Factoring Polynomials over Finite Fields

David Marquis david.marquis@carleton.ca

January 15, 2014

Abstract

Chapter 1 - Introduction

In this thesis we consider the problem of factoring polynomials over finite fields. Let q be a prime power, $\mathbb{F}_q$ a finite field. Given a monic, univariate polynomial $f \in \mathbb{F}_q[X]$, we want to find the complete factorization $f = f_1^{e_1} \cdots f_k^{e_k}$, where $f_1 \dots f_k$ are pairwise distinct monic irreducible polynomials and $e_1, \dots e_k$ are positive integers.

Computing the complete factorization reduces to the following problem. Given a monic, univariate polynomial $f \in \mathbb{F}_q[X]$ find monic polynomials f_1 and f_2 st $f = f_1 f_2$ and $0 < \deg(f_1) < \deg(f_2) < \deg(f)$. By an algorithm for polynomial factorization over finite fields (FPFF) we mean an algorithm that solves the above problem. FPFF has applications in computer algebra, coding theory, and cryptography. There are a number of algorithms that solve this problem in polynomial time: the number of operations used is polynomial in $\deg(f)$ and $\log(q)$. An issue with the existing algorithms is that they are probabilistic rather than deterministic. A longstanding question is if an algorithm for this problem exists that is deterministic and polynomial time.

A fundamental problem in theoretical computer science is whether the use of randomness allows computation to be done more efficiently. Formally this is the question of whether the complexity classes P and BPP are equal. Respectively these are the classes of decision problems that can be solved in polynomial time and bounded-error probabilistic polynomial time by a Turing machine. It is widely believed that these classes are equal but little progress has been made. For many computational problems it has proved possible to construct probabilistic algorithms more easily then deterministic ones. However, in many instances it has been possible to eventually replace these probabilistic algorithm's with more sophisticated deterministic algorithms.

The first explicit description of a probabilistic algorithm was Pocklington's 1917 algorithm for computing square roots in finite fields, a special case of FPFF. A polynomial time algorithm for solving the general FPFF problem probabilistically was given by Berlekamp in 1970. Since that time there has been little progress on solving the problem deterministically and unconditionally. More progress has been made on this problem assuming conjectures such as the Riemann Hypothesis, or generalization of it like the Extended Riemann Hypothesis, and the Generalized Riemann Hypothesis. We give a new partial result on deterministically factoring polynomials over finite fields assuming the Generalized Riemann Hypothesis.

1 Chapter 2 - Background

Definition 1. *If F is a nonempty a field then a function from F to the nonnegative real numbers is a norm if it satisfies the following properties*
(1) $|x| = 0$ *iff* $x = 0$
(2) $|xy| = |x||y|$
(3) $|x + y| \leq |x| + |y|$

Definition 2. *If M is a nonempty a set and λ a function from pairs of elements (γ, τ) to the nonnegative real numbers then λ is a metric if it satisfies the following properties:*
(1) $\lambda(\gamma, \tau) = \lambda(\tau, \gamma)$ *(2)* $\lambda(\gamma, \tau) = \lambda(\gamma, \rho) + \lambda(\rho, \tau)$ *for all* $\rho \in M$ *(3)* $\lambda(\gamma, \tau) = 0$ *iff* $x = y$

If λ is a norm then the pair (M, λ) is called a metric space. The properties are called symmetry, triangle inequality, and identity of indiscernibles respectively. If $|\cdot|$ is a norm then $d(x, y) = |x - y|$ is a metric. Let x be a nonnegative integer, l be a prime, and t be the largest power of l dividing x let

Definition 3. *The group of units of a ring R is denoted R^*.*

Definition 4. *Let x and d be positive integers then $v_d(x)$ is the largest power of d dividing x.*

1.1 Finite Fields Background

To Do: Stuff on finite fields. Existence and isomorphism of equal element finite fields.

