with m edges. Then*

$$W(L(G)) - W_e(G) = \binom{m}{2}.$$

Corollary 2.8. *Let G be a bipartite distance-regular graph of diameter D with n vertices. Then*

$$W(L(G)) = W_e(G) + \binom{nb_0/2}{2} = \frac{nb_0}{4} \sum_{i=1}^{D-1} \big(ik_i b_i + (i-1)b_1 b_2 \dots b_i\big) + \binom{nb_0/2}{2}$$

References

[1] N. Biggs, Algebraic Graph Theory, 2nd ed., Cambridge University Press, Cambridge, 1993.

[2] A.E. Brouwer, A. M. Cohen, A. Neumaier, Distance–Regular Graphs, Springer–Verlag, Berlin, 1989.

[3] A.A. Dobrynin, I. Gutman, On a graph invariant related to the sum of all distances in a graph, *Publ. Inst. Math. Beograd* **56** (1994) 18–22.

[4] I. Gutman, W. Linert, I. Lukovits and Ž. Tomovi, The Multiplicative Version of the Wiener Index, *J. Chem. Inf. Comput. Sci.*, **40** (1) (2000), 113–116.

[5] H. Hosoya, On some counting polynomials in chemistry, *Discr. Appl. Math.* **19** (1988), 239–257.

[6] M.H. Khalifeh, H. Yousefi-Azari, A.R. Ashrafi, S.G. Wagner, Some new results on distance-based graph invariants, *European J. Combin.*, **30** (2009)1149–1163.

[7] J. A. Rodríguez, On the Wiener index and the eccentric distance sum of hypergraphs, *MATCH Communications in Mathematical and in Computer Chemistry* **54** (1) (2005) 209–220.

[8] H. Wiener, Structural determination of paraffin boiling points, *J. Amer. Chem. Soc.* **69**(1974) 17–20.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 155-158.

Oral Presentation

Secret Sharing Based on Elliptic Curves

M. Bahramian
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
bahramianh@kashanu.ac.ir

M. Sheikhi-Garjan
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
sheikhi.math@gmail.com

F. Seifi-Shahpar
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran
fatemeh.seifishahpar@gmail.com

Abstract

In this paper we propose a secret sharing scheme based on elliptic curves over unsecured channel. The security of this method is based on hardness of Discrete Logarithm Problem (DLP) of elliptic curves. In addition we use Edwards curve because it provides a time effiecient for point addition formula.

Keywords: Secret sharing schemes, elliptic curves, Edwards curves.

MSC(2010): Primary: 94A62; Secondary: 11G07.

1 Introduction

Secret sharing is a method of distributing a secret amongst a group of people by giving each person a part of secret (a share), in which each of whom have equal rigths in decrypting the secret. Secret sharing schemes were introduced independetly by Blakley [1] and Shamir [2] in 1979.

Here we explain two types of secret sharing schemes:

I) (k,k) Threshold Scheme
A dealer, who distributes shares to peolpe, splits a secret S amongst k people such that all k people are needed to construct the secret.

II) (k,n) Threshold Scheme
Dealer splits a secret S into n people such that any group of k people can reconstruct the secret, but no group of people less than k people can do so.

The special case of threshold secret sharing invented by Shamir in 1979, based on k points S needed to uniquely determining a polynomial of degree $k-1$.
Dealer divides secret $S \in \mathbb{Z}_p$ into pieces S_i by randomly choosing $k-1$ elements denoted by $\{a_1, a_2, ..., a_{k-1}\}$ in which $a_0 = S$ and

$$f(x) = a_0 + a_1 x + ... + a_{k-1} x^{k-1}$$

where each share is a point $(x_i, f(x_i)), (1 \leq i \leq n)$.
To reconstruct the secret S any group of k elements uses a method of calculating the polynomial $f(x)$, which is based on the Lagrange interpolation formula for polynomials,

$$f(x) = \sum_{i=1}^{k} f(x_i) \prod_{j=1, j \neq i}^{k} \frac{x - x_i}{x_i - x_j}.$$

Every group of people only interested to compute the secret $S = a_0$, therefore we can make simplification, since $S = a_0 = f(0)$, we substitute $x = 0$ into Lagrange interpolation formula and get

$$S = \sum_{i=1}^{k} f(x_i) \prod_{j=1, j \neq i}^{k} \frac{-x_i}{x_i - x_j}.$$

So we can calculate the secret S with an explicit formula.

2 Review of Elliptic Curves

In this section we briefly give the definitions and some properties of elliptic curve. For more information see [4].

Definition. let F be a field of the characteristic different from 2 or 3. An elliptic curve E defined over F is nonsingular plane curve with the equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in F$. So that $4a^3 + 27b^2 \neq 0$ in F.
Let $E(F)$ be the set of all solutions $(x, y) \in F$ together with a point $\mathcal{O}$, called the point at infinity.
For any two points $P = (x_p, y_p)$ and $Q = (x_q, y_q)$ in $E(F)$, operation $R = P + Q$ defines as

$$R = \begin{cases} \mathcal{O} & x_p = x_q,\ y_p = -y_q \\ Q & P = \mathcal{O} \\ (x_r, y_r) & o.w. \end{cases}$$

where

$$x_r = \lambda^2 - x_p - x_q, \quad y_r = \lambda(x_p - x_r) - y_p$$

and

$$\lambda = \begin{cases} (y_q - y_p)/(x_q - x_p) & P \neq Q \\ (3x_p^2 + a)/2y_p & P = Q, y_p \neq 0 \end{cases}$$

and if $y_p = 0$ then $2P = \mathcal{O}$.

With above definition, $E(F)$ forms an additive abelian group with identity $\mathcal{O}$.

Discrete Logarithm Problem on Elliptic Curve (ECDLP)

Let E be an elliptic curve, $G \in E$ be a point and $C \in \langle G \rangle$. Discrete logarithm problem on E is the problem of finding an integer m such that $C = mG$.
There is no subexponential-time method for solving and the security of elliptic curve cryptograghy depends on the hardness of discrete logarithm problem [3].

2.1 Edwards Curves

In [5] Edwards introdused an alternative model of elliptic curves over feild F with $char(F) \neq 2$.
Bernstein and Lang [6] improved the Edwards curves form and obtained

$$E_d : x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in F \setminus \{0, 1\}$ with the identity element $\mathcal{O} = (0, 1)$.
Edwards curves have unified formula that can be use for point addition and point doublings.
For $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $E_d(F)$, the addition law is defined as $R = P + Q = (x_3, y_3)$, where

$$x_3 = \frac{x_1y_2 - x_2y_1}{1 + dx_1x_2y_1y_2}, y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

This algorithim is fast and provides a natural protection from side channel attacks.

3 Main Results

In this paper we present a method for secret sharing on elliptic curves.
Let $\mathbb{F}_q$ be a Galois field, where q is a power of a prime. We consider a group of k people, each of them identified as $\{d_1, d_2, ..., d_k\} \subset \mathbb{F}_q$ known by every one. Also we define notations D and $M = \{M_i\}_{i=1}^k$ for dealer and the set of points of an elliptic curve, where $M = \{M_i\}_{i=1}^k$ are parts of the message M.

3.1 Our Scheme

First D chooses elliptic curve E defined over $\mathbb{F}_q$ with base point G, such that the number of ellements of $E(\mathbb{F}_q)$ is a large prime or has a large prime factor and D selects a private key $c \in \mathbb{F}_q$, and computes $T = cG$. Then D publishes $\{\mathbb{F}_q, a, b, G, T\}$ as a public information.
1. D selects random numbers $c_i \in \mathbb{F}_q$, $(1 \le i \le k-1)$ and defines $f(x) = c + \sum_{i=1}^{k-1} c_i x^i$.
2. D randomly chooses $r_i \in \mathbb{F}_q$, $(1 \le i \le k)$ and computes $r_i G$.
3. D sends $(M_i + r_i T, r_i G, f(d_i))$ to each $d_i, (1 \le i \le k)$ as the shares.

3.2 Recovery of the Message by k People

1. k People together can compute private key c by using Lagrange interpolation

$$c = f(0) = \sum_{i=1}^{k} f(d_i) \prod_{j=1, j \neq i}^{k} \frac{-d_i}{d_i - d_j}.$$

2. For $1 \le i \le k$, d_i computes $r_i cG$ and then achieve $M_i = M_i + r_i T - r_i cG$.

The security of this scheme is based on hardness of discrete logarithm problem and the security of Shamir scheme. No one can reveal M_i, and no group of less than k elements can reconstract M.

References

[1] G. Blakley, *Safeguarding cryptoghraphic keys*, Proc AFIPS 1979 National Computer Conference, AFIPS Press, Newyork, (1979), 313-317.

[2] A. Shamir, *How to share a secret*, Communications of ACM **vol. 22**, (1979), 612-613.

[3] N. Koblitz, *A course in number theory and cryptograghy*, second edition, Springger- Verlag, New York, (1994), 178-185

[4] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed. Graduate Texts in Mathematics, **vol. 106**, Springer, Dordrecht, (2009). MR MR2514094.

[5] H. M. Edwards. *A Normal Form for Elliptic Curves*. Bulletin of the American Mathematical Society, (2007) 44:393C422.

[6] D. J. Bernestein and T. Lange, *Faster addition and doubling on Elliptic Curves*. In K. Kurosawa, editor, Advances in Cryptolology-ASIACRYPT 2007, **vol. 4833** of Lect. Springer (2007), 29-50.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 159-161.

Oral Presentation

Computation of the Topological Indices of the Mobius Ladder Graph

S. Shokrolahi
Faculty of Mathematics, Shahid Chamran University of Ahvaz. Ahvaz, Iran
shokrolahisara@yahoo.com

Abstract

A topological index of a simple connected graph G is a numeric quantity related to the structure of the graph G. The set of all automorphisms of G under the composition of mapping forms a group which is denoted by Aut(G). In this paper we study the Mobius ladder graph G=(V,E) with the vertex set V and the edge set E and based on the feature of the action Aut(G) on the vertex set V and the edge set E, we compute the Wiener, Szeged and pI indices this graph.

Keywords: Wiener index, Szeged index, PI index, mobius ladder graph .

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1 Introduction

A topological index of a simple connected graph G is a graph invariant which is related to the structure of the graph,so when G is a molecular graph it's topological indices are called as a molecular structure descriptor and are used to undrstand properties of chemical compounds,also the oldest topological index of a graph Wiener index was first studied by a chemist named H.Wiener[4] for the determination of the boiling point of paraffin.Today many kinds of topological indices are known and they have many chemical applications for chemical molecular graphs so, many scientists in over the world like,H.Hosoya,A.A.Dobrynim,I.gutman,...,have studied about the calculation of the topological indices of the graphs also recently many researches in this case have done by

,S.Yousefi,H.yousefi-Azari,A.R.Ashrafi and M.H.khalifeh in Iran. Let $G=(V,E)$ be a simple connected graph where$V$ and E are the vertex set and the edge set of G respectively. The Wiener index of G, is denoted by W(G) and is defined as:

$$W(G)=\sum_{u,v\in V} d(u,v)$$

Where d(u.v) is the distance between vertices u and v.If the sum of distances between the vertex u with all other vertices of the graph G is denoted by d(u) then we have:

$$W(G)=\frac{1}{2}\sum_{u\in V} d(u)$$

The Szeged index,see [1] is a topological index of the graph G which is closely related to the Wiener index of G and coincides with the Wiener index in the case that G is a tree. This index concerned about how the vertices of the graph G are distributed.and is denoted by $SzG)$ and is defined as :

$$Sz(G)=\sum_{e=uv\in E} n_u(e|G)n_v(e|G)$$

The Padmakar-Ivan,*PI* index [3] is another topological index of a simple connected graph that takes into account the distribution of edges,so is closely related to Szeged index. The PI index of G is defined by :

$$PI(G)=\sum_{e=uv\in E} n_{eu}(e|G)+n_{ev}(e|G)$$

All topological indices are based on a graph representation which in the case of molecular graphs is related to physico-chemical properties of compounds.

We define a Mobious ladder graph G=(V,E) as a ladder with k steps such that the set of all nodes of . steps forms the vertex set V of G,so $|V|$ is even.Therefore n is of the forms n=4k or n=4k+2 ,where $k\in N$. Let $|V|=n$,and the adjacent and opposite vertices are joint by an edge, also the vertices of the first and the last steps are connected diagonally.

In this paper the Wiener, Szeged and *PI* index of a certain graph (Mobius ladder), based on the feature of the action $Aut(G)$ on the vertex set V and the edge set E of G which introduced in [2] are computed. In [2] it has been proved for a vertex-transitive graph G the Wiener index can be calculated by the following formula:

$$W(G)=1/2|V|d(v)$$

Where v is an arbitrary vertex . Here by using the vertex-transitive property of graph, the Wiener index is computed and the PI index of G is calculated by applying the proposition in [2] which implies:

Let G=(V,E) be a simple connected graph.If Aut(G) on E has orbits $E_1,E_2,...,E_r$ with representatives $e_1,e_2,...,e_r$, where $e_i=u_iv_i\in E$ then:

$$PI(G)=\sum_{i=1}^{r}|E_i|[n_{e_iu_i}(e_i|G)+n_{e_iv_i}(e_i|G)]$$

2 Results

1.Let $G = (V,E)$ be a Mobius ladder graph, and $|V| = n$, $n > 4$,TheWiener index of$G$ is:

$$W(G) = \begin{cases} 1/2(n)(n/2)((n+4)/4) - 1 & , \; n = 4k \\ 1/2n(((n+2)^2)/8 - 1) & , \; n = 4k+2 \end{cases}$$

2. Let G= (V,E) be a Mobius ladder graph, and $|V| = n$. The Szeged index of G is:

$$Sz(G) = \begin{cases} 3/2n(n/2-1)^2 & , \; n = 4k \\ 3/8n^3 & , \; n = 4k+2 \end{cases}$$

3.Let G=(V,E) be a Mobius ladder graph and,$|V| = n$. The padmakar Ivan index of G is:

$$PI(G) = \begin{cases} 2n(n-5) & , \; n = 4k \\ 2n(n-3) & , \; n = 4k+2 \end{cases}$$

References

[1] I.Gutman and A.A.Dobrynim,*The Szeged index-a success story*,Graph Theory N.Y, **34** (1998),37-44.

[2] M.R.Darafshe,*The wiener,Szeged and PI index of the triangle graph*,kualalampur,Malaysia,22-26 June 2009.

[3] P.V.khadikar,*On a novel structural descriptor pI Nat*,A cad.sci.lett, **23** (2000),113-118.

[4] Wiener.H,*determination of paraffin boiling points* ,J.Am.Chem.Soc ,**69**17-20(1947)

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 163-165.

Oral Presentation

On the Signless Laplacian Spectral Moment of Graphs

Fatemeh Taghvaee
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
taghvaei19@yahoo.com

Gholam-Hossein Fath-Tabar
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
fathtabar@kashanu.ac.ir

Abstract

Suppose G be a graph with signless Laplacian eigenvalues q_1, q_2, ..., q_n.The signless Laplacian spectral moments of G is defined $T_k(G) = \sum_{i=1}^{n} q_i^k(G)$. In this paper we compute $T_i(G)$, $0 \leqslant i \leqslant 5$, for any graph G and compare some graphs with respect to signless Laplacian spectral moments.

Keywords: Signless laplacian, spectral moments, tree.

2010 AMS classification Number: 05C50, 15A18.

1 Introduction

In this section we recall some definitions that will be used in the paper. Let G is a simple graph. The characteristic polynomial $\det(\lambda I - A)$ of a $(0,1)-$adjacency matrix of G is called the characteristic polynomial of G and denoted by $P_G(\lambda)$. The eigenvalues of A(i.e. the zeros of $\det(\lambda I - A)$) and the spectrum of A are also called the eigenvalues and the spectrum of G, respectively. The eigenvalues of G are usually denoted by $\lambda_1(G)$, $\lambda_2(G)$, $\cdots$, $\lambda_n(G)$. Let n, m, R be the number of vertices, the number of edges and the vertex-edge incidence matrix of a graph G.

Lemma 1. (see [1]) Suppose G is a graph, A is the adjacency matrix of G and A_L is the adjacency matrix of the line graph $L(G)$ of G. Then:

1) $RR^t = A + D$,

2) $R^tR = A_L + 2I$,

where D is the diagonal matrix of vertex degrees. The matrix $L = D - A$ is known as the Laplacian of G and the matrix $A + D$ is called signless Laplacian, where D is the diagonal matrix of vertex degrees. Since non-zero eigenvalues of RR^t and R^tR are the same, from the above relations we immediately obtain following result.

Lemma 2.(see [1])Let G is a graph with n vertices and m edges. Then the characteristic polynomial of $L(G)$ is

$$P_{L(G)}(\lambda) = (\lambda + 2)^{m-n} Q_G(\lambda + 2),$$

where $Q_G(\lambda)$ is the characteristic polynomial of the matrix $Q = A + D$.

Definition 3. A semi-edge walk of length k in an undirected graph G is an altrnating sequence v_1, e_1, v_2, e_2, $\cdots$, v_k, e_k, v_{k+1}, of vertices v_1, v_2, $\cdots$, v_{k+1} and edges e_1, e_2, $\cdots$, e_k such that for any $i = 1, 2, \cdots, k$ the vertices v_i and v_{i+1} are end vertices (not necessarily distinct) of the edge e_i.

Lemma 4.(see [2]) Let Q be the signless Laplacian of a graph G. The $(i, j)-$entry of the matrix Q^k is equal to the number of semi-edge walks of length k starting at vertex i and terminating at vertex j.

Let $T_k = \sum_{i=1}^{n} q_i^k(G)$, $k = 0, 1, 2, ...$ be the kth spectral moment for the $Q-$spectrum. Since $T_k = tr(Q^k)$, we have the following corollary.

Corollary 5.(see [2]) The spectral moment T_k is equal to the number of closed semi-edge walks of length k.

In [3,4], we ordered some regular graphs with respect to spectral moments and in this paper we obtain the formullas for some signless Laplacian spectral moments for any graph G.

2 Main Results

In this section, we find our description for the signless Laplacian spectral moments of graphs and order the set of trees of order of n respect to spectral moment. The following two results are crucial throughout this paper. Let $(T_0(G), T_1(G), \ldots, T_{n-1}(G))$ be the sequence of spectral moments of G. For two graphs G_1 and G_2, we have $G_1 \prec_T G_2$ if for some k $(k = 1, 2, ..., n-1)$, we have $T_i(G_1) = T_i(G_2)$ $(i = 0, 1, ..., k-1)$ and $T_k(G_1) < T_k(G_2)$. An $H-$subgraph of G is a subgraph isomorphic to the graph H. The number of all $H-$subgraphs of G is denoted by $\phi_G(H)$ or $\phi(G)$. for short. Let C_n and U_n are the cycle of size n, and a graph obtained from C_{n-1} by attaching a leaf to one of its vertices, respectively. In this paper, we determine the first and the last tree, in an $T-$order, in the set of all trees of order n, respectively.

In following we have the formulas for T_i, $0 \leqslant i \leqslant 5$, that the three of them are proved in [2].

Theorem 6. Let G be a graph with n vertices, m edges and vertex degrees $d_1, d_2, ..., d_n$. Then we have:

$$\begin{aligned}
T_0(G) &= n, \\
T_1(G) &= \sum_{i=1}^{n} d_i = 2m, \\
T_2(G) &= 2m + \sum_{i=1}^{n} d_i^2, \\
T_3(G) &= 6\phi(C_3) + 3\sum_{i=1}^{n} d_i^2 + \sum_{i=1}^{n} d_i^3, \\
T_4(G) &= \sum_{i=1}^{n} d_i + 2\sum_{i=1}^{n} d_i(d_i - 1) + 8\phi(C_4) + \sum_{i=1}^{n} d_i^4 \\
&+ \ 2\sum_{i=1}^{n} d_i^3 + 4\sum_{i=1}^{n} t_i d_i + 4\sum_{j=1}^{n}\sum_{i \neq j} d_i d_j, \quad j \sim i, \\
T_5(G) &= 30\phi(C_3) + 10\phi(U_4) + 10\phi(C_5) + \sum_{i=1}^{n} d_i^5 + 6\sum_{i=1}^{n} d_i^4 + 6\sum_{i=1}^{n} t_i d_i^2 \\
&+ \ 5\sum_{i=1}^{n} [d_i^2 + d_i(d_i^* - 1) + 2q_i]d_i + 6\sum_{j=1}^{n}\sum_{i=1}^{n} d_i d_j^2, \ j \sim i.
\end{aligned}$$

where d_i is degree of ith vertex, d_i^* is the degree of its neighbours and t_i and q_i are the number of triangles and quadrangles containing the ith vertex, respectively.

Theorem 7. In an $T-$order of trees on n vertices, the first graph is the path P_n, and the last graph is the star $K_{1,n-1}$.

Acknowledgments

The research of this paper is partially supported by the University of Kashan under grant no 159021/12.

References

[1] N. Biggs, Algebric Graph Theory, *Cambridge University Press, Cambridge*, (1993).

[2] D. Cvetković, P. Rowlinson and S.K.Simić, Signless Laplacian of finite graphs, *Linear Algebra Appl.* **423** (2007)155-171.

[3] F. Taghvaee and A. R. Ashrafi, Ordering some regular graphs with respect to spectral moments, submitted.

[4] F. Taghvaee and A. R. Ashrafi, On spectrum of $I-$graphs and its ordering with respect to spectral moments, submitted.

***The First Conference on Computational Group Theory, Computational Number Theory and Applications*,**
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 167-169.

Oral Presentation

Some Results on a New Comaximal Graph of Commutative Rings

Zahra Yarahmadi
Department of Mathematics, Faculty of Science, Khorramabad Branch, Islamic Azad University, Khorramabad, Iran
z.yarahmadi@khoiau.ac.ir,
z.yarahmadi@gmail.com

Abstract

Let R be a commutative ring without identity. We define the graph $G(R)$ with vertex set $V(G(R))$ and edge set $E(G(R))$ as follows:

$$V(G(R)) = \{I \,|\, I \neq \{0\} \,, I \lhd R\},$$

$$E(G(R)) = \{IJ \,|\, I + J = R\}.$$

The set $\Delta(R)$ consists of all ideals I of R such that I is not contained in $J(R)$, where $J(R)$ denotes the Jacobson radical of R. Throughout this paper we consider only commutative ring not necessary unital. In this paper we study about this graph. We show that under some conditions on the $G(R)$, the ring R is Noetherian or Artinian.

Keywords: Commutative ring, graph.

MSC(2010): 05C75, 13A15.

1 Introduction

Let G be a graph and L be a set. A *coloring* of G by L is a function $c : V(G) \longrightarrow L$ with this property: if $u, v \in V(G)$ are adjacent, then $c(u)$ and $c(v)$ are different. The *chromatic number* of G is the minimum number of colors which is needed for a proper coloring of G, and is denoted by $\chi(G)$.

Recall that a graph is said to be *connected* if for each pair of distinct vertices v and w, there is a finite sequence of distinct vertices $v = v_1, v_2, ...v_n = w$ such that each $v_i v_{i+1}$ is an edge. A *complete graph* is a simple graph in which every pair of distinct vertices is connected by a unique edge. A *clique* of the graph is its maximal complete subgraph. We denote the size of the largest clique of G by $\omega(G)$. Obviously for every graph G, $\chi(G) \geq \omega(G)$.

In [3], Beck considered $\Gamma(R)$ as a graph with vertices as elements of R, where two different vertices a and b are adjacent if and only if $ab = 0$. He showed that $\chi(\Gamma(R)) = \omega(\Gamma(R))$ for certain class of rings.

In [6], Sharama and Bhatwadekar defined another graph on R, $\Gamma(R)$, with vertices as elements of R, where two distinct vertices a and b are adjacent if and only if $Ra + Rb = R$. They showed that $\chi(\Gamma(R)) < \infty$ if and only if R is a finite ring. In this case $\chi(\Gamma(R)) = \omega(\Gamma(R)) = t + l$, where t and l are the number of maximal ideals of R and the number of units of R, respectively.

Maimani et al. in [5] study further the graph defined by Sharama and Bhatwadekar. They study on connectivity and diameter of this graph. In addition, they completely characterize the diameter of comaximal graph of commytative rings. In this paper we define a new graph on R, where R be a commutative ring not necessary unital.

The notation we use is mostly standard and taken from standard graph theory textbooks, such as [4] and [7].

2 Main Results

Throughout this section R will be a commutative ring with identity.

Definition 1. *Let R be a commutative ring without identity. We define the graph $G(R)$ with vertex set $V(G(R))$ and edge set $E(G(R))$ as follows:*

$$V(G(R)) = \{I \,|\, I \neq \{0\}\ , I \triangleleft R\},$$

$$E(G(R)) = \{IJ \,|\, I + J = R\}.$$

A ring R is quasi local if it has a unique maximal ideal. A quasi local ring R with unique maximal m is denoted by (R, m). Obviously R is quasi local ring if and only if $E(G(R)) = \emptyset$. In the graph $G(R)$, the induced subgraph $Max(R)$ is complete. In this case we have $\omega(G(R)) = |Max(R)|$. Moreover $\mathsf{m} \in V(G(R))$ is a maximal ideal of R not contained in nonezero ideals of R. So m is adjacent with all vertices of $G(R)$ and in this case $J(R) = \{0\}$. In this section we look at the conditions on the $G(R)$ to prove R is Noetherian or Artinian.

Theorem 2.1. *Let R be a ring, Assume that $J(R)$ is finitely generated and each maximal ideals of R as vertices of $G(R)$ have finite degree and $|Max(R)| \geq 2$. Hence R is Noetherian.*

Example. In the ring $\mathbf{Z}$, degree of all maximal ideals as vertices of $G(\mathbf{Z})$ is infinite, but $\mathbf{Z}$ is Noetherian ring. Hence the converse of above theorem is not true.

Corollary. Let R be a ring, Assume that $J(R)$ is finite and each maximal ideals of R as vertices of $G(R)$ have finite degree and $|Max(R)| \geq 2$ and $Spec(R) = Max(R)$. Then R is Artinian.

Recall that in this type of comaximal graph the clique number of $G(R)$ is equal to $|Max(R)|$.

Theorem 2.2. *The following statements are hold:*
i. Let R be an Artinian ring then $\omega(G(R)) < \infty$ and $\langle Spec(R) \rangle$ is a complete subgraph.

ii. Let R be an infinite integral domain such that $|U(R)| < \infty$. Then $G(R)$ doesn't have isolated vertex and $\omega(G(R)) = \infty$.

A ring is said to be *clean* if all of its elements can be written as the sum of a unit and an idempotent see [1], [2] For example, a quasi local ring is clean. The following theorem characterize clean rings.

Theorem 2.3. *For the ring R, the following are equivalent:*
i. R is a finite product of quasi local rings.
ii. R is clean and $\omega(G(R)) < \infty$.

References

[1] D.D. Anderson, V.P. Camillo, *Commutative rings whose elements are a sum of a unit and idempotent*, J. Comm. Algebra, **30** (2002), 3327–3336.

[2] D.D. Anderson, M. Naseer, *Beck's coloring of a commutative ring*, J. Algebra, **159** (1993), 500–514.

[3] I. Beck, *Coloring of commutative rings*, J. Algebra, **116** (1988), 208–226.

[4] G. Chartrand, O.R. Oellermann, Applied and Algorithmic Graph Theory, McGrawHill, Inc., New York, (1993).

[5] H. R. Maimania, M. Salimia, A. Sattaria, S. Yassemi, *Comaximal graph of commutative rings*, J. Algebra,**319**(2008), 1801–1808.

[6] P.K. Sharma, S.M. Bhatwadekar, *A note on graphical representation of rings*, J. Algebra,**176**(1995) 124–127.

[7] D.B. West, Introduction to Graph Theory, Prentice-Hall, Upper Saddle River, NJ, (1996).

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 171-174.

Oral Presentation

A Note on the Capacity of some Gaussian Channels

Masoomeh Yazdany Moghaddam
Department of Pure Mathematics, Faculty of Mathematical Sciences,
University of Kashan, Kashan, I. R. Iran
yazdany.mo@gmail.com.

Reza Kahkeshani
Department of Pure Mathematics, Faculty of Mathematical Sciences,
University of Kashan, Kashan, I. R. Iran
kahkeshanireza@kashanu.ac.ir

Abstract

In this paper, we review the capacity of some Gaussian channels: the Gaussian channels with power constraint, the AWGN channels with their idealized duty cycle and the AWGN channels with duty cycle constraint.

Keywords: Mutual information, channel capacity, Gaussian channel.

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1 Introduction

Definition 1.1. The mutual information $I(X;Y)$ between two random variables with the joint density $f(x,y)$ is

$$I(X;Y) = \int f(x,y)\ \log \frac{f(x,y)}{f(x)f(y)}\ dx\,dy.$$

Definition 1.2. A Gaussian channel is a channel with output Y_i at time i such that Y_i is the sum of the input X_i and the noise Z_i such that Z_i is drawn independent identically distributed from a Gaussian distribution with variance N. Thus,

$$Y_i = X_i + Z_i,\ Z_i \sim \mathcal{N}(0,N).$$

The noise Z_i is assumed to be independent of the signal X_i.

Definition 1.3. AWGN is a Gaussian channel that is added to any noise and it has uniform power across the frequency band.

The most common limitation on the input is an energy or power constraint. We assume an average power constraint. For any codeword $(x_1, x_2, ..., x_n)$ transmitted over the channel, we require that

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P.$$

Definition 1.4. The information capacity of a Gaussian channel with power constraint P is

$$C = \max_{\substack{f(x) \\ E\{X^2\} \leq P}} I(X;Y).$$

Theorem 1.5. *[1] The capacity of a Gaussian channel with power constraint P and the noise variance N is*

$$C = \frac{1}{2}\log(1+\frac{P}{N}).$$

Definition 1.6. An (M,n)-code for the Gaussian channel with power constraint P consist of the following:

1. An index set $\{1,2,...,M\}$.
2. An encoding function $x : \{1,2,...,M\} \to \chi^n$ yielding codewords $x^n(1), x^n(2), ..., x^n(M)$, satisfying the power constraint P, i.e., for every codeword:

$$\sum_{i=1}^{n} x_i^2(w) \leq nP,\ w = 1,2,\ldots,M.$$

3. A decoding function

$$g : \Upsilon^n \to \{1,2,\ldots,M\}.$$

Definition 1.7. A duty cycle is the precentage of one period in witch a signal is active. A duty cycle may be expressed as

$$D = \frac{T}{P} * 100,$$

where D is duty cycle, T is the time the signal is active and P is the total period of the signal.

We assume that $1-q$ is the maximum duty cycle allowd. It is required that every codeword $(x_1, x_2, ..., x_n)$ satisfies in

$$\frac{1}{n}\sum_{i=1}^{n} 1_{\{x_i \neq 0\}} + \frac{1}{n}2c(1_{\{x_n=0, x_1\neq 0\}} + \sum_{i=1}^{n-1} 1_{\{x_i=0, x_{i+1}\neq 0\}}) \leq 1-q.$$

We refer to this as *duty cycle constraint* (q,c).

Definition 1.8. The idealized duty cycle constraint is the special case $(q,0)$.

2 The Recent Results

The set of all distributions of the channel input X with duty cycle constraint $(q,0)$ and power constraint P is denoted by

$$\Lambda(P,q) = \{\mu|\mu \textit{ is a distribution of } X,\ \mu(\{0\}) \geq q, E_\mu\{X^2\} \leq P\}.$$

Theorem 2.1. *[2] The capacity of the AWGN channel with its idealized duty cycle no greater than $1-q$ and power constraint no greater than P is*

$$C(P,q) = \max_{\mu\in\Lambda(P,q)} I(X;X+N).$$

In particular,

1. *the maximum is ashieved by a uniqe distribution $\mu_0 \in \Lambda(P,q)$.*
2. *μ_0 is symmetric about 0 and its second moment is exactly equal to P.*
3. *μ_0 is discrete with an infinite number of probability mass points, whereas the number of probability mass points in any bounded interval is finite.*

We consider that μ is the probability distribution of the process $X_1, X_2, ...,$ μ_{X_i} is the marginal distribution of X_i and μ_{X_i,X_j} is the joint probability of (X_i, X_j).

Let $\Lambda^n(P,q,c)$ be the set of n-dimensional distributions witch satify duty cycle constraint (q,c) and power constraint P:

$$\{\mu|E_\mu(\frac{1}{n}\sum_{i=1}^{n} X_i^2) \leq P, \frac{1}{n}\sum_{i=1}^{n}[\mu_{X_i}(\{0\}) - 2c\mu_{X_i,X_{i+1}}(\{0\} * (\mathbf{R}-\{0\}))] \geq q\},$$

where $\mu_{X_i,X_j}(\{0\} * (\mathbf{R}-\{0\})) = P(X_i = 0, X_j \neq 0)$.

Theorem 2.2. *[2] The capacity of the AWGN channel with duty cycle constraint (q,c) and power constraint P is*

$$C(P,q,c) = \lim_{n\to\infty} \frac{1}{n} \max_{\mu\in\Lambda^n(P,q,c)} I(X^n;Y^n).$$

The set of stationary distributions which satisfy duty cycle constraint (q,c) and power constraint P, $\Lambda(P,q,c)$, is

$$\{\mu|\mu \textit{ is stationary},\ E_\mu(X_1^2) \leq P, \mu_{X_1}(\{0\}) - 2c\mu_{X_1,X_2}(\{0\} * (\mathbf{R}-\{0\})) \geq q\}.$$

Theorem 2.3. *[2] For any $\mu \in \Lambda(P,q,c)$, we let*

$$L(\mu) = I(X_1;X_1+N) - I(X_1;X_2,X_3,\ldots),$$

where N is standard Gaussian and independent of X_1. Then we have:

1. *$L(\mu)$ is a lower bound of the channel capacity.*
2. *The maximum of L is achieved by a discrete first-order Markov process, denoted by μ^*.*
3. *μ^* satisfied in this property: If $B_i = 1_{\{X_i\neq 0\}}$ then the variables X_i and X_{i+1} are independant, for all i conditioned on B_i and B_{i+1}, and*

$$L(\mu^*) = I(X_1;X_1+N) - I(B_1;B_2).$$

Acknowledgments

The second author is partially supported by the University of Kashan under grant number 364996/2.

References

[1] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 2006.

[2] Lei Zhang, Hui Li and Dongning Guo, *Capacity of Gaussian Channels With Duty Cycle and Power Constraints*, IEEE Transaction On Information Theory, Vol. 60, NO. 3, 2014, 1615–1629.

The First Conference on Computational Group Theory, Computational Number Theory and Applications,
University of Kashan, 26-28 Azar, 1393 (December 17-19 2014), pp: 175-176.

Oral Presentation

On 12 and 13 $-$Decomposable Finite Groups

Masoumeh Yousefi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, I. R. Iran
s_yousefi68@yahoo.com

Ali Reza Ashrafi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, I. R. Iran
ashrafi@kashanu.ac.ir

Abstract

Let G be a finite group and $\mathcal{N}_G$ denote the set of all non-trivial proper normal subgroups of G. An element K of $\mathcal{N}_G$ is said to be $n-$decomposable if K is a union of n distinct conjugacy classes of G. G is called $n-$decomposable, if $\mathcal{N}_G \neq \emptyset$ and every element of $\mathcal{N}_G$ is $n-$decomposable.

In this paper, the problem of finding the structure of non$-$solvable non$-$perfect 12 and 13$-$ decomposable finite groups are considered into account.

Keywords: Conjugacy class, n-decomposable group.

MSC(2010): Primary: 20D06; Secondary: 20E45.

1 Introduction

Let G be a finite group and let $\mathcal{N}_G$ be the set of non-trivial proper normal subgroups of G. An element K of $\mathcal{N}_G$ is said to be $n-$decomposable if K is a union of n distinct conjugacy classes of G. If $\mathcal{N}_G \neq \emptyset$ and every element of $\mathcal{N}_G$ is $n-$decomposable, then we say that G is $n-$decomposable.

In [1], the problem of classifying n-decomposable finite groups was proposed and the authors characterized the solvable $n-$decomposable finite groups under certain conditions. In the mentioned paper, the structure of $2-$, $3-$ and $4-$decomposable finite groups are obtained. In [2, 3, 4], the authors continued this problem by characterizing $n-$decomposable finite groups, when $5 \leq n \leq 10$. It is merit to state here that such type of problems in group theory was started by Wu Jie Shi in the field of quantitative structure of finite groups [5].

Throughout this paper, as usual, $G^{'}$ denotes the derived subgroup of G, $Z(G)$ is the center of G, x^G, $x \in G$, denotes the conjugacy class of G with the representative x and G is called non-perfect, if $G^{'} \neq G$. Also, $SmallGroup(n,i)$ denotes the i^{th} group of order n in the small group library of GAP. Our other notations are standard and can be taken from the standard books of group theory.

2 Main Results

In this section we report our new results on the characterization problem of finite non-perfect non-solvable 12 and 13$-$decomposable finite groups. To do this, we first introduce some notations. Let $T = \{L_2(q) \mid q = p^m, p \text{ and } m \text{ are primes}\}$ and $S = \{L_2(p) \mid p \text{ is prime}\}$.

Proposition 1. If G is finite non-perfect non-solvable 13$-$decomposable finite group and $p \notin \pi(Aut(G'))$ then G' is simple.

Proposition 2. Suppose G is non-perfect non-solvable 13$-$decomposable finite group and $G' \in T \cup S$. Then $G \cong Aut(PSL(2,23))$.

Proposition 3. Suppose G' is simple and $\psi(G^{'}) \leq 2$ then there is no non-perfect non-solvable 13$-$decomposable finite group.

Proposition 4. Suppose G is finite non-perfect non-solvable finite group and $p \notin \pi(Aut(G'))$ then there is no 12$-$decomposable finite group.

Proposition 5. Suppose G is non-perfect non-solvable 12$-$decomposable finite group and $G' \in T \cup S$. Then there is no non-perfect non-solvable 12$-$decomposable finite group.

Proposition 6. Suppose G' is simple and $\psi(G^{'}) \leq 2$ then there is no non-perfect non-solvable 12$-$decomposable finite group.

Proposition 6. If G is finite non-perfect non-solvable 12$-$decomposable finite group

$$G \cong U_3(5).3, Aut(M_{12}), Aut(M_{22}), Aut(A_8).$$

References

[1] A. R. Ashrafi and H. Sahraei, On Finite Groups Whose Every Normal Subgroup is a Union of the Same Number of Conjugacy Classes, Vietnam J. Math., **30** (3) (2002) 289–294.

[2] A. R. Ashrafi and Y. Q. Zhao, On 5$-$ and 6$-$decomposable finite groups, Math. Slovaca **53** (4) (2003)373–383.

[3] A. R. Ashrafi and W. J. Shi, On 7$-$ and 8$-$decomposable finite groups, Math. Slovaca **55** (3) (2005) 253–262.

[4] A. R. Ashrafi and W. J. Shi, On 9$-$ and 10$-$decomposable finite groups, J. Appl. Math. Comput. (2008) **26** 169–182.

[5] W. J. Shi, The Quantitative Structure of Groups and Related Topics, Group Theory in China, Zhe-Xian Wan and Sheng-Ming Shi(Eds.), 163-181, Science Press New York, Ltd. and Kluwer Academic Publishers, 1996.

The First Conference on Computational Group Theory ,Computational Number Theory and Applications ,
University of Kashan, 26-28 Azar, 1393(December 17-19 2014), pp: 177-181.

Poster Presentation

A Note on Channel Coding and Lossy Source Coding

Neda Zarrin
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
nedazarin2@yahoo.com

Reza Kahkeshani
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan,
Kashan, I. R. Iran
kahkeshanireza@kashanu.ac.ir

Abstract

In this paper, we review the stochastic encoders for channel coding and lossy source coding with a rate close to the fudemental limits, where the input alphabet for channel coding and the reproduction alphabet for lossy source coding are finite.

1 Introduction

The sequence $U \equiv \{U^n\}_{n=1}^{\infty}$ of random variables is called a general source, where $U^n \in \mathscr{U}^n$. For a general source U, the spectral Sup-entropy rate $\overline{H}(U)$ and the spectral Inf-entropy rate $\underline{H}(U)$ are:

$$\overline{H}(U) = \inf\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{1}{\mu_{U^n}(U^n)} > \theta\big) = 0\big\}$$
$$\underline{H}(U) = \sup\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{1}{\mu_{U^n}(U^n)} < \theta\big) = 0\big\}.$$

For a pair $(U,V) = \{(U^n,V^n)\}_{n=1}^{\infty}$ of general source, the spectral conditional Sup-entropy rate $\overline{H}(U|V)$, the spectral conditional Inf-entropy rate $\underline{H}(U|V)$, the spectral Sup-mutual information rate

$\overline{I}(U;V)$ and the spectral Inf-mutual information rate $\underline{I}(U;V)$ are:

$$\overline{H}(U|V) = \inf\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{1}{\mu_{U^nV^n}(U^n|V^n)} > \theta\big) = 0\big\},$$
$$\underline{H}(U|V) = \sup\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{1}{\mu_{U^nV^n}(U^n|V^n)} < \theta\big) = 0\big\},$$
$$\overline{I}(U;V) = \inf\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{\mu_{U^nV^n}(U^n,V^n)}{\mu_{U^n}(U^n)\mu_{V^n}(V^n)} > \theta\big) = 0\big\},$$
$$\underline{I}(U;V) = \sup\big\{\theta : \lim_{n\to\infty} p\big(\frac{1}{n}\log\frac{\mu_{U^nV^n}(U^n,V^n)}{\mu_{U^n}(U^n)\mu_{V^n}(V^n)} < \theta\big) = 0.$$

A sequense $W \equiv \{\mu_{Y_n|X^n}\}_{n=1}^{\infty}$ of conditional probability distributions is called a general channel. For a general channel W, the channel capacity $C(W)$ is

$$C(W) = \sup_X \underline{I}(X;Y). \tag{1.1}$$

In [2], the concept of channel capacity is described in detail.

A pair (R,D) consisting of a rate R and a distortion D is called achievable if for all $\delta > 0$ and all sufficiently large n there is a pair consisting of an encoder $\phi_n : \mathscr{Y}^n \longrightarrow \mathscr{M}_n$ and a decoder $\psi_n : \mathscr{M}_n \longrightarrow \mathscr{X}^n$ such that

$$\frac{1}{n}\log|\mathscr{M}_n| \leqslant R \quad \text{and} \quad P(d_n(\psi_n(\phi_n(Y^n)),Y^n) > D) \leqslant \delta.$$

For a pair (X,Y) of general sources, $\overline{D}(X,Y)$ is

$$\overline{D}(X,Y) = \inf\{\theta : \lim_{n\to\infty} P(d_n(X^n,Y^n) > \theta) = 0\}.$$

For general source Y, the rate distortion $R(y)$ is obtained as [3]:

$$\mathscr{R}(Y) = \bigcup_W \left\{ (R,D) : \begin{array}{c} \overline{I}(X;Y) \leqslant R \\ \overline{D}(X,Y) \leqslant D \end{array} \right\}$$

Let us define $\mathscr{C}_A(c) = \{u : Au = c\}$. We continue according the definitions in [4]. Let $\mathscr{A} = \{\mathscr{A}_n\}_{n=1}^{\infty}$ be a sequence of sets, where $\mathscr{A}_\setminus$ is a set of functions on $\mathscr{U}^n$. For a probabiliy $P_{A,n}$ on $\mathscr{A}_\setminus$, the sequence $(\mathscr{A}_\setminus, P_A) \equiv \{(\mathscr{A}_\setminus, P_{A,n})\}_{n=1}^{\infty}$ is an ensemble. Hence, $(\mathscr{A}_\setminus, P_A)$ has an (α_A, β_A)-*hash property* if there are two sequence $\alpha_A \equiv \{\alpha_A(n)\}_{n=1}^{\infty}$ and $\beta_A \equiv \{\beta_A(n)\}_{n=1}^{\infty}$, depending on $\{P_{A,n}\}_{n=1}^{\infty}$ such that:

$$\lim_{n\to\infty} \alpha_A(n) = 1 \quad , \quad \lim_{n\to\infty} \beta_A(n) = 0$$

and

$$\sum_{\substack{u' \in \mathscr{U}^n \setminus \{u\}: \\ P_{A,n}(\{A:Au=Au'\}) > \frac{\alpha_A(n)}{|\mathrm{Im}\mathscr{A}_n|}}} P_{A,n}(\{A : Au = Au'\}) \leqslant \beta_A(n)$$

for any n and $u \in \mathscr{U}^n$.

For given $r > 0$ and $R > 0$, let $(\mathscr{A}, P_A)$ and $(\mathscr{B}, P_B)$ be ensembles of functions on the same set $\mathscr{X}^n$ satisfying

$$r = \frac{1}{n}\log|\mathrm{Im}\mathscr{A}| \quad \text{and} \quad R = \frac{1}{n}\log|\mathrm{Im}\mathscr{B}|.$$

Let $\tilde{X}^n = \tilde{X}^n_{AB}(c,m)$ be a random variable corresponding to the distribution

$$\nu_{\tilde{X}^n|M_n}(x|m) \equiv \begin{cases} \dfrac{\mu_{X^n}(x)}{\mu_{X^n}(\mathscr{C}AB(c,m))} & x \in \mathscr{C}_{AB}(c,m) \\ 0 & x \notin \mathscr{C}_{AB}(c,m). \end{cases}$$

The stochastic encoder $\phi : \mathrm{Im}\mathscr{B} \longrightarrow \mathscr{X}^n$ is

$$\phi_n(m) = \begin{cases} \tilde{X}^n_{AB}(c,m) & \mu_{X^n}(\mathscr{C}_{AB}(c,m)) > 0 \\ \text{"}error\text{"} & \mu_{X^n}(\mathscr{C}_{AB}(c,m)) = 0 \end{cases}$$

and also the decoder $\psi_n : \mathscr{Y}^n \longrightarrow \mathrm{Im}\mathscr{B}$ is

$$\psi_n(y) \equiv Bx_A(c|y),$$

where x_A is defined by

$$x_A(c|y) \equiv \arg \max_{x' \in \mathscr{C}_A(c)} \mu_{X^n|Y^n}(x'|y).$$

The Error probability $Error(A,B,C)$ is given by

$$Error(A,B,C) = \sum_{\substack{m: \\ \mu_{X^n}(\mathscr{C}_{AB}(c,m)=0}} \frac{1}{|\mathscr{M}_n|} + \sum_{\substack{m,n,y: \\ \mu_{X^n}(\mathscr{C}_{AB}(c,m)>0 \\ x \in C_{AB}(c,m) \\ \psi_n(y) \neq m}} \frac{\mu_{Y^n|X^n}(y|x)\mu_{X^n}(x)}{|\mathscr{M}_n|\mu_{X^n}(\mathscr{C}_{AB}(c,m)).}$$

For introducing a lossy source code, a constrained random-number generator is used for constructing an encoder. Let $\tilde{X}^n = \tilde{X}^n_A(c|y)$ be a random variable corresponding to the distribution

$$\nu_{\tilde{X}^n|\tilde{Y}^n}(x|y) = \begin{cases} \dfrac{\mu_{X^n|Y^n}(x,y)}{\mu_{X^n|Y^n}(\mathscr{C}_A(c)|y)} & x \in \mathscr{C}_A(c) \\ 0 & x \notin \mathscr{C}_A(c) \end{cases}$$

and define the stechastic encoder $\phi : \mathscr{Y}^n \longrightarrow \mathrm{Im}\mathscr{B}$ by

$$\phi_n(y) = \begin{cases} B\tilde{X}^n_A(c|y) & \mu_{X^n|Y^n}(\mathscr{C}_A(c)|y) > 0 \\ \text{"}error\text{"} & \mu_{X^n|Y^n}(\mathscr{C}_A(c)|y) = 0 \end{cases}$$

The decoder $\psi : \mathrm{Im}\mathscr{B} \longrightarrow \mathscr{X}^n$ is

$$\psi_n(m) = x_{AB}(c,m),$$

where x_{AB} is defined as

$$x_{AB}(c,m) = \arg\max_{x'} \in \mathscr{C}_{AB}(c,m)\mu_{X^n}(x').$$

The error probability $Error(A,B,C,D)$ is given by

$$Error(A,B,C,D) = P(d_n(\psi_n(\phi_n(Y^n)),Y^n) > D),$$

where $P(d_n(\psi_n(\phi_n(Y^n)),Y^n) = \infty$ and $\mu_{X^n|Y^n}(\mathscr{C}_A(c)|y) = 0$.

2 The Recent Results

Lemma 1. *[5] For a general channel W,*

$$C(W) = \sup_X [\underline{H}(X) - \overline{H}(X|Y)],$$

Where the supremum is taken over all general sources X.

Theorem 1. [1] *Assume that $r, R > 0$ satisfy*

$$r > \overline{H}(X|Y) \quad , \quad r + R < \overline{H}(X). \tag{2.1}$$

Let an ensemble $(\mathscr{A}, P_A)$ (resp. $(\mathscr{B}, P_B)$) has an (α_A, β_A)-hash (resp. (α_B, β_B)-hash) property. Then for any $\delta > 0$ and all sufficeintly large n there are functions $A \in \mathscr{A}$ and $B \in \mathscr{B}$ and a vector $c \in Im\mathscr{A}$ such that

$$Error(A, B, C) \leqslant \delta.$$

The channel capacity is achievable with the proposed code by letting X be a source that attains the supremum on the right hand side of (1.1).

Theorem 2. *[1] Assume that $r, R > 0$ satisfy*

$$r < \underline{H}(X|Y) \quad , \quad r + R > \overline{H}(X)$$

And an ensemble $(\mathscr{A}, P_A)$ (resp. $(\mathscr{B}, P_B)$) has an (α_A, β_A)-hash (resp. (α_B, β_B)-hash) property. Then for any $\delta > 0$ and all sufficeintly large n there are functions $A \in \mathscr{A}$ and $B \in \mathscr{B}$ and a vector $c \in Im\mathscr{A}$ such that

$$Error(A, B, C, D) \leqslant P(d_n(X^n, Y^n) > D) + \delta.$$

By assuming that $\{\mu_{X^n|Y^n}\}_{n=1^\infty}$ satisfies

$$\overline{D}(X, Y) < D,$$

we have the fact that $\lim_{n\to\infty} P(d_n(X^n, Y^n) > D) = 0$ from the definition of $\overline{D}(X, Y)$. If $n \to \infty$, $\delta \to 0$ and $r \to \underline{H}_{(X|Y)}$ then for any (R, D) close to the boundary of $\mathscr{R}(Y)$, there is a sequence of proposed codes such that

$$\lim_{n\to\infty} Error(A, B, C, D) = 0.$$

References

[1] J. Muramatsu, Channel Coding And Lossy Source Coding Using a Generator of Constrained Random Numbers, *IEEE Transactions on Information Theory*, Vol. 60, No. 5, May 2014.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd. ed. New York, Wiley, 2006.

[3] T. S. Han, *Information-Spectrum Methods of Information Theory*, New York, Springer-Verlag, 2003.

[4] J. Muramatsu and S. Miyake, Hash Property and Coding Theorems for Sparse Matrices and Maximal-Likelihood Coding, *IEEE Transactions on Information Theory*, Vol. 56, No. 5, pp. 2143–2167, May 2010.

[5] S. Verdu and T. S. Han, A General Formula for Channel Capacity, *IEEE Transactions on Information Theory*, Vol. 40, No. 4, pp. 1147–1157, July 1994.

Index of Names for Papers in English

فهرست مقالات

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۱ تا ۵.

سخنرانی

درباره سرشت‌های دقیق

سیده رقیه ادهمی
دانشکده علوم ریاضی، دانشگاه تربیت مدرس
r.adhami@modares.ac.ir

علی ایرانمنش
دانشکده علوم ریاضی، دانشگاه تربیت مدرس
iranmanesh@modares.ac.ir

چکیده

مسئله رده‌بندی تمام زوج‌های دقیق (G,χ) از نوع L ،برای مجموعه مفروض L از اعداد صحیح جبری، توسط محققین بسیاری مورد مطالعه قرار گرفته‌است. این مسئله در حالتی که L شامل یک عدد غیرگویا است، حل شده‌است؛ اما نتایج برای حالتی که L تنها شامل اعداد گویاست، بسیار محدود است. برخی از این حالت‌ها عبارت‌اند از: $L=\{l\}$، که در آن l یک عدد گویاست؛ $L=\{-۱,۱\}$؛ $L=\{-۱,۲\}$؛ $L=\{-۲,۱\}$؛ $L=\{l,l+p\}$، که در آن $l=-۱$ یا $l=۱-p$ و p عددی اول و فرد است.

در این مقاله حالت‌های $L=\{-۱,۳\}$ و $L=\{-۳,۱\}$ را مورد مطالعه قرار داده‌ایم.

واژه های کلیدی: سرشت دقیق، گروه متناهی، زوج دقیق.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $۲۰C۱۵$.

۱ مقدمه

فرض کنید G یک گروه متناهی است و χ سرشتی باوفا از G. تعریف می کنیم:

$$L(\chi):=\{\chi(g)|۱\neq g\in G\}$$

و $Sh(\chi)=\prod_{l\in L(\chi)}(\chi(1)-l)$. ثابت شده‌است که $|G|$، $Sh(\chi)$ را می‌شمارد [۲]. زوج (G,χ) (یا به اختصار سرشت χ) را دقیق از نوع L نامیده می‌شود، هرگاه $L=L(\chi)$ و $Sh(\chi)=|G|$.
پس از ارائه این تعریف، مسئله رده‌بندی همه زوج‌های دقیق (G,χ) از نوع L، به ازای مجموعه مفروض L از اعداد صحیح جبری مطرح شد [۲].
اگر سرشت اصلی 1_G از G جزء اصلی χ با درجه تکرار m باشد و قرار دهیم: $\chi'=\chi-m1_G$ و $L'=\{l-m|l\in L\}$، در این صورت، (G,χ) دقیق از نوع L است اگر و تنها اگر (G,χ') دقیق از نوع L' باشد. (G,χ) نرمال‌شده نامیده می‌شود، هرگاه $(\chi,1_G)_G=0$. در مطالعه زوج‌های دقیق فرض می‌کنیم (G,χ) نرمال‌شده است.

مسئله رده‌بندی تمام زوج‌های دقیق (G,χ) از نوع L در حالتی که L شامل عددی غیرگویاست، در قضیه زیر حل شده است:

قضیه ۱.۰.۱. (قضیه ۱.۰۳ در [۱]) فرض کنید (G,χ) دقیق و نرمال‌شده است و χ مقداری غیرگویا اختیار می‌کند؛ در این صورت داریم:

۱. G گروهی دوری از مرتبه m است که $m\geq 3$ و χ خطی است، یا $m\geq 5$ و χ مجموع دو سرشت خطی مزدوج مختلط از G است؛

۲. G گروهی دو وجهی از مرتبه $2m$ است که $m\geq 5$ فرد است و χ سرشتی تحویل‌ناپذیر از درجه ۲؛

۳. G گروه چهارگانی تعمیم یافته از مرتبه $2m$ است که $m\geq 8$ زوج است و $\chi=\psi$ یا $\chi=\psi+\varepsilon$، که در آن ψ سرشتی تحویل‌ناپذیر از درجه ۲ و ε سرشتی خطی با هسته دوری از مرتبه m؛

۴. G گروهی یکریخت با گروه هشت وجهی باینری است و χ سرشتی تحویل‌ناپذیر از درجه ۲؛

۵. G گروهی یکریخت با $SL(2,5)$ است و χ سرشتی تحویل‌ناپذیر از درجه ۲؛

۶. G گروهی یکریخت با A_6 و χ سرشتی تحویل‌ناپذیر از درجه ۳.

از طرفی نتایج برای حالت‌هایی که L تنها شامل اعداد گویاست، اندک‌اند (برای نمونه ر. ک. [۲]، [۳]، [۴]).
ساده‌ترین حالت در این بین، حالت $L=\{l\}$ است که در آن l عددی گویاست. اگر (G,χ) دقیق از نوع $\{l\}$ باشد، به‌سادگی می‌توان دید $l=-1$ و $\chi=\rho_G-1_G$، که در آن ρ_G سرشت منظم G است.
اگر (G,χ) نرمال‌شده و دقیق از نوع $L=\{l_1,l_2\}$ باشد، که در آن l_1 و l_2 اعداد گویای متمایز هستند، از $\rho_G=(\chi-l_1 1_G)(\chi-l_2 1_G)$ نتیجه می‌شود که $(\chi,\chi)_G=1-l_1l_2$ و $l_1<0\leq l_2$. این ایجاب می‌کند که $(\chi,\chi)_G=1$ اگر و تنها اگر (G,χ) از نوع $\{l,0\}$ باشد، که $l<0$؛ $(\chi,\chi)_G=2$ اگر و تنها اگر (G,χ) از نوع $\{-1,1\}$ باشد؛ و $(\chi,\chi)_G=3$ اگر و تنها اگر (G,χ) از نوع $\{-1,2\}$ یا $\{-2,1\}$ باشد. برای حالت اول، برخی از ویژگی‌های G و χ در [۲] و [۶] آمده‌است:

قضیه ۲.۱. (قضیه ۲.۲ در [۲]) فرض کنید χ سرشتی باوفا از گروه متناهی G است. در این صورت، گزاره‌های زیر معادل‌اند:

۱. (G,χ)، دقیق از نوع $\{۰,l\}$ است؛

۲. G زیرگروهی نرمال و آبلی‌مقدماتی مانند N دارد، به طوری‌که $N-\{۱\}$ یک کلاس تزویج تنها است و به ازای هر $g\in G-N$ و هر $x\in N$، g با gx مزدوج است؛

۳. χ سرشتی تحویل‌ناپذیر است و روی همه کلاس‌های تزویج بجز یکی صفر می‌شود.

قضیه ۳.۱. (قضیه ۲ در [۶]) فرض کنید G سرشتی نرمال‌شده و دقیق مانند χ از نوع $\{۰,l\}$ دارد. در این صورت، گزاره‌های زیر برقرارند:

۱. اگر τ یک سرشت دقیق نابدیهی و نرمال‌شده از G باشد، آنگاه $L(\tau)=\{m,m-l\}$ که در آن $m<۰$ و m، l را عاد می‌کند.

۲. تعداد سرشت‌های دقیق و نرمال‌شده از نوع $\{m,m-l\}$ از G برابر است با تعداد زیرگروه‌های نرمال با اندیس l/m در G.

