Universal Matrices for Counting Fibo-Multinomial and C-Multinomial Coefficients With a Cryptographic Application

Chand, Arav (School: Half Hollow Hills High School West)

Cryptographic systems securing global communications depend on computationally hard mathematical problems. Yet, the divisibility structure of combinatorial objects like Pascal's Triangle remains a largely untapped source of such hardness. Rowland established a matrix product formula encoding prime divisibility behavior for binomial coefficients, raising the question of whether this structure extends to far more general objects and higher dimensions. In this research, I derived matrix product formulas for the prime divisibility of C-multinomial coefficients, a family of generalized binomial coefficients defined by an integer sequence C, extended to all dimensions k >= 2. After performing large-scale symbolic computation in Mathematica to detect structural patterns and formulate conjectures, I then proved them via bijective counting arguments and the Principle of Inclusion-Exclusion. The central result is a universality theorem: the same family of matrices governs the divisibility of binomial, C-nomial, multinomial, and C-multinomial coefficients simultaneously, regardless of the choice of sequence C. This is surprising because the matrices carry no information about C whatsoever. My theorem reduces computational complexity from O(n^3 log n) to O(log n). Leveraging this efficiency, I constructed a cryptographically secure pseudorandom number generator grounded in this number-theoretic structure, whose output passed all NIST statistical tests over 500 million bits and resisted state-compromise extension attacks via time-based reseeding. These results unify the divisibility theory of infinitely many combinatorial sequences under one framework, and establish that combinatorial number-theoretic structures can serve as an independent cryptographic hardness foundation.

Awards Won:
Second Award of $2,400
American Mathematical Society: One-Year Membership to American Mathematical Society to each winner (7 winning projects, up to 3 team members per project)
American Mathematical Society: Third Award of $500
Mu Alpha Theta, National High School and Two-Year College Mathematics Honor Society: Second Award of $1,000