Definition 5. *Let $x \in \mathbb{F}_q$ then* $\mathrm{ord}(x)$ *is the multiplicative order of x in $\mathbb{F}_q$.*

Definition 6. *Let g be a primitive root in $\mathbb{F}_q$ then* $\mathrm{Ind}(x)$ *wrt g is the least k st $g^k = x$ in $\mathbb{F}_q$.*

Definition 7. *A primitive dth root of unity in $\mathbb{F}_q$ is an element x st $x^d = 1$ and $x^{d/r} \neq 1$ for each prime r dividing d.*

Definition 8. *A primitive root (also called a generator) in ${\mathbb{F}_q}^*$ is an element x st* $\mathrm{ord}(x) = q - 1$.

Definition 9. *Let $\mathbb{F}_q$ be a finite field. The Frobenius automorphism is defined*

$$\tau(\alpha) = \alpha^q$$

for any $\alpha \in \mathbb{F}_q$.

To Do: Stuff on polynomials over finite fields.

Definition 10. *Let k be a field. Every polynomial over k has a unique factorization. Polynomials in which no factor appears in the factorization more than once are called squarefree. Polynomials which are products of linear factors are said to be splitting*

1.2 Deterministic Algorithms related to factoring polynomials

Bach and Shallit use notation which can simplify the statements of some of the theorems on polynomial factorization

For n a positive integer

$$\lg n = \begin{cases} 1 : n = 0 \\ 1 + \log_2(n) : n \neq 0 \end{cases}$$

For a finite field F define

$$\lg f = \begin{cases} 1 : f = 0 \\ (1 + \deg f)(\lg |F|) : f \neq 0 \end{cases}$$

Theorem 1.1. *(Bach and Shallit [1996]) Let f be a nonzero polynomial in $\mathbb{F}_q[X]$, $R = \mathbb{F}_q[X]/(f)$*
(a) Addition and subtraction of elements in R using $O(\lg f)$ bit operations
(b) Multiplication of elements in R using $O((\lg f)^2)$ bit operations
(c) Inversion of elements in R^* using $O((\lg f)^2)$ bit operations
(d) Exponentiation of elements in R to the power e using $O((\lg e)(\lg f)^2)$ bit operations

Definition 11. *Let $\mathbb{F}_q$ be a finite field and $f \in \mathbb{F}_q[X]$. The Berlekamp subalgebra B is the subring of $R = \mathbb{F}_q[X]/(f)$ st an element of R is in B iff all its components are in $\mathbb{F}_q$.*

Note that there is an equivalent characterization of the Berlekamp subalgebra as the elements of $r \in R$ st $r^q = r$. The Berlekamp algebra is used in Berlekamp's original polynomial factorization algorithm and almost all subsequent results on factoring polynomials over finite fields.

Theorem 1.2. *(Bach 7.4.4 p.166). Let $\mathbb{F}_q$ be a finite field, f a polynomial in $\mathbb{F}_q[X]$, and $R = \mathbb{F}_q[X]/(f)$, and let B denote the Berlekamp algebra of R considered as a $\mathbb{F}_q$-vector space. A basis for B can be found using $O((\deg f + \lg q)(\lg f)^2)$ bit operations.*

Note that when f splits into a product of linear factors the Berlekamp algebra of $R = \mathbb{F}_q[X]/(f)$ is equal to R. It is possible to reduce factorization of an arbitrary polynomial in $\mathbb{F}_q$ to factoring a polynomial with coefficients in $\mathbb{F}_p$ that splits into a product of linear factors. This reduction is too slow to be used by the better probabalistic algorithms. However, some theorems on deterministic factoring in the literature use this reduction to assume that the polynomial to be factored has coefficients in $\mathbb{F}_p$ and splits into a product of linear factors.

Most algorithms for FPFF procede in three stages. First factorization of the polynomial is reduced to factoring a set of squarefree polynomials. Then factorization of each of these squarefree polynomials is reduced to factoring a set of polynomials st each irreducible factor of these polynomial has the same degree. Deterministic polynomial time algorithms are known for both these problems. The precise running times are given in 1.3 and 1.4.

