Binary Irreducible Quadratic-Residue Codes and the Good Code Problem

Author
Claire Thompson

Advisor
Asher Auel

Description
My project fit well with my academic background in Abstract Algebra/Galois Theory and the few coding classes I had taken in high school and at Yale. The first month or so was reading as much as I could about Coding Theory and specifically the open problem of the minimal Hamming distance. After deciding that binary cyclic codes were of most interest to me, Professor Auel and I focused my reading on this topic, trying to search for patterns in previous results and the methods other mathematicians were using to approach the problem. Meanwhile, I justified my theoretical explorations and findings by using the Magma Computational Algebra System to compute upper bounds on base cases of the problem to direct our approach and question a previously published finding.

Abstract
Efficiently computing the minimal Hamming distance is a long standing problem in error-correcting coding theory. We describe the importance of this problem and focus on a corresponding open question: whether or not there exist good cyclic codes, or an infinite family of cyclic codes such that the ratios of the dimension and minimal distance to the length is bounded below by a constant. Most work so far points towards a negative answer, and special attention has been given to the quadratic-residue cyclic codes.

We present existing bounds and conjectures on the Hamming weights of binary quadratic-residue codes and explore a subset of these codes, irreducible cyclic codes of prime length such that the order of 2 $\in$ Fp is (p-1)/2. After establishing the symmetry of the Hamming weight distribution of these codes and equivalence classes between irreducible cyclic codes of the same dimension (results relevant in simplifying weight computations), we consider these codes as a potential family of good codes. Using upper bound computations found through utilization of the Magma Computational Algebra System [4], we conjecture that this family is not a family of good codes, contrary to the heuristic presented in [9]