The polynomial method in additive number theory

Supervisor: Taboka Prince Chalebgwa

Synopsis:

This project falls within the (relatively) new and rapidly developing area that goes by several aliases, including: "*additive/arithmetic combinatorics*", "*additive number theory*", "*combinatorial number theory*". Loosely speaking, this can be described as the study of "*arithmetic properties*" of sums of sets of integers. More concretely: suppose $A, B \subseteq \mathbb{Z}$, what facts can be deduced about the *sumset* $A + B := \{a + b : a \in A, b \in B\}$. For instance, can we say something about the cardinality $|A + B|$ given the cardinalities $|A|$ and $|B|$?

Traces of this line of enquiry can be traced back to some works of Cauchy, namely:

The **Cauchy-Davenport Theorem**: Let p be a prime number, and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$. Then, we have that $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

This theorem can in turn be used to deduce the rather beautiful:

Erdös-Ginzburg-Ziv Theorem: Let $S = \{a_1, a_2, \ldots, a_{2n-1}\}$ be *any* sequence of $2n - 1$ elements of the group $\mathbb{Z}/n\mathbb{Z}$. Then we can always find n elements of S which sum to zero modulo n. (In other words, the sum of these n elements is divisible by n).

Now, let $A \dot{+} B := \{a + b : a \in A, b \in B, \quad \text{and} \quad a \neq b\}$. In the 1960s, Erdös and Heilbronn conjectured that, under this "new" set addition, the bound in the Cauchy-Davenport theorem "changes". More specifically:

The **Erdös - Heilbronn Conjecture**: Let p be a prime number, and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty sets. Then, we have that $|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}$.

The conjecture was first verified by Dias da Silva and Hamidoune in 1994. Over time, these results have been extended in many different directions, for instances, extensions to more general groups than just $\mathbb{Z}/p\mathbb{Z}$, or to more than just two sets A and B.

Now, these theorems can all be proved in a unified manner via the so-called "*polynomial method*". The underlying philosophy here is to "capture" the combinatorial properties of one's problem, and then proceed to use techniques from linear algebra, abstract algebra, and (sometimes) algebraic geometry to tackle the now "algebraic" problem, followed by "translating" the solution back to the combinatorial setting .

Notable amongst these techniques is Alon's *Combinatorial Nullstellensatz*, which is essentially the multivariate version of the (extremely trivial) observation that given a polynomial $P(x)$ of degree d, say, and a set S of $n > d$ elements, there necessarily exists a point, say $t \in S$, such that

$P(t) \neq 0$. Despite it's seemingly simplistic nature, the nullstellensatz has far reaching consequences! In particular, the results discussed above all readily follow from the theorem, whereas the purely combinatorial versions of their proofs often require deep and technical arguments.

Besides just furnishing beautiful and remarkably efficient proofs of already known results, the polynomial method (and in particular, the nullstellensatz), has resulted in the resolution of many deep and longstanding problems in additive number theory, finite geometry (finite field Kakeya conjecture), and discrete mathematics (many graph colouring problems), and the full extent of its power and flexibility is still subject of intense study.

The goal:

Any subset of the following.

- To study and understand the nullstellensatz, its proof, and some of its recent extensions.
- Explore its various applications to different problems.
- Obtain analogues of some of the classical applications, in light of some of the extensions of the theorem.
- If you are particularly adventurous, upon gaining a thorough understanding of the theorem and the types of problems it has had success being applied to, you can tackle one or two of the numerous open problems in this general area, some of which are at a level appropriate for an honours project investigation.

Keywords: Cauchy-Davenport, polynomial method, combinatorial nullstellensatz, (un)restricted sumsets.

The following is not absolutely necessary, since any gaps may be filled through some reading assignments (or even a reading course), BUT, you will get more out of the project if you:

- have taken WTW 221 (Linear algebra), WTW 285 (Discrete structures), WTW 381 (Algebra).
- are taking WTW 731 (Algebra).