TITLE: Polynomial Functions Over Finite Fields

AUTHORS: John Hull

FACULTY SPONSOR: Florian Enescu, Ph.D., Associate Professor, College of Arts and Sciences

Introduction: Polynomial functions over finite fields are important in computer science and electrical engineering in that they present a mathematical representation of digital circuits. The validity of circuit designs can be tested abstractly using polynomial representations of circuits instead of physical testing the circuits post-construction. Toward this end, we aim to find necessary and sufficient conditions for polynomial functions with coefficients in a field of characteristic p, when restricted to a subfield, to map from the restricted domain to a different subfield of the original field. This problem is of particular interest in the aforementioned context when $p = 2$ due to the relationship between fields of characteristic 2 and binary structures.

Method: For univariate polynomials, relationships between powers of the indeterminate and the behavior of indeterminate's evaluation at elements of the restricted domain was examined to determine patterns that could be used to verify a mapping's image through the equation-of-coefficients method. This relationship was examined in the general case of the characteristic prime and powers of that prime.

Results: A method satisfying the above requirements is presented for all primes and all positive powers of those primes through the discovery of a permutation on a particular set related to the largest degree of a polynomial with coefficients in the original field of characteristic p but evaluated at the subfield of restriction. This permutation is cyclic and permutes the coefficients of the restricted polynomial in such a way that the requirements of the restricted polynomial mapping to the target subfield are met if and only if an equation-of-coefficients system is satisfied. For cases of a prime p, an algorithm for construction of an n-by-n matrix representing this permutation, where n is the order of the subfield of restriction, is presented.

Conclusion: Our findings demonstrate that it is possible to greatly reduce the computational expense of the problem outlined above. Further research should aim to outline the behavior of the aforementioned permutation with respect to specific primes and solve the above problem for multivariate cases.