زوج‌های دقیق از نوع $\{۱,-۱\}$ نیز در [۳] داده شده‌اند:

قضیه ۴.۱. فرض کنید G گروهی متناهی و χ سرشتی از G با درجه n است. همچنین فرض کنید (G,χ) نرمال‌شده و دقیق از نوع $\{۱,-۱\}$ است. در این صورت، G با یکی از ۱۲ گروه زیر یکریخت است:
$D_۸$ و $Q_۸$ $(n=۳)$؛ $S_۴$ و $SL(۲,۳)$ $(n=۵)$؛
$GL(۲,۳)$ و گروه هشت وجهی باینری $(n=۷)$؛
$S_۵$ و $SL(۲,۵)$ $(n=۱۱)$؛ $PSL(۲,۷)$ $(n=۱۳)$؛ $A_۶$ $(n=۱۹)$؛
پوشش دوم $\hat{A_۷}$ از $A_۷$ $(n=۷۱)$؛ $M_{۱۱}$ $(n=۸۹)$.

حالت آخر هم برای گروه‌های دارای مرکز نابدیهی در [۴] آمده‌است که در [۵] اصلاح شد و به حالت $L(\chi)=\{l,l+p\}$، به ازای $l=-۱$ یا $l=۱-p$ و عدد اول فرد p، به صورت زیر تعمیم داده شد:

قضیه ۵.۱. فرض کنید (G,χ) یک زوج نرمال‌شده و دقیق از نوع $\{-۱,p-۱\}$ باشد، که در آن p عددی اول و فرد است. به‌علاوه، اگر مرکز گروه G یعنی، $Z=Z(G)$ نابدیهی باشد، آنگاه Z گروهی دوری از مرتبه p است و یکی از موارد زیر برقرار است:
$G=Z\times D(۲p)$؛ $G=Z\times PSL(۲,q)$ با $q=p+۱$ یا $q=۲p+۱$؛
$G=Z\times Sz(q)$ با $q=p+۱$؛ $|G|=p^۳(p-۱)$ و G گروه خودریختی $ES(p^۳,p^۲)$ است.

قضیه ۶.۱. فرض کنید (G,χ) یک زوج نرمال‌شده و دقیق از نوع $\{۱,p۱\}$ باشد، که در آن p عددی اول و فرد است. به‌علاوه، اگر مرکز گروه G یعنی، $Z=Z(G)$ نابدیهی باشد، آنگاه Z گروهی دوری از مرتبه p است و یکی از موارد زیر برقرار است:
$G=Z\times PSL(۲,q)$ با $q=p-۱$ یا $q=۲p-۱$؛

$p=۳$ و $G=Z\times D(۶)$؛ $p=۵$ و $G=Z\times PSL(۳,۴)$؛
$p=۳$، $|G|=۵۴$ و G گروه خودریختی $ES(۲۷,۹)$ است؛ $p=۳$، $|G|=۱۰۸$ و G/Z یک گروه فروبینیوس است؛
$p=۳$ و G پوشش سوم $M_{۱۰}$ یا $M_{۲۲}$ است.

در ادامه حالتهای $L(\chi)=\{-۱,۳\}$ و $L(\chi)=\{-۳,۱\}$ را درنظر میگیریم، با این فرض که مرکز گروه‌های مورد نظر نابدیهی هستند.

۲ نتایج اصلی

فرض کنید G گروهی متناهی و χ سرشتی باوفا از G است، به‌طوری که (G,χ) زوجی نرمال‌شده و دقیق از نوع $\{\varepsilon,-۳\varepsilon\}$ باشد که در آن $\varepsilon=\pm ۱$. $Z(G)$ نماد مرکز G است و فرض بر این است که $Z(G)\neq ۱$. قرار می‌دهیم $n:=\chi(۱)$؛ و بنابر تعریف زوج‌های دقیق داریم $|G|=(n-\varepsilon)(n+۳\varepsilon)$.
همچنین تعریف می‌کنیم:
$A_\varepsilon:=\{g\in G|\chi(g)=\varepsilon\}$ و $A_{(-۳\varepsilon)}:=\{g\in G|\chi(g)=-۳\varepsilon\}$ و قرار می‌دهیم $a_\varepsilon:=|A_\varepsilon|$ و $a_{(-۳\varepsilon)}:=|A_{(-۳\varepsilon)}|$.
ویژگی‌های زیر را برای زوج‌های مورد نظر به‌دست آورده‌ایم:

گزاره ۱.۲. فرض کنید p و q اعدادی اول و فرد باشند، به‌گونه‌ای که p، $n-\varepsilon$ را عاد می‌کند و q، $n+۳\varepsilon$ را. در این صورت داریم:

۱. به‌ازای هر عنصر g در G از مرتبه p، $\chi(g)=\varepsilon$؛

۲. به‌ازای هر عنصر g در G از مرتبه q، $\chi(h)=-۳\varepsilon$؛

۳. هیچ عضوی از مرتبه pq در G وجود ندارد.

گزاره ۲.۲. $g.c.d(n-\varepsilon,n+۳\varepsilon)\neq ۱$.

لم ۳.۲. $a_\varepsilon=\frac{۳}{۴}n^۲+\frac{۵\varepsilon}{۴}n-۳$ و $a_{(-۳\varepsilon)}=\frac{۱}{۴}n^۲+\frac{۳\varepsilon}{۴}n-۱$.

نتیجه ۴.۲. اگر $\varepsilon=۱$ آن‌گاه $n=۴k+۱$؛ و اگر $\varepsilon=-۱$ آن‌گاه $n=۴k+۳$.

قضیه ۵.۲. عددی طبیعی مانند k موجود است به‌طوری که $|G|=۱۶k(k+۱)$.

مراجع

[1] D. Alvis and S. Nozawa, *Sharp characters with irrational values*, J. Math. Soc. Japan **48** (1996), no. 3, 567-591.

[2] P. J. Cameron and M. Kiyota, *Sharp characters of finite groups*, J. Algebra **115** (1988), no. 1, 125-143.

[3] P. J. Cameron, T. Kataoka, and M. Kiyota, *Sharp characters of finite groups of type* $\{-۱, ۱\}$, J. Algebra **152** (1992), no. 1, 248-258.

[4] S. Nozawa and M. Uno, *On sharp characters of rank ۲ with rational values*, J. Algebra **286** (2005), no. 2, 325-340.

[5] T. Yoguchi, *On sharp characters of type* $\{l, l+p\}$, Kyushu J. Math. **65** (2011), no. 1, 179-195.

[6] T. Yoguchi, *On determining the sharp characters of fiite groups*, JP J. Algebra, Number Theory Appl. **11** (2008), no. 1, p. 85-98.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۷ تا ۱۰.

سخنرانی

بررسی ۲-همبندی گراف توان برخی از گروه‌های ساده

نرگس اکبری
دانشکده ریاضی، دانشگاه کاشان
nargesakbari1391@gmail.com

علی‌رضا اشرفی
دانشکده ریاضی، دانشگاه کاشان
ashrafi@kashanu.ac.ir

چکیده

گراف توان گروه متناهی G، $P(G)$، گرافی است با مجموعه رئوس G که در آن دو رأس g و h مجاورند اگر و تنها اگر یکی از آن‌ها برابر با توانی از دیگری باشد. این مقاله به مطالعه ۲-همبندی گراف توان گروه‌های ساده پراکنده، گروه‌های ساده ری نوع ${}^2F_4(q)$ و ${}^2G_2(q)$، گروه‌های شواله نوع $A_1(q)$، $B_2(q)$، $C_2(q)$ و $F_4(q)$، گروه‌های سیمپلکتیک خاص تصویری $S_4(q)$ گروه‌های یکانی خاص تصویری $U_3(q)$ و گروه‌های خطی خاص تصویری $PSL(3, q)$ می‌پردازد.

واژه های کلیدی: گروه ساده، گراف توان، ۲-همبندی.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $05E15$، $05C75$، $20D08$، $20D06$.

مقدمه

فرض کنید G یک گروه متناهی است. گراف توان $P(G)$ گرافی است با مجموعه رئوس G که در آن دو عنصر متمایز x و y مجاورند اگر و تنها اگر یکی از آن‌ها توانی از دیگری باشد.

گراف توان سره که با حذف رأس همانی از $P(G)$ به‌دست می‌آید با $P^*(G)$ نشان داده می‌شود. در واقع $P^*(G) = P(G) - \{e\}$. درجه x در گراف توان را با $deg(x)$ و مجموعه مرتبه‌های عناصر G را با $\pi_e(G)$ نشان می‌دهند. رأس برشی در یک گراف، رأسی است که حذف آن موجب افزایش تعداد مؤلفه‌های همبندی گراف می‌گردد. گراف Γ، ۲-همبند گفته می‌شود هرگاه رأس برشی نداشته باشد. بنابر تعریف گراف توان، در صورتی در گراف توان یک گروه، میان دو رأس یال وجود دارد که یکی به صورت توانی از دیگری قابل نوشتن باشد. بنابراین می‌توان نتیجه گرفت در صورت متباین بودن مرتبه دو رأس، یالی میان آن دو رأس وجود ندارد. ما در این مقاله با در نظر گرفتن افرازهایی برای مجموعه مرتبه‌های عناصر هر یک از گروه‌های ساده فوق ثابت می‌کنیم گراف توان گروه‌های فوق ۲-همبند نیستند.

نتایج اصلی

در این بخش ثابت می‌شود گراف توان گروه‌های ساده پراکنده، گروه‌های ساده ری نوع ${}^2F_4(q)$ و ${}^2G_2(q)$، گروه‌های شواله نوع $A_1(q)$، $B_2(q)$ و $C_2(q)$، گروه‌های سیمپلکتیک خاص تصویری $S_4(q)$ و گروه‌های خطی خاص تصویری $PSL(3,q)$ ۲-همبند نیستند.

بررسی ۲-همبندی گراف توان گروه‌های پراکنده

بنابر رده بندی گروه‌های ساده، ۲۶ گروه وجود دارند که در هیچ دسته نامتناهی از گروه‌های ساده قرار نمی‌گیرند. این گروه‌ها را گروه‌های ساده پراکنده می‌نامند. گروه‌های ساده پراکنده عبارتند از:

$$\left\{ \begin{array}{c} M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, Co_1, Co_2, Co_3, Fi_{22}, Fi_{23}, \\ Fi_{24}, HS, Msl, He, Ru, SUZ, O'N, HN, Ly, Th, B, M \end{array} \right\}$$

می‌دانیم در گراف توان یک گروه در صورتی میان دو رأس یال وجود دارد که یکی به صورت توانی از دیگری قابل نوشتن باشد. حال با توجه به این‌که در صورت متباین بودن مرتبه دو رأس یالی میان آن دو رأس وجود ندارد، گراف توان گروه‌های پراکنده را در نظر می‌گیریم. با یک بررسی ساده روی مرتبه عناصر هر یک از گروه‌های پراکنده فوق، حداقل یک عدد وجود دارد که نسبت به سایر مرتبه عناصر گروه متباین است. بنابراین قضیه زیر را داریم:

قضیه ۱. گراف توان گروه‌های پراکنده، ۲-همبند نیستند.

بررسی ۲-همبندی گراف توان گروه‌های ری نوع ${}^2F_4(q)$ و ${}^2G_2(q)$

با محاسباتی خسته کننده و استفاده از نتایج [۱] قضیه زیر به اثبات می‌رسد.

قضیه ۲. گراف توان گروه‌های ری نوع ${}^2F_4(q)$ که در آن $q = 2^{2m+1}$، $m > 1$، می‌باشد، ۲-همبند نیستند.

با استفاده از نتایج [۴] و محاسباتی خسته کننده چون $^{2}G_{2}(q)$ که در آن q توانی از یک عدد اول فرد است، دارای افرازی است با این ویژگی که فرازهای آن هیچ عامل مشترکی ندارند، قضیه زیر را داریم:

قضیه ۳. گراف توان گروه‌های ری نوع $^{2}G_{2}(q)$ که در آن q توانی از یک عدد اول فرد است، ۲-همبند نیستند.

بررسی ۲-همبندی گراف توان گروه‌های شواله نوع $A_{1}(q)$، $C_{2}(q)$ و $B_{2}(q)$

با استفاده از نتایج [۴] و محاسباتی خسته کننده چون $\pi_e(A_{1}(q))$ و $\pi_e(C_{2}(q))$ که در آن q توانی از یک عدد اول فرد است، هر یک دارای افرازی است با این ویژگی که فرازهای آن هیچ عامل مشترکی ندارند، قضایای زیر را داریم:

قضیه ۴. گراف توان گروه‌های شواله نوع $A_{1}(q)$ که در آن q توانی از یک عدد اول فرد است، ۲-همبند نیستند.

قضیه ۵. گراف توان گروه‌های شواله نوع $C_{2}(q)$ که در آن q توانی از یک عدد اول فرد است، ۲-همبند نیستند.

با استفاده از نتایج [۳] و محاسباتی خسته کننده چون $\pi_e(B_{2}(q))$ که در آن q توانی از یک عدد اول است، دارای افرازی است با این ویژگی که فرازهای آن هیچ عامل مشترکی ندارند، قضیه زیر را داریم:

قضیه ۶. گراف توان گروه‌های شواله نوع $B_{2}(q)$ که در آن q توانی از یک عدد اول است، ۲-همبند نیستند.

بررسی ۲-همبندی گراف توان گروه‌های سیمپلکتیک خاص تصویری

با استفاده از نتایج [۳]، چون $\pi_e(S_{4}(q))$که در آن q توانی از یک عدد اول فرد است دارای افرازی است با این ویژگی که فرازهای آن هیچ عامل مشترکی ندارند، قضیه زیر را داریم:

قضیه ۷. گراف توان گروه‌های سیمپلکتیک خاص تصویری $S_{4}(q)$ که در آن q توانی از یک عدد فرد است، ۲-همبند نیستند.

بررسی ۲-همبندی گراف توان گروه‌های خطی خاص تصویری

با استفاده از نتایج [۲]، می‌توان ۲-همبندی گروه‌های $PSL(3,q)$ را نیز بررسی نمود. به طور دقیق:

قضیه ۸. گراف توان گروه‌های $PSL(3,q)$، ۲-همبند نیستند.

مراجع

[1] H. Deng, W. Shi, *The characterization of ree groups* $^2F_4(q)$ *by their element orders*, J. Algebra, **217** (1999), no. 1, 180-187.

[2] W. A. Simpson, S. Frame, *The character tables for* $SL(3,q)$, $SL(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$, Can J Math, **25** (1973), no. 3, 486-494.

[3] B. Srinivasan, *The characters of the finite symplectic group* $Sp(4,q)$, Trans. Amer. Math. Soc., **131** (1968), no. 2, 488–525.

[4] A. M. Staroletove, *On recognition by spectrum of the simple groups* $B_3(q), C_3(q), D_4(q)$, Sib. Math. J, **53** (2012), no. 3, 532-538.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۱۱ تا ۱۳.

سخنرانی

یادداشتی بر تفاضل دو شاخص سگد و سگد اصلاح شده یک گراف

نادر حبیبی
دانشکده فنی مهندسی و علوم پایه، دانشگاه آیت الله العظمی بروجردی
habibi@abru.ac.ir

چکیده

شاخص سگد اصلاح شده توصیفگر ساختار مولکولی است برابر با حاصل جمع

$$[n_u(e)+\frac{n_\circ(e)}{۲}][n_v(e)+\frac{n_\circ(e)}{۲}]$$

روی تمام یال‌های $e=uv$ گراف مولکولی G است، که در آن $n_\circ(e)$ تعداد رأس‌هایی است که فاصله‌ی آن‌ها از u و v یکسان می‌باشد و $n_u(e)$ تعداد رأس‌هایی که به u نزدیکترند تا به v و $n_v(e)$ نیز بطور مشابه تعریف می‌شود. در این نوشته کران‌هایی برای تفاضل بین شاخص سگد اصلاح شده Sz^* و شاخص سگد Sz یک گراف G به‌دست می‌آید.

واژه های کلیدی: شاخص سگد، شاخص سگد اصلاح شده، شاخص پادماکار-ایوان.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۰۵C۳۵، ۰۵C۱۲.

۱ مقدمه

شاخص توپولوژی ناوردای گرافی است که در شیمی کابرد دارد. نخستین شاخص توپولوژی شاخص وینر است. شاخص سگد[۱] به صورت $Sz(G)=\sum_{e=uv\in E(G)} n_u(e)n_v(e)$، شاخص سگد اصلاح شده [۴] توصیفگر ساختار مولکولی است برابر با حاصل جمع $[n_u(e)+\frac{n_\circ(e)}{۲}][n_v(e)+\frac{n_\circ(e)}{۲}]$ روی تمام یال $e=uv$ گراف مولکولی G است، که در آن $n_\circ(e)$ تعداد رأس‌هایی است که فاصله‌ی آن‌ها از u و v یکسان می‌باشد و $n_u(e)$ تعداد رأس‌هایی که به u نزدیکترند تا به v و $n_v(e)$ نیز بطور مشابه تعریف می‌شود. در این نوشته کران‌هایی برای تفاضل بین شاخص سگد اصلاح شده Sz^* و شاخص سگد Sz یک گراف G به‌دست می‌آید. شاخص پادماکار ایوان رأسی [۲] گراف G، بنا بر تعریف برابر است با $PI_v(G)=\sum_{e=uv\in E(G)}[n_u(e)+n_v(e)]$.

لم ۱. [۳، قضیه ۱] فرض کنید G یک گراف باشد. آن‌گاه $Sz(G)\le Sz^*(G)$. تساوی برقرار است اگرو تنها اگر G دوبخشی باشد.

باتوجه به لم قبل که $Sz^*(G)-Sz(G)\ge ۰$، یک شاخص جدید تعریف می کنیم

$$\beta(G)=Sz^*(G)-Sz(G).$$

۲ نتایج اصلی

در این بخش کران‌هایی برای شاخص جدید معرفی شده ارائه می‌شود.

لم ۲. فرض کنید G یک گراف همبند و غیر دوبخشی n رأسی باشد. در این‌صورت،

$$\sum_{e\in E(G)} n_\circ^۲(e)\ge n.$$

قضیه ۳. برای یک گراف $n\ge ۳$ رأسی غیر دوبخشی همبند G داریم:

$$n\le \sum_{e\in E(G)} n_\circ^۲(e)\le \binom{n}{۲}(n-۲)^۲$$

تساوی چپ برقرار است اگر و تنها اگر وقتی که $G\cong C_n$ و تساوی راست در گراف کامل K_n اتفاق می‌افتد.

قضیه ۴. فرض کنید G یک گراف همبند و غیر دو بخشی n رأسی باشد. در این‌صورت

$$\frac{۱}{۲}PI_v(G)+\frac{n}{۴}\le\beta(G)\le\frac{n-۲}{۲}PI_v(G)+\frac{(n-۲)^۲}{۴}\binom{n}{۲}$$

مراجع

[1] I. Gutman, A formula for the Wiener number of trees and its extension to the graphs containing cycles, *Graph Theory Notes Ney York* **17** (1994) 9-15.

[2] M.H. Khalifeh, H. Yousefi-Azari, A.R. Ashrafi, Vertex and edge PI indices of cartesian product graphs, *Discrete Appl. Math.* 156 (2008) 1780-1789.

[3] T. Pisanski, M. Randić, *Use of the Szeged index and the revised Szeged index for measuring network bipartivity*, *Discrete Applied Mathematics* **158** (2010) 1936-1944.

[4] M. Randić, On generalization of Wiener index to cyclic structures, *Acta Chim. Slov.* **49** (2002), 483-496.

[5] H. Wiener, Structural determination of paraffin boiling points, *J. Am. Chem. Soc.* **69** (1947) 17-20.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۱۵ تا ۱۸.

سخنرانی

فاصله طیف نرمال‌ساز لاپلاسی گراف‌ها

مرجان حکیمی نژاد
دانشکده علوم ریاضی، دانشگاه تربیت دبیر شهید رجایی تهران،
m.hakiminezhaad@srttu.edu

مجتبی قربانی
دانشکده علوم ریاضی، دانشگاه تربیت دبیر شهید رجایی تهران،
mghorbani@srttu.edu

Abstract

In this paper, we compute the normalized Laplacian spectral distances and normalized Laplacian cospectrality of some particular classes of graphs.

Keywords: normalized Laplacian spectral distance, normalized Laplacian cospectrality.

MSC(2010): 05C05, 05A12, 05C50.

مقدمه

گراف $G=(v,e)$ را ساده با n رأس در نظر بگیرید. درجه هر رأس $v\in V(G)$ را با $deg(v)$ نشان می‌دهیم. اگر درجه تمام رئوس گراف برابر r باشد، آنگاه گراف را r-منظم می‌نامیم. $\mathbf{D}$ ماتریس قطری $n\times n$ است که درایه‌های روی قطر اصلی آن درجه رئوس گراف G و بقیه درایه‌ها صفر هستند. مقادیر ویژه‌ی ماتریس مجاورت $\mathbf{A}(G)$ از گراف G را مقادیر ویژه G نامیده و آن‌ها را به‌صورت $\lambda_1\leq\lambda_2\leq\cdots\leq\lambda_n$ مرتب می‌کنیم. فرض کنید $\lambda_1\leq\lambda_2\leq\cdots\leq\lambda_s$ مقادیر ویژه متمایز گراف G از مرتبه n با ماتریس

مجاورت $\mathbf{A}$ هستند. در این صورت طیف گراف G را که در آن $m(\lambda_i)$ مرتبه تکرار مقدار ویژه λ_i است، به‌شکل زیر تعریف می‌کنیم:

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_s \\ m(\lambda_1) & m(\lambda_2) & \dots & m(\lambda_s) \end{pmatrix}.$$

مجموع قدرمطلق تمام مقادیر ویژه ماتریس مجاورت G را انرژی گراف گوییم و با $E(G)$ نشان می‌دهیم[۵].

فرض کنید گراف G، بدون رأس تنها است. در این صورت ماتریس نرمال‌ساز لاپلاسی $\mathbf{L}(G)$ را به‌صورت $\mathbf{L}(G) = \mathbf{D}^{-\frac{1}{2}}(\mathbf{D}\text{-}\mathbf{A})\mathbf{D}^{-\frac{1}{2}}$ تعریف می‌کنیم که درایه (i,j)-ام آن برابر با ۱ است هرگاه $i = j$ و برابر با $-1/\sqrt{deg(v_i)deg(v_j)}$ است هرگاه رأس‌های v_i و v_j با هم مجاور باشند که در آن $i \neq j$ و در غیر این صورت برابر صفر است. مقادیر ویژه‌ی $\mathbf{L}(G)$ را طیف نرمال‌ساز لاپلاسی G نامیده و با $\mathbf{L}spec(G)$ نشان می‌دهیم و آن‌ها را به‌صورت $\delta_1 \leq \delta_2 \leq \dots \leq \delta_n$ مرتب می‌کنیم [۴]. در ادامه، $\mathbf{L}\sigma(G_1, G_2) = \sum_{i=1}^{n} |\delta_i(G_1) - \delta_i(G_2)|$ را فاصله طیف نرمال‌ساز لاپلاسی دو گراف G_1 و G_2 روی n رأس می‌نامیم [۶].

اینک به معرفی برخی از گراف‌های مورد نیاز می‌پردازیم. اتصال $G_1 + G_2$، گرافی است که از کنار هم قرار دادن دو گراف G_1 و G_2 و متصل کردن هر رأس گراف G_1 به هر رأس گراف G_2 حاصل می‌شود. گراف $\overline{G}$ را مکمل گراف G می‌نامیم. گراف کامل از مرتبه n و گراف دوبخشی کامل را به‌ترتیب با K_n و K_{n_1,n_2} نشان می‌دهیم. گراف CP_n، گرافی است که از حذف یک جورسازی کامل از گراف کامل $2n$ رأسی به‌دست می‌آید.

نتایج اصلی

در این بخش، برخی از نتایج اصلی روی فاصله طیف نرمال‌ساز لاپلاسی میان دو گراف دلخواه را بیان می‌کنیم.

قضیه ۱. فرض کنید G_1 و G_2 گراف‌های n رأسی به‌ترتیب r_1 و r_2 -منظم هستند. در این صورت اگر $r_1 \leq r_2$ باشد، آن‌گاه $\mathbf{L}\sigma(G_1, G_2) \leq \frac{1}{r_2}E(G_2) + \frac{1}{r_1}E(G_1)$.

نتیجه ۲. اگر G_1 و G_2 گراف‌های n رأسی r-منظم باشند، آن‌گاه $\mathbf{L}\sigma(G_1, G_2) = \frac{1}{r}\sigma(G_1, G_2)$.

قضیه ۳. فرض کنید G گرافی r-منظم روی n رأس است به‌طوری که درجه آن بزرگ‌تر از درجه مکمل گراف G نباشد. در این صورت $\mathbf{L}\sigma(G, \bar{G}) \leq \frac{n-1}{r(n-r-1)}E(G) + \frac{r+1}{(n-r-1)}$.

قضیه ۴. گراف همبند G را دلخواه با $n \geq 2$ رأس در نظر بگیرید. اگر $n^*(G)$ معرف مقادیر ویژه G که بزرگ‌تر یا مساوی $\frac{n}{n-1}$ باشد، آن‌گاه $\mathbf{L}\sigma(K_n, G) = n + (n - 2n^* - 1)\frac{n}{n-1} - 2\sum_{i=2}^{n-n^*} \delta_i(G)$.

کاربردها

در این قسمت، قصد داریم مفهوم اندازه هم‌طیفی نرمال‌ساز لاپلاسی گراف‌ها را مطرح کرده و سپس با ارائه یک مثال اهمیت آن‌ها را در مورد نظریه طیف نرمال‌ساز لاپلاسی گراف‌ها نشان دهیم و نتایج بیشتری را درباره‌ی فاصله طیف نرمال‌ساز لاپلاسی برخی از جفت گراف‌های خاص مطرح کنیم.

فرض کنید X زیر مجموعه دلخواه از مجموعه گراف‌های n رأسی است. در این صورت حالت هم‌طیفی نرمال‌ساز لاپلاسی و اندازه هم‌طیفی نرمال‌ساز لاپلاسی از $G \in X$، به‌ترتیب به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned}\mathbf{L}CS_X(G) &= min\{\mathbf{L}\sigma(G,H) : H \in X, H \neq G\},\\ \mathbf{L}CS(X) &= max\{\mathbf{L}CS_X(G) : G \in X\},\end{aligned}$$

که به کمک آن می‌توان میزان دوری فاصله‌ی طیف نرمال‌ساز لاپلاسی یک گراف در X را از فاصله طیف نرمال‌ساز لاپلاسی هر گراف دیگر متعلق به همان مجموعه، اندازه گرفت. جهت آشنایی بیشتر با مفاهیم فوق، مثال زیر را ببینید.

مثال ۵. مجموعه $X = \{G_0, \ldots, G_n\}$ را طوری بسازید که $G_0 = CP_n$ و G_i از اضافه کردن i یال به G_0 به‌دست آید. از این‌رو $G_n = K_{2n}$. در حقیقت، گراف G_i برابر با $K_{2i} + CP_{n-i}$ می‌باشد که در آن $1 \leq i \leq n$. حال برای به‌دست آوردن مقادیر هر یک از توابع مورد نظر، به طیف نرمال‌ساز لاپلاسی گراف‌های متعلق به مجموعه X نیاز داریم. طیف نرمال‌ساز لاپلاسی اتصال این گراف برابر است با:

$$\begin{pmatrix} 0 & 1 & \frac{2n}{2n-1} & \frac{2n(n-1)+i}{(2n-1)(n-1)} & \frac{n}{n-1} \\ 1 & n-i & 2i-1 & 1 & n-i-1 \end{pmatrix}.$$

لذا از طیف فوق تمام مقادیر ویژه نرمال‌ساز G_i، $0 < i < n$، حاصل می‌شود. فاصله طیف نرمال‌ساز لاپلاسی میان دو گراف $2n$ رأسی G_j و G_i که در آن $0 \leq i < j \leq n$، به‌صورت زیر است:

$$\begin{aligned}\mathbf{L}\sigma(G_j,G_i) &= (j-i)\Big(\frac{2n}{2n-1}-1\Big)+\Big(\frac{2n(n-1)+i}{(2n-1)(n-1)}-\frac{2n}{2n-1}\Big)\\ &+ (j-i-1)\Big(\frac{n}{n-1}-\frac{2n}{2n-1}\Big)\\ &+ \Big(\frac{n}{n-1}-\frac{2n(n-1)+j}{(2n-1)(n-1)}\Big).\end{aligned}$$

اگر $j = n$، آن‌گاه با استفاده از قضیه ۴ داریم، $\mathbf{L}\sigma(K_{2n},G_i) = \frac{2(n-i)}{2n-1}$. پس برای هر $1 \leq i \leq n$، $\mathbf{L}CS_X(G_i) = \frac{2}{2n-1}$. بنابراین $\mathbf{L}CS(X) = \frac{2}{2n-1}$.

قضیه ۶. برای $n \geq 2$، $\mathbf{L}cs(\overline{K_n}) = 2\sqrt{n-1}+n$.

قضیه ۷. برای $n \geq 2$، $\mathbf{L}cs(K_n) = 2(1-\frac{1}{n-1})$.

هم‌چنین، برای گراف همبند G، $\mathbf{L}\sigma(K_n,G) = \mathbf{L}cs(K_n)$ اگر و تنها اگر $G = K_{i,n-i}$ که در آن $1 \leq i \leq [\frac{n}{2}]$.

مراجع

[1] Abdollahi, Alireza; Oboudi, Mohammad Reza. *Cospectrality of graphs*, Linear Algebra Appl. **451** (2014), 169-181.

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

[3] D. Cvetković; M. Doob; H. Sachs, Spectra of Graphs: Theory and Applications, Academic Press, New York, (1980).

[4] F. R. K. Chung, Spectral Graph Theory, Amer. Math. Soc., Providence, (1997).

[5] I. Gutman, The energy of a graph: old and new results, in: A. Betten, A. Kohner, R. Laue, A. Wassermann (Eds.), Algebraic Combinatorics and Applications, Springer, Berlin, (2001). 196-211.

[6] Hakimi-Nezhaad, Mardjan; Ashrafi, Ali Reza. *Laplacian and normalized Laplacian spectral distances of graphs*, Southeast Asian Bull. Math. **37** (2013), 731-744.

[7] Li, Xueliang; Shi, Yongtang. *A survey on the Randić index*, MATCH Commun. Math. Comput. Chem. **59** (2008), 127-156.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۱۹ تا ۲۲.

پوستر

شاخص راندمان عملگرها

سمانه حسین زاده
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
hosseinzadeh.samaneh@yahoo.com

علی ایرانمنش
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
iranmanesh@modares.ac.ir

محمدعلی حسین زاده
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
ma.hoseinzade@gmail.com

اسما حمزه
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
hamze2006@yahoo.com

مصطفی توکلی
دانشکده ریاضی، دانشگاه فردوسی مشهد، مشهد، ایران
m.tavakoli@ut.ac.ir

علی رضا اشرفی
دانشکده ریاضی، دانشگاه کاشان، کاشان، ایران
alir.ashrafi@gmail.com

چکیده

در این مقاله به بررسی شاخص راندمان برخی از عملگرهای مهم گرافی مانند حاصلضرب دکارتی، ترکیب و پیوند گراف ها می‌پردازیم.

واژه های کلیدی: شاخص راندمان، عملگرهای گرافی، گراف مولکولی.
رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $۰۵A۲۰$، $۰۵C۱۲$، $۰۵C۳۵$، $۰۵C۷۵$.

۱ مقدمه

فرض کنید که G یک گراف ساده با مجموعه رئوس $V(G)$ و مجموعه یال‌های $E(G)$ باشد. اگر u,v دو رأس از این گراف باشند، فاصله این دو رأس را که با نماد $d(u,v)$ نمایش می دهند، عبارت است از طول کوتاهترین مسیری که این دو رأس را به یکدیگر متصل می‌کنند. همچنین درجه رأس u، عبارت است از تعداد یال‌هایی که روی u قرار گرفته‌اند و آن را با نماد $d(u)$ نشان می‌دهند. در گراف G، نماد $\Delta(G)$ نشان دهنده بزرگترین درجه رئوس G است. برای مفاهیم و تعاریف اولیه مورد نیاز در این مقاله، به خوانندگان منابع [۱، ۲، ۳] را توصیه می کنیم.

اگر u یک رأس از G باشد، مجموع فاصله رئوس G از u را با نماد w_v یا w_v^G نشان می دهیم، به عبارت دیگر داریم $w_v = \sum_{u\in V(G)} d_G(v,u)$. همچنین تعریف می کنیم $w(G) = min\{w_v : v \in V(G)\}$. از مهمترین و قدیمی ترین شاخص های توپولوژیک می توان به شاخص وینر اشاره کرد که این شاخص در سال ۱۹۴۷ توسط هارولد وینر معرفی شد. این شاخص بر اساس فاصله رئوس در گراف بصورت $W(G) = \frac{۱}{۲}\sum_{u\in V(G)} w_u$ تعریف شد و تاکنون بسیاری از خواص شیمیایی، فیزیکی و ریاضی مورد بررسی قرار گرفته است. اکنون شاخص راندمان یک گراف [۲] را که نشان دهنده میزان پراکندگی رئوس براساس کمترین فواصل است را بصورت زیر در نظر بگیرید:

$$\rho(G) = ۲W(G)/nw(G),$$

که در بالا n نشان دهنده تعداد رئوس گراف G است.

فرض کنید G و H گراف‌هایی با مجموعه رئوس مجزا باشند. در این صورت پیوند $G+H$، را از روي دو گراف G و H، چنین تعریف می‌کنیم:

$$\begin{aligned} V(G+H) &= V(G)\cup V(H), \\ E(G+H) &= E(G)\cup E(H)\cup \{xy : x\in V(G), y\in V(H)\}. \end{aligned}$$

گراف با مجموعه رئوس $V(G)\times V(H)$، به طوری که دو رأس $(u_۱,v_۱)$ و $(u_۲,v_۲)$ با هم مجاورند اگر و تنها اگر $u_۱$ و $u_۲$ مجاور باشد، یا $u_۱ = u_۲$ و$v_۱$ با $v_۲$ مجاور باشد، را ترکیب یا حاصل‌ضرب

لغت‌نامه‌ای G و H گوییم و با $G[H]$ نشان می‌دهیم. هم چنین گراف با مجموعه رئوس $V(G)\times V(H)$، به طوری که دو رأس $(u_۱,v_۱)$ و $(u_۲,v_۲)$ با هم مجاورند اگر و تنها اگر $v_۱ = v_۲$و $u_۱$ و $u_۲$ مجاور باشد، یا $u_۱ = u_۲$ و$v_۱$ با $v_۲$ مجاور باشد، را حاصل‌ضرب دکارتی G و H گوییم و با $G\times H$ نشان می‌دهیم.

در این مقاله به محاسبه شاخص راندمان برخی از اعمال گراف ها می پردازیم. در همین راستا، شاخص راندمان حاصلضرب دکارتی، ترکیب و پیوند گراف ها را بررسی می کنیم.

۲ نتایج اصلی

یکی از روش های ساختن یک گراف بزرگ، استفاده از یک عملگر بین دو گراف کوچکتر است. در این قسمت ما به محاسبه شاخص راندمان برخی از اعمال بین گراف ها می پردازیم تا با استفاده از آن به محاسبه این شاخص برای گراف های بزرگ بر حسب محاسبه شاخص راندمان گراف های کوچکتر بپردازیم. در ادامه به بیان برخی از این نتایج می پردازیم.

قضیه ۱. فرض کنید G و H گراف‌هایی با مجموعه رئوس مجزا باشند. آنگاه داریم:

$$w(G\Box H) = |V(H)|w(G)+|V(G)|w(H).$$

در قضیه بعد، شاخص راندمان ترکیب دو گراف محاسبه شده است.

قضیه ۲. فرض کنید G و H دو گراف مجزا باشند. در اینصورت داریم:

$$w(G[H]) = |V(H)|w(G)+۲(|V(H)|-۱)-\Delta(H).$$

در قضیه زیر، شاخص راندمان پیوند دو گراف را بدست آورده ایم.

قضیه ۳. برای دو گراف مجزای G با n رأس و H با m رأس داریم:

$$w(G+H) = \frac{۳(n+m)-(\Delta(G)+\Delta(H)+۴)-|n+\Delta(H)-(m+\Delta(G))|}{۲}$$

مراجع

[1] J.A. Bondy, U.S.R. Murty, Graph Theory, Graduate texts in mathematics, 244, Springer, New York, 2008.

[2] F. Cataldo, O. Ori, S. Iglesias-Groth, Topological Lattice Descriptors of graphene. Sheets with Fullerene-like Nanostructures, Mol. Sim. 36 (5) (2010) 341-353.

[3] T. Došlić, M. Ghorbani, M.A. Hosseinzadeh, Eccentric connectivity polynomial of some graph operations, Util. Math. 84 (2011) 297-309.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۲۳ تا ۲۵.

پوستر

برخی نتایج در رابطه با شاخص راندمان گراف‌ها

محمدعلی حسین زاده
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
ma.hoseinzade@gmail.com

علی ایرانمنش
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
iranmanesh@modares.ac.ir

سمانه حسین زاده
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
hosseinzadeh.samaneh@yahoo.com

اسما حمزه
دانشکده ریاضی، دانشگاه تربیت مدرس، تهران، ایران
hamze2006@yahoo.com

چکیده

در این مقاله ما به یافتن تعدادی کران بالا و پایین برای شاخص راندمان یک گراف بر حسب تعدادی از شاخص های توپولوژیک می پردازیم. همچنین شاخص راندمان اتصال و تفاضل متقارن دو گراف را محاسبه می کنیم.

واژه های کلیدی: شاخص راندمان، قطر گراف، شعاع گراف، حاصلضرب گراف ها.
رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۰۵A۲۰، ۰۵C۱۲، ۰۵C۳۵، ۰۵C۷۵.

۱ مقدمه

در این مقاله ما تمامی گراف ها را ساده و همبند در نظر میگیریم. تمامی نمادهای به کار رفته در این مقاله برگرفته از کتابها و منابع معتبر مانند [۱، ۲، ۳، ۴، ۵] می باشد. در گراف G فرض کنید که $V(G)$ نشان دهنده مجموعه رئوس با اندازه n و $E(G)$ نشان دهنده مجموعه یال‌ها با اندازه m باشد. درجه رأس u، عبارت است از تعداد یال‌هایی که روی u قرار گرفته‌اند و آن را با نماد $d(u)$ نشان می‌دهند. در گراف G، نماد $\delta(G)$ نشان دهنده کمترین درجه رئوس و $\Delta(G)$ نشان دهنده بزرگترین درجه رئوس G است. اگر u,v دو رأس از این گراف باشند، فاصله این دو رأس را که با نماد $d(u,v)$ نمایش می دهند که عبارت است از طول کوتاهترین مسیری که این دو رأس را به یکدیگر متصل می‌کنند. قطر این گراف را با نماد $d(G)$ نشان می دهیم و برابر است با بزرگترین فاصله بین رئوس این گراف. همچنین شعاع این گراف را که با نماد $r(G)$ نشان می دهیم عبارت است از $r(G)=min\{max\{d(u,v):v\in V(G)\}:u\in V(G)\}$. اگر u یک رأس از G باشد، مجموع فاصله رئوس G از u را با نماد w_v یا w_v^G نشان می دهیم، به عبارت دیگر داریم $w_v=\sum_{u\in V(G)}d_G(v,u)$. همچنین تعریف می کنیم $w(G)=min\{w_v:v\in V(G)\}$. از مهمترین و قدیمی ترین شاخص های توپولوژیک می توان به شاخص وینر اشاره کرد که این شاخص در سال ۱۹۴۷ توسط هارولد وینر معرفی شد. این شاخص بر اساس فاصله رئوس در گراف بصورت $W(G)=\frac{۱}{۲}\sum_{u\in V(G)}w_u$ تعریف شد و تاکنون بسیاری از خواص شیمیایی، فیزیکی و ریاضی مورد بررسی قرار گرفته است. اکنون شاخص راندمان یک گراف [۲، ۵] را که نشان دهنده میزان پراکندگی رئوس براساس کمترین فواصل است را بصورت $\rho(G)=۲W(G)/nw(G)$ نظر بگیرید که در آن n نشان دهنده تعداد رئوس گراف G است.

فرض کنید G و H گراف‌هایی با مجموعه رئوس مجزا باشند. در این صورت اتصال $G\vee H$، را از روی دو گراف G و H، چنین تعریف می‌کنیم که مجموعه رئوس آن $V(G)\times V(H)$ است و دو رأس $(u_۱,v_۱)$ و $(u_۲,v_۲)$ با هم مجاورند اگر و تنها اگر $u_۱$ و $u_۲$ مجاور باشد، یا $v_۱$ با $v_۲$ مجاور باشد. هم چنین گراف تفاضل متقارن $G\oplus H$ با مجموعه رئوس $V(G)\times V(H)$ است، به طوری که دو رأس $(u_۱,v_۱)$ و $(u_۲,v_۲)$ با هم مجاورند اگر و تنها اگر و $u_۲$ مجاور باشد، یا $v_۱$ با $v_۲$ مجاور باشد اما نه هر دو با هم رخ دهد.

در این مقاله به محاسبه برخی کران ها برای شاخص راندمان گراف ها بر حسب برخی پارامترهای گرافی می پردازیم. همچنین شاخص راندمان اتصال و تفاضل متقارن گراف ها را محاسبه می کنیم.

۲ نتایج اصلی

در این بخش ابتدا به بیان برخی از کران ها برای شاخص راندمان یک گراف می پردازیم.

قضیه ۱. فرض کنید G یک گراف باشد. آنگاه داریم:

(۱) $\rho(G) \leq \frac{2W(G)}{n\delta(G)}$ و تساوی رخ می دهد اگر و تنها اگر G یک گراف کامل باشد.

(۲) $\rho(G) \geq \frac{4W(G)}{n((n-1)(n+2)-2m)}$.

(۳) $\frac{2W(G)}{n(n-1)d(G)} \leq \rho(G) \leq \frac{4W(G)}{nr(G)(r(G)+1)}$.

در قضیه بعد، شاخص راندمان اتصال و تفاضل متقارن دو گراف را محاسبه می کنیم. فرض کنید که G و H دو گراف باشند. تعداد رئوس G و H را به ترتیب با n_1 و n_2 نشان می دهیم. همچنین تعداد یال های این دو گراف را به ترتیب با m_1 و m_2 نشان می دهیم.

قضیه ۲. فرض کنید G و H گراف‌هایی با مجموعه رئوس مجزا باشند. آنگاه داریم:

(۱) $\rho(G \vee H) = \frac{2n_1^2m_2+2n_2^2m_1-4m_1m_2+4(n_1\bar{m}_2+n_2\bar{m}_1+2\bar{m}_1\bar{m}_2)}{n_1n_2(2(n_1n_2-1)-n_2\Delta(G)-n_1\Delta(H)+\Delta(G)\Delta(H))}$.

(۲) $\rho(G \oplus H) = \frac{2n_1^2m_2+2n_2^2m_1+4(n_1\bar{m}_2+n_2\bar{m}_1+2\bar{m}_1\bar{m}_2)}{n_1n_2(2(n_1n_2-1)-n_2\Delta(G)-n_1\Delta(H)+2\Delta(G)\Delta(H))}$.

مراجع

[1] J.A. Bondy, U.S.R. Murty, Graph Theory, Graduate texts in mathematics, 244, Springer, New York, 2008.

[2] F. Cataldo, O. Ori, S. Iglesias-Groth, *Topological Lattice Descriptors of graphene. Sheets with Fullerene-like Nanostructures*, Mol. Sim. 36 (5) (2010), 341-353.

[3] T. Došlić, M. Ghorbani, M.A. Hosseinzadeh, *The relationships between Wiener index, stability number and clique number of composite graphs*, Bull. Malys. Math. Sci. Soc.(2), 36(1) (2013), 165–172.

[4] M. Liu, B. Liu, *A survey on recent results of variable Wiener index*, MATCH Commun. Math. Comput. Chem., 69 (2013), 491-520.

[5] O. Ori, F. Cataldo, A. Graovac, *Topological Ranking of C_{28} Fullerenes Reactivity*, Fullerenes, Nanotubes Carbon Nanostruct., 17 (3) (2009), 308-323.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۲۷ تا ۳۱.

سخنرانی

مروری بر جدول نمره‌ی یک گروه متناهی

عالیه زلفی
دانشکده ریاضی، دانشگاه کاشان
zolfi.aliye@gmail.com

علی‌رضا اشرفی
دانشکده ریاضی، دانشگاه کاشان
ashrafi@kashanu.ac.ir

چکیده

فرض کنید G گروهی متناهی است. در این‌صورت جدول نمره‌ی G ماتریسی مربعی است که از روی کلاس‌های تزویج زیرگروه‌های G حاصل می شود. این جدول مشبکه‌ی زیرگروه‌های G را توصیف کرده و با استفاده از آن می‌توان حلقه‌ی برنساید G را محاسبه کرد. هدف این مقاله مروری بر نتایج اخیر در این بخش از نظریه محاسباتی گروه‌هاست.

واژه های کلیدی: جدول نمره، حلقه‌ی برنساید، کلاس تزویج، زیرگروه.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $20D30$، $19A22$.

مقدمه

مفهوم جدول نمره‌ی گروه متناهی G برای اولین بار در مرجع [۱] که دومین ویرایش کتاب ویلیام برنساید است، مطرح شد. این جدول نمایش‌های جایگشتی G در حد هم‌ارزی را به‌دست می دهد. به‌علاوه با استفاده از این جدول می‌توان اطلاعات با ارزشی از مجموعه مرتب جزئی کلاس‌های تزویج زیرگروه‌های G به‌دست آورد که این می‌تواند به محاسبه‌ی مشبکه‌ی زیر گروه‌های G منجر شود. مفهوم جدول نمره‌ی گروه

G برای اولین بار با ساختن مشبکه‌ی زیرگروه‌های G شروع شد. بعد از این محاسبات می‌توان جدول نمره را با شمارش روابط شمول بین کلاس‌های تزویج زیرگروه‌های G به‌دست آورد. این روش برای اولین بار در مرجع [۲] تشریح شد. روش فوق الذکر الگوریتمی برای محاسبه‌ی جدول نمره به‌دست می‌هد که در بیشتر سیستم‌های کامپیوتری که برای کار با گروه‌ها فراهم آمده است مورد استفاده می‌باشد. فایفر در مرجع [۲] روشی ارائه نمود که با استفاده از آن می‌توان جدول نمره‌ی یک گروه را بدون نیاز به دانشی از مشبکه‌ی کامل زیرگروه‌های G به‌دست آورد. این روش می‌تواند برای گروه‌هایی که مرتبه‌ی نسبتا بزرگی دارند مورد استفاده قرار بگیرد. به این‌صورت که ابتدا جدول نمره‌ی زیرگروه‌های G را استخراج کرده و با القای آن به G بخش‌هایی از جدول نمره‌ی G حاصل می‌شود. سپس با استفاده از روابط موجود بین درایه‌های جدول نمره، جدول نمره‌ی گروه محاسبه می‌شود. برای استفاده از جدول نمره‌ی زیرگروه‌ها جهت محاسبه‌ی جدول نمره‌ی گروه باید نگاشت پیونددهی $(fusion)$ از مجموعه کلاس‌های تزویج زیرگروه‌های G به خودش به طور کامل تعیین شود.

جدول نمره‌ی یک گروه و حلقه‌ی برنساید

در این بخش ابتدا جدول نمره‌ی گروه را معرفی کرده سپس چند لم و قضیه در رابطه با نحوه‌ی محاسبه‌ی درایه‌های این جدول ارائه می‌دهیم. در ادامه حلقه‌ی برنساید را معرفی می‌کنیم.

تعریف ۱. فرض کنید G گروهی متناهی بوده و روی مجموعه متناهی X عمل کند. نیز فرض کنید U یک زیرگروه G باشد. در این‌صورت $\beta_X(U)$ به‌صورت زیر تعریف می‌شود:

$$\beta_X(U) = |Fix_X(U)|$$

به‌طوری‌که برای هر $u \in U$،

$$Fix_X(U) = \{x \in X : x.u = x\}.$$

$\beta_X(U)$ را یک نمره‌ی G گویند.

لم ۲. فرض کنید U زیرگروه G باشد و G روی مجموعه X عمل کند. در این‌صورت برای هر $g \in G$،

$$\beta_X(U) = \beta_X(U^g).$$

تعریف ۳. فرض کنید G یک گروه متناهی و H_1، ...، H_r نماینده‌های کلاس‌های تزویج تمام زیرگروه‌های G باشند. در این‌صورت ماتریس $M(G) = (\beta_{G/H_i}(H_j))$ را جدول نمره‌ی G گوییم.

لم ۴. فرض کنید H_1، ...، H_r نماینده‌های کلاس‌های تزویج تمام زیرگروه‌های G باشد به‌طوری‌که بر حسب مرتبه از کوچک به بزرگ مرتب شده‌اند. در این‌صورت، $\beta_{G/H_i}(H_r) = 1$.

قضیه ۵. فرض کنید U و V دو زیر گروه G باشند. در این صورت:

$$\beta_{G/V}(U) = |\{V^g : g \in G, U \leqslant V\}||N_G(V) : V|.$$

کلاس تزویج زیرگروه V از G را با $[V]$ نشان می‌دهیم. نیز اگر G روی مجموعه X عمل کند آنگاه X را یک G-مجموعه گوییم.

لم ۶. فرض کنید U و V دو زیرگروه G باشند. در این‌صورت:

الف) اولین درایه از هر سطر $M(G)$ برابر است با:

$$\beta_{G/V}(۱) = |G : V|.$$

ب) درایه‌های قطری $M(G)$ برابرند با:

$$\beta_{G/V}(V) = |N_G(V) : V|.$$

پ) اندازه‌ی کلاس تزویج $[V]$ برابر است با:

$$|[V]| = |G : N_G(V)| = \frac{\beta_{G/V}(۱)}{\beta_{G/V}(V)}.$$

ت) تعداد مزدوجهای V که شامل U هستند برابر است با:

$$|\{V^g : g \in G, U \leqslant V^g\}| = \frac{\beta_{G/V}(U)}{\beta_{G/V}(V)}.$$

تعریف ۷. فرض کنید U و V دو زیرگروه از G باشند. در این‌صورت $\nu_G(V,U)$ را که برابر با تعداد مزدوج‌های زیرگروه U از G مشمول در زیرگروه ثابت V است به‌صورت زیر تعریف می‌کنیم:

$$\nu_G(V,U) = |\{U^g : g \in G, U^g \leqslant V\}|.$$

قضیه ۸. فرض کنید U و V دو زیرگروه G باشند. در این‌صورت:

$$\nu_G(V,U) = \frac{|V|}{N_G(U)}\beta_{G/V}(U) = \frac{\beta_{G/V}(U)\beta_{G/U}(۱)}{\beta_{G/U}(U)\beta_{G/V}(۱)}.$$

قضیه ۹. فرض کنید U و V دو زیرگروه G باشند. در این‌صورت:

$$\beta_{G/V}(U) = \frac{|G : V|\nu_G(V,U)}{\nu_G(G,U)}.$$

تعریف ۱۰. فرض کنید $H_۱$، ...، H_r نماینده‌های کلاس‌های تزویج زیرگروه‌های G باشند. حلقه‌ی برنساید G که با $\Omega(G)$ نشان داده می‌شود گروهی آبلی آزاد، تولید شده توسط کلاس‌های یکریختی G-مجموعه‌های انتقالی G/H_i است. در واقع

$$\Omega(G) = \{\sum_{i=1}^{r} a_i[G/H_i] : a_i \in \mathbb{Z}\}.$$

فرض کنید X و Y دو مجموعه متناهی هستند که G روی آن‌ها عمل می‌کند. نیز فرض کنید U یک زیرگروه G باشد. در این‌صورت:

$$Fix_{X\cup Y}(U) = Fix_X(U) \cup Fix_Y(U)$$

و

$$Fix_{X\times Y}(U) = Fix_X(U) \times Fix_Y(U).$$

بنابراین

$$\beta_{X\cup Y}(U) = \beta_X(U) + \beta_Y(U)$$

و

$$\beta_{X\times Y}(U) = \beta_X(U) \times \beta_Y(U).$$

اگر β_X را r–تایی $\beta_X = (\beta_X(H_1), ..., \beta_X(H_r))$ تعریف کنیم آن‌گاه برای هر $X \in \Omega(G)$ نگاشت $\beta : X \mapsto \beta_X$ یک همومرفیسم حلقه از $\Omega(G)$ به $\mathbb{Z}^r$ است.
فرض کنید $X = \sum a_i[G/H_i] \in \Omega(G)$. در این‌صورت β_X را می‌توان به‌صورت جملاتی از جدول نمره به‌صورت زیر بیان کرد.

$$\beta_X = (a_1, ..., a_r) \times M(G).$$

قضیه ۱۱. فرض کنید G روی X و Y عمل می‌کند. در این‌صورت X و Y یکریختند اگر و تنها اگر $\beta_X = \beta_Y$. کلاس یکریختی X را با $[X]$ نشان می‌هیم.

القای جدول نمره‌ی زیرگروه‌ها

فرض کنید H زیرگروهی از G باشد. در این‌صورت با استفاده از جدول نمره‌ی H می‌توانیم جدول نمره‌ی G را به‌دست آوریم. یک زیرگروه K از H، یک زیرگروه G نیز هست. K وقتی به‌عنوان زیرگروهی از H در نظر گرفته می‌شود دارای زیرگره‌هایی یکسان با حالتی است که به‌عنوان زیرگروه G باشد. اما به‌طور کلی هر زیرگروه از K که در G با زیرگروهی چون U مزدوج است، در H ممکن است با U مزدوج نباشد. می‌توان گفت که هر G–کلاس تزویج از زیرگروه‌های K اجتماع مجزایی از H–کلاس‌های تزویج K است.

لم ۱۲. فرض کنید U، V و H زیر گروه‌های G باشند. نیز فرض کنید V مشمول در H باشد. در این‌صورت تعداد G–مزدوج‌های U که مشمول در V هستند برابر است با:

$$\nu_G(V,U) = \sum_{U'\sim U} \nu_H(V,U')$$

جایی‌که مجموع روی همه‌ی نماینده‌های U' از کلاس‌های تزویج H که با U در G مزدوجند گرفته شده است.

قضیه ۱۳. فرض کنید U، V و H زیرگروه‌های G باشند به‌طوری‌که V مشمول در H باشد. در این‌صورت نمره‌ی $\beta_{G/V}(U)$ با فرمول زیر محاسبه می‌شود:

$$\beta_{G/V}(U) = |N_G(U)| \sum_{U' \sim U} \frac{1}{|N_H(U')|} \beta_{H/V}(U')$$

به‌طوری‌که مجموع روی تمام نماینده‌های U' از کلاس‌های تزویج H که در G با U مزدوجند گرفته شده است.

مراجع

[1] W. Burnside, *Theory of groups of finite order*, 2nd ed, Cambridge University Press, Cambridge, (1911). Reprinted by Dover, New York, (1955).

[2] L. Naughton, G. Pfeiffer, *Computing the table of marks of a cyclic extension*, Math. Comp. **81** (2012), no. 280, 2419-2438.

[3] G. Pfeiffer, *The subgroups of M24, or how to compute the table of marks of a finite group*, Experiment. Math. **6** (1997), no. 3, 247–270. MR 1481593 (98h:20032).

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۳۳ تا ۳۷.

سخنرانی

گراف کیلی یال انتقالی نرمال و کمان انتقالی نرمال گروه های غیر آبلی مرتبه‌ی $9p$ (p عدد اول)

بیژن سلیمانی
دانشکده ریاضی دانشگاه کاشان
bijan_s 59@yahoo.com

سید علی‌رضا اشرفی
دانشکده ریاضی دانشگاه کاشان
ashrafi@kashanu.ac.ir

چکیده

در این مقاله گراف کیلی یال انتقالی نرمال و کمان انتقالی نرمال گروه های غیر آبلی مرتبه ی $9p$ که در آن p یک عدد اول است، بررسی می شود. اگر گرافی یال انتقالی نرمال باشد ولی کمان انتقالی نرمال نباشد آن را نیم کمان انتقالی نرمال گوییم. نتیجه می شود تمام گراف های کیلی گروه های غیر آبلی مرتبه ی $9p$ یال انتقالی نرمال هستند ولی کمان انتقالی نرمال نیستند. بنابراین این گراف ها نیم کمان انتقالی نرمال می باشند.

واژه های کلیدی: گراف کیلی، یال انتقالی نرمال،کمان انتقالی نرمال.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $05B25$، $20D60$.

۱ مقدمه

فرض کنید$\Gamma = (V,E)$ یک گراف ساده باشد که در آن $V = V(\Gamma)$ مجموعه ی رئوس و $E = E(\Gamma)$ مجموعه ی یال‌های Γ می باشد. گروه اتومورفیسم $Aut(\Gamma)$ روی مجموعه‌ی رئوس، یال‌ها و کمان‌های Γ عمل می‌کند. اگر $Aut(\Gamma)$ به ترتیب روی مجموعه‌ی رئوس ، یال‌ها و کمان‌ها به‌صورت انتقالی عمل کند آن‌گاه گراف را رأس انتقالی، یال انتقالی یا کمان انتقالی گوییم. اگر گراف Γ رأس انتقالی و یال انتقالی باشد ولی کمان انتقالی نباشد، آن را نیم کمان انتقالی می‌نامیم. فرض کنید G یک گروه متناهی و S زیر مجموعه‌ای ناتهی از آن باشد به‌طوری‌که $S = S^{-1}$ و $1 \notin S$. گراف کیلی روی گروه G نسبت به مجموعه ی S را با نماد $Cay(G,S)$ نمایش می‌دهیم و به‌صورت زیر تعریف می‌کنیم:

$$V(Cay(G,S)) = G, E(Cay(G,S)) = \{(g,sg) \mid g \in G, s \in S\}$$

برای هر $g \in G$ دلخواه جایگشت $\rho_g : G \to G$ را با ضابطه‌ی $\rho_g(x) = xg \forall x \in G$ تعریف می‌کنیم. فرض کنیم $R(G) := \{\rho_g \mid g \in G\}$، در این‌صورت $R(G)$ یک گروه است که آن را نمایش منظم از راست گروه G می‌نامیم. گزاره‌ها و قضایای زیر در مورد گراف‌های کیلی برقرار هستند:

لم ۱.۱. هر گراف کیلی رأس انتقالی است.

قضیه ۱.۱. گراف $Cay(G,S)$ همبند است اگر وتنها اگر $G = \langle S \rangle$. فرض کنید $\Gamma = Cay(G,S)$ یک گراف کیلی باشد، در این صورت تعریف می‌کنیم: $Aut(G,S) = \{\alpha \in Aut(G) \mid \alpha(S) = S\}$

قضیه ۲.۱. اگر $G = \langle S \rangle$ آن‌گاه $Aut(G,S)$ روی S با وفا عمل می‌کند.

گراف $\Gamma = Cay(G,S)$ را یال انتقالی نرمال یا کمان انتقالی نرمال نامیم هرگاه $N_{Aut(\Gamma)}(R(G))$ روی مجموعه‌ی یال‌ها یا کمان‌های گراف Γ انتقالی عمل کند. گراف $\Gamma = Cay(G,S)$ را نیم کمان انتقالی نرمال گوییم اگر یال انتقالی نرمال بوده ولی کمان انتقالی نرمال نباشد.

لم ۲.۱. هر گراف کیلی کمان انتقالی نرمال، یال انتقالی نرمال نیز هست.

اگر $\Gamma = Cay(G,S)$ یک گراف کیلی G روی S باشد، Γرا نرمال نامیم، هرگاه$R(G)$ یک زیرگروه نرمال $Aut(\Gamma)$ باشد.

قضیه ۳.۱. فرض کنید G یک گروه غیر آبلی ساده باشد و $\Gamma = Cay(G,S)$ گرافی ساده با درجه ی ۳ باشد. اگرΓ یال انتقالی نرمال باشد، آن‌گاه Γ نرمال است.

قضیه ۴.۱. [۳] فرض کنید $\Gamma = Cay(G,S)$ یک گراف کیلی از یک گروه متناهی توسط مجموعه‌ی ناتهی S باشد و $N = R(G) \rtimes N_0$ که در آن $N_0 \leq Aut(G,S)$ ، در این‌صورت:

الف) N روی کمان‌های Γ انتقالی عمل می‌کند اگر و فقط اگر S یک مدار N_0 باشد.

ب) N روی یال‌های Γ انتقالی عمل می‌کند اگر و فقط اگر یا S یک $N_\circ$ مدار باشد و یا S اجتماع دو مجموعه‌ی T و T^{-1} باشد که T و T^{-1} هر دو $N_\circ$ مدار هستند.

نتیجه ۱.۱. گراف Γ کمان انتقالی نرمال است اگر و فقط اگر $Aut(G,S)$ روی S انتقالی عمل کند و یال انتقالی نرمال است اگر و فقط اگر $Aut(G,S)$ یا روی S انتقالی عمل کند و یا روی S دارای دو مدار باشد که وارون یکدیگرند.

نتیجه ۲.۱. اگر گراف کیلی $\Gamma = Cay(G,S)$ یال انتقالی نرمال باشد، آنگاه تمام عناصر S دارای مرتبه ی یکسان هستند.

لم ۳.۱. گراف کیلی $\Gamma = Cay(G,S)$ را در نظر بگیرید. فرض کنید H مجموعه ی تمام عناصر مرتبه ی ۲ در گروه G باشد. اگر $G \neq \langle H \rangle$ و گراف Γ یال انتقالی نرمال و همبند باشد، آنگاه درجه‌ی گراف Γ زوج است.

نتیجه ۳.۱. اگر $\Gamma = Cay(G,S)$ یک گراف کیلی باشد که در آن G یک گروه آبلی متناهی است. در این صورت Γ نیم کمان انتقالی نرمال نخواهد بود.

گروه های غیر آبلی مرتبه ی $۹p$ که در آن pیک عدد اول است به یکی از صورت های زیر می باشد.

$$
\begin{aligned}
G_۱(۹p) &= \langle a,b \mid a^۹ = b^۳ = ۱, b^{-۱}ab = a^۴ \rangle \\
G_۲(۹p) &= \langle a,b,c \mid a^۳ = b^۳ = c^۳ = ۱, [a,b] = c, [a,c] = [b,c] = ۱ \rangle \\
G_۳(۹p) &= \langle a,b \mid a^p = b^۹ = ۱, b^{-۱}ab = a^r \rangle \\
G_۴(۹p) &= \langle a,b \mid a^p = b^۹ = ۱, b^{-۱}ab = a^s \rangle \\
G_۵(۹p) &= \langle a,b,c \mid a^p = b^۳ = c^۳ = [b,c] = [a,b] = ۱, c^{-۱}ac = a^t \rangle
\end{aligned}
$$

که در آن $r^۳ \equiv ۱(modp)$، $s^۹ \equiv ۱(modp)$ و $t^۳ \equiv ۱(modp)$. در این مقاله گراف کیلی یال انتقالی نرمال و کمان انتقالی نرمال گروه‌های غیر آبلی مرتبه‌ی $۹p$ ونیم کمان انتقالی نرمال بودن آن‌ها را بررسی می‌کنیم که نتایج زیر حاصل شده است.

در [۱] گراف‌های کیلی نرمال روی گروه‌های غیر آبلی از مرتبه‌ی $۴p$، در [۲] گراف‌های یال انتقالی از مرتبه‌ی ۴ روی گروه‌های غیر آبلی ساده و در [۴] گراف‌های کیلی یال انتقالی نرمال گروه‌های دو وجهی بررسی شده است.

۲ نتایج اصلی

قضیه ۱.۲. گراف کیلی $\Gamma = Cay(G_۱,S)$، همبند یال انتقالی نرمال است اگر و فقط اگر شرایط زیر برقرار باشد.

الف) درجه‌ی گراف، زوج، بزرگتر از ۲ باشد، $S = S^{-۱}$ و $G_۱ = \langle S \rangle$.

ب) $\{a^ib \mid (i,9)=1\} \subseteq T$ و یا $\{a^ib \mid i=3k, k=1,2\} \subseteq T$ و $S=T\cup T^{-1}$جایی‌که T و T^{-1} مدارهای عمل گروه $Aut(G_1,S)$ روی S هستند.

قضیه ۲.۲. گراف کیلی $\Gamma = Cay(G_2,S)$ ، همبند یال انتقالی نرمال است اگر و فقط اگر شرایط زیر برقرار باشد.

الف) درجه‌ی گراف، زوج، بزرگ‌تر از ۲ باشد، $S=S^{-1}$ و $G_2=\langle S\rangle$.

ب) $\{c^ia^ib \mid i=1,2\} \subseteq T$ و $S=T\cup T^{-1}$ جایی که T و T^{-1} مدارهای عمل گروه $Aut(G_2,S)$ روی S هستند.

قضیه ۳.۲. گراف کیلی $\Gamma = Cay(G_3,S)$ ، همبند یال انتقالی نرمال است اگر و فقط اگر شرایط زیر برقرار باشد.

الف) درجه‌ی گراف، زوج، بزرگ‌تر از ۲ باشد، $S=S^{-1}$ و $G_3=\langle S\rangle$.

ب) $\{a^lb, a^kb^4, a^tb^7\} \subseteq T$ که در آن l ،k و t دو به دو متمایزند و$1 \leq l,k,t \leq p-1$ و یا $\{a^lb, a^kb^3 \mid l\neq k, 1\leq l,k\leq p-1\} \subseteq T$ و $S=T\cup T^{-1}$ جایی‌که T و T^{-1} مدارهای عمل گروه $Aut(G_3,S)$ روی S هستند.

قضیه ۴.۲. گراف کیلی $\Gamma = Cay(G_4,S)$ ، همبند یال انتقالی نرمال است اگر و فقط اگر شرایط زیر برقرار باشد.

الف) درجه‌ی گراف، زوج، بزرگ‌تر از ۲ باشد، $S=S^{-1}$ و $G_4=\langle S\rangle$.

ب) $\{a^lb^j \mid 1\leq l\leq p-1, j$ثابت$\} \subseteq T$ و $S=T\cup T^{-1}$ جایی‌که T و T^{-1} مدارهای عمل گروه $Aut(G_4,S)$ روی S هستند.

قضیه ۵.۲. گراف کیلی $\Gamma = Cay(G_5,S)$ ، همبند یال انتقالی نرمال است اگر و فقط اگر شرایط زیر برقرار باشد.

الف) درجه‌ی گراف، زوج، بزرگ‌تر از ۲ باشد، $S=S^{-1}$ و $G_5=\langle S\rangle$.

ب) $\{a^ib^jc, a^{p-i}b^jc \mid 1\leq i\leq p-1, j$ثابت$\} \subseteq T$ و $S=T\cup T^{-1}$ جایی‌که T و T^{-1} مدارهای عمل گروه $Aut(G_5,S)$ روی S هستند.

نتیجه ۱.۲. تمام گراف‌های کیلی گروه‌های غیر آبلی مرتبه‌ی $9p$ یال انتقالی نرمال هستند ولی کمان انتقالی نرمال نیستند. بنابراین این گراف‌ها نیم کمان انتقالی نرمال می باشند.

مراجع

[1] M. Darafsheh, A. Assari, *Normal edge-transitive Cayley graphs on non-abelian groups of order* $4p$*,where* p *is a prime number*,Sci. China Math. **56(1)** (2013),213-219.

[2] X. G. Fang, C. H. Li and M. Y. Xu, *On edge-transitive Cayley graphs of valency four*,European J. Combin. **(25)** (2004),1107–1116.

[3] C. E. Praeger, *Finite normal edge-transitive Cayley graphs*, Bull Aust Math Soc. **(60)** (1999) , 207–220.

[4] A. A. Talebi, *Some normal edge-transitive Cayley graphs on dihedral groups*, J Math Comput Sci. **(2)** (2011),448–452.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۳۹ تا ۴۲.

پوستر

ارتباط زنجیرهای مارکوف و بسندگی از دیدگاه نظریه اطلاع

مهدی شمس
دانشکده علوم ریاضی، دانشگاه کاشان
mehdishams@kashanu.ac.ir

نسرین برقی اسکوئی
دانشکده علوم ریاضی، دانشگاه تبریز
n_barghi@tabrizu.ac.ir

چکیده

با توجه به اهمیت زنجیر مارکوف در نظریه اطلاع، تعریف احتمال شرطی این فرآیند تصادفی می‌تواند برحسب اطلاع توأم نیز تعریف شود. در این مقاله ارتباط بین مفهوم بسندگی با زنجیر مارکوف مطرح می‌شود که این ارتباط بر مبنای اصول نظریه اطلاع است.

واژه های کلیدی: تابع بسنده، زنجیر مارکوف، اطلاع توأم، آنتروپی.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۹۴A۱۵، ۶۰J۱۰، ۹۷D۴۰.

۱ مقدمه

امروزه، تئوری فرآیندهای مارکوف یک بخش اصلی از نظریه احتمال است و کاربردهای گسترده‌ای در بسیاری از علوم دیگر دارد. مارکوف آغاز کننده این نظریه در سال ۱۹۰۷ بوده است. یکی از اولین

کاربردهای این تئوری، تحقیق روی حروف صدادار و بی‌صدا در زبان روسی بوده است. اگرچه زبان شناسان مدرن نشان داده‌اند که در برخی زبان‌ها خصوصیت زنجیر مارکوف برقرار نیست. شاخه نظریه اطلاع وقتی به کار می‌آید که احتمال وقوع یک نماد در یک پیام بستگی به تعداد متناهی نمادهای قبلی خواهد داشت. در این حالت می‌توان از منبع اطلاع با حافظه نام برد و دنباله تولید شده توسط چنین منبعی را یک زنجیر مارکوف در نظر گرفت. در این مقاله با تعریف تابع بسنده و بررسی مفهوم آن از طریق احتمال شرطی، ارتباط بین مفهوم بسندگی با زنجیر مارکوف نتیجه گرفته می‌شود.

فضای احتمال $(\Omega, \mathscr{F}, P)$ را در نظر بگیرید که فضای نمونه Ω متناهی است. متغیر تصادفی گسسته X با مقادیر $x_۱, \ldots, x_N$ را در نظر بگیرید که $P(X = x_k) = p_k$، $k = ۱, \ldots, N$. آنتروپی X به صورت $H(X) = \sum_{k=۱}^{N} p_k log_۲ \frac{۱}{p_k}$ تعریف می‌شود [۱]. به وضوح $H(X) \geq ۰$ و شرط لازم وکافی برای این که $H(X) = ۰$ آن است که $N = ۱$، یعنی X یک متغیر تصادفی تباهیده باشد. آنتروپی مقدار اطلاعاتی که از X دریافت شده است را بعد از مشاهده مقدار واقعی X نشان می‌دهد. حال اگر f یک تابع با دامنه $\{x_۱, \ldots, x_N\}$ باشد به طوری که برای $i \neq j$، $f(x_i) \neq f(x_j)$، در این صورت $P(f(X) = f(x_k)) = P(X = x_k) = p_k$ و از این رو $H(f(X)) = H(X)$. در حالت کلی‌تر برای هر تابع f، $H(f(X)) \leq H(X)$. از این که $H(X)$ تنها به توزیع $\mathscr{P} = \{p_۱, \ldots, p_N\}$ مربوط به X بستگی دارد، برخی مواقع آنتروپی به صورت $H(\mathscr{P}) = \sum_{k=۱}^{N} p_k log_۲ \frac{۱}{p_k}$ نوشته می‌شود. حال اگر $\mathscr{Q} = \{q_۱, \ldots, q_N\}$ احتمال‌های مربوط به متغیر تصادفی دیگر Y باشد و $N \geq ۲$، واگرایی توزیع $\mathscr{P}$ از $\mathscr{Q}$ را به صورت $D(\mathscr{P}, \mathscr{G}) = \sum_{k=۱}^{N} p_k log_۲ \frac{p_k}{q_k}$ تعریف می‌کنند که آن را فاصله کولبک–لایبلر یا آنتروپی نسبی نیز گویند [۲]. به راحتی مشاهده می‌شود که $D(\mathscr{P}, \mathscr{G}) \geq ۰$ و تساوی برقرار است اگر و تنها اگر برای هر $k = ۱, \ldots, N$، $p_k = q_k$. برای متغیر تصادفی گسسته X که در بالا تعریف شد، آنتروپی بیشین است، اگر و تنها اگر برای $k = ۱, \ldots, N$، $p_k = \frac{۱}{N}$ و در این حالت $H(X) = log_۲ N$. اطلاع توأم متغیرهای تصادفی X و Y که هر یک تعداد متناهی از مقادیر مجزا را اختیار می‌کند به صورت

$$I(X, Y) = H(X) + H(Y) - H(X, Y)$$

تعریف می‌شود که $H(X, Y)$، آنتروپی (X, Y) است [۳]. به وضوح $I(X, Y) \geq ۰$ و شرط لازم و کافی برای برقراری تساوی استقلال X و Y است. کمیت $I(X, Y)$ مقدار اطلاع به دست آمده راجع به متغیر تصادفی X بر اساس مشاهدات متغیر تصادفی Y را اندازه می‌گیرد. اگر $\mathscr{P}_k$ معرف خانواده توزیع‌های شرطی $\{p_{j|k}, j = ۱, \ldots, N\}$ باشد که در آن $p_{j|k} = P(X = x_j | Y = y_k)$ میانگین آنتروپی شرطی X به شرط Y به صورت $H(X|Y) = \sum_{k=۱}^{N} q_k H(\mathscr{P}_k)$ تعریف می‌شود و به راحتی می‌توان نشان داد که $H(X|Y) = H(X, Y) - H(Y) \geq ۰$ و $I(X, Y) = H(X) - H(X|Y)$. همچنین $I(X, Y) \leq min(H(X), H(Y))$. برای متغیرهای تصادفی $\{X_i : i = ۱, \ldots, n\}$ که $n > ۲$ و تعداد متناهی از مقادیر مجزا را اختیار می‌کنند داریم: $H(X_۱, \ldots, X_n) \leq \sum_{k=۱}^{n} H(X_k)$ و شرط لازم و کافی برای برقراری تساوی آن است که $X_۱, \ldots, X_N$ مستقل باشند. قرار دهید

$$I(X_۱, \ldots, X_N) = H(X_۱, \ldots, X_N) - \sum_{k=۱}^{N} H(X_k)$$

که آن را اطلاع توأم فراهم آمده توسط متغیرهای تصادفی $X_۱,\ldots,X_N$ گویند. شرط لازم و کافی برای استقلال $X_۱,\ldots,X_n$ آن است که اطلاع توأم آن‌ها صفر باشد و یا معادلاً برای هر $k=۱,\ldots,n-۱$، $I((X_۱,\ldots,X_k),X_{k+۱})=۰$. اگر متغیرهای تصادفی مستقل $X_۱,\ldots,X_n$ و متغیر تصادفی Z همگی تعداد متناهی از مقادیر مجزایی را اختیار کنند می‌توان ثابت کرد:

$$\sum_{k=۱}^{n} I(X_k,Z) \leq I((X_۱,\ldots,X_k),Z).$$

۲ تابع بسنده و زنجیرهای مارکوف

عنصر اصلی فرمول‌بندی خاصیت مارکوف برحسب آنتروپی و اطلاع استفاده از دیدگاه تابع بسنده است.

تعریف ۱.۲. اگر X و Y متغیرهای تصادفی روی یک فضای احتمال $(\Omega,\mathscr{F},P)$ باشند به طوری که $I(X,Y)<\infty$ و g یک تابع با مقدار حقیقی و بورل اندازه‌پذیر باشد، در این صورت متغیر تصادفی $g\circ X=g(X)$ را یک تابع بسنده از متغیر تصادفی X برای متغیر تصادفی Y گویند هرگاه $I(g(X),Y)=I(X,Y)$. به عبارت دیگر $g(X)$ برای Y بسنده است هرگاه $g(X)$ شامل تمام اطلاعات متغیر تصادفی Y که توسط متغیر تصادفی X فراهم می‌آیند باشد.

قضیه ۲.۲. اگر متغیرهای تصادفی X و Y و با تکیه‌گاه‌های به ترتیب $\{x_۱,\ldots,x_N\}$ و $\{y_۱,\ldots,y_M\}$ و تابع با مقادیر حقیقی و بورل اندازه پذیر g را در نظر بگیرید، شرط لازم و کافی برای آن که $g(X)$ یک تابع بسنده برای Y باشد آن است که توزیع احتمال شرطی Y به شرط X تنها به مقدار $g(X)$ بستگی داشته باشد یعنی اگر برای $i=۱,\ldots,N$ و $j=۱,\ldots,N$، $g(x_i)=g(x_j)$، آن گاه

$$P(Y=y_k|X=x_i)=P(Y=y_k|X=x_j). \qquad (۱)$$

به عبارت دیگر X و Y متغیرهای تصادفی مستقل هستند هنگامی که مقدار $g(X)$ ثابت باشد یعنی برای هر z که $P(g(X)=z)>۰$ داریم:

$$P(X=x_j,Y=y_k|g(X)=z)=P(X=x_j|g(X)=z)P(Y=y_k|g(X)=z). \qquad (۲)$$

برهان. تعریف کنید $\mathscr{P}=\{p_۱,\ldots,p_N\}$ که $p_j=P(X=x_j)$، $\mathscr{Q}=\{q_۱,\ldots,q_M\}$ که $q_k=P(Y=y_k)$ و $\mathscr{R}=\{r_{jk},j=۱,\ldots,N,k=۱,\ldots,M\}$ که در آن $r_{jk}=P(X=x_j,Y=y_k)$. فرض کنید $\{z_۱,\ldots,z_s\}$ مجموعه مقادیر مجزا از تابع g که مقادیر خود را روی مجموعه $\{x_۱,\ldots,x_N\}$ اختیار می‌کنند باشد و قرار دهید $g(x_j)=z_l$، $j\in D_l$ که $D_۱,\ldots,D_s$ یک افراز از مجموعه $\{۱,\ldots,N\}$ است. بعلاوه تعریف کنید $v(x_j)=l$ در حالتی که $j\in D_l$، $t_{lk}=P(g(X)=z_l,Y=y_k)$ و $t_l=P(g(X)=z_l)$. اعداد

$$u_{jk}=\frac{t_{v(x_j)k}\cdot p_j}{t_{v(x_j)}},\ \ j=۱,\ldots,N,\ \ k=۱,\ldots,M$$

از یک توزیع احتمال $\mathscr{U} = \{u_{jk}\}$ می‌آیند و $I(X,Y) - I(g(X),Y) = D(\mathscr{R},\mathscr{U})$. از این رو شرط لازم و کافی برای $I(X,Y) = I(g(X),Y)$ آن است که $\mathscr{R} = \mathscr{U}$. یعنی اگر $r_{jk} = \dfrac{t_{v(x_j)k} \cdot p_j}{t_{v(x_j)}}$ و این یعنی اگر $g(x_i) = g(x_j)$، آن گاه $\frac{r_{jk}}{p_j} = \frac{r_{ik}}{p_i}$ و در پی آن (۱) شرط لازم و کافی برای آن است که $I(g(X),Y) = I(X,Y)$. بعلاوه اگر $g(x_j) = z_l$، آن گاه

$$P(X = x_j, Y = y_k | g(X) = z_l) = \frac{P(X = x_j, Y = y_k)}{P(g(X) = z_l)}$$
$$= P(X = x_j | g(X) = z_l) P(Y = y_k | X = x_j)$$

و لذا (۲) معادل است با $P(Y = y_k | X = x_j) = P(Y = y_k | g(X) = z_l)$ به شرط این که $g(x_j) = z_l$. بنابراین (۱) و (۲) معادل هستند. □

تعریف ۳.۲. دنباله $\{X_n\}_{n\in\mathbb{N}}$ از متغیرهای تصادفی با مقادیر حقیقی روی فضای احتمال $(\Omega, \mathscr{F}, P)$ که تعداد متناهی از مقادیر را اختیار می‌کند را زنجیر مارکوف گسسته-پارامتر گویند هرگاه برای $n \in \mathbb{N}$، $I((X_1, \ldots, X_n), X_{n+1}) = I(X_n, X_{n+1})$.

نتیجه ۴.۲. تساوی بالا بیان کننده این حقیقت است که برای یک زنجیر مارکوف گسسته-پارامتر اطلاعی که راجع به X_{n+1} بر اساس مشاهدات $X_1, \ldots, X_n$ به دست می آید برابر با اطلاعی است که راجع به X_{n+1} بر اساس تنها مشاهده آخر یعنی X_n به دست می آید و از این رو، X_n که به صورت یک تابع از $X_1, \ldots, X_n$ است برای هر $n \in \mathbb{N}$ یک تابع بسنده برای X_{n+1} می‌باشد. به طور معادل

$$P(X_{n+1} = x_{n+1} | X_1, \ldots, X_n) = P(X_{n+1} = x_{n+1} | X_n).$$

مراجع

[1] Thomas M. Cover, Joy A. Thomas, Elements of Information Theory, 2nd edition, Wiley, 2006.

[2] David J.C. MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003.

[3] Robert M. Gray, Entropy and Information Theory, Springer, 2009.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۴۳ تا ۴۷.

سخنرانی

آزمون های فرضیه‌ی بهینه از دیدگاه آنتروپی نسبی

مهدی شمس
دانشکده علوم ریاضی، دانشگاه کاشان
mehdishams@kashann.ac.ir

غلامرضا حسامیان
دانشکده علوم، تهران، دانشگاه پیام نور
gh.hesamian@pnu.ac.ir

چکیده

در این مقاله به بررسی کابردهایی از نظریه‌ی اطلاع در آزمون‌های فرضیه‌ی آماری می‌پردازیم. در ابتدا رابطه نسبت درست‌نمایی با فاصله کولبک-لایبلر را پیدا می‌کنیم. در حالتی که خطای نوع اول ثابت است، خطای نوع دوم به گونه‌ای کمینه می‌شود که لگاریتم آن متناسب با فاصله آنتروپی نسبی بین دو توزیع داده شده در فرضیه‌های آماری است. در انتها آزمون‌های بیزی را از دیدگاه نظریه‌ی اطلاع بررسی می‌کنیم.

واژه های کلیدی: آنتروپی نسبی، لم نیمن-پیرسن، پرتوان‌ترین آزمون، آزمون نسبت درست‌نمایی، آزمون بیز.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۶۲F۰۳، ۶۲F۱۵، ۵۴C۷۰، ۹۴A۱۵.

۱ مقدمه

در جامعه امروزی با سیستم‌هایی سروکار داریم که اساس کار آن‌ها انتقال، ذخیره‌سازی و پردازش اطلاعات است. نظریه‌ی اطلاع به بررسی چگونگی ارسال سریع و دقیق داده‌ها از یک منبع و از طریق یک کانال به یک گیرنده و به چگونگی ذخیره و فشرده‌سازی اطلاعات به منظور ارسال سریع آن‌ها می‌پردازد. در نظریه‌ی اطلاع به دو سوال اصلی در نظریه‌ی ارتباطات پاسخ داده می‌شود. یکی آنتروپی نهایی‌ترین فشرده‌سازی برای داده‌هاست و دیگر اینکه سرعت مخابره نهایی، ظرفیت کانال است [۲]. مبانی نظریه‌ی اطلاع از سال ۱۹۴۸ توسط شانون آغاز شد و کولبک در حدود سال ۱۹۵۰ برای اولین بار مطالعات خود را در زمینه ارتباط بین این شاخه با آمار شروع کرد [۲]. در این مقاله کاربردهایی از نظریه‌ی اطلاع در آزمون‌های فرضیه‌ی آماری مطرح می‌شوند. در ابتدا با استفاده از لم نیمن–پیرسن، پرتوان‌ترین آزمون‌ها که همان آزمون‌های نسبت درست‌نمایی هستند مورد بررسی قرار می‌گیرند. ثابت می‌شود لگاریتم نسبت درست‌نمایی برابر با تفاضل بین فواصل آنتروپی نسبی نمونه‌ها با هر دو نوع توزیع داده شده در آزمون‌های فرضیه‌ی آماری است. سپس با ثابت قرار دادن احتمال خطای نوع اول، نشان داده می‌شود که احتمال خطای نوع دوم به صورت نمایی کوچک می‌شود و نرخ نمایی آن برابر با فاصله کولبک–لایبلر بین دو توزیع است. در پایان با کمینه کردن ترکیب خطی از دو نوع خطا با ضرایب توزیع‌های پیشین متناظر آن‌ها از دیدگاه بیزی به دنبال یک آزمون بهینه می‌گردیم.

۲ نظریه‌ی اطلاع و آزمون‌های فرضیه‌ی آماری

فرض کنید $X_1, \cdots, X_n \overset{iid}{\sim} Q(x)$ و آزمون فرضیه‌ی $H_0 : Q = P_1$ در مقابل $H_1 : Q = P_2$ و تابع تصمیم $g(\mathbf{x}) = I_{\bar{C}}(\mathbf{x}) + 2I_C(\mathbf{x})$ را در نظر بگیرید که در آن C ناحیه‌ی بحرانی است. احتمال خطای نوع اول و دوم به‌صورت $\alpha = P(g(X) = 2 \mid H_0 \text{ درست}) = P_1^n(C)$ و $\beta = P(g(X) = 1 \mid H_1 \text{ درست}) = P_2^n(\bar{C})$ تعریف می‌شوند. در حالت کلی با افزایش حجم نمونه می‌توان هر دو خطا را کاهش داد. اگر حجم نمونه ثابت باشد، این امر امکان‌پذیر نیست و برای این منظور با ثابت فرض کردن α، احتمال خطای β را کمینه می‌کنند که لم نیمن–پیرسن بر این اساس استوار است [۱]. در این لم برای $k \geq 0$ ناحیه‌ی $C_n(k) = \{\mathbf{x} : P_2(\mathbf{x})/P_1(\mathbf{x}) > k\}$ و احتمال‌های خطای نوع اول و دوم متناظر با ناحیه‌ی مذکور را در نظر می‌گیرند، یعنی $\alpha^* = P_1^n(C_n(k))$ و $\beta^* = P_2^n(\bar{C}_n(k))$. اگر ناحیه‌ی تصمیم دیگر با خطاهای متناظر α و β طوری باشد که $\alpha \leq \alpha^*$، دراین‌صورت $\beta \geq \beta^*$. در اصطلاح ناحیه‌ی $C_n(k)$ آزمونی می‌سازد که آن را پرتوان‌ترین آزمون گویند. به $P_1(\mathbf{x})/P_2(\mathbf{x})$ نسبت درست‌نمایی گویند و لم نیمن–پیرسن نشان می‌دهد که پرتوان‌ترین آزمون، یک آزمون نسبت درست‌نمایی است [۲]. لگاریتم نسبت درست‌نمایی

برابر است با:

$$L(\mathbf{X}) = \log\frac{P_۱(\mathbf{X})}{P_۲(\mathbf{X})} = \log\frac{\prod_{i=۱}^{n} P_۱(X_i)}{\prod_{i=۱}^{n} P_۲(X_i)} = \sum_{i=۱}^{n}\log\frac{P_۱(X_i)}{P_۲(X_i)} = \sum_{a\in\mathscr{X}} nP_{\mathbf{X}}(a)\log\left(\frac{P_۱(a)}{P_۲(a)}\frac{P_{\mathbf{X}}(a)}{P_{\mathbf{X}}(a)}\right)$$
$$= \sum_{a\in\mathscr{X}} nP_{\mathbf{X}}(a)\log\frac{P_{\mathbf{X}}(a)}{P_۲(a)} - \sum_{a\in\mathscr{X}} nP_{\mathbf{X}}(a)\frac{P_{\mathbf{X}}(a)}{P_۱(a)} = nD(P_{\mathbf{X}}\parallel P_۲) - nD(P_{\mathbf{X}}||P_۱),$$

که در آن $D(p\parallel q)$ آنتروپی نسبی یا فاصله‌ی کولبک-لایبلر است و فاصله‌ی بین دو تابع چگالی احتمال p و q را اندازه‌گیری می‌کند. بنابراین $L(\mathbf{X})$ برابر با تفاضل بین فواصل آنتروپی نسبی نمونه‌ی هر دو توزیع است و

$$\mathbf{x} \in C_n(k) \quad \Leftrightarrow D(P_{\mathbf{X}}\parallel P_۲) - D(P_{\mathbf{X}}\parallel P_۱) < -\frac{۱}{n}\log k.$$

از این‌که ناحیه‌ی رد فرضیه‌ی $H_۰$ یعنی C یک مجموعه‌ی محدب است به کمک قضیه‌ی سانوف [۲]، احتمال خطا توسط آنتروپی نسبی نزدیک‌ترین عضو C به $P_۱$ تعیین می‌شود، بنابراین احتمال خطای نوع اول برابر است با $\alpha_n = P_۱^n(P_{\mathbf{X}}\in C) = ۲^{-۲D(P_۱^*\|P_۱)}$ که در آن $P_۱^*$ نزدیک‌ترین عضو C به توزیع $P_۱$ است. به طور مشابه $\beta_n = ۲^{-۲D(P_۲^*\|P_۲)}$ که $P_۲^*$ نزدیک‌ترین عضو $\bar{C}$ به توزیع $P_۲$ است. اکنون با استفاده از روش ضرایب لاگرانژ $D(P\parallel P_۲)$ را نسبت به شرط $D(P\parallel P_۲) - D(P\parallel P_۱) = -\log k/n$ کمینه می‌کنیم:

$$J(P) = \sum P(x)\log(P(x)/P_۲(x)) + \lambda\sum P(x)\log(P(x)/P_۲(x)) + \nu\sum P(x).$$

با مشتق‌گیری نسبت به $P(x)$ و قرار دادن آن برابر صفر نتیجه می‌شود

$$\log(P(x)/P_۲(x)) + ۱ + \lambda\log(P(x)/P_۲(x)) + \nu = ۰.$$

با حل مجموعه معادلات مقدار کمینه P به صورت

$$P_۲^* = P_{\lambda*} = P_۱^{\lambda}(x)P_۲^{۱-\lambda}(x)/\sum_{a\in\mathscr{X}} P_۱^{\lambda}(a)P_۲^{۱-\lambda}(a) \qquad (۱)$$

به دست می‌آید و λ طوری انتخاب می‌شود که $D(P_{\lambda^*}\parallel P_۱) - D(P_{\lambda^*}\parallel P_۲) = -\log k/n$. اکنون با ثابت فرض کردن خطای نوع اول، خطای نوع دوم را کمینه می‌کنیم.

