Discrete Mathematics at Peking University

Xingui Fang, Rongquan Feng, Chunwei Song,
Jie Wang, Maozhi Xu and Chuanming Zong

School of Mathematical Sciences, Peking University

August 2015 • Melbourne

Contents

1. Groups and Graphs
2. Directed Strongly Regular Graphs
3. Enumerative combinatorics
4. Cryptology
5. Tetrahedral Packings

Outline

1. Groups and Graphs

2. Directed Strongly Regular Graphs

3. Enumerative combinatorics

4. Cryptology

5. Tetrahedral Packings

Research Team

Peking University: Xingui Fang, Jie Wang

University of Melbourne: Sanming Zhou

University of Western Australia: Cheryl Praeger, Caiheng Li

Main problems

1. Study the symmetric properties of the graph $\Gamma = (V, E)$, such as vertex-symmetric, edge-symmetric etc. The main method is to study the transitivity of automorphism group $Aut(\Gamma)$ acting on the corresponding sets.
2. Construct graphs with various kind of symmetric properties by using group-theoretical methods. For example, all graphs with regular automorphism group can be reconstructed through Cayley graphs. Arc-transitive graphs (symmetric graphs) can be reconstructed by using coset graphs.

Some works

Let Γ be a symmetric Cayley graph of a finite simple group G. We give the description of the structure of $Aut(\Gamma)$ when the valency of Γ is small (≤ 20) or a prime. In most cases, we have $G \lhd Aut(\Gamma)$.

We complete the classification of 2-arc transitive graphs on simple groups $Sz(q)$, $Re(q)$ and $U_3(q)$.

We construct some interesting examples on the regular graph representations of groups and non-quasiprimitive graphs on finite simple groups.

Some works

Let Γ be a symmetric Cayley graph of a finite simple group G. We give the description of the structure of $Aut(\Gamma)$ when the valency of Γ is small (≤ 20) or a prime. In most cases, we have $G \lhd Aut(\Gamma)$.

We complete the classification of 2-arc transitive graphs on simple groups $Sz(q)$, $Re(q)$ and $U_3(q)$.

We construct some interesting examples on the regular graph representations of groups and non-quasiprimitive graphs on finite simple groups.

Some works

Let Γ be a symmetric Cayley graph of a finite simple group G. We give the description of the structure of $Aut(\Gamma)$ when the valency of Γ is small (≤ 20) or a prime. In most cases, we have $G \lhd Aut(\Gamma)$.

We complete the classification of 2-arc transitive graphs on simple groups $Sz(q)$, $Re(q)$ and $U_3(q)$.

We construct some interesting examples on the regular graph representations of groups and non-quasiprimitive graphs on finite simple groups.

Next step:

Go further in these areas mentioned above;

Investigate the relations between graphs and other combinatoric structures through collaboration with Sanming Zhou.

Outline

1. Groups and Graphs
2. Directed Strongly Regular Graphs
3. Enumerative combinatorics
4. Cryptology
5. Tetrahedral Packings

Directed Strongly Regular Graphs

A *directed strongly regular graph* with parameters (n, k, t, λ, μ), denoted simply by DSRG(n, k, t, λ, μ), is a directed graph Γ with n vertices such that

1. every vertex has in-degree and out-degree k;
2. every vertex x has t out-neighbors that are also in-neighbors of x; and
3. the number of directed paths of length two from a vertex x to another vertex y is λ if there is an edge from x to y, and is μ if there is no edge from x to y.

Directed Strongly Regular Graphs

A DSRG can be regarded as a directed version of a *strongly regular graph* where $t = k$. A DSRG with $t = 0$ is a graph known as *doubly-regular tournament*. Thus the constructions of DSRGs with $0 < t < k$ are much interesting. What we have done are as follows:

Directed Strongly Regular Graphs

1. A characterization of DSRG via its adjacency matrix. Let A be the adjacency matrix of a directed graph Γ. The Γ is a DSRG(n, k, t, λ, μ) with $0 < t < k$ if and only if each row and each column of A has k 1's, A is diagonalizable and A has three distinct integral eigenvalues;
2. Constructions of DSRG by $1\frac{1}{2}$-designs. Several infinite families of $1\frac{1}{2}$-designs from symplectic, unitary and orthogonal geometries over finite fields are constructed. And then several DSRGs are obtained from them;
3. Constructions of DSRG by (generalized) Cayley graphs;

Outline

1. Groups and Graphs
2. Directed Strongly Regular Graphs
3. Enumerative combinatorics
4. Cryptology
5. Tetrahedral Packings

Enumerative combinatorics

Professor Chunwei Song works on enumerative combinatorics and graph theory, more specifically, the combinatorial theory on lattice paths, special sequences, q-theory and combinatorial statistics. Sometimes extremal structures and algebraic/probabilistic methods are concerned.

The following sample results has variations and applications. For convenience, we only present the most understandable forms.

Enumerative combinatorics

(Least Child Being Monk Formula)

The number of labelled trees on the alphabet 0,1,2,...,n,n+1 such that the minimally labelled neighbor of 0 is a leaf, i.e. nonadjacent to any other vertex besides the vertex 0, is counted by n^n.

Enumerative combinatorics

(The m-Schröder number)

The number of paths going from (0,0) to (mn, n)*, using only steps (0,1), (1,0) and (1,1) and never going below the main diagonal* $\{\,(mi, i) \mid 0 \le i \le n\,\}$*, is counted by*

$$\sum_{d=0}^{n} \frac{(mn+n-d)!}{(mn-d+1)!(n-d)!d!}.$$

Outline

1. Groups and Graphs
2. Directed Strongly Regular Graphs
3. Enumerative combinatorics
4. Cryptology
5. Tetrahedral Packings

Cryptology

Cryptology consists of two aspects: Cryptography and Cryptanalysis. We are interested mainly in the following areas:

1. Efficient computation methods for scalar multiplications and pairing on certain classes of elliptic curves, especially by using some efficiently computable endomorphisms;
2. Solving the discrete logarithm problem on algebraic curves by Index Calculations methods;
3. Computations on the elliptic curves on local fields;
4. Designing Boolean Bent functions with higher algebraic immunity degree;
5. Construct lattice-based key exchange protocols on small integer solution problem.

Outline

1. Groups and Graphs
2. Directed Strongly Regular Graphs
3. Enumerative combinatorics
4. Cryptology
5. Tetrahedral Packings

Tetrahedral Packings

At the ICM 1900 in Paris, David Hilbert proposed 23 unsolved mathematical problems. At the end of his 18th problem, he asked “How can one arrange most densely in space an infinite number of equal solids of given form.”

The problem has a long history. For example, in 1611 Kepler asserted that the densest sphere packing was given by the face-centered cubic lattice packing. This assertion, known as Kepler’s Conjecture, was proved by Hales. Concerning the densest packing of regular tetrahedra, Aristotle stated that regular tetrahedra fill space. Unfortunately, this is not the case.

Tetrahedral Packings

This problem and its generalizations have been studied by many prominent mathematicians, like Gauss, Minkowski, Hlawka, Rogers and many others. Recent years, important applications of this problem have been discovered in Material Science.

Tetrahedral Packings

Professor Chuanming Zong has studied this problem for more than two decades, and has obtained the first upper bound for the translative tetrahedral packings. Precisely speaking, he proved that the density of the densest translative packings by identical regular tetrahedral is between 0.3673469 and 0.3840610. Jeff Lagarias and Chuanming Zong surveyed this topic and reported Zong's breakthrough. For this work, they were awarded a Conant Prize in 2015 by the American Mathematical Society.

Thank you!