To Do: explicit description of squarefree and equal degree factorization algorithms

Theorem 1.3. *Theorem 5.9. (Bach 7.5.1-7.5.2 p.170) If f is a monic element of $\mathbb{F}_q[X]$ and $\deg f > 0$, then a factorization $f = f_1^{e_1} \dots f_r^{e_r}$ where each f_i is monic and squarefree can be computed in $O((\deg f)(\lg f)^2)$ bit operations.*

Theorem 1.4. *Let f be a squarefree polynomial of degree d. Then $f = f_1^{e_1} \dots f_r^{e_r}$ where f_i is the product of all the monic degree i irreducible factors of f can be computed in $O((\deg f + \lg q)(\lg f)^2)$ bit operations.*

There are a varity of probabalistic distinct degree factorization algorithms. The Cantor Zassenhaus algorithm is a conceptually simple variant. This is given in algorithm 1.

Algorithm 1: Algorithm 1: Cantor Zassenhaus

Contruct a random α on $B(f, \mathbb{F}_q)$;
g = gcd(f, α);
if $1 < \deg g < \deg f$ **then**
    return g;
end
s = $\chi_2(g)$;
g = gcd$(s - 1, f)$;
if $1 < \deg g < \deg f$ **then**
    return g;
end

The next theorem reduces the problem of factoring polynomials over $\mathbb{F}_q$ to root finding of polynomials of degree less than p over $\mathbb{F}_p$.

Theorem 1.5. *Let q be a prime power p^n, f a polynomial of degree n in $\mathbb{F}_q[X]$, and assume f has k irreducible factors for $k \geq 2$. Then there are polynomials $g, h \in \mathbb{F}_q[X]$ with the following properties*
1) h splits completly in $\mathbb{F}_p[X]$
2) For any zero a of h, $\gcd(g - a, f)$ is a nontrivial divisor of f
3) deg $g < n$
4) deg $h = k$
These polynomials can be computed using $O((\lg p + n + \deg f)(\lg f)^2)$ bit operations.

Note that if $\deg(h) \geq p$ then Theorem 5.9 can be used to produce a factorization of f into a product of powers of irreducible polynomials of degree less than p.

Corollary 1.6. *Let q be a prime power, $\mathbb{F}_q$ a finite field, f a squarefree polynomial in $\mathbb{F}_q[X]$ of degree n, and E a splitting field of f. Let*

$$f = \prod_{i=1}^{r} f_i$$

with $f_1, \dots, f_r$ irreducible polynomials and $e_1, \dots, e_r$ positive integers. If there exists $1 \leq j \leq n$ st $1 < \deg(h_j) < \deg(f)$ then completely factoring f in E reduces to factoring $h_1, \dots, h_r$ in E reduces to factoring polynomials $h, g_1, \dots, g_t$ for $t \leq r$ st $\deg(h_i) < \deg(f)$ with coefficients in E.

Proof. The reduction is done in two stages. First, factoring f in $\mathbb{F}_q[X]$ reduces to factoring a polynomial h st $\deg(h) = \sum_{j \neq i} \deg h_j + \deg h_i \leq \deg(f)$.

If the factorization of these polynomials is given then we can obtain f_j in $\mathbb{F}_q$ in polynomial time in $\deg(f)$ and $\log q$. Each f_j splits in E so its factorization reduces to factoring polynomials h_j with coefficients in $\mathbb{F}_p$ st $\deg h_j < \deg f$. □

[Draft note : the splitting field can have degree up to $n!$ over $\mathbb{F}_q$: The theorem applies as well to factoring each of the h_j in the respective subfields of the splitting field in which they split. Still have to bound the complexity]

Theorem 1.7. *Let q be a prime power, f a polynomial with coefficients in $\mathbb{F}_q$, and $\alpha \in \mathbb{F}_q[X]/(f)$. There is an algorithm to compute the norm of α that is polynomial time in $\log q$ and the degree of f.*

This theorem is a consequence of that fact that the minimal polynomial of $g \in \mathbb{F}_q[X]/(f)$ can be computed in polynomial time. See Bach and Shallit [1996] Theorem 7.8.1.

