1 Inverse Problems of Arithmetic Combinatorics

Take a set of n elements A. It does not really matter what the elements are – only the size of the set is key.

Consider a finite abelian group A. Suppose that for any $a \in \mathbb{Z}$, $a \neq 0$, the sum of n a's is not equal to zero.

Now, let's think about Minkowski sums of the set A with itself. What can we say about its size?

Trivially, we can bound $|A + A|$ as $|A| \leq |A + A| \leq |A|^2$.

Theorem 1.1

$|A + A| \geq 2|A| - 1$.

Proof.

Write two columns representing elements as hinges, with one hinge over another if an element is bigger than the other. Imagine a stick lying on these hinges. Assume first that the stick lies on the lowest hinge. Each time another element is added on the right to the element on the left, the stick goes up.

□

Theorem 1.2 (Cauchy-Davenport's Theorem)

Suppoe that two sets A and B are given such that $A, B \subseteq \mathbb{Z}_p$, where p is prime. Then $|A + B| \geq \min(|A| + |B| - 1, p)$.

Now, denote $\sigma[A] = \frac{|A+A|}{|A|}$ as $\sigma(A)$. Then $\sigma[A] \leq 3 \Rightarrow \exists P(|P| = 2|A| \,|A \subseteq P))$.

We can construct Freiman isomorphisms, such that $a_1 + a_2 \neq a_3 + a_4 \Leftrightarrow \phi(a_1) + \phi(a_2) \neq \phi(a_3) + \phi(a_4)$, while $a_1 + \cdots + a_8 = a_9 + \cdots + a_{16}$.

In this way, we construct sets with the low value of σ, so that $\sigma[A] \leq \frac{2^d}{\rho}$ and $\frac{|A|}{Q} \geq \rho$ by taking a parallelopiped, choosing a dense subset and projecting onto the integer lattice.

Theorem 1.3 (Freiman's Theorem)

Suppose that $K > 0$ is a constant.

Let $A \subseteq \mathbb{Z}$ and $\sigma[A] \leq K$. Then $A \subseteq Q$, and Q is a $\delta(K)$-dimensional arithmetic progression, where δ is some function, and $|A| \geq \rho(K)|Q|$.

For applications of Freiman's theorem, see Rouge inqualities, stating that, if $\sigma[A] \leq K$, then $|A - A|, |A + A - A|, \ldots, |mA - nA| \leq K^{m+n}|A|$.

Another important result was obtained by Bogolyubov:

Lemma 1.4 (Bogolyubov's Lemma)

For any A there exists a generalised arithmetic progression Q such that $Q \subseteq 2A - 2A$ and $|Q| \ \ geq\rho|2A - 2A|$.

1.1 Discrete Fourier Transformation

Consider homomorphisms in the form $\chi : \mathbb{Z}_p \to \mathbb{C}^*$ such that $\chi(a+b) = \chi(a)\chi(b)$, $\chi(1) = \xi$, and $\chi(0) = 1 = \xi^p$.

Then $\chi_m(a) = e^{\frac{2\pi ami}{p}}$.

Take $f : \mathbb{Z}_p \to \mathbb{C}$. We have $\widehat{f}(\chi) = \frac{1}{p}\sum_{a\in\mathbb{Z}_p} f(a)\chi(a)$.

Define $\mathbf{1}_A(a = \begin{cases} 1, a \in A \\ 0, a \notin A \end{cases})$.

Parseval's inequality states that $Spec_\alpha(A) \leq \alpha^2$, while $\widehat{1}_A(\chi) \geq \alpha$.

Now, let's consider convolutions of characteristic functions. $(f * g)(z) = \sum_{x+y=z} f(x)g(y)$.

For example, if f and g are probability distributions, then their convolution is also a probability distribution.