قضیه ۱.۲: فرض کنید $X_۱,\cdots,X_n \overset{iid}{\sim} Q(x)$ و آزمون فرضیه‌ی $H_۰ : Q = P_۱$ در مقابل $H_۱ : Q = P_۲$ مورد نظر باشد که در آن $D(P_۱\parallel P_۲) < \infty$. اگر ناحیه‌ی رد آزمون $C_n \subseteq \mathscr{X}^n$ و احتمال خطای نوع اول و دوم به ترتیب $\alpha_n = P_۱^n(C_n)$ و $\beta_n = P_۲^n(\bar{C}_n)$ باشند، برای هر $۰ < \varepsilon < ۰/۵$ باتعریف $\beta_n^\varepsilon = \min_{C_n\subseteq\mathscr{X}^n}\beta_n$ داریم $\lim_{n\to\infty}\log\beta_n^\varepsilon/n = -D(P_۱\parallel P_۲)$.

از قضیه‌ی ۱.۲ می‌توان نتیجه گرفت که اگر $\alpha_n < \varepsilon$، می‌توان به کمترین مقدار خطای نوع دوم یعنی $\beta_n = ۲^{-nD}$ دست یافت که D آنتروپی نسبی بین دو توزیع $P_۱$ و $P_۲$ است.

در پایان به مسأله‌ی کمینه‌سازی ترکیب وزنی خطاها از دیدگاه بیزی می‌پردازیم. فرض کنید π_1 و π_2 به ترتیب احتمال‌های پیشین متناظر با فرضیه‌های H_0 و H_1 باشند، در این صورت احتمال خطای کلی به‌صورت $P_e^{(n)} = \pi_1\alpha_n + \pi_2\beta_n$ است.

قضیه ۲.۲: بهترین نما در احتمال بیزی خطا برابر با $D^* = \lim_{n\to\infty} -\frac{1}{n}\log\min_{C_n\subseteq x^n} P_e^{(n)}$ است و $D^* = D(P_{\lambda^*} \parallel P_1) = D(P_{\lambda^*} \parallel P_2)$ که در آن P_λ به‌صورت (۱) است و λ^* در شرط

$$D(P_{\lambda^*} \parallel P_1) = D(P_{\lambda^*} \parallel P_2)$$

صدق می‌کند.

با توجه به ناحیه‌ی رد آزمون بیز، $C = \{\mathbf{x} : \pi_1 P_1(\mathbf{x})/\pi_2 P_2(\mathbf{x}) < 1\}$، احتمال خطا

$$\begin{aligned} P_e = \pi_1\alpha_n + \pi_2\beta_n &= \sum_C \pi_1 P_1 + \sum_{\bar{C}} \pi_2 P_2 = \sum \min\{\pi_1 P_1, \pi_2 P_2\} \\ &\le \sum (\pi_1 P_1)^\lambda (\pi_2 P_2)^{1-\lambda} \le \sum P_1^\lambda P_2^{1-\lambda} \end{aligned}$$

می‌باشد. برای یک نمونه تصادفی n تایی داریم:

$$\begin{aligned} P_e^{(n)} &\le \sum \pi_1^\lambda \pi_2^{1-\lambda} \prod_i P_1^\lambda(x_i) P_2^{1-\lambda}(x_i) = \pi_1^\lambda \pi_2^{1-\lambda} \prod_i \sum P_1^\lambda(x_i) P_2^{1-\lambda}(x_i) \\ &\le \prod_{x_i} \sum P_1^\lambda P_2^{1-\lambda} = \left(\sum P_1^\lambda P_2^{1-\lambda}\right)^n. \end{aligned}$$

مثال ۳.۲ فرض کنید متوسط و انحراف معیار امتیازات بازیکنان لیگ برتر فوتبال به ترتیب ۲۶۰ و ۱۵ و برای بازیکنان والیبال ۲۴۰ و ۱۵ باشد. یک گروه ۱۰۰ تایی از بازیکنان والیبال از یک لیگ (که به تصادف انتخاب شده است) به طور متوسط بیش از ۲۵۰ امتیاز کسب کرده‌اند و باید عضو لیگ برتر انتخاب شوند. برای بررسی صحت این دو ادعا نشان می‌دهیم امتیازات این بازیکنان دارای توزیعی با میانگین ۲۵۰ و انحراف معیار ۱۵ است. برای این منظور آزمون فرضیه‌ی $H_0 : f_1 = N(1, \sigma^2)$ در مقابل $H_1 : f_2 = N(-1, \sigma^2)$ را در نظر بگیرید. آزمون نسبت درست‌نمایی و آزمون بیز به ترتیب ناحیه‌ی رد $\bar{X} < k$ و $\bar{X} < 0$ را پیشنهاد می‌کنند. اکنون فرض کنید مرتکب یک خطای نوع اول شده‌ایم. توزیع شرطی نمونه به شرط مرتکب شدن خطا به f^* میل می‌کند. با توجه به تقارن، این حقیقت متناظر با $\lambda = 0.5$ در (۱) است. برای محاسبه‌ی f^* به صورت زیر عمل می‌کنیم:

$$\begin{aligned} f^*(x) &= \frac{(1/\sqrt{2\pi\sigma^2} exp(-(x-1)^2/2\sigma^2))^{0.5} (1/\sqrt{2\pi\sigma^2} exp(-(x+1)^2/2\sigma^2))^{0.5}}{\int_\infty^{-\infty} (1/\sqrt{2\pi\sigma^2} exp(-(x-1)^2/2\sigma^2))^{0.5} (1/\sqrt{2\pi\sigma^2} exp(-(x+1)^2/2\sigma^2))^{0.5} dx} \\ &= \frac{1/\sqrt{2\pi\sigma^2} exp(-(x^2+1)/2\sigma^2)}{\int_\infty^{-\infty} 1/\sqrt{2\pi\sigma^2} exp(-(x^2+1)/2\sigma^2) dx} = \frac{1}{\sqrt{2\pi\sigma^2}}\, e^{-\dfrac{x^2}{2\sigma^2}} = N(0, \sigma^2). \end{aligned}$$

مراجع

[1] Lehmann, E. L. and Romano, J. P. (2005), Testing Statistical Hypotheses, 3rd edition,Springer, New York.

[2] Robert M. Gray, Entropy and Information Theory, Springer, 2009

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۴۹ تا ۵۳.

پوستر

پیاده سازی نرم افزاری الگوریتم زمان چندجمله ای ازمون اول بودن

مجید فرهادی
دانشکده علوم ریاضی و کامپیوتر، دانشگاه دامغان
Farhadi@du.ac.ir

مصطفی بهرامی
دانشکده برق، دانشگاه صنعتی مالک اشتر
mostafa.bahrami2013@gmail.com

چکیده

آزمون AKS مخفف Agrawal–Kayal–Saxena یک آزمون قطعی در تشخیص اعداد اول می‌باشد که توسط سه هندی به نام‌های آگراوال، کایال و ساکسن از دانشگاه کانپور هند در سال ۲۰۰۲ ابداع شده است. این سه نفر نتیجه تحقیقات خود را طی مقاله‌های به نام " PRIMES is in P " منتشر کردند و موفق به دریافت جوایز Godel و Fulkerson شدند.این الگوریتم نخستین الگوریتمی است که در هر چهار خاصیت قطعیت، عمومیت، در زمان چندجمله ای بودن و بدون شرط بودن هم‌زمان صدق می‌نماید. در این مقاله یک پیاده سازی نرم افزاری مناسب از این الگوریتم که قابلیت ترکیب با شبیه سازی الگوریتم کوانتومی مربوطه دارد ارائه می‌شود.

واژه های کلیدی: الگوریتم‌های عامل یابی ، الگوریتم شور، آزمون اول بودن.

۱ انواع الگوریتم AKS:

این الگوریتم در چهار نوع زیر ارائه شده است. تمامی این الگوریتم‌ها بر پایه یک قضیه در نظریه اعداد بنا شده اند.

Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, and $(a,b) = 1$ Then n is prime if and only if $(X+a)^n = X^n + a(mod n)$

۲ الگوریتم AKS Original:

این الگوریتم اولین الگوریتمی بود که تیم سه نفره آگراوال[۱]، کایال [۲] و ساکسنا [۳] در سال ۲۰۰۲ ارائه دادند. پیچیدگی زمانی این الگوریتم برابر $O^{\sim}(Log^{12} n)$ می‌باشد. این الگوریتم دارای سه مرحله کلی زیر میباشد.

d) Perfect power checking the input n

e) Find r, q = Largest Prime Factor(r) that $q \geq 4\sqrt{r}logn$ & $n^{\frac{r-1}{q}} \neq 1(mod\ r)$

f) $a = 1$ to $2\sqrt{r}logn$ check $(x-a)^n \neq x^n - a(mod\ x^r - 1, n)$

شبه کد این الگوریتم به صورت زیر میباشد.

```
Input:   integer n > 1
If(n is of the form  a^b , b> 1) output COMPOSITE;
 r = 2;
while (r< n ){
                 If(gcd(n, r ≠ 1) ) output COMPOSITE
                 If( r is prime)
                     Let q be the largest prime factor of r-1;
                     If( q > 4 √r  log n)  and  (n^((r-1)/q)  ≠ 1 (mod r))
                                   Break;
      r = r + 1;
 }
for  a=1  to  2 √r log n
             If ( (x-a)^n  ≠ (x^n - a)  (mod x^r - 1,n)) output COMPOSITE
```

Agrawal[۱]
Kayal[۲]
Saxena[۳]

13. Output PRIME;

۳ الگوریتم۳ AKS Version:

این الگوریتم در سال ۲۰۰۳ جهت بهبود پیچیدگی زمانی الگوریتم قبلی معرفی گردید. پیچیدگی زمانی این الگوریتم برابر $O^{\sim}(Log^{۱۰٫۵}n)$ است.این الگوریتم از سه مرحله تشکیل شده است.

a) Perfect power checking the input n
b) Find $r, O_r(n) \geqslant 4log^2n$
c) $a = 1to[2\sqrt{\phi r}logn]$ check $(x+a)^n \neq x^n + a(mod\ x^r - 1, n)$

۴ الگوریتم AKS By Daniel Bernstein:

این الگوریتم نیز در سال ۲۰۰۳ جهت بهبود پیچیدگی زمانی الگوریتم اصلی ارائه شد. این الگوریتم دارای سه مرحله اصلی میباشد.

a) Perfect Power Checking the input n
b) Find r ,q=Largest Prime Factor(r) that$\binom{2q-1}{q} \geqslant 2^{(2\lfloor\sqrt{r}\rfloor logn)}$ & $n^{(r-1)/q} \leqslant 1$
c) $a = 1\ to\ 2\sqrt{r}logn\ check(x-a)^n \equiv x^n - a(mod\ x^r - 1, n)$

۵ الگوریتم AKS Conjecture:

این الگوریتم سریع‌ترین الگوریتم AKS موجود است که پیچیدگی زمانی آن برابر $O^{\sim}(Log^{۳}n)$ می‌باشد و بسیار سریع‌تر از الگوریتم‌های پیشین است. البته درستی این الگوریتم تاکنون اثبات نشده است. این الگوریتم درواقع از حدس زیر استفاده می‌کند.
if$(x-a)^n \equiv x^n - 1(mod\ x^r - 1, n)$,then weather n is prime or $n^2 \equiv 1(modr)$

۶ پیاده سازی روش AKS:

این نرم افزار به منظور پیاده‌سازی انواع مختلف الگوریتم AKS در تشخیص اول بودن یک عدد طراحی شده است. در طراحی این نرم افزار از زبان ++VC و پلتفرم MFC استفاده شده است. جهت انجام اعمال ریاضی (عملیات بر روی چندجمله ای‌ها، اعمال ریاضی بر روی اعداد بسیار بزرگ و ...) از کتابخانه آماده

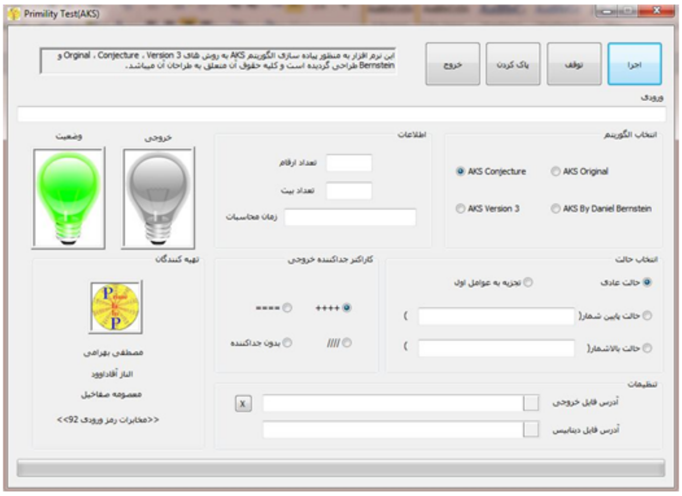
و رایگان NTL نوع ۶ استفاده شده که این کتابخانه به زبان C++ نوشته شده است. از قابلیت‌های این نرم افزار می‌توان به موارد زیر اشاره کرد:

- تعیین اول بودن یا نبودن یک عدد به وسیله الگوریتم AKS و انواع مختلف آن شامل:

Original AKS - Conjecture AKS - 3 Version AKS - D.Bernstein AKS

- ذخیره اعداد اول بیشتر و یا کمتر از یک عدد بخصوص و با تعداد دلخواه در یک فایل با فرمت دلخواه جهت استفاده در خود نرم افزار به عنوان دیتابیس در حالت تجزیه و یا استفاده در نرم افزار های دیگر(مثلا ذخیره ۱۰۰۰۰۰۰۰۰ عدد اول بزگتر از ۱ در یک فایل و ...)

- تجزیه اعداد به عوامل اول به روش های تقسیمات متوالی و یا با استفاده از پایگاه داده شامل اعداد اول ذخیره شده توسط نرم افزار صفحه اصلی نرم افزار به صورت زیر میباشد



بخش انتخاب حالت:

- **حالت عادی:** از این حالت می‌توانید جهت تست اول بودن یا نبودن یک عدد استفاده نمایید.
- **حالت پایین شمار:** با انتخاب این حالت می‌توانید از یک عدد شروع نموده و تعداد مشخصی عدد اول کمتر از آن را در یک فایل با فرمت دلخواه ذخیره نمایید .
- **حالت بالا شمار:** با انتخاب این حالت می‌توانید از یک عدد شروع نموده و تعداد مشخصی عدد اول بیشتر از آن را در یک فایل با فرمت دلخواه ذخیره نمایید.
- **تجزیه به عوامل اول:** از این حالت می‌توانید جهت تجزیه اعداد به عوامل اولشان با استفاده از دو الگوریتم تقسیمات متوالی و دیتابیس اعداد اول استفاده نمایید .

۷ حالت های مختلف نرم افزار:

حالت تست اول بودن :
در این بخش می‌توان با انتخاب الگوریتم مورد نظر اول بودن یک عدد را به وسیله یکی از الگوریتم‌های AKS تست نمود.
ذخیره اعداد اول:
به‌وسیله این نرم افزار می‌توان تعداد مشخصی عدد اول را به صورت بالا شمار و یا پایین شمار در یک فایل ذخیره نمود. از این ویژگی می‌توان جهت تولید فایل پایگاه داده جهت استفاده در بخش تجزیه اعداد استفاده نمود. هم‌چنین می‌توان از این بخش جهت تولید اعداد اول بزرگ استفاده نمود.

۸ تجزیه به عوامل اول:

از این حالت می‌توانید جهت تجزیه عدد ورودی به عوامل اولش و با الگوریتم دلخواه استفاده نمایید. در این حالت می‌توان از دو روش مختلف جهت تجزیه عدد مورد نظر استفاده کرد:
روش اول: اگر فایل دیتابیس اضافه نشود، نرم افزار با روش تقسیمات متوالی از عدد ۲ شروع کرده عمل تقسیم را انجام می‌دهد تا عوامل اول را پیدا نماید.
روش دوم: در این روش از یک دیتابیس که محتوی اعداد اول می‌باشد استفاده می‌شود و نرم افزار جهت تشخیص عوامل اول از اعداد درون این دیتابیس استفاده می‌نماید. این روش بسیار سریع تر از روش اول است.

مراجع

[1] R. G. Salembier and P. Southerington, An Implementation of the AKS Primality Test, Computer Engineering, 2005.

[2] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Annals of Math., 160 (2004) 781–793.

[3] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. on Computing, 26 (1997) 1484-1509.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۵۵ تا ۵۹.

پوستر

بهبود تحلیل جبری رمز جریانی QUAD با استفاده از گراف جزء بندی شده

هدی ترابی زاده
دانشکده علوم ریاضی و کامپیوتر، دانشگاه دامغان
hoda_tb29@yahoo.com

مجید فرهادی
دانشکده علوم ریاضی و کامپیوتر، دانشگاه دامغان
Farhadi@du.ac.ir

احد روانشاد
دانشکده علوم ریاضی و کامپیوتر، دانشگاه دامغان
ar1091@yahoo.com

چکیده

در مجله‌یeurocrypt سال ۲۰۰۶ ، در مقاله‌ای تحت عنوان" QUAD ، یک رمز جریانی کاربردی با امنیت قابل اثبات" QUAD به عنوان یک خانواده پارامتری از رمزهای جریانی توسط گیلبرت ، بربین و پاتارین معرفی شد. سرعت اجرا برای نمونه‌ای از QUAD ها با ۱۶۰ بیت و خروجی بلوکی روی میدان‌های$GF(۲)$ ، $GF(۱۶)$، $GF(۲۵۶)$ ارائه شده است در این مقاله روشی جدید برای پردازش دستگاه‌های معادلات چندجمله‌ای از طریق گراف جزءبندی شده راارائه می‌کنیم که این روش سرعت محاسبه‌ی جواب معادلات را افزایش می‌دهد، همچنین نشان می‌هیم که چگونه یک گروه مخرب می‌تواند سیستم‌های منطبقی برای رمز جریانیQUAD تولید کنند که به راحتی شکسته شوند. نتایج روش فوق یک مسیر جدید برای ارزیابی امنیت رمزهای متقارن در برابر حملات جبری ایجاد می‌کند.

واژه های کلیدی: رمزهای جریانی، امنیت قابل‌اثبات، گراف جزء بندی.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۱۳D۰۲، ۱۳D۴۵، ۱۳C۱۴، ۱۳D۰۷.

۱ مقدمه

رمز جریانیQUAD توسط بربین و همکارانش ارائه شد[۱]. این رمز جریانی و امنیت آن بر پایه حل مسئله MQ فرضیه‌سازی شده است.رمز جریانی QUAD از یک وضعیت درونی $X=(x_1,...,x_n)$ و دستگاه چندمتغیره درجه ۲ تصادفی $S(x_1,...,x_n)$ با m تابع درجه ۲ چندمتغیره $Q(X):GF(q^n)\longmapsto GF(q)$ ،تشکیل شده است به طوری که $S(X)=\{Q_1(X),...,Q_m(X)\}$ به عنوان یک مولد اعداد شبه‌تصادفی در نظر گرفته می‌شود .این رمز با QUAD(q،n،r) نشان داده می‌شود، که r تعداد خروجی کلید جریانی است و $r=m-n$. به طور معمول $m=kn$در نظر گرفته می‌شود که $k\geq 2$ و بنابراین $r=(k-1)n$. فرایند تولید کلید جریانی به سادگی شامل ۳ مرحله با تکرار به منظور تولید k-۱)n) مقدار کلید رمز جریانی در هر تکرار می باشد.

- محاسبه kn تا از مقادیر GF(q) ، $S(X)=(Q_1(X),...,Q_{kn}(X))$ که X مقدار فعلی از وضعیت درونی است.
- دنباله خروجی $S_{out}(X)=(Q_{n+1}(X),...,Q_{kn}(X))$ از k-۱)n) مقدار کلید جریانی GF(q)
- به روز رسانی وضعیت درونی X با دنباله ای از n مقداراولیه تولید شده‌ی GF(q) ، $S_{it}(X)=(Q_1(X),...,Q_n(X))$

تعریف:فرایند حذف رأسها یا یالها برای ناهمبند ساختن یک گراف را به ترتیب جزء‌بندی رأسها یا جزء‌بندی یالها می‌نامیم

تعریف :گراف اشتراک- متغیر:فرض کنید F دستگاه چندجمله‌ای

$$\begin{aligned}
f_1(x_1,x_2,...,x_n)&=0\\
f_2(x_1,x_2,...,x_n)&=0\\
&\vdots\\
f_m(x_1,x_2,...,x_n)&=0
\end{aligned}$$

از m معادله چندجمله‌ای با $x_1,x_2,...,x_n$ متغیر باشد.گراف اشتراک -متغیر $G=(V,E)$ ازF با ایجاد رأس $v_i\in V$ برای هر متغیر x_i ، و ایجاد یک یال $(v_i,v_j)\in E$ بدست می‌آیداگر دومتغیر x_i,x_jدر هر چندجمله‌ای f_k با یکدیگر ظاهر شوند(با ضرایب غیرصفر) .

با استفاده از روش گراف جزء‌بندی یک دستگاه معادلات چندجمله‌ای را می‌توان به اندازه‌های کوچکتر تقسیم کرد،که هریک را به طور جداگانه می‌توان حل نمود. طبق قضیه نگاشت جهانی[۲] ، چون نگاشتهای fوg از یک مجموعه متناهی به یک مجموعه متناهی دیگر هستند،می‌توان آنها را به شکل دستگاه معادلات چندجمله‌ای روی هر میدانی نوشت اما میدان $GF(2)$ مناسب‌تر می‌باشد . هر معادله درجه دو یک نگاشت

$GF(2) \longrightarrow GF(2^n)$ است، بنابراین اولین مجموعه‌ی n معادله‌ای نگاشتی از $GF(2^n) \longrightarrow GF(2^n)$ به نام f_1 و دومین مجموعه‌ی n معادله‌ای نیز نگاشتی با ابعاد مشابه قبل به نام f_2 می‌باشد.وضعیت درونی بردار s با ۱۶۰ بیت می‌باشد. ۱۶۰ معادله اول در s ارزیابی شده واز نتایج بردار $f_1(s_t) = s_{t+1}$ وضعیت جدید بدست می‌آید.۱۶۰ معادله دوم نیز برای ارزیابی خروجی $z_t = f_2(s_t)$ می‌باشند.بردار z_t به n بیت بعدی پیام متن p_t روی $GF(2)$ اضافه می‌شود و پیام رمز منتقل شده بدست می‌آید $c_t = p_t + z_t$. حمله پیام متن شناخته شده را که حمله‌کننده هر دو پیام متن $p_1, p_2, ..., p_n$ و پیام رمز $c_1, c_2, ..., c_n$ را می‌شناسد درنظرمی‌گیریم، می‌توان دستگاه معادلات را به صورت زیر نوشت:

$$
\begin{aligned}
c_1 + p_1 &= z_1 = f_2(s_1) \\
c_2 + p_2 &= z_2 = f_2(s_2) = f_2(f_1(s_1)) \\
&\vdots \\
c_t + p_t &= z_t = f_2(s_t) = f_2\underbrace{(f_1(f_1(f_1(...f_1}_{t-1}(s_1)...))))
\end{aligned}
$$

واقعیت جالب در اینجا این است که $f_2(f_1(f_1(f_1(...f_1(s_1)...))))$ و تکرارهای بالاتر ممکن است کاملاً متراکم شود حتی اگر f_1 پراکنده باشد. طراحان QUAD امنیت بسیار خوبی برای این رمز وقتی که دستگاه چندجمله‌ای توسط سکه‌های سالم تولید شده باشد بیان کردند. اگر یک دستگاه پراکنده انتخاب شودبه طوری که شامل یک رأس کوچک متعادل شده‌ی مجزا باشد، آنگاه رمز می‌تواند توسط یک دشمن مخرب به صورت زیرناامن شود :

معادلات آسیب‌دیده و QUAD می‌توان حمله زیر را که از دستگاه پاتارین " Oil and Vinegar " الهام گرفته شده است تصور کرد. یک تولید کننده‌ی مخرب نمی‌تواند دستگاه را به صورت تصادفی تولید کند ،بلکه یک دستگاه پراکنده با ۲۰رأس متصل (همبند) ، برای چند رأس جزء‌بندی شده با $\beta \approx ۰/۶$ را ایجاد می‌کند. تولیدکنندگان مخرب ادعا می‌کنند که این دستگاه به دلایل پراکندگی کارا است و این امر ممکن است سبب رمزگذاری سریعتر نسبت به دیگر دستگاههای QUAD که با معادلات درجه ۲ توسط سکه‌های سالم تولید شده‌اند ، شود. برخی جداکننده‌ها ۲۰ رأس نسبت داده شده به متغیرهای گراف اشتراک-متغیر را به ۵۶ یا ۸۴ رأس تقسیم می‌کنند.این بدین معنی است که حمله‌کننده فقط نیازبه دانستن پیام متن و پیام رمز از یک دنباله ۱۶۰ بیتی دارد ومعادلات زیر را حل می‌کند. $f_2\underbrace{(f_1(f_1(f_1(...f_1}_{i-1}(s_1)...)))) = p_t + c_t$
برای هر حدس کلید ، باید ۵۶ معادله در ۵۶ متغیر و ۸۴ معادله در ۸۴ متغیر را حل کرد .

۲ بهبود تحلیل جبری QUAD با روش جزء‌بندی گراف

الگوریتم رمز جریانی QUAD

Algorithm 1 Preprocessing
Input: key k → Fn, IV →f0; 1g80

Output: initial state IS $\rightarrow$ Fn
1: IS $\leftarrow$ k
2: for i = 0 to 79 do
3: if IV[i]=1 then
4: IS $\leftarrow$ S1(IS)
5: else
6: IS $\leftarrow$ S0(IS)
7: end if
8: end for
9: for i = 0 to 79 do
10: IS $\leftarrow$ P(IS)
11: end for
12: return IS

Algorithm 2 keystream generation
Input: initial state IS $\rightarrow$ Fn
Output: keystream ks $\rightarrow$ Fm_L
1: ks $\longleftarrow$ []
2: for i = 0 to L - 1 do
3: ks $\longleftarrow$ ks$\|$ Q(IS)
4: IS $\longleftarrow$ P(IS)
5: end for
6: return ks

الگوریتم گریدی:
ورودی: B جداکننده یالی گراف $G=(V,E)$ است
خروجی: C جداکننده رأسی کوچک گراف G است بر پایه B

begin
1: D $\leftarrow$ B
2:R $\leftarrow \oslash$
3:whileD$\neq \oslash$ do
آن رأسی در V که بیشترین اتصال به یالها را دارد و vنامیده می شود بردار. v را بریز داخلC. تمام یالهایی که به vوصل هستند را حذف کن

4: return C

مراجع

[1] C. Berbain, H. Gilbert, and J. Patarin, *Quad: A practical stream cipher with provable security*, EUROCRYPT, **vol.** (2006), 109–128.