For q a prime power and $f \in \mathbb{F}_q[X]$ and squarefree let $B(f, \mathbb{F}_q)$ be the Berlekamp subalgebra of $\mathbb{F}_q[X]/(f)$. For d dividing $q - 1$, and H_d the multiplicative subgroup of ${\mathbb{F}_q}^*$ of elements of order dividing d let

$$\chi_d : {\mathbb{F}_q}^* \to H_d$$
$$\chi_d(x) = x^{\frac{q-1}{d}}$$

Theorem 1.8. *(Euler's criterion). Let $x \in {\mathbb{F}_q}^*$ and l a prime st $l \mid q-1$ then $\chi_l(x) \neq 1$ iff x is a lth nonresidue in ${\mathbb{F}_q}^*$.*

Euler's criterion is generalized by the following theorem.

Theorem 1.9. *Let $x \in {\mathbb{F}_q}^*$ and l a prime st $l \mid q-1$ then $\chi_{l^i}(x) \neq 1$ iff $i < v_l(\mathrm{Ind}(x))$.*

For $f \in \mathbb{F}_q[X]$ st f is squarefree and has degree k, and $\alpha \in B(f, Fq)$ define

$$\chi_d(\alpha) = (\chi_d(\alpha_1), \ldots, \chi_d(\alpha_k))$$

Theorem 1.10. *Let $\alpha \in B(f, \mathbb{F}_q)$ and l a prime st $l \mid q-1$ then $\chi_{l^i}(\alpha) \in \mathbb{F}_q[X]$ iff there exists ω an l^i root of unity in ${\mathbb{F}_q}^*$ st*

$$\chi_{l^i}(\alpha_j) = \omega$$

for all $1 \leq j \leq n$.

Finally we state an important theorem of Lenstra on constructing isomorphisms between finite fields.

Theorem 1.11. *Let p be a prime number, m be a natural number, and f_1, f_2 two irreducible polynomials in $\mathbb{F}_p[X]$ of degree m. All isomorphisms between the fields $\mathbb{F}_p[X]/(f_1)$ and $\mathbb{F}_p[X]/(f_2)$ can be found in polynomial time in $\log p$ and m.*

1.11 can be generalized to models of finite fields other than $\mathbb{F}_q[X]/(f)$.

1.3 Riemann Hypothesis

Most of the results on factoring polynomials over finite fields assume either the Riemann Hypothesis or a generalization of it. The two generalizations that are commonly used are the Extended Riemann Hypothesis and the Generalized Riemann Hypothesis. We give the statement of these conjectures in their simplest form. Let

$$li(x) = \int_2^x \frac{dt}{\log t}$$

and let $\pi(x)$ be the number of primes less than or equal to x. First we state the ordinary Riemann Hypothesis

Conjecture 1.12. *Riemann Hypothesis: Let x be a positive integer for any $\epsilon > 0$*

$$\pi(x) = li(x) + O(x^{\frac{1}{2}+\epsilon})$$

It was proved by Dirichlet that if $\gcd(a, n) = 1$ then there are infinitely many primes congruent to a modulo n. (These are called primes in an arithmetic progression). Let $\pi(x, n, a)$ be the primes p less than or equal to x st $p \equiv a \bmod n$. The Extended Riemann Hypothesis (ERH) is a generalization of the Riemann hypothesis which can be stated in terms of primes in arithmetic progressions.

Conjecture 1.13. *Extended Riemann Hypothesis: Let x, n, a be positive integers and a and n be relatively prime then for any $\epsilon > 0$*

$$\pi(x, n, a) = \frac{li(x)}{\phi(n)} + O(x^{\frac{1}{2}+\epsilon})$$

Any finite extension of the rationals of finite degree is called an *algebraic number field*. The generalization of the Riemann Hypothesis to algebraic number fields is called the Generalized Riemann Hypothesis.
Algebraic number fields are often represented in the form $\mathbb{Q}[X]/(f)$ where f is an irreducible polynomial in $\mathbb{Z}[X]$. The *degree* of an algebraic number field is its dimension as a vectorspace over $\mathbb{Q}$.

Theorem 1.14. *If k is an algebraic number field of degree n there are n field homomorphisms from k into $\mathbb{C}$. These are given by the factorization of f and are called* embeddings.

Let k be an algebraic number field of degree n and $\alpha_1, \ldots, \alpha_n$ be its embeddings.

Definition 12. *The norm of $x \in k$ is defined*

$$N(x) = \prod_{i=1}^{n} \alpha_i(x).$$

Theorem 1.15. *If k is an algebraic number field of degree n and $x \in k$ then there is a unique monic polynomial $f \in \mathbb{Q}[X]$ of degree less than or equal to n st $f(x) = 0$ and for any polynomial $g \in \mathbb{Q}[X]$ if $g(x) = 0$ then $f \mid g$. f is called the* minimal polynomial *of f.*

Theorem 1.16. *Algebraic number fields have a subring of* algebraic integers*, all those elements in k st their minimal polynomial is in $\mathbb{Z}[X]$.*

A nonzero ideal A of the ring of integers R of an algebraic number field is a *prime ideal* if A/P is an integral domain. An analogue of the prime number theorem is known for prime ideals. For any algebraic number field the number of prime ideals is infinite.
For an algebraic number field k let $\pi_k(x)$ be the number of prime ideals with norm less than or equal to x.

Conjecture 1.17. *Generalized Riemann Hypothesis: Let k be an algebraic number field then for any $\epsilon > 0$*

$$\pi_k(x) = li(x) + O(x^{\frac{1}{2}+\epsilon})$$

1.4 Constructions depending on RH, ERH, GRH

Definition 13. *Let $\mathbb{F}_q$ be a finite field and n be a positive integer. An element $x \in \mathbb{F}_q$ is an nth nonresidue if it is not an nth power of any element in $\mathbb{F}_q$.*

Nonresidues are useful for the construction of many polynomial factorization algorithms. They are also used in the construction of irreducible polynomials and hence models of $\mathbb{F}_q$. There is an elegant way to test if an element in $\mathbb{F}_q$ is an lth nonresiude that is due to Euler.

It is easy to construct a nonresidue probabalistically. Finding nonresidues deterministically is more challenging. In $\mathbb{F}_p$ testing $1, 2, \ldots$ until an nth nonresidue is found is the best known approach known. Under ERH this algorithm is polynomial time.

Theorem 1.18. *The least nth nonresidue* $\mod p$ *is $O((\log p)^2)$ under the ERH.*

The proof is largely due to Ankeny [1952]. See Bach and Shallit [1996] Ch 8 for a proof.

Definition 14. *The nth cyclotomic polynomial is Φ_n.*

Theorem 1.19. *Theorem 5.3 (Huang [1991]). The following have algorithms that use a polynomial number of bit operations in q and* $\log p$ *under the Generalized Riemann Hypothesis (GRH).*
1) Given primes q, p to factor Φ_q mod p
2) Given primes q, p to construct a qth nonresidue in $\mathbb{F}_p[X]/(h)$ where h is an irreducible factor of Φ_q mod p.

Using Huang's algorithm nth nonresidues in $\mathbb{F}_q[X]$ can be constructed in $poly(n, \log q)$ bit operations.

The problems of finding lth nonresidues and taking lth roots are closely related. Given an lth nonresidue, lth roots can found deterministically. In the other direction, if a primitive lth root of unity ω_l in $\mathbb{F}_q$ is known, an algorithm for taking lth roots could be used to repeatedly take roots of ω_l until an lth nonresidue is found. In the case $l = 2$, -1 is a primitive 2th root of unity so the problem of computing quadratic nonresidue reduces to the problem of computing square roots.

Theorem 1.20. *Let x be an element of $\mathbb{F}_q$. Suppose* $\gcd(n, \mathrm{ord}(x)) = 1$ *then an nth root of x can be computed in deterministic polynomial time.*

The following theorem generalizes Tonelli's result on computing square roots mod p. Another way to think of this theorem is that binomial equations can be solved quickly in finite fields.

Theorem 1.21. *(See Bach 7.3.2 p.161) Let q be a prime power, l be a prime, and $l \mid q - 1$. Given an lth nonresidue in $\mathbb{F}_q$. Given an lth nonresidue in ${\mathbb{F}_q}^*$ there is an deterministic algorithm to compute all solutions to $X^l - a$ with running time $O(lv_r(q-1)(lgq)^3)$. We now state some of the basic theorems related to computation in $\mathbb{F}_p$ algebras and polynomial factorization.*

Theorem 1.22. *(Theorem 7.8.3 Bach and Shallit [1996]) Assume GRH. There is a deterministic polynomial time algorithm to find an irreducible polynomial of degree n over $\mathbb{F}_p$. The algorithm uses $O(n^6(\lg p + \lg n)^4(\lg p)^2)$ bit operations.*

Theorem 1.23. *Assume GRH. Let $\mathbb{F}_q$ be a finite field and $g \in \mathbb{F}_q[X]$. Let v be the degree of the splitting field of g over $\mathbb{F}_q$. A splitting field for g can be constructed in polynomial time in* $\log q$ *and v.*

This follows from Theorem 5:10, Theorem 5:13, and Theorem 5:14.

Theorem 1.24. *(Evdokimov [1992] Theorem 1.3) Assume GRH. Let $\mathbb{F}_q$ a finite field represented in the form $\mathbb{F}_q = \mathbb{F}_p[X]/(g)$ for g an irreducible polynomial over $\mathbb{F}_p$, and l be a prime. There is an deterministic algorithm to construct an lth nonresidue in $\mathbb{F}_q$ in poly(l, q) bit operations.*

Conditions on the degree group

Theorem 1.25. *(Ronyai Theorem 1.1) Let $f \in \mathbb{F}_p[X]$ be a polynomial such that f has no multiple roots and the roots of f are in $\mathbb{F}_p$. Let r be a prime divisor of $n = \deg(f) > 1$ and suppose that the rth cyclotomic field F over $\mathbb{F}_p$ and an rth nonresidue b from F are given. Then we can find a nontrivial factor of f in* $\text{poly}(\log p, n^r)$ *time under GRH.*

The approach of Ivanyos, Karpinski, Saxena gives a result that depends on the largest prime factor of the $\deg(f) - 1$ when the degree of the polynomial is prime.

Theorem 1.26. *(Ivanyos, Karpinski, Saxena Theorem 1.1) If $n > 2$ is prime, r the largest prime factor of $(n-1)$ and $f(x)$ is a degree n polynomial over $\mathbb{F}_p$ then we can find a nontrivial factor of $f(x)$ deterministically in time* $\text{poly}(\log p, n^r)$ *under GRH*

Theorem 1.27. *(Arora, Ivanyos, Karpinski, Saxena Theorem 1.1) Let f be a polynomial of prime degree n over $\mathbb{F}_q$. Assume that $n-1$ has a r-smooth divisor s, with $s \geq \sqrt{n/l} + 1$ and $l \in \mathbb{N} > 0$. Then we can find a nontrivial factor of $f(x)$ deterministically in time* $\text{poly}(\log q, n^{r+\log l})$ *uner GRH.*

Conditions on the galois group

Theorem 1.28. *Let p be prime, m be a natural number, and let $f \in \mathbb{Z}[X]$ be a polynomail with leading coefficient relatively prime to p and solvable Galois group over $\mathbb{Q}$. Then assuming the generalized Riemann hypothesis, the polynomial f mod p can be factored into irreducible factors in time polynomial in* $\log p, m,$ *and* $\deg(f)$.

