Finite Field Elements of High Order from Subspace Polynomials

by

Nha Hoang (aka Liv)

Submitted to the

Department of Computer Science

May 03, 2013

In Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Science

ABSTRACT

A finite field is a field with finitely many elements. A basic class of finite fields is the fields $\boldsymbol{F}_p$ with p elements (p is a prime number): $\boldsymbol{F}_p = Z/pZ = \{0, 1, \ldots, p-1\}$, where the operations are defined by performing addition and multiplication operations in the set of integers **Z**. This paper will use the extension fields of $\boldsymbol{F}_p$: $\boldsymbol{F}_{p^n} = \boldsymbol{F}_p[x] / (f(x))$ where $f(x)$ is a modulo p irreducible polynomial of degree n over $\boldsymbol{F}_p$. By the "order" of a nonzero element g we mean the least positive integer k such that $g^k = 1$. The well-known problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field has acquired additional importance, as in cryptology, groups with elements of high orders are used in cryptosystems in order to be safe from attacks. This paper is to continue the work in "Constructing high order elements through subspace polynomials" [1]: surveys and analyzes the construction of high order elements in finite field extensions using subspace polynomials. We compute the exact multiplicative order of elements in finite field extensions $\boldsymbol{F}_{q^{(q^c-1)/(q-1)}}$ for field size up to 677 bits, where q is a prime and c is a positive integer and observe that the largest order an element in these finite fields can have is $\left(q^{(q^c-1)/(q-1)} - 1\right)$.

Date: Friday, May 03, 2013
Time: 1:00 PM
Place: Devon Energy Hall (DEH) Room # 151

Committee Members

Dr. Qi Cheng (Chair, CS)
Dr. Sridhar Radhakrishnan (CS)
Dr. Changwook Kim (CS)
Dr. Mohammed Atiquzzaman (CS)