[2] Bard, G.V, Algebraic Cryptanalysis, Springer, (2009).

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۶۱ تا ۶۴.

پوستر

الگوریتم شور وکاربردها و چالش هایش در رمزنگاری

بهروز فتحی واجارگاه
گروه آمار دانشکده علوم ریاضی دانشگاه گیلان
fathi@guilan،ac.ir

رحیم اصغری
ریاضی کاربردی دانشگاه گیلان
Meisam.mathhome@gmail.com

مجید فرهادی
دانشکده ریاضی دانشگاه دامغان
Farhadi@du.ac.ir

چکیده

مساله فاکتورگیری،عبارت از یافتن عامل های صحیح اول مثبت مرکب وفرد N است. تاکنون هیچ الگوریتم کلاسیکی یافت نشده است که بتواند در زمان چندجمله ای این کار را انجام بدهد به همین خاطر از این اصل برای ساختن الگوریتم های رمزنگاری کلاسیکی مانند RSA استفاده شده است.

الگوریتم شور با بکارگیری تبدیل فوریه کوانتومی به تسریع الگوریتم فاکتورگیری پرداخته ونشان داده می شود که در زمان چندجمله ای عمل فاکتورگیری انجام می پذیرد.اجرای الگوریتم شور دارای چالش هایی است که به کوانتومی بودنش مربوط می گردد.از طرفی کاربردهای وسیعش درشکستن الگوریتم های رمز شاخص کلاسیک از نکات قابل توجه اش می باشد که در این مقاله به بررسی آن

می پردازیم.همچنین روشهای شبیه سازی کلاسیک و پیاده سازی کوانتومی این الگوریتم مورد بحث واقع میشود.

واژه های کلیدی: رمزنگاري کوانتومی،الگوریتم های عامل یابی ، الگوریتم شور،تبدیل فوریه کوانتومی،الگوریتم تخمین فاز.

۱ مقدمه

امروزه سیستم‌هاي رمز نگاري متعددي نظير RSA به طور گسترده مورد استفاده قرار مي‌گيرند که براساس اين فرضيه استوارندكه عامل يابي صحيح از نظر محاسباتي از ضرب صحيح سخت تر است. به عبارت ديگرالگوريتم‌هاي زيادي به زمان چند جمله‌اي براي ضرب صحيح موجود است در حالي كه هيچ الگوريتمي با زمان چند جمله‌اي براي عامل يابي صحيح وجود ندارد. از زمان اقليدس دانشمندان مي دانستند كه هر عدد صحيح مثبت N را مي‌توان به صورت يكتا به حاصلضرب عامل‌هاي اول تجزيه كرد. همچنين تشخيص اول يا مركب بودن اعداد نيز در زمان چند جمله‌اي قابل انجام است. الگوريتم ميلر– رابين با $O(slgN)$عمليات محاسباتي و با احتمال $prop_{error} \leqslant ۲^{-s}$ اول بودن را تشخيص مي‌دهد. حال اگر يك عدد مركب فرد باشد، يافتن عامل‌هاي اول آن براي يك كامپيوتر كلاسيك در زمان چند جمله‌اي قابل انجام نيست. كاراترين الگوريتم كلاسيكي كه براي اين امر موجود است الگوريتم غربال اراتستن است كه در زمان $O(cEXP[(lgN)^{۱۳}(lglgN)^{۲۳}]$ انجام مي‌شود.
تمام الگوريتم‌هايی كه تاكنون برای فاكتورگيری عدد صحيح فرد بزرگ طراحی شده اند بر روي كامپيوترهاي كلاسيك اجرامی‌شوند. حال اگر كامپيوتري را بتوان ساخت كه هم بر اساس مكانيك كلاسيك و هم مكانيك كوانتومي قادر باشد كار كند، چه خواهد شد؟ در سال ۱۹۹۴پيتر شور بر اساس تحقيقات بنت، دوويچ ؛ بنويف، فاينمن، سيمون و ديگران، الگوريتمي ساخت كه بتواند روي يك كامپيوتر كوانتومي اجرا شود و عامل‌هاي صحيح را در زمان چند جمله‌اي بيابد. اين الگورتيم را الگوريتم فاكتورگيری كوانتومي شور مي‌گويند.
اکثر گامهای این الگوریتم در کامپیوتر های کلاسیک انجام می شود وتنها یک گامش در کامپیوتر های کوانتومی انجام می پذیرد که در گام کوانتومی آن از تبدیل فوریه کوانتومی والگوریتم تخمین فاز برای محاسبه سریع مرتبه عدد تصادفی بهx هم نهشتی عددnاستفاده می شود که مهم ترین گام الگوریتم بوده وضعف بزرگ الگوریتم های کلاسیک فاکتورگیری که در محاسبه مرتبه عدد است را مرتفع می کند. مهم ترین کاربرد این الگوریتم ، شکستن سیستم رمز کلید عمومی RSAو رمزهای مبتنی بر منحنی های خم بیضوی است که وابسته به مساله لگاریتم گسسته هستند.
در این الگوریتم اززیرالگوریتم های کلاسیک کسرهای متوالی واقلیدسی استفاده می شود که در زمان چندجمله ای اجرا می شوند.
در ادامه به طور خلاصه به این الگوریتم می پردازیم : [۲,۳,۴]
گام اول:
عدد تصادفي صحيح مثبت m را انتخاب مي‌كنيم.بزرگترین مقسوم علیه مشترک N،m و$gcd(N,m)$ را با الگوريتم اقليدسي در زمان چند جمله‌اي مي‌يابيم. اگر $gcd(N,m) \neq ۱$ یک عامل غير بديهي از N را

یافته ایم درغیر این صورت به گام ۲ مي رويم .
گام دوم:
از يك كامپيوتر كوانتومي براي تعيين دوره P از تابع زير استفاده ميكنيم.

$$f_N : N \longmapsto N$$
$$a \longmapsto m^a modN$$

گام سوم:
اگر P عددي فرد و صحيح بود، برو به گام ۱ (احتمال اينكه P فرد باشد برابر با$(۱/۲)^{(k-۱)}$است كه k تعداد عاملهاي اول N است .) اگر P زوج بود برو به گام۴ .
گام چهارم:
چون P زوج است

$$(m^{(p/۲)} - ۱)(m^{(p/۲)} + ۱) = (m^p - ۱) = \circ modN$$

اگر$m^{(p/۲)} + ۱) = \circ modN$) برو به گام ۱ در غير اين صورت برو به گام ۵. ميتوان نشان داد كه احتمال اينكه$d = gcd(m^{(p/۲)} - ۱, N)$كمتر از$(۱/۲)^{(k-۱)}$است كه k تعداد عاملهاي اول مجزا از N است.
گام پنجم:
با استفاده از الگوريتم اقليدس$d = gcd(m^{(p/۲)} - ۱, N)$را محاسبه ميكنيم. اگر

$$(m^{(p/۲)} + ۱) = \circ modN$$

باشد بسادگي ميتوان نشان داد كه d يك عامل غير بديهي از N است. d را به عنوان جواب بده و خارج شو.

۲ کاربردهای الگوریتم شور در رمزنگاری

در این بخش می خواهیم به چند کاربردالگوریتم شور در شکستن رمز ها بپردازیم واز طرفی چالش های احتمالی این الگوریتم را هم بیان کنیم.
تمامی الگوریتم های رمزی که با مساله فاکتورگیری در ارتباط هستند می توانند با الگوریتم شور شکسته شوند.این الگوریتم های رمز شامل موارد زیر هستند .

a. RSA Problem
b. Rabin Problem
c. quadratic residuosity Problem
d. The square root modulo n problem (SQROOT)

از طرفی تمامی الگوریتم هایی که به نوعی به مساله لگاریتم گسسته وابسته می شوند تحت الگوریتم شور خواهند شکست که شامل موارد زیر هستند .

a. Diffie-Hellman key agreement and its derivatives
b. ElGamal encryption, and the ElGamal signature scheme and its variant
c. ECC

از طرفی الگوریتم شور از تبدیل فوریه کوانتومی برای تسریع در محاسبه مرتبه مورد استفاده قرار می دهد. اگر محاسبات طوری باشد که در آن نتوان از QFT استفاده کرد آنگاه انجام این محاسبات نمی تواند با کامپیوتر های کوانتومی تسریع داده شود .
از مهم ترین چالش های این الگوریتم وجود یک کامپیوترکوانتومی در اجرای الگوریتم کوانتومی است.

مراجع

[1] M.A. Nielsen, I.L. Chuang, ”Quantum computation and quantum information”, Cambridge Univ. Press, (2000).

[2] R.C. Vidya, H.D. Phaneendra, M.S. Shivakumar, ”Quantum algorithms and hard problems”, IEEE/ICCI, pp.783- Beijing, (July 2006).

[3] Jozsa, R., Quantum Algorithms and the Fourier Transform, Proc. Roy. Soc. Lond. A, 454, pp. 323-337 ,(1998).

[4] R. deWolf. Quantum Computation and Shor’s Factoring Algorithm. Unpublished, (1999).

[5] P. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,(1995).

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۶۵تا ۶۶ .

پوستر

مقادیر ویژه گراف توان یک گروه متناهی

مرتضی فغانی
گروه ریاضی ، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷-۱۹۳۹۵)
mo_faghan@yahoo.com

سیامک فیروزیان
گروه ریاضی، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷ – ۱۹۳۹۵)
siamfirouzian@pnu.ac.ir

مهدی عزیزی مرزونی
گروه ریاضی، دانشگاه پیام نور بابل
sg.ghadir@gmail.com

چکیده

فرض کنید G یک گروه متناهی است گراف توان این گروه را با P(G) نشان داده و عبارتست از گرافی با مجموعه رئوس G و دو راس x و y مجاورند اگر و تنها اگر یکی توانی از دیگری باشد. بنا بر نتیجه ای معروف در این زمینه گراف توان یک گروه کامل است اگر و تنها اگر G یک p –گروه دوری باشد یعنی طیف گراف توان P(G) برابر $\{n-۱, -۱\}$ است اگر وتنها اگر G یک p–گروه متناهی باشد. یک جور سازی از گراف T عبارتست از مجموعه ای از یال ها ی T بطوریکه دو بدو راس مشترک نداشته باشند گراف کوکتل – میهمانی گرافی است که از روی $K_{۲n}$با حذف یک جور سازی کامل بدست می آید هدف این مقاله یافتن گرو ههایی است که طیف گراف توان آن برابر طیف گراف کوکتل – میهمانی است.

واژه های کلیدی: گراف توان ، P–گروه ، گراف کوکتل – میهمانی.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): $۱۳D۰۲$، $۱۳D۴۵$، $۱۳C۱۴$، $۱۳D۰۷$.

مراجع

[1] J. Abawajy, A. Kelarev and M. Chowdhury, *Power Graphs: A Survey*, Electronic Journal of Graph Theory and Applications, **vol. 1(2)** (2013), 125–147.

[2] P. J. Cameron and S. Ghosh, *The power graph of a finite group*, Discrete Mathematics, **vol. 311** (2011).

[3] P. J. Cameron, *The power graph of a finite group*, J. Group Theory, **vol. 13** (2010), 779-783.

[4] I. Chakrabarty, S. Ghosh and M. K. Sen, *Undirected power graphs of semigroups*, Semigroup Forum, **vol. 78** (2009), 410–426.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۶۷ تا ۶۸.

پوستر

مقادیرویژه گراف جابجایی یک گروه متناهی

سیامک فیروزیان
گروه ریاضی، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷ – ۱۹۳۹۵)
siamfirouzian@pnu.ac.ir

مرتضی فغانی
گروه ریاضی ، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷-۱۹۳۹۵)
mo_faghan@yahoo.com

رضا قربانی
گروه ریاضی، دانشگاه پیام نور بابل
M.a.TH.33140@gmail.com

چکیده

فرض کنید G یک گروه متناهی غیر آبلی و $\Gamma(G)$ گرافی باشد که مجموعه رئوس آن عناصر غیر مرکزی G یعنی برابر $G-z(G)$ و دو راس x و y مجاور باشند اگر و تنها اگر $xy=yx$ این گراف را اصطلاحا گراف جابجایی گروه G می نامیم ثابت شده است که گراف جابجایی یک گروه غیر آبلی متناهی نمی تواند کامل باشد به عبارتی گروهی غیر آبلی و متناهی نمی توان یافت که طیف آن برابر $\{-1, n-1\}$ باشد. هدف این مقاله مطالعه گراف جابجایی گروههای متناهی و غیر آبلی G که طیف آن ها با طیف گراف دو بخشی کامل $K_{m,n}$ برابر است می باشد تشریحی کامل از این گراف ها ارائه خواهد شد.

واژه های کلیدی:طیف ، گروه ، گراف.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۱۳D۰۲، ۱۳D۴۵، ۱۳C۱۴، ۱۳D۰۷.

مراجع

[1] J. Abawajy, A. Kelarev and M. Chowdhury, *Power Graphs: A Survey*, Electronic Journal of Graph Theory and Applications, **vol. 1(2)** (2013), 125–147.

[2] P. J. Cameron and S. Ghosh, *The power graph of a finite group*, Discrete Mathematics, **vol. 311** (2011).

[3] P. J. Cameron, *The power graph of a finite group*, J. Group Theory, **vol. 13** (2010), 779-783.

[4] I. Chakrabarty, S. Ghosh and M. K. Sen, *Undirected power graphs of semigroups*, Semigroup Forum, **vol. 78** (2009), 410–426.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۶۹ تا ۷۰.

پوستر

مقادیر ویژه لاپلاسی گراف توان سره

سیامک فیروزیان
گروه ریاضی، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷ − ۱۹۳۹۵)
siamfirouzian@pnu.ac.ir

مرتضی فغانی
گروه ریاضی ، دانشگاه پیام نور، جمهوری اسلامی ایران، (صندوق پستی ۳۶۹۷-۱۹۳۹۵)
mo_faghan@yahoo.com

سید احمد حسنی
گروه ریاضی ، دانشگاه پیام نور بابل

چکیده

فرض کنید G یک گروه متناهی و $P(G)$ گرافی با مجموعه رئوس G باشد که دو راس آن مجاورند اگر و تنها اگر یکی توانی از دیگری باشد. این گراف را اصطلاحا گراف توان گروه G می نامیم . اگر از این گراف عضو همانی را حذف کنیم گراف حاصل را گراف توان سره گروه می نامیم. همچنین برای گراف دلخواه T ماتریس مجاورت $A(T)$ و ماتریس قطری $D(T)$ که درایه های روی قطر درجات رئوس T می باشد را در نظر می گیریم. ماتریس $D(T) - A(T) = L(T)$ را ماتریس لاپلاسی گراف T می نامیم و مقادیر ویژه آن را مقادیر ویژه لاپلاسی می نامند. در این مقاله مقادیر ویژه لاپلاسی گراف توان سره گروه های آبلی مورد مطالعه قرار می گیرد ثابت خواهیم کرد که گروه های آبلی با طیف لاپلاسی آن ها به طور کامل مشخص می شوند.

واژه های کلیدی: مقادیر ویژه ، ماتریس لاپلاسی ، طیف ، گراف توان.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۱۳D۰۲، ۱۳D۴۵، ۱۳C۱۴، ۱۳D۰۷.

مراجع

[1] J. Abawajy, A. Kelarev and M. Chowdhury, *Power Graphs: A Survey*, Electronic Journal of Graph Theory and Applications, **vol. 1(2)** (2013), 125–147.

[2] P. J. Cameron and S. Ghosh, *The power graph of a finite group*, Discrete Mathematics, **vol. 311** (2011).

[3] P. J. Cameron, *The power graph of a finite group*, J. Group Theory, **vol. 13** (2010), 779-783.

[4] I. Chakrabarty, S. Ghosh and M. K. Sen, *Undirected power graphs of semigroups*, Semigroup Forum, **vol. 78** (2009), 410–426.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۷۱ تا ۸۰.

سخنرانی

بیت‌کوین: همه چیز از هیچ

رضا کابلی نوش‌آبادی
دانشکده ریاضی، دانشگاه صنعتی شریف
rezakaboli69@yahoo.com

چکیده

بیت‌کوین ارزی دیجیتالی است که انتشار و عرضه آن، وابسته به هیچ دولت، بانک و یا سازمانی نیست. ضرب، نگهداری و تایید تراکنش‌های بیت‌کوین توسط خود کاربران سیستم انجام می‌شود و تنها به پروتکل های رمزنگاری وابسته است. بیت‌کوین ابتدا در دسامبر ۲۰۰۸ توسط شخصی با نام مستعار ساتوشی ناکاماتو معرفی و در ژانویه ۲۰۰۹ این ایده به طور کامل توسط خود ناکاماتو عملی شد. مخترع بیت کوین هرگز هویت واقعی خود را فاش نکرد و به راحتی اختراع خود را برای جهانیان باقی گذاشت. هنوز هم منشا و انگیزه پشت بیت کوین یک راز بزرگ است. در این‌جا سعی می‌کنیم بیت‌کوین را به زبانی ساده شرح داده، جزییات فنی آن را با یکدیگر بررسی نماییم.

واژه های کلیدی: بیت‌کوین، ارز دیجیتالی، کریپتوکارنسی، رمزپول.

۱ مقدمه

عملکرد ضعیف دولت‌ها و عدم کنترل درست پول و همچنین، ظهور تکنولوژی‌های جدید مثل الکترونیک، کامپیوتر و اینترنت و قابلیت جابجایی و نگهداری امن اطلاعات در چند دهه‌ی اخیر، سب شد بسیاری به تحقیق درباره پول بپردازند و با استفاده از تکنولوژی‌های جدید، راه‌حل‌هایی برای مشکلات این حوزه ارائه

دهند. یکی از این راه‌حل ها، پول الکترونیکی بود. در سال ۱۹۹۰ پروژه‌ای به نام E-cash توسط دیوید چام شروع شد ولی از آن‌جایی که این پروژه به زیر ساخت های دولتی و کمپانی‌های کارت‌های اعتباری نیاز داشت، دوام چندانی پیدا نکرد. پروژه‌های دیگری نیز مثل bitgold ، PROW و b-money همگی روی زمین ماندند. در آن دوره همه به این فکر می‌کردند که چگونه می‌توان پولی الکترونیکی ایجاد کرد که جایگزین پول‌های کاغذی شود و چگونه می‌شود این پول را روی تراشه‌ها یا در حافظه کامپیوترها نگهداری کرد؟ همه به دنبال این بودند که شکل پول را عوض کنند و کسی به این فکر نمی‌کرد که پول الکترونیکی را(بدون هیچ پشتوانه‌ای) می‌توان طوری ایجاد کرد که بشود از آن برای دوام و ادامه حیات سیستم استفاده کرد. شاید خود ناکاماتو هم به این موضوع فکر نکرده بود. با شکستهای پیش آمده محققین کم‌کم به این نتیجه رسیدند که برای دست‌یافتن به ایده‌ای موفق و جلب نظر عمومی، باید به طریقی مناسب شرط متمرکز بودن پول را حذف کرد. می‌دانیم برای انجام یک تراکنش و انتقال پول بین دو شخص، بدون در نظر گرفتن جزئیات، وجود بانک برای تایید صحت و درستی تراکنش‌ها ضروری است. اما چگونه می‌توان این نقش را به نهادی دیگر سپرد که غیرمتمرکز بوده و در عین‌حال بتوانیم به او اعتماد کنیم. بهترین پاسخ به این سوال از آن ناکاماتو بود. پاسخی که در ظاهر عملی‌کردن آن غیرممکن به نظر می‌رسید.

۲ ماهیت بیت‌کوین‌ها و چگونگی ایجاد تراکنش‌ها

در یک بیان ساده می‌توان گفت بیت‌کوین‌ها چیزی جز تراکنش‌های قبلی صورت‌گرفته نیستند. برای روشن‌شدن این موضوع به مثال زیر توجه نمایید:
فرض کنید در یک کشور دولت برگه‌هایی که امضای دولت در آن‌ها است و ارزش برگه و نام اشخاص در آن‌ها ذکر شده، به طور عادلانه بین مردم تقسیم می‌کند. مردم می‌توانند از این برگه‌ها به عنوان پول استفاده کنند. با این تفاوت که به جای دادن برگه به عنوان پول به دیگران، در برگه‌ی دیگری نام گیرنده و مبلغ را می‌نویسند و آن را امضا می‌کنند. همچنین در برگه‌ی جدید، به برگه‌ی قبلی ارجاع داده می‌شود و با این کار، برگه‌ی جدید دارای ارزش شده و به مقداری که شخص اول خرج کرده است از ارزش برگه خودش کاسته می شود . باز قرارداد می‌کنیم که شخص در زمان خرج‌کردن پول، باید بقیه حسابش را در برگه‌ای دیگری برای خود امضا کند. با این کار برگه‌ی ابتدایی دیگر فاقد ارزش خواهد بود و تنها فایده‌اش در این است که به برگه‌های جدید ارزش می‌دهد. اما باید توجه کنیم که در این روش شخص می‌تواند یک پول را دوبار خرج کند. برای حل این مشکل توافق می‌کنیم که شخص پس از خرج کردن پولش، باید برگه‌ی خرج‌شده را در یک تابلو اعلانات مشخص، برای دید همه نصب کند تا همه بدانند این پول خرج شده است و اگر این کار را انجام ندهد برگه‌های جدید معتبر نخواهند بود.
مثال فوق مثال روشنی برای چیستی بیت کوین‌ها و نحوه انجام تراکنش‌ها در سیستم بیتکوین می‌باشد. با این وجود ذکر چند نکته ضروری است :

- مانند مثال فوق موجودی یک فرد در سیستم بیت‌کوین، تراکنش‌هایی است که نام فرد در آنها ذکر شده است. یعنی چیزی به نام بیت‌کوین وجود ندارد و بیت‌کوین‌ها همان تراکنش‌های معتبری هستند که هنوز خرج نشده‌اند. هر شخص می‌تواند تنها تراکنش‌هایی را خرج کند که نامش در آن

تراکنش‌ها ذکر شده است. هر شخص می‌تواند با امضای خود ثابت کند که کدام تراکنش‌ها متعلق به اوست.

- در مثال فوق برای سهولت یک کشور را در نظر گرفتیم و فرض کردیم دولت برگه‌های دارای ارزش را بین مردم تقسیم می‌کند اما نحوه عرضه بیت‌کوین این‌گونه نیست و به روشی بسیار جالب و ابتکاری صورت می‌پذیرد که در بخش‌های بعدی به تفصیل به آن می‌پردازیم.

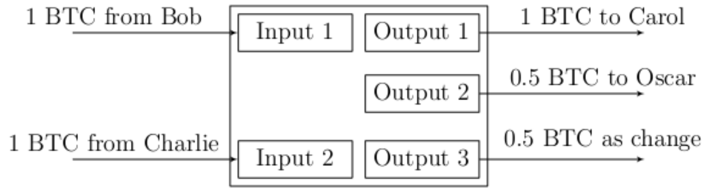
- خاطر نشان می‌کنیم در سیستم بیت‌کوین، امضا به معنای امضای دیجیتال است و امضای دیجیتال با امضای معمولی متفاوت است. در امضای دیجیتال هر شخص یک کلید خصوصی و یک کلید عمومی متناظر با آن دارد. کلید عمومی معرف شخص است و همه از آن آگاه‌اند و کلید خصوصی تنها برای امضا و اثبات هویت شخص به کار می‌رود. در امضای دیجیتال لازم نیست شخص هویت اجتماعی خود را فاش کند تنها کافی است با استفاده از کلید خصوصی، به همه نشان دهد یک کلید عمومی خاص، که همه می‌شناسند، مال اوست. نتیجه این‌که وقتی گفته می‌شود "برگه‌ای که نام گیرنده در آن است توسط فرستنده امضا شده است" منظورمان از نام گیرنده، کلید عمومی گیرنده و منظور از امضا، امضای دیجیتال شخص با استفاده از کلید خصوصی‌اش است.

- هر شخص می‌تواند چند زوج کلید داشته باشد. بدون کاستن از کلیت، می‌توان فرض کرد هر کلید عمومی شخص، یک شماره حساب جداگانه برای اوست و رمز این حساب، کلید خصوصی متناظر آن است. در سیستم بیت کوین به هر حساب یک آدرس گفته می‌شود و کیف پول یک شخص، مجموعه‌ی آدرس‌های او به همراه کلیدهای خصوصی متناظر می‌باشد.

- تراکنش‌ها در بیت‌کوین از آن‌چه در مثال فوق ارائه کردیم ساده‌ترند. در بیت‌کوین هر شخص می‌تواند از چندین حساب خود، به بطور همزمان به چند حساب دیگر(آدرس دیگر) پول واریز کند. برای این منظور کافی است آدرس[1] تراکنش‌های واریزی قبلی به حساب خود را به عنوان ورودی تراکنش و آدرس‌هایی که قصد دارد به حساب آنها پول واریز کند، خروجی تراکنش در نظر بگیرد. البته با این شرط که مجموع ورودی با مجموع خروجی برابر باشد. با قرارگرفتن این تراکنش در تابلو اعلانات، همه از انتقال صورت گرفته با خبر می‌شوند و به این ترتیب مبالغ ذکر شده در تراکنش، به حساب گیرنده‌ها در نظر گرفته می‌شود و تراکنش‌هایی که به عنوان ورودی این تراکنش ذکر شده‌اند و متعلق به فرستنده هستند، از این به بعد فاقد اعتبار خواهند بود.

- با قرارگرفتن تراکنش‌ها در تابلو اعلانات، همه از حساب‌ها، دارایی‌ها و ریز انتقالات شبکه آگاه می‌شوند، ولی نکته اینجاست که کسی نمی‌داند این حساب‌ها متعلق به کیست. در سیستم بیت‌کوین نقش تابلو اعلانات به عهده زنجیره‌ی بلوک‌ها می‌باشد که در ادامه به جزئیات آن خواهیم پرداخت.

[1] در بیت‌کوین برای آدرس‌دهی و نام‌گذاری یک شی(تراکنش،بلوک و ..)، از هش آن شی استفاده می‌کنیم. پس در اینجا منظور از آدرس تراکنش، هش آن تراکنش است. بنا به ویژگی توابع هش، این نامگذاری یکتاست.



شکل ۱: یک تراکنش با چند ورودی و خروجی.

۳ استخراج

در سیستم بیت‌کوین وقتی فرستنده پولی را به آدرس گیرنده واریز می‌کند گیرنده باید مطمئن باشد این پول قبلا خرج نشده است. ایده تابلوی اعلانات که در مثال قبل ذکر شد، ظاهرا این مشکل را برطرف می‌کند اما در عمل برای یک شخص عادی، بررسی این همه تراکنش تقریبا کاری غیرممکن است و به صرفه نمی‌باشد. همچنین ممکن است فرستنده پول را در آن واحد دو بار خرج کرده باشد پس احتمال دارد گیرنده حتی با بررسی تمام تراکنش‌های تابلو اعلانات متوجه این موضوع نشود. از طرفی مایل نیستیم تایید تراکنش‌ها توسط یک مرجع رسمی انجام شود(زیرا تلاش‌های قبلی در این مسیر به شکست انجامید). پس با این وجود راه چاره چیست؟
ناکاماتو به درستکاری و صداقت اکثریت کاربران اطمینان کرد و این کار را به عهده خود کاربران سپرد. او پیشنهاد کرد کاربرانی که مایل باشند می‌توانند تراکنش‌های صادرشده از سوی دیگر کاربران را در صورت صحت تایید کنند و به ازای وقت و هزینه‌ای که صرف می‌کنند بیت‌کوین نو بگیرند. اوج ابتکار ناکاماتو در همین‌جاست. زیرا به این روش، عده‌ای به بیت‌کوین به عنوان یک منبع درآمد نگاه می‌کنند و لازم نیست بیت‌کوین خریداری کنند. خودشان می‌توانند بیت کوین بدست آورند و یا در یک کلام می‌توانند بیت‌کوین استخراج کنند. این روش، عرضه بیت‌کوین و تزریق آن به سیستم را نیز آسان می‌کند و می‌توان ادعا کرد عادلانه ترین حالت ممکن است. با این روش بیت کوین بیشتر، مال کسی است که زحمت بیشتری می‌کشد و در این‌جا تبعیضی نیست و هر کس به اندازه وقت و هزینه‌ای که صرف کرده، سود می‌برد.

۱.۳ جزئیات فنی استخراج

در ایده استخراج، از کاربران خواسته می‌شود تراکنش هایشان را برای مشاهده بقیه و تایید، انتشار دهند. معدنچیان، همان کسانی که مایل‌اند تراکنش های صورت‌گرفته را تایید کنند، این تراکنش‌ها را دریافت کرده و صحت آنها را بررسی می‌کنند تا کسی یک پول را به دروغ و یا دو بار خرج نکند. سپس تراکنش تاییدشده را در یک پکیج به نام بلوک قرار داده، انتشار می‌دهند. انتشار یک بلوک به معنای تایید تراکنش‌های آن بلوک است. حال اگر بلوکی به دست ما رسید، چگونه می‌توانیم مطمئن شویم استخراج کننده آن دروغ‌گو نبوده و یا در حالت کلی، یک مهاجم نیست؟ برای حل این موضوع پیشنهاد می‌کنیم فرآیند استخراج به

گونه سخت شود که یک مهاجم نتواند به راحتی بلوک معتبر ایجاد کند. در ادامه توضیح می‌دهیم که منظور ما از سختی چیست.

۱.۱.۳ تایید تراکنش‌ها

در این مرحله هر معدنچی سعی می‌کند درستی اطلاعات تراکنش‌های دریافتی را بررسی کند و همچنین با توجه به تراکنش‌های قبلی، بررسی می‌کند یک پول دوبار خرج نشده باشد. پس از این کار، تراکنش های تایید شده را کنار هم قرار می‌دهد و آن‌را یک بلوک می نامد.

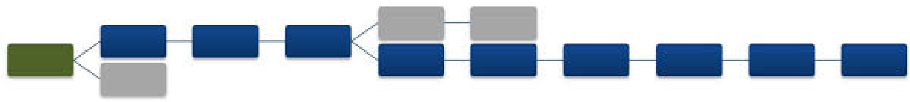
۲.۱.۳ اثبات کار

اثبات کار قسمتی از فرآیند استخراج است که معدن‌چیان پس از تایید تراکنش‌ها ملزم می شوند مقداری عملیات محاسباتی زمان‌بر انجام دهند تا به نتیجه‌ی مطلوب خواسته شده‌ای برسند، که از آن به عنوان حل پازل یاد می‌شود. اثبات کار باید طوری باشد که انجام آن مشکل، ولی بررسی و تایید آن آسان باشد. پازل بیت‌کوین به گونه‌ای انتخاب شده است که می‌توان روند حل آن را بین افراد تقسیم کرد و هرچه تعداد نفرات بیشتر باشد سریع‌تر حل می‌شود. با تمام قدرت محاسباتی که از سرتاسر جهان برای حل پازل بیت کوین صرف می‌شود، به طور میانگین ده دقیقه طول می‌کشد تا یک پازل بیت‌کوین حل شود. این قدرت محاسباتی چندی پیش در حدود قدرت ۴۰ ابر کامپیوتر برتر دنیا، که به طور موازی پردازش کنند، برآورد شده بود. پس اگر فرض کنیم اکثر معدنچیان صادق هستند می‌توانیم بلوکی را که پازل آن سریع‌تر از همه حل شده است، بلوک معتبر در نظر بگیریم و به آن اطمینان کنیم. توافق می‌کنیم معدنچی این بلوک برنده جایزه باشد. حال اگر مهاجمی قصد فریب داشته باشد و بخواهد بلوکش را معتبر جلوه دهد باید حداقل توانی به اندازه نصف توان تمام معدنچنیان داشته باشد، که هزینه‌ی آن، برای هیچ مهاجمی به‌صرفه نیست. ارزش جایزه، باید از هزینه‌ای که تمام معدنچیان برای استخراج در این زمان صرف کرده‌اند، بیشتر باشد. می‌توان انتظار داشت بقیه معدنچیان، به میزان درصدی که در فرآیند استخراج شرکت می‌کنند، برنده‌ی حل پازل های بعدی باشند. جایزه حل پازل را کسی به برنده نمی‌دهد، بلکه هر کس پیش از اثبات کار، در بلوک خود، مقدار ثابتی بیت‌کوین جدید به نام Generation به یکی از آدرس‌های خود اختصاص می‌دهد و اگر برنده شد همه قبول می‌کنند این پول برای اوست.

۲.۳ برچسب زمانی و زنجیره‌ی بلوک ها

برای پرهیز از بی‌نظمی، که ممکن است در آینده توسط بلوک‌های استخراج شده پدید آید و تنظیم عرضه و تزریق منظم پول به سیستم، به بلوک‌ها برچسب زمانی نسبت می‌دهیم. به این ترتیب بلوک‌ها در یک زنجیره زمانی قرار می گیرند. باز برای این‌که یک تراکنش در دو بلوک تایید نشود و یا این‌که شخصی یک پول برای دو نفر، در دو بلوک تایید نکند توافق می‌کنیم بلوک‌های قبلی در زنجیره‌ی بلوک‌ها، مرجع تایید تراکنش‌های بلوک‌های بعدی باشند. برای این منظور، هر بلوک باید آدرس بلوک قبلی را در خود داشته باشد. حال اگر دو بلوک معتبر به طور همزمان تولید شوند، بلوکی در زنجیره اصلی قرار می گیرد که تلاش بیشتری برای

استخراج آن شده و زنجیره‌ی حاصل از آن، طولانی‌تر است. دقت کنید زنجیره اصلی، زنجیره ثابت از پیش تعیین شده‌ای نیست بلکه زنجیره‌ای است که بلوک‌های بیشتری در آن وجود دارد(شکل۲). توافق می‌کنیم جایزه هر بلوک ۵۰ بیت کوین باشد و بعد از هر ۲۱۰۰۰۰ بلوک، این جایزه نصف شود. به این ترتیب، حجم کل بیت کوین‌ها که تا سال ۲۱۴۰ وارد سیستم می‌شود، از ۲۱ میلیون تجاوز نخواهد کرد(؟).



شکل ۲: نحوه‌ی شکل‌گیری زنجیره اصلی بلوک‌ها.

۴ نتایج اصلی

بیت‌کوین یک پول دیجیتال بدون پشتوانه است که هیچ قدرت مرکزی بر آن کنترلی ندارد. همانگونه که مشاهده کردیم هیچ مرجع رسمی و یا بانکی در این سیستم نیست که تراکنش‌ها را تایید کند. تایید تراکنش‌ها به عهده خود کاربران است و با توافق اکثریت حاصل می‌شود. برای انتقال وجه از حساب یک شخص به حساب شخصی دیگر در سیستم بیت‌کوین، فرستنده تراکنشی ایجاد می کند که ورودی آن آدرس تراکنش های قبلی واریزی به حساب اوست و خروجی تراکنش، آدرسی بیت‌کوینی شخص گیرنده می‌باشد. فرستنده تراکنش را امضا کرده، برای رسیدن به دست بقیه‌ی افراد شبکه، آنرا انتشار می‌دهد. افرادی که معدن‌چی بیت‌کوین هستند با دریافت تراکنش‌های جدید درستی آنها را با توجه به بلوک‌های قبلی بررسی می کنند و با قرار دادن تراکنش‌های صحیح در یک بلوک جدید، سریعا به حل پازل بلوک می‌پردازند و به محض یافتن پاسخ، بلوک را به همراه پاسخ پازل انتشار می دهند. اگر یک معدنچی در حین حل پازلش متوجه شود شخص دیگری پازل بلوک خود را زودتر حل کرده و تراکنش ها و اثبات‌کار آن شخص معتبر است، پازلش را رها می کند و در ادامه بلوک جدید، استخراج تازه‌ای را شروع می کند. یک تراکنش زمانی یک تراکنش تاییدشده تلقی می‌شود که در یکی از بلوک های زنجیره اصلی ظاهر شود. تمامی حساب‌ها و تراکنش‌های تایید شده بیت‌کوین آشکار است ولی صاحبان این حساب‌ها مشخص نیستند. با توجه به جزئیات ارائه شده در قسمت‌های قبل و متن‌باز بودن نرم‌افزار بیت‌کوین، هیچ شبهه‌ای درباره‌ی بیت‌کوین باقی نمی‌ماند و ادعاهایی چون ’’هرمی بودن‘‘ و یا ’’کلاه برداری به شیوه مدرن‘‘،درباره بیت‌کوین، کاملا بی‌اساس است.

مراجع

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

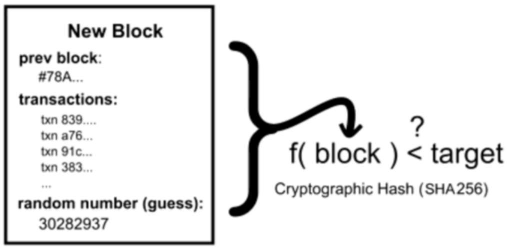
[2] Benjamin Wallace, The Rise and Fall of Bitcoin, Wired Magazine, November 23, 2011.

[3] Danielle Drainville, An Analysis of the Bitcoin Electronic Cash System, University of Waterloo, December 21, 2012.

[4] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries, Princeton University.

ضمیمه ۱ : توابع چکیده‌ساز و پازل بیت کوین

تابع چکیده‌ساز، تابعی است که رشته‌ای از داده را با طول دلخواه می‌گیرد و رشته‌ای با طول ثابت، به عنوان خروجی می‌دهد. بنابراین واضح است که یک تابع چکیده ساز نمی‌تواند یک‌به‌یک باشد، زیرا برد آن متناهی و دامنه‌اش نامتناهی است. اما توابع چکیده‌ساز به گونه‌ای انتخاب می‌شوند که در برابر برخورد مقاوم باشند. یعنی اگر f یک تابع چکیده‌ساز باشد با تمام توان محاسباتی‌ای که در اختیار داریم، نتوانیم رشته‌های y و x را پیدا کنیم که $f(x) = f(y)$.
از توابع چکیده‌ساز می‌توان، MD۵ و خانواده های معروف SHA و RIPEMD را نام برد. در سال‌های اخیر، برای MD۵ برخورد پیدا شد و به همین خاطر در عمل، از این تابع به طور مستقیم استفاده نمی‌شود. چون هر رشته از داده، قابل نمایش به صورت دودوئی است، پس خروجی تابع چکیده‌ساز را می‌توان یک عدد طبیعی در نظر گرفت. حال، پازل بیت کوین عبارت است از یافتن عدد طبیعی nonce که با قراردادن آن در بلوک، مقدار ((بلوک)SHA۲۵۶(SHA۲۵۶ از مقدار خواسته‌شده‌ای به نام target کمتر باشد. مقدار target هر ۲۰۱۶ بلوک توسط نرم افزار بیت‌کوین به گونه‌ای به‌روز می شود که میانگین زمان استخراج، همواره ده دقیقه باقی بماند.



شکل ۳: پازل بیت‌کوین با تصویر.

ضمیمه ۲ : اجماع

اجماع مهمترین ویژگی بیت‌کوین است و کمتر کسی به این موضوع می‌کند. اگر بتوانیم با نیمی از معدنچیان یک صنف تشکیل دهیم، آنگاه قادر خواهیم بود در تمام قوانین حاکم بر بیت‌کوین تغییر ایجاد کنیم. سیستم بیت‌کوین یک شی نیست که کاربران درحال استفاده از آن باشند. بیت‌کوین یک توافق جمعی است که برای ادامه‌ی حیات آن، کافی است حداقل نیمی از معدنچیان با هم درباره قوانین آن هم‌نظر باشند. به این ترتیب بقیه نیز برای ماندن در این سیستم، مجبور به رعایت قوانین خواهند بود زیرا در غیر اینصورت اکثریت آن‌ها را نخواهند پذیرفت. شما به عنوان یک معدنچی می‌توانید هر کاری انجام دهید. مثلا تراکنش های غیر معتبر را تایید کنید، مرحله اثبات کار را انجام ندهید، یا اینکه اصلا بلوکی نسازید و کاری دیگر

انجام دهید. در این صورت بقیه نتایج کار شما را نخواهند پذیرفت، زیرا قوانین اجماع را رعایت نکرده اید.اما اگر بتوانید اجماع را به نظر خودتان متمایل کنید می‌تواند هر قانونی وضع کنید. اجماع، ویژگی منحصر به فرد و بی‌بدیل بیت‌کوین است. اگر در آینده مشکلی برای سیستم پیش آید، معدنچیان می‌توانند برای حل آن مشکل به اجماع برسند و قوانین حاکم بر بیت‌کوین را عوض کنند. حتی اگر در حال حاضر معدنچیان به این اجماع برسند که جایزه حل بلوک، باید همواره ۵۰ بیت‌کوین باشد، این اجماع یک قانون برای سیستم خواهد بود و بقیه برای اینکه در سیستم بمانند ملزم به رعایت آن خواهند شد.
با توجه به بحث فوق، بعید به نظر می‌رسد بیت‌کوین توسط یک برنامه‌نویس و یا حتی یک ریاضیدان پدید آمده باشد. احتمالا بیت‌کوین نتیجه‌ی یک کار گروهی است و پیش از معرفی، مطالعات دقیق اجتماعی و اقتصادی درباره آن صورت گرفته است. حتی بسیار دور از ذهن است که برنامه‌نویسی بیت‌کوین و جنبه‌های ریاضی و امنیتی آن نیز، توسط یک شخص به تنهایی انجام شده باشد.

شکل ۴: اجماع معدنچیان.

ضمیمه ۳ : استخراج اشتراکی

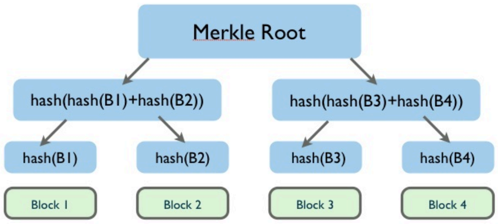
برخی معدنچیان برای اینکه بتوانند بیت‌کوین بیشتری استخراج کنند با یکدیگر شریک می‌شوند. این معدنچیان توافق می‌کنند که با هم و به طور موازی، پازل یک بلوک را حل کرده و در صورت برنده شدن، جایزه‌اش را به نسبت شراکت تقسیم کنند.در حال حاضر سایت های فراوانی می‌توان یافت که از کاربران دعوت می‌کنند با شرکت کردن در استخراج اشتراکی، بیت‌کوین بدست آورند. استخراج های اشتراکی را نباید دست کم گرفت زیرا به طور غیر مستقیم باعث شکل‌گیری اصناف بیت‌کوینی می‌شوند که به مرور زمان ممکن است کنترل بیت‌کوین را در دست بگیرند. برای نمونه یکی از سایت‌هایی که به این شکل بیت‌کوین استخراج می‌کند مدتی پیش، نزدیک به نیمی از قدرت محاسباتی سیستم را در اختیار داشت.

ضمیمه ۴ : درخت مرکل

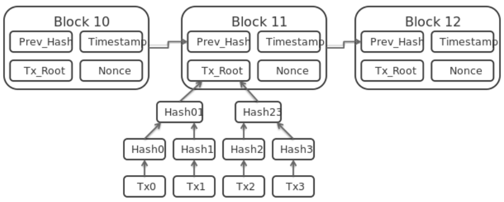
در رمزنگاری و علم کامپیوتر، درخت درهم‌سازی یا درخت مرکل، درختی از داده ساختارها است که خلاصه‌ی اطلاعات یک داده‌ی بزرگتر را در خود جای داده است و برای تشخیص محتویات آن داده به کار می‌رود. درخت‌های درهم سازی می‌توانند برای محافظت از هر نوع داده‌ای که ذخیره شده است و یا در بین رایانه‌ها منتقل می‌شود مورد استفاده قرار بگیرد. در حال حاضر، بیشترین و مهم‌ترین کاربرد درخت های درهم‌سازی در شبکه‌های نظیر به نظیر است.در این شبکه‌ها برای حصول اطمینان از اینکه بسته‌های دریافت

شکل ۵: نتیجه استخراج اشتراکی.

شده، بدون عیب و بدون تغییر هستند و اینکه بسته‌ها جعلی نیستند، از این درخت‌ها استفاده می‌شود. در سیستم بیت‌کوین نیز برای آسان نمودن بررسی جواب پازل، ریشه‌ی مرکل تراکنش‌ها را در سربرگ بلوک قرار می‌دهند.



شکل ۶: درخت مرکل.



شکل ۷: استفاده از ریشه مرکل تراکنش‌ها در سربرگ هر بلوک.

اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها
ایران، دانشگاه کاشان، ۲۸-۲۶ آذر ۱۳۹۳ (۱۹-۱۷ دسامبر ۲۰۱۴)، صفحات ۸۱ تا ۸۶.

سخنرانی

مقادیر ویژه گراف خط و انرژی خط شبه کاترپیلارها

علی‌محمد نظری
دانشکده علوم، دانشگاه اراک
am-nazari@araku.ac.ir

بهنام سپهریان
دانشکده علوم، دانشگاه اراک
B-Sepehrian@araku.ac.ir

مهدیه اسکندری
دانشکده علوم، دانشگاه اراک
m-skandari@arshad.araku.ac.ir

چکیده

انرژی گراف، مجموع قدرمطلق مقادیرویژه‌ی ماتریس مجاورت گراف G است و با نماد $E(G)$ نشان داده می شود. فرض کنید P_n مسیری با n رأس و S_{p+1} ستاره ای با $(p+1)$ رأس باشد. یک کاترپیلار $C(p)$ درختی است که با حذف رئوس آویزان آن می توان یک مسیر ساخت. فرض کنید

$P = [p_1, p_2, ..., p_{d-1}],$

مجموعه‌ای باشد که اعضای آن رئوس آویزان کاترپیلار هستند و

$p_1 \geq 1, p_2 \geq 1, ..., p_{d-1} \geq 1.$

$C(p)$ کاترپیلار به‌دست آمده از ستاره‌های $S_{p_۱+۱}, S_{p_۲+۱}, ..., S_{p_{d-۱}+۱}$است و مسیر $p_{d-۱}$ با مشخص کردن ریشه ستاره $S_{p_i+۱}$ در $i-$ امین رأس مسیر $p_{d-۱}$ می باشد.

واژه های کلیدی: شبه کاترپیلار، ماتریس لاپلاسین، گراف خط.

رده بندی موضوعی انجمن ریاضی امریکا (۲۰۱۰): ۱۳D۰۲، ۱۳D۴۵، ۱۳C۱۴، ۱۳D۰۷.

۱ مقدمه

فرض کنید G یک گراف ساده غیرجهت دار با n راس باشد. ماتریس لاپلاسین G یک ماتریس $n \times n$ بصورت $L(G) = D(G) - A(G)$ است، که در آن $A(G)$ ماتریس مجاورت گراف G و $D(G)$ ماتریس قطری از درجه رئوس می باشد. $L(G)$ یک ماتریس نیمه معین مثبت و $(۰, e)$ یک جفت ویژه از ماتریس $L(G)$ و e یک بردار یکه است. فیدلر در [۱] نشان می دهد که G یک گراف همبند است اگر و فقط اگر دومین کوچکترین مقدار ویژه از $L(G)$ مثبت باشد. این مقدار ویژه اتصال جبري از گراف G نام دارد و با نماد $a(G)$ نشان داده می شود .
ماتریس $L^+(G) = D(G) + A(G)$ ماتریس لاپلاسین از G نام دارد. $A(G)$ و $L(G)$ و $L^+(G)$ به ترتیب مقادیر ویژه ،مقادیر ویژه لاپلاسین و مقادیر ویژه لاپلاسین از گراف G نام دارند. یک ماتریس نیمه معین مثبت است و اگر G یک گراف دوبخشی باشد آنگاه $L(G)$و $L^+(G)$ چندجمله اي های مشخصه یکسان دارند. کوچکترین مقادیر ویژه لاپلاسین از گراف همبند G برابر با صفر است اگر و فقط اگر گراف دوبخشی باشد که در این صورت صفر یک مقدار ویژه ساده است. گراف خط G ، گراف $L(G)$ است که مجموعه رئوس و یال‌های G در تناظر ۱ − ۱ هستند. دو رأس از $L(G)$ مجاورند اگر و فقط اگر یالهای متناظر در G ، در یک رأس مشترك باشند. [۲] برای مثال، گراف خط از گراف ستاره S_n با n رأس برابر با گراف کامل $K_{n-۱}$ با $(n - ۱)$ رأس خواهد بود. همچنین انرژی ماتریس M، مجموع قدرمطلق مقادیر تکین ماتریس M است و $E(M)$نماد آن است. اگر G گرافی با n راس و m یال باشد، ماتریس وقوع آن یک ماتریس $m \times n$ است که در آن درایه (i, j)ام برابر ۱ است اگر یالی موجود باشد و در غیر این صورت صفر می‌باشد و با $I(G)$نمایش داده می شود،و داریم:

$$I(G) + I(G)^T = D(G) + A(G) = L^+(G),$$
$$I(G)^T + I(G) = ۲ \times I(m) + A(L(G)),$$

$I(m)$ هم یک ماتریس همانی $m \times m$ است.

۲ کاترپیلارها

فرض کنید P_n مسیري با n رأس و $S_{p+۱}$ ستاره اي با $(p + ۱)$ رأس باشد. یک کاترپیلار درختی است که با حذف رئوس آویزان آن می توان یک مسیر ساخت. فرض کنید $P = [p_۱, p_۲, ..., p_{d-۱}]$ مجموعه ای

باشد که اعضای آن رئوس آویزان کاترپیلار هستند و $p_1 \geq 1, p_2 \geq 1, \ldots, p_{d-1} \geq 1$.
$C(p)$ کاترپیلار به‌دست آمده از ستاره‌های $S_{p_1+1}, S_{p_2+1}, \ldots, S_{p_{d-1}+1}$است و مسیر p_{d-1} با مشخص کردن ریشه ستاره S_{p_i+1} در $-i$ امین رأس مسیر p_{d-1} می باشد. قرار می‌دهیم

$$C = C(p) : P_1 + P_2 + \ldots + P_{d-1} = n - d + 1$$

$C(p) \in C$ درختی با راس nاست و d قطر آن می‌باشد.

۳ مقادیر ویژه و انرژی گراف خط کاترپیلارها

لم۱: اگر v یک رأس آویزان از گراف $\tilde{G}$ باشد و Gگراف بدست آمده از حذف رأس v و یال مربوط به آن باشد، آنگاه مقادیر ویژه $L(G)$ از مقادیر ویژه $L(\tilde{G})$ بدست می آیند. نتایج را برای مشخص کردن مقادیرویژه $C(p)$ به‌کار می بریم. قرار می دهیم:

$$A(x) = \begin{bmatrix} 1 & \sqrt{x} \\ \sqrt{x} & x+1 \end{bmatrix}, \quad B(x) = \begin{bmatrix} 1 & \sqrt{x} \\ \sqrt{x} & x+2 \end{bmatrix}, \quad F = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

و $\sigma(A)$ مجموعه مقادیرویژه‌های ماتریس Aاست.
لم۲: فرض کنید بازای $1 \leq j \leq d-1$ ، $p_j \geq 1$باشد. بنابراین مقادیر ویژه لاپلاسین $C(p)$ برابرند با ۱ با چندگانگی $\sum_{i=1}^{d-1} p_i - d + 1$ و مقادرویژه های ماتریس $(2d-2) \times (2d-2)$ زیر :

$$G(p) = \begin{bmatrix} A(p_1) & F & & \\ F & B(p_2) & & \\ & & & \\ & & B(p_{d-2}) & F \\ & & F & A(p_{d-1}) \end{bmatrix}, \qquad (1)$$

۴ شبه کاترپیلارها

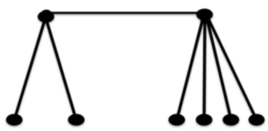
با فرض این‌که m یال به یال‌های کاترپیلار اضافه کرده باشیم، مقدارویژه‌های شبه کاترپیلارها برابر با مقدارویژه ۱ با چندگانگی $(\sum_{i=1}^{d-1} p_i - d + 1) - m$ و مقادیرویژه ماتریس (۱) است.
اگر یال های اضافه شده نامجاور باشند ،مقدارویژه ۳ با چندگانگی m وجود دارد. اگر برخی از یال ها مجاور و برخی نامجاور باشند، بازای هر دو یال مجاور اضافه شده مقدارویژه های ۲و۴ با تکرار ۱ و بازای یال های نامجاور اضافه شده مقدارویژه ۳ با تکرار تعداد یال های نامجاور وجود دارد. بازای هر یال اضافه شده به کاترپیلار یک مقدارویژه اضافه می شود.

۵ مقدارویژه‌های گراف خط متناظر با شبه کاترپیلارها

اگر δ_i ها و λ_i ها به ترتیب مقدارویژه‌های کاترپیلارها و گراف خط متناظر با آن ها بصورت نزولی باشند، درگراف حط متناظر با شبه کاترپیلار $\delta_i - ۲ \le \lambda_i$ و برای m مقدارویژه ی باقی مانده ۲− یک کران پایین برای مقدارویژه های گراف خط است.
برای هر m یال اضافه شده انرژی گراف خط کاترپیلارها یک کران پایین برای انرژی شبه کاترپیلارهاست.

۶ مثال

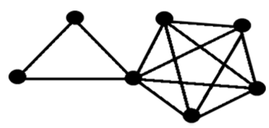
کاترپیلار زیر را در نظر می گیریم. مقدار ویژه‌های این شکل عبارتند از :



$\underline{۱}$ با چندگانگی $(\sum_{i=۱}^{d-۱} p_i - d + ۱) - ۱$ و $\underline{۳}$ با تکرار یک و مقادیرویژه ماتریسی $G(p)$. یعنی

$۰/۳۷۳۸۰۱۹۳۳۱۵, ۱, ۱, ۱, ۱, ۳, ۳/۴۸۴۸۶۱۹۵۳, ۶/۱۴۱۳۳۶۱۱۶$

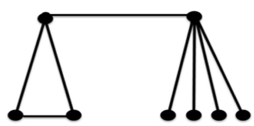
گراف خط متناظر:



مقادیر ویژه گراف خط برابرند با:

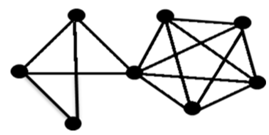
$-۱/۶۲۶۱۹۸۰۹۶, -۱, -۱, -۱, -۱, ۱/۴۸۴۸۶۱۹۵۳, ۴/۱۴۱۳۳۶۱۱۶$

اگر $\underline{m = ۱}$ یال به این کاترپیلار اضافه کنیم، مقدارویژه‌های این شبه کاترپیلار بصورت زیر هستند:



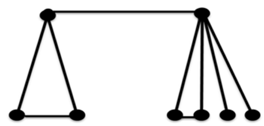
$۰/۳۷۳۸۰۱۹۳۳۱۵, ۱, ۱, ۱, ۳, ۳/۴۸۴۸۶۱۹۵۳, ۶/۱۴۱۳۳۶۱۱۶$

مقادیرویژه گراف خط این شبه کاترپیلار $\delta_i - ۲ \le \lambda_i$ می باشد که δ_i و λ_i به ترتیب مقدارویژه‌های کاترپیلارها و گراف خط متناظر هستند.
گراف خط و مقادیر ویژه متناظر با این شبه کاترپیلار به‌صورت زیر است:



$-۱٫۸۹۹۴۹۳۵۰۸, -۱, -۱, -۱, -۱, -۰٫۴۶۰۹۱۲۲۰۶, ۲٫۱۹۲۲۴۹۴۴۲, ۴٫۱۶۸۱۵۶۲۷۵$

اگر $\underline{m = ۲}$ یال به این کاترپیلار اضافه کنیم، مقدارویژه های این شبه کاترپیلار به‌صورت زیر هستند
زمانی که یال های اضافه شده نامجاورند

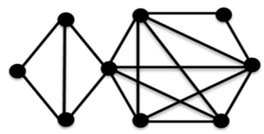


مقادیرویژه شبه کاترپیلار برابرند با:

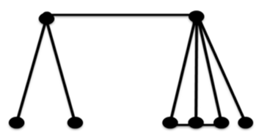
$۰٫۳۷۳۸۰۱۹۳۱۵, ۱, ۱, ۳, ۳, ۳٫۴۸۴۸۶۱۹۵۳, ۶٫۱۴۱۳۳۶۱۱۶$

در این حالت گراف خط و مقادیر ویژه متناظر با شبه کاترپیلار به‌صورت زیر است:

$-۲, -۱٫۶۰۶۸۰۰۹۳۸, -۱, -۱, -۱, -۰٫۴۹۷۹۰۵۰۷۸۱, ۰٫۵۱۱۰۳۱۸۷۲۳,$
$۲٫۲۵۴۹۹۷۷۵۰, ۴٫۳۳۸۶۷۶۳۹۴$



زمانی که یال های اضافه شده مجاورند

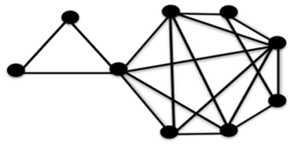


مقادیرویژه برابرند با:

$۰٫۳۷۳۸۰۱۹۳۱۵, ۱, ۱, ۲, ۴, ۳٫۴۸۴۸۶۱۹۵۳, ۶٫۱۴۱۳۳۶۱۱۶$

در این حالت گراف خط و مقادیر ویژه متناظر با شبه کاترپیلار به‌صورت زیر است:

$-۲, -۱٫۸۲۴۴۱۰۶۴۴۸, -۱٫۳۴۶۹۶۴۶۵۷, -۱, -۱, ۰, ۰٫۷۸۹۴۲۸۴۷۱۶,$
$۱٫۸۰۰۰۳۹۹۱۸, ۴٫۵۸۱۹۰۶۹۱۵$



References

[1] M. Fiedler, Algebraic connectivity of graphs, Czechoslovak Math. J. 23 (1973) 298–305.

[2] F. Harary, Graph Theory, Addison-Wesley, Reading, 1969.

[3] O. Rojo, L. Medina, Spectra of generalized Bethe trees attached to a path, Linear Algebra Appl. 430 (2009) 483–503.

[4] O. Rojo, L. Medina, N. Abreu, C. Justel, On the algebraic connectivity of some caterpillars: a sharp upper bound and a total ordering, Linear Algebra Appl. 432 (2010) 586–605.

[5] O. Rojo, Line graph eigenvalues and line energy of caterpillars, Linear Algebra Appl. (2011).

اسامی نویسندگان مقالات فارسی: