Quantum-Sound Factorization: On the Distribution and Structure of Irreducible Sets

Aggarwal, Anay (School: Westview High School)

The difficulty of prime factorization is essential to keeping our world secure. However, the rise of quantum computing poses a major threat to this security, and thus, it is imperative to discover and study structures for which factorization is even more difficult, as these make for potentially quantum-secure cryptographic schemes. Sets equipped with the Minkowski Sum operation provide such a structure, allowing a natural definition of "prime" or irreducible sets and factorization of sets. Kim and Roush (2005) showed that a cryptosystem based on set factorization could likely resist even the most powerful quantum computers. On the other hand, we lack enough mathematical understanding to craft such a cryptosystem. Additive combinatorics, one of the most active fields of math, with over 3000 papers published in the past 60 years, seeks to better understand set factorization- in particular, irreducible sets. Such understanding is vital for real-world application. In this work, I make foundational progress by developing a strengthened "Prime Number Theorem" for sets, resolving a four-year-old conjecture of Dr. Alfred Geroldinger and Dr. Salvo Tringali. In particular, I show that sparse sets are highly likely to be irreducible, whereas the opposite holds for exceedingly dense sets, with precise asymptotics. I further develop a primality test that identifies 6-18% of prime sets- an unprecedented result in any mathematical domain, including the integers. Finally, I establish additional results of interest to statisticians, mathematicians, and cryptographers, such as demonstrating that irreducible sets, when normalized, approximately follow a binomial distribution.

Awards Won: