An Examination of the Structure of Extension Families of Irreducible Polynomials Over Finite Fields

Matthew Psioda

A Thesis Submitted to
University North Carolina Wilmington in Partial Fulfillment
Of the Requirements for the Degree of
Master of Science

Department of Mathematics and Statistics

University North Carolina Wilmington

2006

Approved by

Advisory Committee

_____ _____

_____

Chair

Accepted by

_____

Dean, Graduate School

This thesis has been prepared in the style and format
consistent with the journal
American Mathematical Monthly.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In this paper we examine the behavior of particular family of polynomial over a finite field. The family studied is that obtained by composing an irreducible polynomial with prime power monomials. We examine methods of testing irreducibility via a new method of discriminant calculation. We also provide new incite into how the members of the given family factor when not irreducible. Further, we provided a finite field generalization to "Roots Appearing in Quanta", an article presented by Perlis.

ACKNOWLEDGMENTS

I would like to thank all of the UNCW faculty who have offered guidance, advice, and motivation to me during the past six years. A special thanks is extended to Dr. Freeze for serving as my faculty advisor. Without his supervision and encouragement, I could not have succeeded in this endeavor.

I am equally grateful to my family and friends for their support during my work at UNCW. Any successes I have had during this time are as much a testimony to their love and support as they are to any abilities I may posses.

Finally, I would like to that my fiance Ashley Thompson. It is certain that she had to weather as much frustration as I did during this time. However, her care and support never wavered. For that, I am eternally grateful.

1 INTRODUCTION

The behavior of polynomials over finite fields is a topic of major interest for mathematicians from a variety of disciplines. Even the beginning algebraist would recognize that arithmetic over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is governed by the irreducible polynomials of degree m in $\mathbb{F}_q[x]$.

In this paper we examine specific families of finite field polynomials obtained by composing an irreducible polynomial with a prime power monomial. The family can be formally defined as follows.

Definition 1.1 *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ and let p be an odd prime rational integer. The set $\{f_{p,k}(x)\}$ is defined to be all polynomials of the form $f(x^{p^k})$ where k is a positive rational integer. We refer to this set as the set of monomial p^{th} power extensions of $f(x)$. We say that $\{f_{p,k}(x)\}$ is irreducible over $\mathbb{F}_q$ if each element is irreducible over $\mathbb{F}_q$.*

Much of our effort will be dedicated to showing how this family can be used to construct irreducible polynomials over the given base field. First, we provide a collection of interesting results aimed at providing quick and useful tests to determine whether the members of a given family are irreducible. Initially we introduce an efficient formula for calculating the discriminants of the polynomial members of a given family and then apply a result of Swan [2] to develop an efficient irreducibility.

Gao and Panario [1] provided conditions for when this family will be irreducible and we discuss those at some length. Violating these conditions will be the basis for our examination of the factorability of non-irreducible families. In addition to these ideas, we provide an alternative algorithm which determines all of the irreducible polynomials of appropriate degree over $\mathbb{F}_q$ that have irreducible extension families when composed with x^{p^k} for some prime p.

We then provide an interesting discussion of how these results can be cast in a slightly different light to serve as a residue test. The Law of Quadratic Reciprocity is well known; however, higher order reciprocity laws are not as useful for direct computation of whether or not a given field element is a residue for a given prime. The information presented in this paper provide a rather simple algorithm for determining when the roots of an polynomial $f(x)$ are p^{th} residues in the splitting field.

The remaining discussion of the paper deals with the factorization of the members of a family given that it is reducible. In this section we present the main result of the paper. That is, given reducibility of an extension family, one can determine the number of factors and the degrees of each factor for every member of the family. We then apply these results in concert with ideas from Agou [6] to provide conditions on the number of roots that any one extension polynomial may have in a given field extension. This is a generalization of the ideas provided by Perlis in [5].

2 DISCRIMINANTS

Initially, it would be useful to recall the definition for the discriminant of a polynomial. There are many ways to compute this number and the common derivative representation is provided here.

Definition 2.1 *Let $f(x)$ be a polynomial in the ring $R[x]$. Let $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ denote the set of roots of $f(x)$. We define the discriminant of $f(x)$, denoted $D(f)$, to be as follows:*

$$D(f) = \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i)$$

Above, the first expression is provided to convey that the discriminant of a polynomial is a measure of the distance between the roots. When finding the actual value of a discriminant, the second representation will be used.

Since the initial goal here is to examine the relationship between the discriminants of the members of $\{f_{p,k}(x)\}$ and their respective factorizations, it would be useful if the discriminant of $f(x^{p^k})$ could be written in terms of the discriminant of $f(x)$. Fortunately, this is achievable.

Proposition 2.1 *Let $f(x) \in R[x]$ be a polynomial of degree n having α as a root. Denote $N(\alpha)$ as the product of the conjugates of α. Define $F(x) = f(x^{p^k})$ where $p, k \in \mathbb{Z}^+$ and p is an odd prime. Then $D(F)$ can be found as follows:*

$$D(F) = (-1)^{\frac{np^k(np^k-1)}{2} - \frac{n(n-1)}{2}} (p^k)^{np^k} D(f)^{p^k} N(\alpha)^{p^k - 1}$$

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. Define $F(x)$ as in the proposition. Then it follows that

$$D(F) = (-1)^{\frac{np^k(np^k-1)}{2}} \prod_{i=1}^{np^k} F'(\beta_i) \tag{1}$$

where the β_i are the roots of $F(x)$. Noting that $F(x) = x^{np^k} + a_{n-1}x^{(n-1)p^k} + \cdots + a_1x^{p^k} + a_0$, it is quickly verifiable that $F'(x) = p^k x^{p^k-1} f'(x^{p^k})$. Substituting this in (1) yields

$$D(F) = (-1)^{\frac{np^k(np^k-1)}{2}} \prod_{i=1}^{np^k} p^k x^{p^k-1} f'(\beta_i^{p^k}). \tag{2}$$

Note that by the way $F(x)$ is defined, each root β_i of $F(x)$ is equal to $p^{k^{th}}$ root of some α_j for $1 \leq j \leq n$. Thus, it is natural to realize the product $\prod_{i=1}^{np^k} f'(\beta_i^{p^k})$ as the product $\prod_{j=1}^{n} f'(\alpha_j)$ taken p^k times. Recalling the definition for the discriminant, it follows that this product is exactly $(-1)^{\frac{-n(n-1)}{2}} D(f)^{p^k}$. Substituting this information into (2) yields

$$D(F) = (-1)^{\frac{np^k(np^k-1)}{2} - \frac{n(n-1)}{2}} (p^k)^{np^k} \prod_{i=1}^{np^k} \beta_i^{p^k-1} D(f)^{p^k}. \tag{3}$$

Finally, again recall the observation that for each i, $\beta_i^{p^k} = \alpha_j$ for some $1 \leq j \leq n$. It then follows directly that

$$\prod_{i=1}^{np^k} \beta_i^{p^k-1} = \prod_{i=1}^{np^k} \beta_i^{p^k} \beta_i^{-1} = \left(\prod_{j=1}^{n} \alpha_j\right)^{p^k} \left(\prod_{i=1}^{np^k} \beta_i\right)^{-1} = N(\alpha)^{p^k} N(\beta)^{-1} = N(\alpha)^{p^k-1}.$$

Here the last equality is justified by noting that the norms of $f(x)$ and $F(x)$ are the same. Making a final substitution of this result into (3) establishes the proposition.

Q.E.D

This result is easily generalizable by replacing x^{p^k} in the composition with $f(x)$ with any monomial of the form x^n with n an odd composite positive integer. This result is stated in the following corollary.

Corollary 2.1 *Let $f(x) \in R[x]$ be a polynomial of degree m having α as a root. Denote $N(\alpha)$ as the product of the conjugates of α. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where each $p_i, e_i \in \mathbb{Z}^+$ and each p_i an odd prime. Define $F(x) = f(x^n)$. Then $D(F)$ can be found as follows:*

$$D(F) = (-1)^{\frac{mn(mn-1)}{2} - \frac{m(m-1)}{2}} (n)^{mn} D(f)^n N(\alpha)^{n-1}$$

The proof here is essentially the same as that of the proposition and is therefore omitted.

Discriminant calculations may be further simplified if the degree of the polynomial under consideration is even. This condition ensures that the discriminant of the $f(x)$ and $F(x)$ have the same sign. This fact can be quickly verified by observing that

$$\frac{np^k(np^k-1) - n(n-1)}{2} = \frac{n^2(p^{2k}-1) - n(p^k-1))}{2} = \frac{n^2(p^{2k}-1)}{2} - \frac{n(p^k-1)}{2}.$$

Noting that $n^2 = 4k$ for some $k \in \mathbb{Z}$ and that both n and $p^k - 1$ are even, it follows that the above quantity is always an even number so that

$$(-1)^{\frac{np^k(np^k-1) - n(n-1)}{2}} = 1.$$

The reformulation of the discriminant for this specific case is provided in the following corollary.

Corollary 2.2 *Let $f(x)$ be a polynomial in $R[x]$ of degree $n \in \mathbb{Z}^{2k}$ with discriminant $D(f)$. Let α be a root of $f(x)$ and p be an odd prime. Then for $F(x) = f(x^{p^k})$ we have the following discriminant:*

$$D(F) = (p^k)^{np^k} D(f)^{p^k} N(\alpha)^{p^k - 1}$$

Leaving behind the corollaries and again considering the original proposition, we focus on the usefulness of the discriminant representation for $D(F)$. It is apparent that the factorization of $D(F)$ can be uncovered quickly given knowledge of the factorization of $D(f)$ and $N(\alpha)$. For example, if both are primes $D(F)$ may be found simply by raising those primes to the appropriate power. Consider, for example, $f(x) = x^2 + 13x + 5 \in \mathbb{Z}[x]$. Simple algebraic techniques verify that $D(f)$=149. Noting that $N(\alpha) = 5$, the discriminant of some monomial composition with $f(x)$ can be computed very quickly. Consider $F(x) = f(x^{3^4})$. It follows immediately, and will little computational cost, that

$$D(F) = (3^4)^{2\cdot 3^4}(149)^{3^4}(5)^{3^4-1} = 3^{648}149^{81}5^{80}.$$

2.1 Applications to Irreducibility

Now our focus shifts to applying this formulation of the discriminant to obtain some information about the factorization of the members of $\{f_{p,k}(x)\}$. For this we refer to a result of Swan. The proof of this theorem can be found in [2].

Theorem 2.1 *Let $f(x)$ be a monic polynomial of degree n with rational integral coefficients. Let $\bar{f}(x)$ denote the polynomial obtained by reducing the coefficients of $f(x)$ modulo p. Assume that $\bar{f}(x)$ has no repeated roots. Let r be the number of irreducible factors of $\bar{f}(x)$ over the residue field. Then $r \equiv n \bmod 2$ if and only if $D(f)$ is a square in the residue field.*

This has nice implications about the general factorability of the polynomial families under consideration since the discriminants of their members are closely related.

Suppose that the base polynomial $f(x)$ has even degree over $\mathbb{F}_q$. Recalling our formulation of the discriminant in this case, it follows that there is only a small checklist of things that must be verified to determine whether $D(f(x^{p^k}))$ is a square

given that $D(f)$ is not. Note that $(p^k)^{np^k}$ and $N(\alpha)^{p^k-1}$ are squares as both n and p^k-1 are even. The term $D(f)^{p^k}$ is clearly not a square from our supposition. Thus, $D(f(x^{p^k}))$ must not be a square either. Thus, from Swan's work it is clear that if $f(x^{p^k})$ does indeed factor over $\mathbb{F}_q$ it must do so into an odd number of irreducibles.

Supposing that $D(f)$ is a quadratic residue it follows that $D(f(x^{p^k}))$ must also be a quadratic residue. It follows as an immediate consequence that $f(x^{p^k})$ cannot be irreducible and must have an even number of factors over $\mathbb{F}_q$.

In the case where the degree of the base polynomial $f(x)$ is odd, one must also examine the Legendre Symbol $\left(\frac{p}{q}\right)$ to be able to discuss the reducibility of the elements of this family. Suppose again that $D(f)$ is a quadratic non-residue. For $D(f(x^{p^k}))$ to be a residue, it is necessary for $\left(\frac{p}{q}\right) = -1$. If this is the case it follows that $f(x^{p^k})$ should be irreducible or factor into an odd number of irreducibles. If $\left(\frac{p}{q}\right) = 1$, $D(f(x^{p^k}))$ is a non-residue and $f(x^{p^k})$ factors into an even number of irreducibles.

Now suppose that $D(f)$ is a quadratic reside. Then the following relationships hold. If $\left(\frac{p}{q}\right) = 1$, then $D(f(x^{p^k}))$ will be a square and $f(x^{p^k})$ is irreducible or it factors into an odd number of factors over $\mathbb{F}_q$. If $\left(\frac{p}{q}\right) = -1$, $D(f(x^{p^k}))$ must be a non-residue and $f(x^{p^k})$ factors into an even number of irreducibles over $\mathbb{F}_q$.

We now present some examples to illustrate the usage of these ideas. To do this we implement a simple Maple code to determine the discriminants of a subset of $\{f_{p,k}(x)\}$ over $\mathbb{F}_q$ and their respective number of factors. First we provide a brief explanation of the implementation of the algorithm used.

The user inputs the base irreducible polynomial to be considered, the prime p with which the extension family will be produced, the field characteristic q, and the number r of members of $\{f_{p,k}(x)\}$ that will be examined. The algorithm computes the discriminant of each member along with the subsequent factorization over $\mathbb{F}_q$ using the Berlekamp Factorization Algorithm [4]. Each polynomial, its discriminant,

and the number of factors are placed in an array and outputted to the user. The code for this procedure follows.

Procedure: Polynomial Discriminant/Factorization Comparison

```
  DiscrimFactor := proc(F, p, r, q)
local T, j, f, B;
    T := Matrix(r + 2, 3);
    T[1, 1] := Polynomial;
    T[1, 2] := Discriminant;
    T[1, 3] := Number_of_Factors;
    for j from 0 to r do f[j] := subs(x = x^(p^j), F) end do;
    for j from 0 to r do
        if Gcd(f[j], diff(f[j], x)) mod q = 1 then
            B[j] := Berlekamp(f[j], x) mod q
        else B[j] := FAIL
        end if
    end do;
    for j from 0 to r do T[j + 2, 1] := f[j] end do;
    for j from 0 to r do
        T[j + 2, 2] := discrim(f[j], x) mod q
    end do;
    for j from 0 to r do T[j + 2, 3] := nops(B[j]) end do;
    print(T)
end proc
```

The following are a few quick results from the application of this procedure.

Example 2.1 (Even Degree Case) *Consider the polynomial* $f(x) = x^2 + 3 \in \mathbb{F}_5[x]$. *The family examined is the* 3^{rd} *power extensions of* $f(x)$. *For computational ease, the* k *values are restricted to small integers. The results are presented in the following table.*

Polynomial	*Discriminant*	*No. of Factors*
$x^2 + 3$	3	1
$x^6 + 3$	2	3
$x^{18} + 3$	3	5
$x^{54} + 3$	2	7
$x^{162} + 3$	3	9

Simple arithmetic verifies that 1 and 4 are the quadratic residues in $\mathbb{F}_5$ and 2 and 3 are non-residues. Thus, the work here supports the above results. Each member of the extension family has a discriminant that is a quadratic non-residue and thus factors into an odd number of irreducible factors. The fact that for this polynomial family the number of irreducible factors seems to grow arithmetically with k is something of interest that will be discussed again later.

Example 2.2 (Odd Degree Case) *Consider* $f(x) = x^3 + 2x + 1 \in \mathbb{F}_7$. *The family under consideration is the* 5^{th} *power extensions of* $f(x)$.*The* k *values are again restricted to small integers to help decrease the computational strain of the procedure. The results are included in the following table.*

Polynomial	*Discriminant*	*No. of Factors*
$x^3 + 2x + 1$	4	1
$x^{15} + 2x^5 + 1$	5	2
$x^{75} + 2x^{25} + 1$	4	7
$x^{375} + 2x^{125} + 1$	5	12

These results may be used in one of two ways. Given the number of factors we have here for the polynomials in question, we see that 4 must be a quadratic residue in $\mathbb{F}_7$ and that 5 is not. Conversely, given knowledge of the Legendre Symbol for 4 and 5 we can determine the relationship between the number of factors of each polynomial and its degree.

2.2 An Algorithm for Testing Irreducibility

These ideas lend themselves to a rather simple and computationally inexpensive irreducibility test for this type of polynomial. The algorithm involved compares favorable with a brute force method such as Or's Test. An implementation of Or's Irreducibility Test is provided in [1]. The method presented in the following pages is, at the most fundamental level, a clever simplification of that brute force procedure.

For simplicity, the discussion here will be restricted to an even degree base polynomial. Suppose the polynomial $f(x^{p^k})$ is to be tested for irreducibility. We require here that the degree of the polynomial f is the multiplicative order of q modulo p for this application to be non-trivial.

First, the discriminant of the polynomial in question is computed. If it is a square modulo q the process terminates and the polynomial is reducible. This is a useful tool provided that the discriminant can be found quickly. If the determinant is non-square, rather than attempt to find factors of $f(x^{p^k})$, the polynomial $f(x^p)$ is used. The validity of this approach is due to the fact that any one member of a

monomial p^{th} power extension family, defined as we have above, is reducible if and only if all members are (the proof of this is not difficult and will be essentially proven in subsequent sections).

So, in fact a reduction in the degree of the polynomial being tested is a key aspect in the efficiency of this algorithm. Another which will be addressed soon, is the efficiency of calculating the discriminant of the polynomial being considered.

As said above, at its heart this is an application of Or's Test with a few clever reductions. Or's Test is used as the shell in the procedure because it its very efficient when the polynomial under consideration is reducible with small degree factors. It will later be shown that when a member of the given family is reducible, it has a factor of the same degree as the base polynomial. Thus since we are typically testing a small degree polynomial, the procedure should terminate quickly.

The code for this procedure is presented below. The user inputs are the base polynomial, the prime p used in composition, the value k which is the power of p, and the field characteristic q.

Prodcedure: Irreducibility Test for Monomial P^{th} Power Extensions

```
NewTest := proc(f, p, k, q)
  m := degree(f, x);df := discrim(f, x) mod q;
  N := coeff(f, x, 0);
  if N = 0 then Dext := 0
  else
      if (1/2*m*p^k*(m*p^k - 1) - 1/2*m*(m - 1)) mod 2 = 1
      then dsign := -1
      else dsign := 1
  end if;
      e[1] := m*p^k mod (q - 1);e[2] := p^k mod (q - 1);
      e[3] := (p^k - 1) mod (q - 1);b[1] := p^k mod q;
      Dext := dsign*b[1]^e[1]*df^e[2]*N^e[3] mod q;
      print(Dext)
  end if;
  if quadres(Dtext, q) = 1 then print(Reducible)
  else for j to ceil(1/2*m) do
          if Gcd(subs(x=x^p,f), x^(q^j) - x) mod q <> 1 then
              print(Reducible); break
          else
              if j = ceil(1/2*m) then print(Irreducible)
              else
              end if
          end if
      end do
  end if
end proc
```

This algorithm could easily be adapted to the case where the base polynomial is odd. The only change necessary would be to determine if the discriminant of the given polynomial is non-square and terminate accordingly.

It was mentioned above that the discriminant calculation for these types of polynomials could be done very efficiently. As it is necessary for the application of the irreducibility test, an explanation of why that calculation is so simple follows.

2.3 Comparing Discriminant Calculation Speeds

In this section we will present computational evidence of the usefulness of the discriminant formula presented. We provide a speed comparison between an implementation of our formula and the standard discriminant calculation method used in Maple.

First, an explanation of the implementation of the formula presented above is warranted. The algorithm used was coded in Maple for ease. Given that $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$, the goal is to compute the discriminant of a member of $\{f_{p,k}(x)\}$. No other assumptions about the structure of the polynomial under consideration have been made. The form of the discriminant presented in Proposition 2.1 is used in this procedure. To determine the quantity $(-1)^{\frac{np^k(np^k-1)-n(n-1)}{2}}$, the exponent is simply reduced mod two to check its parity and then the appropriate sign is applied to the discriminant. The base in each remaining power can be reduced modulo q and their respective exponents reduced modulo $q-1$. This is a major reduction in the complexity of the calculation. For example, note that the quantity p^k grows exponentially as k increases. Thus, $(p^k)^{p^k}$ becomes large extremely quickly. However, the base quantity can be reduced base modulo q and the exponent modulo $q-1$, thus efficiently bounding the quantity for any p and k. The reductions are not costly as they can be thought of as repeated subtractions. This is a major accomplishment as it bounds the difficulty of computing a discriminant regardless

of the p and k chosen.

The algorithm used for comparison with the approach presented in this paper is the built-in procedure for finding a polynomial discriminant in Maple. This algorithm calculates the discriminant using a different, yet still common method. Given $f(x) \in \mathbb{F}_q$ of degree n the discriminant of $f(x)$ can be found by computing the following:

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f(x), f'(x))$$

In this formula,

$$R(f(x), f'(x)) = \prod_{i=1}^{n} \prod_{j=1}^{n-1} (\beta_i - \alpha_j)$$

where the β_i's are the roots of $f(x)$ and the α_j's are the roots of $f'(x)$. $R(f(x), f'(x))$ is commonly called the resultant of the polynomials $f(x)$ and $f'(x)$. The implementation of this that Maple uses computes the discriminant and then reduces it modulo q at the end of the procedure.

The comparison test was completed as follows. A selection of degree 2 irreducible polynomials over $\mathbb{F}_5$ were chosen to act as base polynomials. We composed each degree 2 polynomial with x^{3^k} for a few selected k. This collection of polynomials was used during the test. The running times were computed with the Maple 'time' procedure. The difference in each running time for the two methods was the statistic we use to judge the usefulness of our procedure. The calculation times are displayed in the following arrays.

Table 1: Discriminant Times for Polynomials composed with $x^{3^{11}}$

Polynomial	Resultant Method Time (sec.)	New Method Time (sec.)
x^{177147}	0.141	0.
$x^{354294} + 4x^{177147} + 1$	0.312	0.
$x^{354294} + 2x^{177147} + 3$	0.609	0.
$x^{354294} + 2x^{177147} + 4$	0.656	0.
$x^{354294} + x^{177147} + 1$	0.312	0.
$x^{354294} + 4x^{177147} + 2$	0.547	0.
$x^{354294} + x^{177147} + 2$	0.593	0.
$x^{354294} + 3x^{177147} + 3$	0.609	0.
$x^{354294} + 3x^{177147} + 4$	0.657	0.

Table 2: Discriminant Times for Polynomials composed with $x^{3^{13}}$

Polynomial	Resultant Method Time (sec.)	New Method Time (sec.)
$x^{1594323}$	1.936	0.
$x^{3188646} + 2x^{1594323} + 4$	10.765	0.
$x^{3188646} + 4x^{1594323} + 2$	9.328	0.
$x^{3188646} + x^{1594323} + 1$	4.656	0.
$x^{3188646} + x^{1594323} + 2$	9.765	0.
$x^{3188646} + 3x^{1594323} + 4$	10.656	0.
$x^{3188646} + 2$	10.250	0.
$x^{1594323} + 2$	4.405	0.
$x^{3188646} + 3$	9.546	0.

Do to the storage necessary to compute the discriminant of a polynomial using Maple's resultant method, we could not compute discriminants for the degree 2 polynomials composed with x^{3^k} for k beyond 13 with that method. To illustrate the efficiency of the new procedure, we computed the discriminants of the degree 2 polynomials composed with $x^{3^{21421}}$.

Table 3: Discriminant Times for Polynomials composed with $x^{3^{214221}}$

Polynomial	New Method Time (sec.)
$x^{4782969}$	0.
$x^{9565938} + 4x^{4782969} + 1$	0.063
$x^{9565938} + 2x^{4782969} + 3$	0.061
$x^{9565938} + 2x^{4782969} + 4$	0.079
$x^{9565938} + x^{4782969} + 1$	0.061
$x^{9565938} + 4x^{4782969} + 2$	0.063
$x^{9565938} + x^{4782969} + 2$	0.078
$x^{9565938} + 3x^{4782969} + 3$	0.061
$x^{9565938} + 3x^{4782969} + 4$	0.063

3 PROVING IRREDUCIBILITY OF $\{f_{p,k}(x)\}$ OVER $\mathbb{F}_q$

We begin this section by giving conditions for when each element of $\{f_{p,k}(x)\}$ remains irreducible over a finite field of characteristic q. It will be useful to consider the factorization of $f(x)$ in its splitting field. So, suppose $f(x)$ is irreducible over $\mathbb{F}_q$ and has degree m . Denote its roots $\alpha_1, \alpha_2, \ldots, \alpha_m$. Then each $a_i \in \mathbb{F}_q[\alpha_1]$ for $1 \leq i \leq m$ and we obtain the following factorization in that field extension:

$$f(x) = \prod_{i=1}^{m}(x - \alpha_i).$$

From this we can observe that $f(x^{p^k})$ is irreducible over $\mathbb{F}_q$ precisely if each of the binomials $x^{p^k} - \alpha_i$ is irreducible over $\mathbb{F}_q[\alpha_1]$. According to Lidl and Niederreiter [3], this is the case when $q \equiv m \bmod p$ and each α_i is not a p^{th} power in $\mathbb{F}_q[\alpha_1]$. This second condition is equivalent to p dividing the order of $|\alpha_i|$ but not $\frac{q^m-1}{|\alpha_i|}$. The usefulness of irreducible polynomials over finite fields is well known. The fact that this family of polynomials, when irreducible, provides us with arbitrarily large degree irreducible polynomials with little computation make it worthwhile to develop an algorithm to verify when these conditions are satisfied. Although this algorithm is

deterministic and seemingly more useful then the tests we presented earlier, it is not without shortcomings. To complete it, one must have a method of obtaining the degree of the roots of the irreducible base polynomial. This requires computing multiple GCDs or obtaining a representation of the roots in the extension field in which they exist. We now present an algorithm, coded in Maple, that determines when these conditions are satisfied for all polynomials of degree m where $m = |q|$ mod p for the odd prime p and field $\mathbb{F}_q$.

Procedure.

```
  IrreducibilityTest := proc(p, q)
local k, m, Collection, COrd, r, f, R, ordA;
    for k to p do
        if irem(q^k, p) = 1 then m := k; break
        else null
        end if
    end do;
    Collection := Berlekamp(x^(q^m) - x, x) mod q;
    COrd := nops(Collection);
    for r to COrd do
        if degree(Collection[r], x) = m then
            f := Collection[r];
            if m = 1 then for k to q^m - 1 do
                    R := ((-coeff(f, x, 0)) mod q)^k mod q;
                    if R = 1 then ordA := k; break
                    else null
                    end if
                end do
            else for k to q^m - 1 do
                    R := Rem(x^k - 1, f, x) mod q;
                    if (R = 0) mod q then ordA := k; break
                    else null
                    end if
                end do; end if;
            if irem(ordA, p) = 0 and
            irem((q^m - 1)/ordA, p) <> 0 then
                print(‘Polynomial Family is irreducible‘)
            else print(‘Polynomial Family is reducible‘)
            end if
        else null
        end if; end do; end proc
```

We implement this procedure to determine an exhaustive list off all irreducible p^{th} power extension families for given $\mathbb{F}_q$. Computationally speaking, an exhaustive search is rather straining so we restrict p to be small here. If our goal is to obtain irreducible polynomials of large degree we do not fail due to this restriction because for each successful outcome we will obtain an infinite sequence of irreducible polynomials of increasing degree. This restriction made on p is not a drastic step in reducing the number of computations in the procedure. The bulk of the work in this procedure is done when obtaining the appropriate set of irreducible polynomials over the field under consideration

Given p and q, the procedure determines m, the multiplicative order of q modulo p. Then, Berlekamp's factorization algorithm [4] is used to recover all irreducible degree m polynomials over $\mathbb{F}_q$ by factoring $x^{q^m} - x$. This can be verified in any graduate abstract algebra text. The order of each polynomial is computed and the appropriate divisibility relationships are then checked to determine if the family is or is not irreducible over $\mathbb{F}_q$. For each polynomial, the appropriate result is printed. We provide a few sample results here.

Example 3.1 *Suppose we wish to determine which monomial 3^{rd} power extension families are irreducible over $\mathbb{F}_5$. The given algorithm outputs the following results. Here an asterisk (*) is used to indicate which property is satisfied for the given polynomial.*

Table 4: Irreducible 3^{rd} Power Families Over $\mathbb{F}_5$

Base Polynomial	Irreducible	Reducible
x^2+x+2	*	
x^2+2x+3	*	
x^2+2x+4	*	
x^2+3x+4	*	
x^2+3		*
x^2+2		*
x^2+4x+1	*	
x^2+4x+2	*	
x^2+3x+3	*	
x^2+x+1	*	

We now consider a slightly different use of this procedure. Rather than use this procedure to obtain irreducible polynomials over $\mathbb{F}_q$, it may instead be used as a type of residue test. Assuming that the base polynomial has degree m defined by the aforementioned congruence, we have said above that each extension polynomial is irreducible over $\mathbb{F}_q$ if and only if the roots of the base polynomial are not p^{th} powers in the field $\mathbb{F}_{q^m}$. Thus, if we are able to determine that some extension polynomial is reducible over $\mathbb{F}_q$ then we will have recovered a p^{th} residue in the extension field. This is a very nice result as it provides us with a method for determining the residues, at least in some cases, for primes much larger than 3. The fact that we are determining residues in an extension field provides some utility, albeit with restrictions. The main shortcoming is that we are restricted to a specific extension field for each p and q we deal with. However, it is rather nice that we need no representation of the extension field in order to determine which of its elements are p^{th} powers.

In some cases we can determine residues in the base field. If it happens that $q \equiv 1 \bmod p$, we note that our extension would be degree 1 so we are actually determining residues over $\mathbb{F}_q$. We provide an example of this application of the algorithm.

Example 3.2 *Take* $p = 5$ *and* $q = 11$ *and use the algorithm to determine what elements of* $\mathbb{F}_{11}$ *are* 5^{th} *powers.*

Table 5: Quintic Residues Over $\mathbb{F}_{11}$

Base Polynomial	Non-Residue	Residue
$x+6$	*	
$x+9$	*	
$x+1$		*
$x+8$	*	
$x+5$	*	
$x+10$		*
$x+3$	*	
$x+2$	*	
$x+4$	*	
$x+7$	*	

Note here that for each linear polynomial $x+c$ *the algorithm determines whether* $-c$ *is a* 5^{th} *residue in* $\mathbb{F}_{11}$*. So, it follows that the* 5^{th} *residues of* $\mathbb{F}_{11}$ *are 10 and 1.*

The main use of the procedure presented above is to determine irreducible families of polynomials over a given finite field. However, very often the polynomial families obtained through these types of compositions are not irreducible. With that in mind, the remaining portion of the paper will be devoted to determining how these families factor given that they are reducible.

4 FACTORIZATION OF $\{f_{p,k}(x)\}$ OVER $\mathbb{F}_q$

Let us again consider $f(x)$ an irreducible polynomial of degree m in $\mathbb{F}_q[x]$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_m$. We also stipulate that m is the order of q modulo p. Recall that $f(x)$ splits in $\mathbb{F}_{q^m}$ and thus is $f(x^{p^k})$ is realizable as

$$f(x^{p^k}) = \prod_{i-1}^{m} \left(x^{p^k} - \alpha_i \right)$$

over $\mathbb{F}_{q^m}$. It has already been stated that $f(x^{p^k})$ is irreducible if each root α_i of $f(x)$ is not a p^{th} power in $\mathbb{F}_{q^m}$.

We will now shift our focus to determining the way $f(x^{p^k})$ will factor over the base field, given that the family will be reducible. Recalling the work of Lidl and Niederreiter [3], it happens that this family is reducible when either of the following two conditions are satisfied:

1. p does not divide the order $|\alpha|$ of the roots of $f(x)$ in $\mathbb{F}_{q^m}^*$
2. p divides $\frac{q^m-1}{|\alpha|}$

It is noteworthy to mention that p must divide $q^m - 1$. This is quickly verifiable since the order of q modulo p is m. It follows directly that $q^m \equiv 1\ (p)$ and so $q^m - 1 \equiv 0\ (p)$. Keeping this in mind, it is clear that if the first reducibility condition is satisfied, it may not be done trivially, but rather e will not contain the factor p present in $q^m - 1$.

We will now examine the factorization obtained by from various extension families as we place certain divisibility relationships on p, $q^m - 1$, and $|\alpha|$.

4.1 Factoring $\{f_{p,k}(x)\}$ when $(p, |\alpha|) = 1$

We begin by stipulating that $q^m - 1$ only contain one factor of p and that the roots of the irreducible base polynomial are relatively prime to p. If p and the order

of the roots of f are not relatively prime, the polynomial is irreducible as the roots cannot be p^{th} powers. With these conditions, the polynomial family satisfies the first reducibility condition. In the following theorem, we provide a general description of the factorization for any member of a family of this type.

Theorem 4.1 *Let p be an odd prime. Let $f(x)$ be an irreducible polynomial with of degree m over $\mathbb{F}_q$ where m is the multiplicative order of q modulo p. Suppose $p < q^m - 1$ and p divides $q^m - 1$ but that p^k does not divide $q^m - 1$ for $k > 1$. Let α be a root of $f(x)$ and further suppose $(p, |\alpha|) = 1$. Then $f(x^{p^k})$ splits over $\mathbb{F}_q$ into $1 + (p-1)k$ factors over $\mathbb{F}_q$ of degrees dividing mp^k. The degrees of the irreducible factors can be described as follows.*

1. *$f(x^{p^k})$ will have p irreducible factors of degree m and only one of which will have p^{th} power roots.*

2. *$f(x^{p^k})$ will have $p-1$ irreducible factors of degree mp^{i-1} for $2 \leq i \leq k$.*

Proof. Suppose all the above suppositions hold. Let α be a root of $f(x)$. Denote the conjugates of α by $\alpha_i = \alpha^{q^i}$ for $1 \leq i \leq m-1$. We obtain the following familiar factorization of $f(x)$ in $\mathbb{F}_{q^m}$:

$$f(x) = (x - \alpha)(x - \alpha_1) \cdots (x - \alpha_{m-1}).$$

Considering the composition $f(x)$ with x^p, the following factorization of that polynomial is quickly uncovered:

$$f(x) = (x^p - \alpha)(x^p - \alpha_1) \cdots (x^p - \alpha_{m-1}).$$

Now, given that α is a p^{th} power in $\mathbb{F}_{q^m}$ and that $(p, |\alpha|)$ we may obtain the following equivalence over $\mathbb{F}^*_{q^m}$:

$$\alpha^{p^t} \equiv \alpha \text{ for some positive integer } t.$$

This provides a cyclic sequence of p^{th} roots of α. This idea will be useful in uncovering the factorization of $f(x^{p^k})$ for $k > 1$.

First, we will factor $f(x^p)$ and then extend to higher powers inductively. It is clear that $\alpha^{p^{t-1}}$ is a root of the polynomial $x^p - \alpha$ over $\mathbb{F}^*_{q^m}$. This roots is a p^{th} power from from the equivalence above. Furthermore, the conjugates of this root, denoted $\alpha_i^{p^{t-1}}$ for $1 \leq i \leq m-1$ are also p^{th} powers. The remaining roots of $x^p - \alpha$ may be obtained by multiplying $\alpha^{p^{t-1}}$ by an element β of order p in $\mathbb{F}^*_{q^m}$. This β will necessarily not be a p^{th} power as p does not divide the subgroup of p^{th} powers of $\mathbb{F}^*_{q^m}$. Thus $\beta \cdot \alpha^{p^{t-1}}$ cannot be a p^{th} power. It follows that the conjugates of $\beta \cdot \alpha_i^{p^{t-1}}$ will not be p^{th} powers as well. From these conjugates we can obtain the factors of $f(x^p)$ over $\mathbb{F}_q$. The polynomial

$$f_1(x) = (x - \alpha^{p^{t-1}})(x - \alpha_1^{p^{t-1}})(x - \alpha_2^{p^{t-1}}) \cdots (x - \alpha_{m-1}^{p^{t-1}})$$

will necessarily be in $\mathbb{F}_q[x]$ and it will have roots that are p^{th} powers. The remaining polynomials

$$f_i(x) = (x - \beta_i \cdot \alpha^{p^{t-1}})(x - \beta_i \cdot \alpha_1^{p^{t-1}})(x - \beta_i \cdot \alpha_2^{p^{t-1}}) \cdots (x - \beta_i \cdot \alpha_{m-1}^{p^{t-1}})$$

for $2 \leq i \leq m$ and some element β_i of $\mathbb{F}^*_{q^m}$ with order p will not have p^{th} power roots. Again, each of these polynomials will have factorizations of $\mathbb{F}_q$. In contrast from $f_1(x)$, none of these polynomials will have p^{th} power roots.

We have established that $f(x^p)$ factors as in claimed in (1) and trivially (2) is satisfied. To obtain a nontrivial verification of (2), we examine a higher order composition. For $f(x^{p^2})$ note that it has the following trivial factorization:

$$f(x^{p^2}) = f_1(x^p)f_2(x^p) \cdot f_m(x^p).$$

Note that $f_1(x^p)$ will factor into precisely p factors of degree m. The remaining $f_i(x^p)$ will be irreducible because the roots of $f_i(x)$ are not p^{th} powers in $\mathbb{F}^*_{q^m}$. Thus $f(x^{p^2})$ factors are was claimed in (1) and (2).

Compositions of $f(x)$ with higher order p^{th} powers, say x^{p^k} for $k > 2$ may be thought of as repeated compositions of x^p done k times. Our approach to showing that $f(x^{p^k})$ behaves as we have claimed is an inductive one.

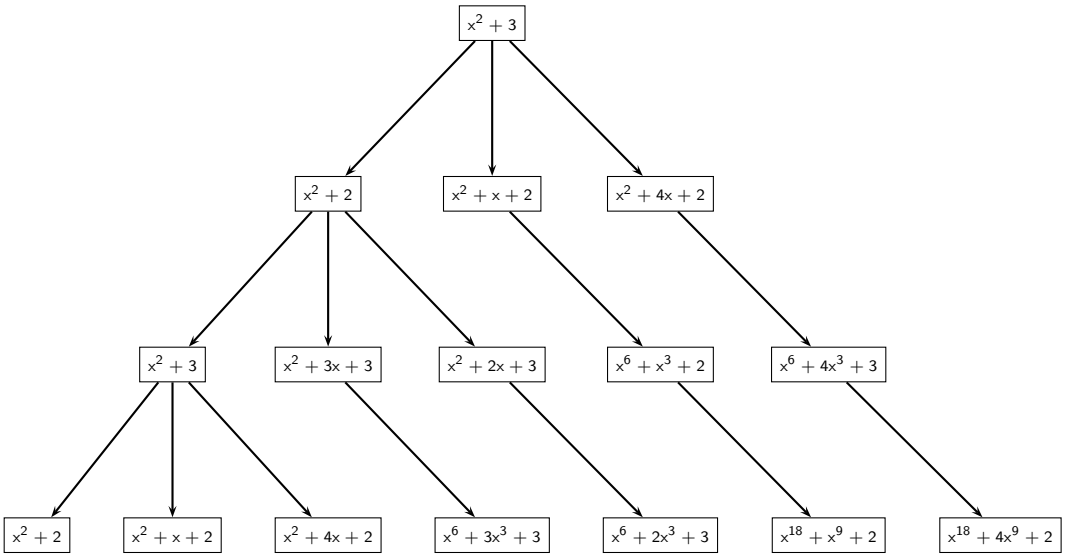
It has been shown that it holds that for $k = 2$, the composition factors as was claimed. Suppose it holds for some larger positive integer k. By hypothesis of induction, $f(x^{p^k})$ has a single degree m factor with p^{th} power roots. This is the only factor of $f(x^{p^k})$ that will be reducible when composed with x^p. Denote this factor $g(x)$. From our arguments before, $g(x)$ will split into p factors of degree m with only one having p^{th} power roots. From the remaining factors we will obtain the $p-1$ factors having each of the appropriate degrees as specified in (2). Thus, $f(x^{p^{k+1}})$ behaves exactly as it should and the claims are satisfied.

Q.E.D

Example 4.1 *Consider the polynomial $f(x) = x^2 + 3$ over $\mathbb{F}_5$. We illustrate the decomposition of the first few members of the polynomial extension family in the following diagram.*

Each tier in the diagram provides the factors of $f(x)$ obtained after another composition with x^p. It is quickly verifiable that the number of factors and their degrees matches the results of the theorem.

Figure 1: Factorization of the 3^{rd} Power Extensions of $x^2 + 3$



A clear cycling pattern emerges amongst the factors of the extension polynomials. For example, the polynomial $x^2 + 2$ is a factor of both $f(x^3)$ and of $f(x^{3^3})$. This is not a coincidence and in general there will be some cycling of the irreducible factor that has p^{th} power roots in the various members of the extension families. It is not too difficult to answer the question of why this occurs. We state the following corollary to Theorem 4.1.

Corollary 4.1 *Let p be an odd prime. Let $f(x)$ be an irreducible polynomial with of degree m over $\mathbb{F}_q$ where m is the multiplicative order of q modulo p. Suppose $p < q^m - 1$ and p divides $q^m - 1$ but that p^k does not divide $q^m - 1$ for $k > 1$. Let α be a root of $f(x)$ and further suppose $(p, |\alpha|) = 1$. Let t be the smallest positive integer solution to the congruence $\alpha^{p^t} \equiv \alpha$ in $\mathbb{F}_{q^m}$. Then $f(x^{p^{tk}})$ is divisible by $f(x)$ for all non negative integers k.*

To prove the corollary, we first state a useful lemma.

Lemma 4.1 *For primes p and q, denote the multiplicative order of q modulo p by m. Suppose $p < q^m - 1$ and p divides $q^m - 1$ but that p^k does not divide $q^m - 1$ for $k > 1$. Let $\alpha \in \mathbb{F}_{q^m}^*$. Further suppose $(p, |\alpha|) = 1$. Choose t to be the smallest integer such that $p^t \equiv 1 \bmod |\alpha|$. Then $x^{p^t} - \alpha$ is reducible over $\mathbb{F}_{q^m}$ and factors as follows:*

$$x^{p^t} - \alpha = (x - \alpha)\, g(x)$$

for some $g(x) \in \mathbb{F}_{q^m}$.

Proof of Lemma 4.1. Let the conditions of the lemma hold. As α is a p^{th} power in $\mathbb{F}_{q^m}$ and $\alpha^{p^t} \equiv \alpha$ the polynomial under consideration can be written as follows:

$$x^{p^t} - \alpha = \left(x^{p^{t-1}}\right)^p - \left(\alpha^{p^{t-1}}\right)^p.$$

The right hand side of this equation may be factored as a difference in prime powers to obtain

$$\left(x^{p^{t-1}}\right)^p - \left(\alpha^{p^{t-1}}\right)^p = \left(x^{p^{t-1}} - \alpha^{p^{t-1}}\right)\left((x^{p^{t-1}})^{p-1} + (x^{p^{t-1}})^{p-2}\alpha^{p^{t-1}} + \cdots + (\alpha^{p^{t-1}})^{p-1}\right)$$

in $\mathbb{F}_{q^m}$. For simplicity, denoted the right most factor in the above expression $g_1(x)$. Now, we iterate this procedure. For each $1 \leq j \leq t-1$, the power $\alpha^{p^{t-j}}$ can be realized as $\left(\alpha^{p^{t-j-1}}\right)^p$ and so the polynomial $x^{p^{t-j}} - \alpha^{p^{t-j}}$ can be factored as

$$x^{p^{t-j}} - \alpha^{p^{t-j}} = \left(x^{p^{t-j-1}} - \alpha^{p^{t-j-1}}\right) g_{j+1}(x)$$

with $g_{j+1} \in \mathbb{F}_{q^m}$. Upon reaching $j = t-1$ we will obtain the following final factorization of $x^{p^t} - \alpha$ in $\mathbb{F}_{q^m}$.

$$x^{p^t} - \alpha = (x - \alpha) \prod_{i=1}^{t-1} g_j(x)$$

Thus, taking $g(x) = \prod_{i=1}^{t-1} g_j(x)$, the proposition is satisfied.

Q.E.D

Proof of Corollary 4.1 Considering $f(x^{p^t})$ in the splitting field for $f(x)$, we once again obtain the factorization

$$f(x) = (x^{p^t} - \alpha)(x^{p^t} - \alpha_1) \cdots (x^{p^t} - \alpha_{m-1}).$$

By the lemma, the first factor is reducible and contains the factor $(x - \alpha)$. Similarly, each remaining factor $(x^{p^t} - \alpha_i)$ for $1 \leq i \leq m-1$ will contain a factor $(x - \alpha_i)$. We may collapse these linear factors to obtain the polynomial $f(x)$ as a factor of $f(x^{p^t})$. This factorization is necessarily over $\mathbb{F}_q$ by closure of the field coefficients.

Inductively we may obtain a factor of $f(x)$ from higher order monomial compositions. For example, let $f(x^{p^t}) = f(x)g(x)$ for some polynomial $g(x)$. Then, $f(x^{p^{2t}}) = f(x^{p^t})g(x^{p^t})$ and thus necessarily has $f(x)$ as a factor. Supposing $f(x^{p^{nt}})$ contains a factor of $f(x)$ it follows directly that $f(x^{p^{(n+1)t}})$ does as well.

Q.E.D

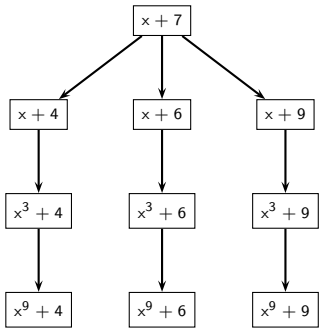
4.2 Factoring $\{f_{p,k}(x)\}$ when $(p, |\alpha|) > 1$

We now shift our focus to dealing with another divisibility case. Namely, we suppose that the roots of the polynomial in question are not relatively prime to p. To achieve reducibility, we now suppose that some that for some positive integer $r > 1$, p^r divides $q^m - 1$.

We begin by identifying what goes wrong in the procedure described above if we let $(p, |\alpha|) = l$ for some integer l greater than one. This leads to the congruence $\alpha \equiv \alpha^{p^k}$ being unsolvable modulo $|\alpha|$. The solvability of this congruence was at the heart of the proof of Theorem 4.1 and Lemma 4.1. This implies the cyclic reduction which continuously generated one degree m irreducible polynomial that was reducible under composition will not necessarily exist. Alternatively, for polynomials satisfying Theorem 4.1, any one p^{th} power polynomial root had a p^{th} root which was also a p^{th} power. This will not be the case in many instances. We now examine a collection of polynomials which highlight this key difference.

Example 4.2 *Consider $x + 7 \in \mathbb{F}_{19}[x]$. Note that the root, (-7), of the given polynomial has order 3 in $\mathbb{F}_{19}$. For this example we take $p = 3$. Below we provide the factorization tree for the polynomial extension family of $x + 7$.*

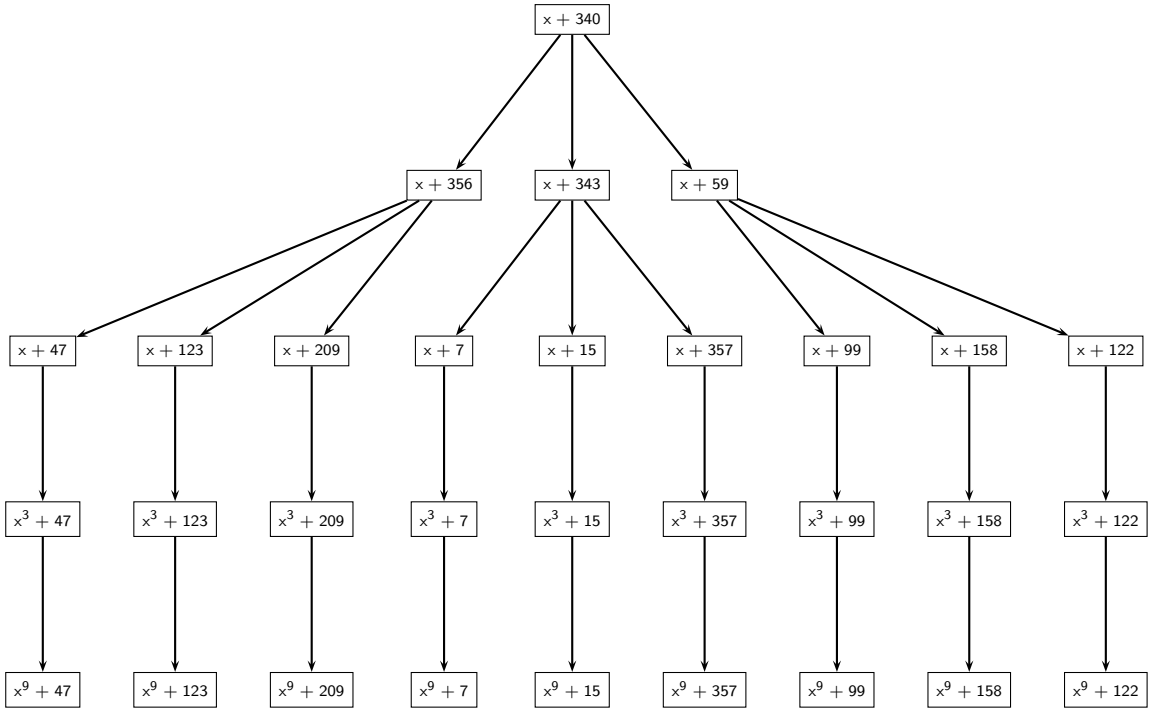
Figure 2: Factorization of the 3^{rd} Power Extensions of $x + 7 \in \mathbb{F}_{19}[x]$



Notice that at the second tier in the composition, the polynomial factors remain irreducible and subsequently grow in degree in further compositions. Note that $-7 = 12$ *is the root of* $x + 7$*. A quick computation shows that* $-9 = 10$*,* $-13 = 6$*, and* $-15 = 4$ *are the cubed roots of* 12 *in* $\mathbb{F}_{19}$*. These elements are not* 3^{rd} *powers in* $\mathbb{F}_{19}$ *and so in higher order compositions the polynomial factors having these roots remain irreducible under compostion and hence we obtain the factorization pattern illustrated in the diagram.*

Example 4.3 *Consider* $x + 340 \in \mathbb{F}_{379}[x]$*. Note that the root,* (-340)*, of the given polynomial has order* 21 *in* $\mathbb{F}_{379}$*. For this example we take* $p = 3$*. Below we provide the factorization tree for the polynomial extension family of* $x + 340$*.*

Figure 3: Factorization of the 3^{rd} Power Extensions of $x + 340 \in \mathbb{F}_{379}[x]$



Notice in this example that we achieve two levels of decomposition before the factors no longer have p^{th} power roots. Once the roots have this property, the factors remain irreducible under composition and subsequent compositions to larger degree factors.

From the two examples we can gather that for different base polynomials we will not eliminate all p^{th} power roots at the same level of composition. We spend a moment now classifying exactly when this phenomena will occur for a given polynomial in an extension family. First we define a few useful terms that will help in this process.

Definition 4.1 *Let p be a positive prime integer. Let r be a positive integer. Define $E_r(p)$ to be the power of p present in the prime factorization of r.*

Definition 4.2 *Let p and q be positive prime rational integers. Let m be a positive integer. Define $E_{q,m}(p)$ to be the power of p present in the prime factorization of $q^m - 1$.*

We state the following theorem as an answer to the question above.

Theorem 4.2 *Let p be a positive prime integer. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q[x]$ whose roots are p^{th} powers in $\mathbb{F}_q$. Suppose that m is the multiplicative order of q modulo p. Let α_0 be a root of $f(x)$. Let $E_{q,m}(p) = T$ and $E_{|\alpha_0|}(p) = t > 0$. Then the factors of $f(x^{p^{T-t}})$ have no roots that are p^{th} powers. Moreover for $k < T - t$, $f(x^{p^k})$ has p^{th} power roots.*

Proof. Suppose the conditions from the theorem hold. We have that $|\alpha_0| = p^t g$ for some positive integer g. As this root is a p^{th} power, there exists p elements of $\mathbb{F}_q$, denoted $\beta_{0,j}$ for $1 \leq j \leq p$, such that $\beta_{0,j}^p = \alpha_0$. Now, given the order of α_0 we can determine the order of $\beta_{0,j}$. Note that

$$|\beta_{0,j}| = |\alpha_0| \cdot (p, |\beta_{0,j}|) = p|\alpha_0|.$$

It follows that $\mathrm{E}_{|\beta_{0,j}|}(p) = t + 1$. Similarly the conjugates of α_0, denoted α_i for $0 \leq i \leq m-1$, have p^{th} roots $\beta_{i,j}$ for $1 \leq j \leq p$. It follows for each of those roots that $\mathrm{E}_{|\beta_{i,j}|}(p) = t + 1$. The collection $\{\beta_{i,j} | 0 \leq i \leq m-1, 1 \leq j \leq p\}$ comprise the roots of the polynomial $f(x^p)$. Similarly, for a root of $f(x^{p^2})$, call it β, we have $\mathrm{E}_{|\beta|}(p) = t + 2$. In general, for a root β of $f(x^{p^i})$, $\mathrm{E}_{|\beta|}(p) = t + i$. We obtain p^{th} power roots for each $f(x^{p^i})$ provided that $t + i \leq T - 1$. This is true as the order of the subgroup of p^{th} powers of $\mathbb{F}_q^*$ is $\frac{q^m-1}{p}$. Thus, $f(x^{p^{T-t}})$ has no roots that are p^{th} powers.

Q.E.D

5 ROOT DISTRIBUTION

In this section we provide a parallel discussion to the ideas presented by Perlis in [5]. Perlis answered the question, for α a root of an irreducible polynomial f with coefficients coming from a field $\mathbb{Q}$, how many roots of f lie in $\mathbb{Q}(\alpha)$. Perlis denotes this quantity $r_K(f)$, called the *root quantum number of f over* $\mathbb{Q}$ and noted that it was independent of the root chosen. The main result presented in his paper is that the roots of f appear in bundles of size $r_K(f)$ in fields laying between K and the splitting field.

The goal here is to generalize the idea above to fit a class of polynomials over a finite field. If we take f to be an irreducible polynomial over $\mathbb{F}_q$ the result of Perlis is trivially true. That is, if we look at $\mathbb{F}_q(\alpha)$, for any root α of f, all the roots of f lay in this field as it is the splitting field for f. So for an irreducible polynomial in the finite field setting, the root quantum number Perlis defined would simply be the degree of the irreducible polynomial. It would be interesting if we could find a less trivial class of polynomial for which the ideas that Perlis developed hold. It turns out that the class of polynomials discussed in this paper have root distributions much like irreducible polynomials over fields of characteristic zero. In fact, the ideas that Perlis developed hold for even more general class of polynomial. Before examining that fact, we state the following definition which is due to Agou [6].

Definition 5.1 *If f is a polynomial over $\mathbb{F}_{q^s}$ and x_0 is a root of f such that $\mathbb{F}_{q^s}[x_0] \subseteq \mathbb{F}_{q^s}[x]$ for all other roots x of f, then we say that f is hyponormal. The degree $[\mathbb{F}_{q^s}(x_0) : \mathbb{F}_{q^s}]$ is called the minimal degree of f over $\mathbb{F}_{q^s}$. Denote this quantity $r_{\mathbb{F}_{q^s}}(f)$.*

As the notation in the definition suggests, the minimal degree of a polynomial f of the described form over $\mathbb{F}_{q^s}$ will be the root quantum number in the finite field setting. It is worthwhile to note the difference for our definition of root quantum number and that given by Perlis. Here we define this number by the smallest degree

irreducible factor. If we were to use the definition provided by Perlis, that the root quantum number is the number of roots in the extension $\mathbb{F}_{q^s}[x_0]$, we would quickly observe that the divisibility relations he developed fails. To verify this, all one needs to do is consider a hyponormal with an irreducible factor of degree five and two linear factors. Before stating analogous theorems to those given by Perlis, we pause to examine this phenomenon in an example.

Example 5.1 *Consider $f(x) = x^2 + 3$ over $\mathbb{F}_5$. We will examine the root distribution for $F(x) = f(x^{3^2})$ in the various extension fields up to $\mathbb{F}_{5^6}$. First, note the factorization*

$$F(x) = (x^2 + 3)(x^6 + x^3 + 2)(x^2 + 3x + 3)(x^6 + 4x^3 + 2)(x^2 + 2x + 3).$$

The smallest irreducible factor of $F(x)$ is $x^2 + 3$ (or $x^2 + 2x + 3$). So the minimal degree for $F(x)$ over $\mathbb{F}_5$ is 2. Thus, in any extension field of $\mathbb{F}_5$ there should be an even number of roots of $F(x)$. To get the factorization of $F(x)$ over $\mathbb{F}_{25}$ we use the fact that $\mathbb{F}_{25} \cong \mathbb{F}_5(\alpha)$ where α is a root of any irreducible degree 2 polynomial. We take α to be a root of $x^2 + 3$ for simplicity. The following factorization of $F(x)$ can be uncovered over $\mathbb{F}_{25}$.

$$\begin{aligned} F(x) &= (x^3 + \alpha + 2)(x + 2\alpha + 4)(x + 4\alpha) \cdot \\ &\quad (x^3 + 4\alpha + 2)(x + 3\alpha + 1)(x^3 + \alpha + 3)(x + 2\alpha + 1) \cdot \\ &\quad (x^3 + 4\alpha + 3)(x + \alpha)(x + 3\alpha + 4) \end{aligned}$$

Here we see that $F(x)$ has six roots present in this field, namely all the roots of the irreducible degree two factors over $\mathbb{F}_5$. If we factor $F(x)$ over $\mathbb{F}_{5^6}$ we obtain the following factorization. In this setting, we take α to be a root of $x^6 + x^3 + 2$.

$$
\begin{aligned}
F(x) \;=\; & (x+4\alpha^3+2)(x+2\alpha^4+3\alpha)(x+4\alpha^5)\cdot \\
& (x+2\alpha^4+4\alpha)(x+4\alpha^5+4\alpha^2)(x+3\alpha^3+3)\cdot \\
& (x+3\alpha^4+2\alpha)(x+2\alpha^3)(x+\alpha^3+3)(x+\alpha^5)(x+3\alpha^5+4\alpha^2)\cdot \\
& (x+3\alpha^4+\alpha)(x+\alpha)(x+\alpha^5+\alpha^2)(x+4\alpha)\cdot \\
& (x+2\alpha^5+\alpha^2)(x+3\alpha^3)(x+2\alpha^3+2)
\end{aligned}
$$

As $\mathbb{F}_{5^6}$ is the splitting field for $F(x)$, it contains all the roots of this polynomial. There are an even number of such roots. An examination of $f(x)$ composed with even higher monomial powers would give even more concreteness to the idea presented above. We restricted to a small power for brevity.

Now, for the finite field setting, we state an analogous theorem to that given by Perlis in [5].

Theorem 5.1 *Let $f(x)$ be a hyponormal polynomial over $\mathbb{F}_{q^s}$.Let L be a field extension over $\mathbb{F}_{q^s}$. Then the number of roots of $f(x)$ in L is a multiple of $r_{\mathbb{F}_{q^s}}(f)$.*

Proof. Let $f(x)$ be a hyponormal polynomial over $\mathbb{F}_{q^s}$, with x_0 a root defined as above. Recall that if we have $\mathbb{F}_{q^s}[x_0] \subseteq \mathbb{F}_{q^s}[x]$ for all other roots x, it follows directly that the degree of the irreducible factor having x_0 as a root divides the degree of the irreducible factor having x as a root. Thus all factors of $f(x)$ have degrees divisible by the factor having x_0 as a root. Hence in any extension, the number of roots will be a multiple of $\mathbb{F}_{q^s}$.

Q.E.D

The clusters of roots present in the various extension fields containing the polynomial roots, which Perlis referred to as "roots appearing in quanta", is evident from

the factorizations we have explored in the preceding examples of the paper. Perlis also discussed how knowledge of a particular root quantum number for a polynomial could be used to limit the types of factorizations that could occur. This can also be done in the finite field situation to a lesser degree. The reason this type of thought process is less useful here is due to the fact that there is only one extension of each degree in the finite field setting. In the characteristic zero setting, the possibility exists that the given polynomial has roots of the same degree corresponding to different field extensions. Regardless, one could take the root quantum number for a polynomial, or the minimal degree, to act as a base for possible factor degrees.

6 CONCLUSION

In this paper, we provide a thorough examination of the behavior of the family $\{f_{p,k}(x)\}$ for an irreducible polynomial f and appropriate prime p has been given. We discussed a variety of ways for determining irreducibility for a given family, some of which are made very efficient do to the discriminant calculation presented in this paper. Favorable time comparisons were presented between the method presented in this paper and Maple's discriminant calculation algorithm. However, the asymptotic complexity of the method presented in this paper was not examined whatsoever.

Even though explicit methods for determining irreducibility were provided in [3], the methods presented in this paper can be used with no representation of the roots of the base polynomial in its splitting field thereby providing some justification for their use.

Following this, much work was devoted to uncovering many useful properties of the irreducible factors of these families when they are not irreducible. Much can now be said about the number and degree of the irreducible factors of a given family.

These ideas presented in this paper point to a variety of possible directions one could take further research. Possible topics include examining compositions of irreducible polynomials with non monomial polynomials over a finite field. For example, one could examine the composition of an irreducible polynomial with $x^{p_1^k} + y^{p_1^r}$ for primes p_1 and p_2.

Another possible topic would be to consider the same families introduced in this paper over various fields simultaneously. One could look for a class of fields $\{\mathbb{F}_{q_1}, \mathbb{F}_{q_2}, \ldots, \mathbb{F}_{q_r}\}$ for which the family $\{f_{p,k}(x)\}$ remains irreducible. It would be equally interesting to fix the field under consideration and look for a set of primes $\{p_1, p_2, \ldots, p_r\}$ for which the respective families $\{f_{p,i}(x)\}$ factor in a similar way.

One could further extend the work stemming from Perlis to look for an even

larger class of polynomials for which the ideas he discussed hold in the finite setting. At first thought, Q-polynomials, discussed in [3] would seem to be a logical place to begin that search.

APPENDIX A: Explanations of the Work of Lidl and Niederreiter

In this section we present the results provided by Lidl and Niederreiter in [3] that lay the foundation for the ideas presented in this paper. We begin by presenting a collection of ancillary results and end with the major foundational theorem. Simple proofs are provided in the Appendix, however, all results are proven in [3].

Theorem 6.1 *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m with $f(0) \neq 0$. Let $|\alpha|$ be a root of f in $\mathbb{F}_{q^m}^*$. Then $ord(f) = |\alpha|$.*

Proof. From basic finite field theory, $\mathbb{F}_{q^m}$ is the splitting field for f. We have already established all the roots of f have the same order in $\mathbb{F}_{q^m}^*$. Let α be an arbitrary root of f. As f is the minimal polynomial for its roots, it follows that $\alpha^e = 1$ if and only if $f(x)$ divides $x^e - 1$. The claim above follows directly.

Q.E.D

Theorem 6.2 *The number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e is equal to $\phi(e)/m$ if $e \geq 2$ and m is the multiplicative order of q modulo e which is equal to 0 any time $m, e \neq 1$. In particular, the degree of an irreducible polynomial in $\mathbb{F}_q[x]$ of order e must be equal to the multiplicative order of q modulo e.*

Proof omitted.

Lemma 6.1 *Let $s \geq 2$ and $e \geq 2$ be relatively prime integers and let m be the multiplicative order of s modulo e. Let t be an odd prime which divides e but not $4(s^m - 1)/e$. Then the multiplicative order of s modulo et is mt.*

Proof. Suppose the assumptions from the lemma hold, the let $d = (s^m - 1)/e$ and so $s^{mt} = 1 + de^t$. So, applying a binomial expansion we obtain

$$s^{mt} = 1 + \binom{t}{1} \cdot de + \binom{t}{2} \cdot d^2e^2 + \cdots + \binom{t}{t-1} \cdot d^{t-1}e^{t-1} + d^te^t.$$

Note in the right-hand expression all terms but but the first are divisible by et. Thus $s^{mt} \equiv 1 \bmod et$. It follows directly that the multiplicative order of s, call it k, divides mt. Furthermore, as $s^k \equiv 1 \bmod e$, k is divisible by m. This means that k can only be m or mt by the primarily of t. If $k = m$ then $s^m \equiv 1 \bmod et$ and so t divides d, a contradiction. Therefore, $k = mt$.

Q.E.D

Theorem 6.3 *Let $f_1(x), f_2(x), \ldots, f_N(x)$ be all the distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e, and let t be an odd prime which divides e but not $(q^m - 1)/e$. Then $f_i(x^t)$ are all the distinct irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et.*

Proof. From above, we have that the irreducible polynomials of degree m and order e exist if and only if m is the multiplicative order of q modulo e and that $N = \phi(e)/n$. By the lemma it follows that the multiplicative order of q modulo et is mt. Since $\phi(et)/mt = \phi(e)/m$, it follows that the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et is N. So if each $f_i(x^t)$ is irreducible, we are done. Since the roots of each $f_i(x)$ are the e^{th} roots of unity over $\mathbb{F}_q$, it follows that $f_i(x)$ divides $x^e - 1$. Thus, $f_i(x^t)$ divides $x^{et} - 1$. If follows quickly that $x^{et} - 1$ is a cyclotomic polynomial over $\mathbb{F}_q$ (see [3], Theorem 2.45). Moreover, the degree of each irreducible factor of $x^{et} - 1$ is mt. Since, $f_i(x^t)$ has degree mt, it follows that it is irreducible over $\mathbb{F}_q[x]$. Furthermore, since $f_i(x^t)$ divides $x^{et} - 1$, the order of $f_i(x^t)$ is et.

Q.E.D

To translate this result into more applied terms, we can think of this result in the following way. A given irreducible polynomial $f(x)$ of degree m and order e will provide an irreducible extension polynomial when composed with x^t if the orders of

the roots of $f(x)$, e, contains every factor of t present in $q^m - 1$. This is equivalent to having the roots of $f(x)$ not be t^{th} powers in $\mathbb{F}_{q^m}^*$. Having roots that are t^{th} powers is enough to ensure reducibility of the extension.

This theorem holds when the prime t is replaced with the prime power t^k for any positive integer k or even in the more general setting where t is some composite odd integer. The proof of this theorem provided in [3] is for the most general setting.

REFERENCES

[1] Gao, S., Panario, D. 1997. Tests and Constructions of Irreducible Polynomials over Finite Fields. *Foundations of Computational Mathematics*, 346-361.

[2] Swan, R. 1962. Factorization of Polynomials over Finite Fields. *Pacific J. Math*, 12, 1099-1106.

[3] Lidl, R., Niederreiter, H. 1983. "Finite Fields." *Addison-Wesley Publishing Company, Inc.*

[4] Berlekamp, E. R. 1970. Factoring Polynomials over Large Finite Fields. *Mathematics of Computation*, 24, 713-735.

[5] Perlis, Alexander R. 2004. Roots Appear in Quanta. *The American Mathematical Monthly*, 111-1, 61-63.

[6] Agou, S. 1981. A Class of Hyponormal Polynomials over a Finite Field. *Acta Arithmetica*, 39, 105-111.