IPM

IPM Biennial Conference on

Combinatorics and Computing

IPMCCC - 2025

20-22 May 2025

40 Years in Designs: Celebrating the Life and Achievements of Professor Gholamreza B. Khosrovshahi

https://math.ipm.ir/IPMCCC2025

IPM Biennial Conference on
Combinatorics and Computing (IPMCCC2025),
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievements of
Professor Gholamreza B. Khosrovshahi

Welcome to the Conference

The organizing committee welcomes you to

IPM biennial conference on combinatorics and computing (IPMCCC 2025).

The conference is organized by the Combinatorics and Computing Group of IPM. The purpose of the IPMCCC is to bring together researchers interested in all areas of Combinatorics and Theoretical Computer Science, to discuss the latest developments and findings in their areas, take stock of what remains to be done and explore different visions for setting the direction for future work.

IPMCCC2025 celebrates the 85th birthday of Professor G. B. Khosrovshahi, one of the forefathers of IPM and combinatorics in Iran.

We would like to thank our distinguished speakers and visitors who have made this meeting possible. We also would like to thank all the participants for their attendance.

Have a pleasant Conference!

Organizing Committee:

Maryam Abdi (IPM)
Omran Ahmadi (IPM)
Milad Barzegar (IPM)
Salman Beigi (IPM)
Omid Etesami (IPM)
Ali Khezeli (IPM)
Behruz Tayfeh-Rezaie (IPM)

About IPM and its School of Mathematics

The Institute for Research in Fundamental Sciences (IPM) is an institute affiliated with the Ministry of Science, Research, and Technology. It was founded in 1989 under the name “Institute for Studies in Theoretical Physics and Mathematics” and its initial goal was the advancement of research and innovation in theoretical physics and mathematics. The foundation of the Institute was also accompanied by hopes and expectations that a model would be developed which could serve as a basis for the promotion of the culture of research all across the country.

The Institute started its activities with three research groups in physics and three research groups in mathematics (Combinatorics and Computing, Dynamical Systems, and Mathematical Logic & Theoretical Computer Science). In 1994, the Commutative Algebra research group was initiated at the Section of Mathematics, and further activities in this field were pursued.

Initially it had few researchers and limited resources, but gradually it managed to expand its manpower in physics and mathematics, and it also attracted scientists from other disciplines. The activities of the Institute thus extended to other fields and in 1997 it acquired its present name. The Institute now consists of nine schools: Analytic Philosophy, Astronomy, Biological Sciences, Cognitive Sciences, Computer Science, Mathematics, Nano-Science, Particles and Accelerator, and Physics. It enjoys an expanding base of infrastructures and facilities (electronic networking, computers, laboratories, a well-equipped and up-to-date library), and has an active presence in the national research activities within the corresponding fields.

The School of Mathematics (formerly called the Section of Mathematics) has been one of the founder schools of IPM. Presently, there are six main research areas at the School:
Algebra, Algebraic Geometry and Number Theory, Analysis, Combinatorics and Computing, Geometry and Topology, and Mathematical Logic.

IPM Biennial Conference on
Combinatorics and Computing (IPMCCC2025),
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievements of
Professor Gholamreza B. Khosrovshahi

Invited Speakers:

Sharareh Alipour (Tehran Institute for Advanced Studies)
The Minimum Dominating Set and Set Cover in Distributed and Streaming Models

Javad Ebrahimi (Sharif University of Technology)
Stretch Hamming Dimension of Graphs

Ebrahim Ghorbani (K. N. Toosi University and Hamburg University of Technology)
Arrival and Multi-Arrival Problems

Ramin Javadi (Isfahan University of Technology)
Random Hypergraphs and the Size-Ramsey Number of Subdivisions of Graphs

Ali Mohammadian (IPM)
Saturation Numbers of Graphs

Morteza Mohammad Nouri (University of Tehran)
Applying Some Variations of Ziv Lempel Factorization to the Infinite m-bonacci Words

Elham Roshanbin (Alzahra University)
On the Burning Number of Graphs

Morteza Saghafian (Institute of Science and Technology, Austria)
Covering with Heavy Triangles: A Generalization of Delaunay's Theorem

Amin Sakzad (Monash University, Australia)
LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices

Masoud Seddighin (Tehran Institute for Advanced Studies)
Fair Allocation of Indivisible Goods: Recent Advances on the Maximin Share Criterion

Amin Shokrollahi (Kandou (CTO) and EPFL, Switzerland)
Algebraic Coding in the Era of AI

Ali Taherkhani (Institute for Advanced Studies in Basic Sciences)
Erdos-Ko-Rado Type Results for Intersecting Families of Subgraphs of Complete Graphs

Manouchehr Zaker (Institute for Advanced Studies in Basic Sciences)
Recent Progress in the First-Fit and z-Coloring of Graphs

Contributed Speakers:

Omran Ahmadi (IPM)
A Very Short Introduction to Post-Quantum Cryptography

Saeid Alikhani (Yazd University)
New upper Bounds for some Kind of Coalition Numbers

Mostafa Einollahzadeh (Isfahan University of Technology)
From Haemer's Energy Conjecture to Laplacian Matrices

Meysam Korivand (Institut Teknologi Bandung, Indonesia)
Number of Metric Bases up to Automorphism

Maryam Safazadeh (National University of Skills)
Fair Coalitions in Graphs

Scientific Committee:

Ali Khezeli (chair) (IPM)
Omran Ahmadi (IPM)
Salman Beigi (IPM)
Omid Etesami (IPM)
Behruz Tayfeh-Rezaie (IPM)

Conference Schedule

Tuesday, May 20, 2025		
8:30 - 9:00	**Registration**	
9:00 – 10:00	**Opening**	
10:00 - 10:45	**Manouchehr Zaker** Institute for Advanced Studies in Basic Sciences	Recent Progress in the First-Fit and z-Coloring of Graphs
Coffee Break		
11:15 - 12:00	**Javad Ebrahimi** Sharif University of Technology	Stretch Hamming Dimension of Graphs
Lunch		
14:00- 14:45	**Ali Mohammadian** IPM	Saturation Numbers of Graphs
Coffee Break		
15:15 - 16:00	**Elham Roshanbin** Alzahra University	On the Burning Number of Graphs
16:00 – 16:30	**Meysam Korivand** Institut Teknologi Bandung, Indonesia	Number of Metric Bases up to Automorphism
16:30– 17:00	**Omran Ahmadi** IPM	A Very Short Introduction to Post-Quantum Cryptography

You can see the abstract of the talks and other information related to the conference on the below website:

https://math.ipm.ac.ir/IPMCCC2025

SCAN ME!

Wednesday, May 21, 2025		
9:00 - 9:45	**Amin Sakzad** Monash University, Australia	LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices
9:45 - 10:15	**Saeid Alikhani** Yazd University	New upper Bounds for some Kind of Coalition Numbers
Coffee Break		
10:45- 11:30	**Sharareh Alipour** Tehran Institute for Advanced Studies	The Minimum Dominating Set and Set Cover in Distributed and Streaming Models
11:30 - 12:15	**Masoud Seddighin** Tehran Institute for Advanced Studies	Fair Allocation of Indivisible Goods: Recent Advances on the Maximin Share Criterion
Group Photo and Lunch		
14:00 - 14:45	**Ramin Javadi** Isfahan University of Technology	Random Hypergraphs and the Size-Ramsey Number of Subdivisions of Graphs
14:45 - 15:15	**Maryam Safazadeh** National University of Skills	Fair Coalitions in Graphs
Coffee Break		
Mathematics Colloquium		
16:00 - 17:00	**Amin Shokrollahi** Kandou (CTO) and EPFL, Switzerland	Algebraic Coding in the Era of AI **(online)**

Thursday, May 22, 2025		
9:00 - 9:45	**Ebrahim Ghorbani** K. N. Toosi University and Hamburg University of Technology	Arrival and Multi-Arrival Problems
9:45 - 10:15	**Mostafa Einollahzadeh** Isfahan University of Technology	From Haemer's Energy Conjecture to Laplacian Matrices
Coffee Break		
10:45- 11:30	**Ali Taherkhani** Institute for Advanced Studies in Basic Sciences	Erdös-Ko-Rado Type Results for Intersecting Families of Subgraphs of Complete Graphs
11:30 - 12:15	**Morteza Mohammad Nouri** University of Tehran	Applying Some Variations of Ziv Lempel Factorization to the Infinite m-bonacci Words
Lunch		

Abstracts of the Conference Talks

(In Alphabetical Order)

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievement of
Professor Gholamreza B. Khosrovshahi

A Very Short Introduction to Post-Quantum Cryptography

Omran Ahmadi
IPM

As the advent of quantum computers is on the horizon, cryptographers have developed cryptosystems that are resistant to them. In this talk, we briefly introduce some of the most prominent ones.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievement of
Professor Gholamreza B. Khosrovshahi

New upper Bounds for some Kind of Coalition Numbers

Saeid Alikhani
Yazd University

A coalition in a graph $G = (V, E)$ consists of two disjoint sets V_1 and V_2 of vertices, such that neither V_1 nor V_2 is a dominating set, but the union $V_1 \cup V_2$ is a dominating set of G. A coalition partition in a graph G of order $n = |V|$ is a vertex partition $\mathcal{P} = \{V_1, V_2, ..., V_k\}$ such that every set V_i either is a dominating set consisting of a single vertex of degree $n - 1$, or is not a dominating set but forms a coalition with another set V_j which is not a dominating set. The maximum cardinality of a coalition partition of G is the coalition number of G and is denoted by $C(G)$. Different types of domination coalitions have been studied recently. These variations are mainly formed by imposing additional conditions on the domination coalition. In this talk, after reviewing some kind of coalitions, such as coalition, total coalition, independent coalition and strong coalition, we present some new bound for these numbers.

Keywords: Coalition partition, Coalition number, Bound.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

The Minimum Dominating Set and Set Cover in Distributed and Streaming Models

Sharareh Alipour
Tehran Institute for Advanced Studies

In this talk, I will cover algorithms for the Minimum Dominating Set and Set Cover problems in three settings: classical (sequential), distributed, and streaming. I will start with greedy approaches, discussing their approximation guarantees and hardness results, and then move on to techniques based on the primaldual method.

Next, I will present new combinatorial algorithms for bounded-arboricity graphs in the distributed model. Finally, I will discuss the main challenges and open questions in addressing these problems.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Stretch Hamming Dimension of Graphs

Javad Ebrahimi
Sharif University of Technology

The *stretch embedding* of a graph G into a metric space (M, d) is a function f from the vertex set of G to the set M such that for every pair $u, v \in V(G)$ we have $d_G(u, v) \leq d(f(u), f(v))$, in which d_G is the shortest distance metric over $V(G)$.

When (M_m, d_H) is the space of all binary sequences of length m equipped with the Hamming metric, then any stretch embedding to (M_m, d_H) is called a *Hamming stretch embedding* of G. The minimum value of m such that a Hamming stretch embedding to (M_m, d_H) exists is called the *stretch Hamming dimension of* G.

In this talk, we present both exact and approximate results concerning the stretch Hamming dimension of graphs, along with some applications in graph metric codes, particularly in Lee metric codes.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

From Haemer's energy conjecture to Laplacian matrices

Mostafa Einollahzadeh
Isfahan University of Technology

The trace norm (or nuclear norm) of a matrix, defined as the sum of its singular values, plays a significant role in matrix analysis with applications ranging from graph theory to quantum mechanics. For Hermitian and real symmetric matrices, this norm coincides with the sum of absolute eigenvalues, often referred to as the "energy" in algebraic graph theory [1]. A fundamental problem in this domain concerns establishing lower bounds for the trace norm of special types of matrices with constrained entries.

This work originates from a conjecture by Haemers [2] regarding the minimal energy of Seidel matrices associated with simple graphs. Restated in matrix-theoretic terms:

Conjecture. Let A be an $n \times n$ real symmetric matrix with zero diagonal and ± 1 off-diagonal entries. Then $\|A\|_1 \geq 2n - 2$, with equality for $A = J_n - I_n$ (where J_n is the all-ones matrix and I_n the identity matrix).

This conjecture was resolved affirmatively in [3, 4]. We generalize this result to broader classes of matrices, establishing sharp lower bounds for the trace norm in terms of the entrywise L^1-norm. Our main theorems are:

Theorem 0.1 *Let $A = [a_{ij}]$ be a real symmetric $n \times n$ matrix with zero diagonal. Then*

$$\|A\|_1 \geq \frac{2}{n} \sum_{i,j} |a_{ij}|,$$

and this bound is tight for all n.

As an application, we obtain a new lower bound for the energy of signed graphs, generalizing known results for simple graphs:

Corollary. For every signed graph Σ, the energy satisfies

$$\mathcal{E}(\Sigma) \geq 2\bar{d},$$

where $\bar{d}$ is the average degree of Σ.

We combine Theorems 0.1 with standard duality arguments to establish tight upper bounds for the spectral norm distance of real symmetric matrices to diagonal matrices, which is the next theorem (where $\mathcal{D}_n$ denotes the space of real diagonal $n \times n$ matrices):

Theorem 0.2 *For any real symmetric matrix $A = [a_{ij}]$ of order $n \geq 2$,*

$$\min_{D \in \mathcal{D}_n} \|A - D\|_\infty \leq \frac{n}{2} \max_{i \neq j} |a_{ij}|,$$

with sharpness for all $n \geq 2$.

Notably, while Theorem 0.2 guarantees the existence of a diagonal matrix at spectral distance $\frac{n}{2}$ for matrices with entries in $[-1, 1]$, finding such a matrix numerically remains an open problem. But we fully characterize the equality cases in Theorem 0.2 and derive explicit formulas for the nearest diagonal matrices in these cases, revealing a surprising connection to graph Laplacians.

Detailed proofs and discussions appear in [5].

References

[1] I. Gutman, and B. Furtula, *Survey of graph energies*, Mathematics Interdisciplinary Research, University of Kashan, 2017, 85–129.

[2] W. Haemers, *Seidel switching and graph energy*, Available at SSRN 2026916. 2012.

[3] S. Akbari, M. Einollahzadeh, M. Karkhaneei, and M. Nematollahi, *Proof of a conjecture on the Seidel energy of graphs*, European Journal of Combinatorics, 103078, 2020.

[4] M. Einollahzadeh, and M. Nematollahi, *A short proof of Haemers' conjecture on the Seidel energy of graphs*, Linear Algebra and its Applications, 75–78, 2024.

[5] M. Einollahzadeh, *Minimum trace norm of real symmetric and Hermitian matrices with zero diagonal*, http://arXivpreprintarXiv:2309.14958

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Arrival and Multi-Arrival Problems

Ebrahim Ghorbani
K. N. Toosi University and Hamburg University of Technology

Consider particle routing in a network from a source to a sink, where movement is governed by a state-dependent rule: upon visiting a node v, a particle departs via the next outgoing arc in a predefined cyclic order specific to that node. Deciding whether the sink is reachable by a single particle in such a network is known as the Arrival problem. This problem lies in the class NP $\cap$ co-NP, though its solvability in polynomial time remains open. In this talk, after reviewing the Arrival game and the basic results about it, I consider Multi-Arrival, an extension of the original problem that accounts for potentially exponentially many particles moving simultaneously. The goal is to compute the final distribution of particles in the sinks, given an initial configuration. A quasi-polynomial-time algorithm for Multi-Arrival on the class of tree-like directed multigraphs will be presented, which in the case of bounded contracted height, yields a polynomial-time algorithm.

This is joint work with Jonah Leander Hoff and Matthias Mnich.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Random Hypergraphs and the Size-Ramsey Number of Subdivisions of Graphs

Ramin Javadi
Isfahan University of Technology

Given a graph G and an integer $k \geq 2$, the multicolor size-Ramsey number of G, denoted by $\hat{R}(G, k)$, is the smallest integer m such that there is a graph H with m edges for which, in every edge coloring of H with k colors, H contains a monochromatic copy of G. After, the counterexample of Rödl and and Szemerédi (2000) on the linearity of the size-Ramsey of bounded degree graphs in terms of the number of its vertices, the problem that which graphs have linear size-Ramsey have been extensively studied in the literature. Different classes of sparse graphs like paths, bounded degree trees and cycles are shown to have linear size-Ramsey number. In this talk, we will show how different new techniques like random hypergraphs, expander graphs and universal embedding methods can be combined to prove linear upper bounds for the size-Ramsey number of the subdivision of bounded degree graphs, when the length of the subdivisions is of order $\Omega(\log n)$, where n is the number of vertices. Interestingly, the bounds, in terms of the maximum degree Δ and the number of colors k, show different behavior when the length of subdivisions is even or odd.

This is a joint work with Yoshiharu Kohayakawa and Meysam Miralaei.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievement of
Professor Gholamreza B. Khosrovshahi

Number of Metric Bases up to Automorphism

Meysam Korivand
Institut Teknologi Bandung, Indonesia

Let G be a connected graph. A subset S of vertices of G is called a *resolving set* if for every pair of vertices $g_1, g_2 \in V(G)$, there exists $s \in S$ with $\mathrm{d}(g_1, s) \neq \mathrm{d}(g_2, s)$. A resolving set of minimum cardinality is called a *metric basis* for G, and the cardinality of such a set is called the *metric dimension* $\dim(G)$.

Let S be a metric basis of G. In certain applications of metric dimension, such as robot navigation, S plays a crucial role, since it uniquely determines the position of each vertex in the graph. Now, suppose that specifying the position of each vertex using S is not allowed. Therefore, a new metric basis S' is required. However, finding a metric basis is a difficult task as it is proven to be NP-hard. Therefore, the process of finding S' is time-consuming. Here, we reduce this calculation by exploiting the symmetries (automorphisms) of the graph. It is demonstrated that it is not necessary to find all metric bases, as a certain number of them suffices, and the remaining metric bases can be derived from them. The following observation is of pivotal importance to the defined concept.

Observation 0.1 Let G be a connected graph with a resolving set S. Then for any $f \in \mathrm{Aut}(G)$, $f(S)$ is a resolving set.

Let $\mathfrak{S}(G)$ be the set of all metric bases of G. Let $\approx$ be a relation on $\mathfrak{S}(G)$ defined by $S_1 \approx S_2$ if and only if there exists $f \in \mathrm{Aut}(G)$ such that $f(S_1) = S_2$, for any $S_1, S_2 \in \mathfrak{S}(G)$. Clearly, $\approx$ is an equivalence relation on $\mathfrak{S}(G)$. A *resolving class* of a resolving set S, is $[S] = \{f(S) \mid f \in \mathrm{Aut}(G)\}$. Then, for any $S_1, S_2 \in [S]$, $S_1 \approx S_2$; and $S_1 \not\approx S_2$ if and only if $[S_1] \neq [S_2]$. Let $\mathfrak{B}(G)$ be the maximal subset of $\mathfrak{S}(G)$ such that for any two sets S_1 and S_2 in $\mathfrak{B}(G)$, we have $[S_1] \neq [S_2]$. The set $\mathfrak{B}(G)$ contains exactly one representative of each resolving class. We say that $\mathfrak{B}(G)$ is a *resolving basis* of G. Indeed, $\mathfrak{B}(G)$ represents a generator for all resolving sets, which may not necessarily be the smallest possible size. By combining $\mathfrak{B}(G)$ with the automorphism group of G, it is possible to generate all resolving sets of G. In this talk, we examine some results on $\mathfrak{B}(G)$ and present a delineation of open problems and potential areas for future research.

This talk is based on joint work with Prof. Edy Tri Baskoro and Dr. Grahame Erskine.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Saturation Numbers of Graphs

Ali Mohammadian
IPM

Typical problems in extremal graph theory ask for the maximum or minimum value of parameters of graphs with certain properties. A classical problem falling within this framework, posed by Turán in 1941, asks for the maximum number of edges in an F-free graph on n vertices. Recall that a graph H is F-free if H has no a subgraph isomorphic to F. A dual problem, posed by Zykov in 1949, asks for the minimum number of edges of an F-saturated graph on n vertices. Recall that a graph H is F-saturated if H is F-free and adding any missing edge to H creates a copy of F. A dynamic version of the saturation problem, posed by Bollobás in 1968, asks for the minimum number of edges of a weakly F-saturated graph on n vertices. Recall that a graph H is weakly F-saturated if H is F-free and all missing edges in H can be added to H in some order so that a new copy of F is created at each step.

In this talk, we briefly review some known results and open conjectures on saturation and weak saturation numbers of graphs and random graphs.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Applying Some Variations of Ziv Lempel Factorization to the Infinite m-bonacci Words

Morteza Mohammad Nouri
University of Tehran

Ziv Lempel factorization is a kind of factorization of words related to text processing. We mention some variations of this factorization and we compute these factorizations for the infinite m-bonacci words, $m \geq 2$.

This talk is based on three joint works with N. Ghareghani, M. Jahannia, N. Rampersad, P. Sharifani and M. Stipulanti.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

On the Burning Number of Graphs

Elham Roshanbin
Alzahra University

Graph burning or the spread of fire in graphs is a graph process that models the spread of social contagion and was introduced by Bonato et al. in 2014. Burning number is a graph parameter corresponding to graph burning that measures the speed of the spread of fire in graphs.

In this talk, we will go over the definition, history, and some known results on the burning number of graphs.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievement of
Professor Gholamreza B. Khosrovshahi

Fair Coalitions in Graphs

Maryam Safazadeh
National University of Skills(NUS)

Let $G = (V, E)$ be a simple graph. A dominating set of G is a subset $D \subseteq V$ such that every vertex not in D is adjacent to at least one vertex in D. The cardinality of a smallest dominating set of G, denoted by $\gamma(G)$, is the domination number of G. For $k \geq 1$, a k-fair dominating set (kFD-set) in G, is a dominating set S such that $|N(v) \cap D| = k$ for every vertex $v \in V \setminus D$. A fair dominating set in G is a kFD-set for some integer $k \geq 1$. We define a fair coalition in a graph G as a pair of disjoint subsets $A_1, A_2 \subseteq A$ that satisfy the following conditions: (a) neither A_1 nor A_2 constitutes a fair dominating set of G, and (b) $A_1 \cup A_2$ constitutes a fair dominating set of G.

A fair coalition partition of a graph G is a partition $\Upsilon = \{A_1, A_2, \ldots, A_k\}$ of its vertex set such that no subset of Υ acts as a fair dominating set of G, but for every set $A_i \in \Upsilon$, there exists a set $A_j \in \Upsilon$ such that A_i and A_j combine to form a fair coalition. We define the fair coalition number of G as the maximum cardinality of a fair coalition partition of G, and we denote it by $\mathcal{C}_f(G)$. We initiate the study of the fair coalition in graphs and obtain $\mathcal{C}_f(G)$ for some specific graphs.

This is a joint work with Saeid Alikhani.

Keywords: Fair domination, Fair coalition, cycle.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices

Amin Sakzad
Monash University, Australia

We introduce the *first* candidate Lattice-based designated verifier (DV) zero knowledge sUccinct Non-interactive Argument (ZKSNARG) protocol, named LUNA, with quasi-optimal proof length (quasi-linear in the security/privacy parameter). By simply relying on mildly stronger security assumptions, LUNA is also a candidate ZK-SNARK (i.e. argument of knowledge). LUNA achieves significant improvements in concrete proof sizes, reaching below 6 KB (compared to $>$ 32 KB in prior work) for 128-bit security/privacy level. To achieve our quasi-optimal succinct LUNA, we give a new regularity result for 'private' re-randomization of Module LWE (MLWE) samples using discrete Gaussian randomization vectors, also known as a lattice-based leftover hash lemma with leakage, which applies with a discrete Gaussian re-randomization parameter that is *polynomial* in the statistical privacy parameter (avoiding exponential smudging), and hides the coset of the re-randomization vector support set. Along the way, we derive bounds on the smoothing parameter of the intersection of short integer solution (SIS), gadget, and Gaussian perp module lattices over the power of 2 cyclotomic rings. We then introduce a new candidate linear-only homomorphic encryption scheme called Module Half-GSW (HGSW), and apply our regularity theorem to provide smudging-free circuitprivate homomorphic linear operations for Module HGSW. Our implementation and experimental performance evaluation show that, for typical instance sizes, Module HGSW provides favourable performance for ZK-SNARG applications involving lightweight verifiers. It enables significantly (around 5×) shorter proof lengths while speeding up CRS generation and encryption time by 4 - 16× and speeding up decryption time by 4.3×, while incurring just 1.2 - 2× time overhead in linear homomorphic proof generation operations, compared to a Regev encryption used in prior work in the ZK-SNARG context. We believe our techniques are of independent interest and will find application in other privacy-preserving applications of lattice-based cryptography.

This is a joint work with Ron Steinfeld, Muhammed F. Esgin, Veronika Kuchta, Mert Yassi, and Raymond K. Zhao.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Fair Allocation of Indivisible Goods: Recent Advances on the Maximin Share Criterion

Masoud Seddighin
Tehran Institute for Advanced Studies

In this talk, I address the challenge of fairly allocating mmm indivisible items among n agents with diverse preferences, focusing on the *maximin share (MMS)* fairness criterion. The MMS captures the minimum value an agent can secure by dividing the items into n bundles and receiving the least desirable one.

I will survey recent approximation results for the MMS guarantee under various valuation classes, including additive, submodular, XOS, and subadditive valuations.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Algebraic Coding in the Era of AI

Amin Shokrollahi
EPFL and Kandou, Switzerland

The emergence of AI, particularly large language models (LLMs), has dramatically reshaped the requirements for error-correcting codes, particularly in the realm of memory I/O during training. Massive data transfers involved in training LLMs necessitate extremely robust error correction to prevent costly retraining scenarios triggered by undetected errors (Silent Data Corruption). Traditional iterative decoding techniques are inadequate due to their latency constraints, pushing the field towards combinational logic implementations capable of achieving multiple-error correction under extremely tight latency budgets. Algebraic codes, which once seemed to have lost ground to iterative decoding algorithms, are experiencing a renaissance driven by these stringent AI-driven performance demands. By exploiting deep results from algebra, notably Galois theory, algebraic codes are now being implemented in fully combinational hardware circuits that offer both the necessary decoding speed and robust error-correction guarantees. This development underscores algebraic coding theory's renewed relevance and critical importance for future high-performance AI systems.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Erdős-Ko-Rado Type Results for Intersecting Families of Subgraphs of Complete Graphs

Ali Taherkhani
Institute for Advanced Studies in Basic Sciences

The Erdős-Ko-Rado (EKR) theorem is a fundamental result in extremal set theory. It was proved by Erdős, Ko, and Rado in 1938 and later published in 1961. It states that if n and k are positive integers satisfying $n \geq 2k$, then the maximum size of an intersecting family of k-element subsets of the set $\{1, 2, \ldots, n\}$ is $\binom{n-1}{k-1}$. Furthermore, when $n > 2k$, this bound is attained if and only if the family consists of all k-subsets containing a fixed element of $[n]$. Since the original proof, numerous generalizations and alternative proofs of the theorem have been developed. For example, in 1977, Deza and Frankl showed that the maximum size of an intersecting family of permutations on $[n]$ is $(n-1)!$. Also, in 2005, Meagher and Moura showed that in the complete graph on an even number of vertices, the largest size of an intersecting family of perfect matchings is precisely the family of all the perfect matchings that share one specific edge. In 2017, Godsil and Meagher presented an algebraic proof of this result. In 2013, Kamat and Misra extended this result to the family of k-matchings.

In this context, the following natural questions arise.

A family $\mathcal{F}$ of subgraphs of the complete graph K_n is said to be intersecting if any two subgraphs in $\mathcal{F}$ share at least one common edge.

- What is the maximum possible size of an intersecting family of k-cycles in K_n, and what is the structure of the intersecting families that attain this maximum?
- Let $\mathcal{H}$ denote the family of all subgraphs of K_n that are isomorphic to a given graph H. What is the maximum size of an intersecting subfamily of $\mathcal{H}$, and what is the structure of the intersecting families that attain this maximum?

In this talk, we introduce a composition lemma for ErdősKoRado families and use it to answer the above questions. In particular, we show that if n is sufficiently large relative to k, then the largest intersecting families of k-cycles in the complete graph K_n are exactly those where all k-cycles share a common edge. We also show that the same result holds for the largest intersecting subfamily of $\mathcal{H}$, where $\mathcal{H}$ is the family of all subgraphs of K_n that are isomorphic to a given graph H.

This is a joint work with Javad B. Ebrahimi.

IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

Recent Progress in the First-Fit and z-Coloring of Graphs

Manouchehr Zaker
Institute for Advanced Studies in Basic Sciences

Vertex coloring of graphs has broad practical and theoretical importance. Due to the inapproximability of optimal vertex coloring, efficient coloring heuristics are worth studying, acknowledging the fact that every such algorithm has hard-to-color instances. In this talk, we focus on coloring heuristics obtained by using some local recoloring techniques, such as the First-Fit (FF) algorithm and a more sophisticated heuristic invented by the speaker, the so-called z-coloring.

The Grundy number is an invariant that quantifies the worst-case behavior of FF. Only a few classes of graphs are known for which the Grundy number can be determined by a polynomial-time algorithm. We present new families of graphs for which the Grundy number is computed within time complexity O(VE). An approximation algorithm is also presented with an approximation ratio in terms of the girth of the graph. Additionally, some advantages of z-coloring in comparison to FF and b-coloring are discussed. We conclude by introducing some unexplored research problems.