SPUR 2007
Abstracts

Sumsets and Graph Theory in Additive Combinatorics

Erika Bakse (Mentor: Catherine Lennon)

Let A be a subset of $\mathbb{F}_2^n$. We explore the bounds of the smallest d such that $A + A$ does not contain a coset of a subspace of dimension d. We use Cayley graphs to study the structure of A, as well as develop a new type of graph that focuses on the structure of $A + A$.

Generalizing Regev's Cryptosystem

Alessandro Chiesa (Mentor: Amit Jayant Deshpande)

In this paper, we describe how the space requirements of Regev's cryptosystem can be reduced with a simple modification of the encryption step. We further show how to generalize Regev's cryptosystem to any number field so that security may be greatly improved.

Variants of the Chromatic Number of the Plane

Joseph Cooper (Mentor: Luis Rademacher)

We start by introducing the problem of the chromatic number of the plane and known results, techniques, and approaches. We then use several inequalities from probability theory in order to derive lower bounds (as an increasing function of n) on the chromatic numbers of the spaces $\mathbb{R}^n$. We then construct a collection of variations of the unit distance graph on $\mathbb{R}^2$ ($G\{D_\theta, \mathbb{R}^2\}$ graphs) and derive upper and lower bounds on their chromatic. Numerous other less fruitful variants and generalizations are also discussed.

Freiman-Type Theory For Small Doubling Constant

Hansheng Diao (Mentor: Catherine Lennon)

In this paper, we study the linear structure of sets $A \subset \mathbb{F}_2^n$ with doubling constant $\sigma(A) < 2$, where $\sigma(A) := \frac{|A+A|}{|A|}$. In particular, we consider the functions $F(K)$ and $G(K)$ (will be defined in the paper) which quantify certain extremal properties of all sets A such that $\sigma(A) \leq K$. We extend the results in [**?**] by determining the exact values of $F(K)$ and $G(K)$ when $1 \leq K < 2$. We also classify all sets with small doubling constant.

A representation of the type B_N dAHA

Rebecca Freund (Mentor: Xiaoguang Ma)

Discussion on Sandglass Conjecture and Generalization

Shinnyih Huang (Mentor: Hoda Bidkhori)

In this report, we define recovering set, strongly cancellative set, and the reformulation of recovering pair on different lattice such as B_n and D_n. We get a bound $2^{0.439n}$ for recovering set on boolean lattice. For strongly cancellative set, on boolean we have a tight bound which is $2^{0.5n}$, and for product of k l-length chains, we have an upper bound which is $(4(l+1))^{\frac{k}{2}}$ and a construction(lower bound) which has $(l+1)^{\lfloor \frac{k}{2} \rfloor}$ elements. The main concepts we use in our proof is a well-known inequality of entropy function in information theory.

On the Basis of $[A_n, A_n]/[[A_n, A_n], A_n]$

John Kim (Mentor: Xiaoguang Ma)

Given a free associative algebra A_n generated by n variables, it is known that $[A_n, A_n]/[[A_n, A_n], A_n]$ is isomorphic to the space of closed positive even forms. We use this knowledge to explicitly construct a basis for the degree l components of $[A_n, A_n]/[[A_n, A_n], A_n]$. As an application of our result, we compute the dimension of $[A_n^R, A_n^R]/[[A_n^R, A_n^R], A_n^R]$, where $A_n^R = A_n/(x_1^{m_1} = \ldots = x_n^{m_n} = 0)$.

Some Noncompact Convexity Theorems for Hermitian Matrices

Khoa Lu Nguyen (Mentor: Zuoqin Wang)

Let $\vec{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{R}^n$. Denote by $\mathcal{H}_a$ the set of $n \times n$ Hermitian matrices whose diagonal entries are $a_1, a_2, \cdots, a_n$. Suppose $A \in \mathcal{H}_a$. We denote by $A^{(k)}$ the k^{th} principal minor of A, which is the $(n-k)\times(n-k)$ matrix in the upper-left corner of A. Let $(\lambda_{k,l})_{1 \leq l \leq n-k}$ be the eigenvalues of $A^{(k)}$ and $\lambda_{k,1} \geq \cdots \geq \lambda_{k,n-k}$. In this paper, we will study the maps from A to its eigenvalues and to the eigenvalues of all of its principal minors. We will prove some convexity theorems for such maps, which describe the image explicitly as convex polyhedral sets. Such convexity theorems can be viewed as dual version of the well-known convexity theorems of Schur-Horn and Gelfand-Cetlin. Inspired by Duistermaat-Heckman's work on symplectic geometry, we will also define the push-forward of the standard measure to this image, which can be viewed as a probability version of the convexity theorems.

Lower bounds for linear locally decodable codes

Anand Rajagopalan (Mentor: Amit Deshpande)

In this paper, we prove the $2^{\Omega(k)}$ lower bound on the rate of linear 2-query locally decodable codes, by counting edges in a hypercube. We also prove an $\Omega(\frac{k^2}{\log k})$ lower bound for 3-query locally decodable codes using the probabilistic method based on techniques from [**?**].

Minimum Partition into Product Sets

Xuancheng Shao (Mentor: Luis Rademacher)

Our main problem arises in the proof of computational lower bound on the complexity of volume algorithms. We wish to derive an upper bound in the ball partitioning problem in order to improve the computational lower bound from $n^2/log(n)$ to n^2. However, the proof in this report shows that this cannot be achieved. On the other hand, we derived a tight bound (up to some constant in the exponent) for the ball partitioning and covering problems. In addition, we also considered the general partitioning and covering problems as a generalization.

Zero-sum problems in finite groups

Charmaine Sia (Mentor: Hoda Bidkhori)

We investigate zero-sum problems in finite groups, a subfield of additive group theory and combinatorial number theory. Upper bounds on Davenport's constant are established for direct products of certain solvable groups. Exact values and upper bounds are obtained for various zero-sum invariants of dihedral groups and groups of the form $C_{p^{a_1}} \times \cdots \times C_{p^{a_{r-1}}} \times C_{mp^{a_r}}$.