Conditions on the field

Theorem 1.29. *(von zur Gathen) Assume ERH. For a prime power $q = p^n$, let $S(p)$ denote the largest prime factor of $p-1$. There is a deterministic algorithm that splits any $f \in \mathbb{F}_q[X]$ using $O((S(p) + \lg p)(\lg f)^4)$.*

$$|x|_l = \begin{cases} 0 : x = 0 \\ l^{-t} : x \neq 0 \end{cases}$$

Theorem 5.17. $|\cdot|$ is a norm.

The *norm* of $\alpha \in R = \mathbb{F}_q[X]/(f)$, where f has k distinct factors, into $\mathbb{F}_q$ is defined

$$N(\alpha) = \prod_{j=1}^{k} \alpha_j$$

The norm of an arbitrary element of R is a homogenous polynomial of the same degree as f.

Of course it is not possible to compute the norm directly from its definition if the roots of f in E are unknown. The norm of a general α can be computed in polynomial time by Theorem 5.7 [fix]. We also have the following special case.

Theorem 1.30. *Let f be a polynomial of degree n and $\alpha = a - bX$ in $\mathbb{F}_q[X]/(f)$. Then*

$$N(\alpha) = b^n f\left(\frac{a}{b}\right.$$

Proof. Let ζ_i be the roots of f then $N(a - bX) = \prod_{i=1}^{n} a - b\zeta_i = b^n f(a/b)$ □

By a reduction between two computational problems A and B we mean a Turing reduction. Intuitively this means that given an algorithm for computing a solution to B a solution for any instance of A can be recovered. A bit operation is a logical operation on two bits. The running time or time complexity of an algorithm is the total number of bit operations it uses. For example, addition of two n bit numbers takes $O(n)$ [fix] bits. An algorithm that has running time that is a polynomial in the number of bits in is input is called polynomial time. For example an algorithm for FPFF is polynomial time if its running time is polynomial in $\deg(f)$ and $\log(q)$. When we say that an algorithm exists we mean that this paper or the papers cited provided a means to construct the algorithm explicitly.

Lemma 1.31. *Let q be a prime power, $\mathbb{F}_q$ a finite field, l a prime, and $s = v_l(q-1)$. For $x, y \in Fq$ we have*

$$\mathrm{ord}_l(xy) \leq \max f\{\mathrm{ord}_l(x), \mathrm{ord}_l(y)\}.$$

Equality holds iff $\mathrm{ord}_l(x) \neq \mathrm{ord}_l(y)$ *or* $\mathrm{Ind}(x) + \mathrm{Ind}(y) \not\equiv 0 \bmod l^{s-t+1}$ *where* $t = v_l(\mathrm{ord}_l(x))$.

If $\sigma_l(\gamma + \tau) > 0$ then $\max\{\sigma_l(\gamma), \sigma(\tau)\} > 0$. In other words if $\alpha\beta$ has index diameter larger than 0 then at least one of α and β has index diameter larger than 0.

Proof. Let $\mathrm{ord}_l(x) = \mathrm{ord}_l(y) = l^t$ for some t and $\mathrm{Ind}(x) + \mathrm{Ind}(y) \equiv 0 \bmod l^{s-t+1}$. Then $l^{s-t+1} \mid \mathrm{Ind}(xy) \equiv \mathrm{Ind}(x) + \mathrm{Ind}(y)$ so by Corollary ?? $\mathrm{ord}_l(xy) < l^t$. □

For example let ω_3 be a primitive 3rd root of unity in $\mathbb{F}_q$, $x = \omega_3, y = \omega_3^2$. $t = v_3(\mathrm{ord}_3(x)) = 1$ and $\mathrm{Ind}(x) + \mathrm{Ind}(y) \equiv 0 \bmod 3^{s-t+1} = 3$ so $\mathrm{ord}_3(xy) \neq \max\{\mathrm{ord}_3(x), \mathrm{ord}_3(y)\}$.

As we did for χ_d we generalize Ind to elements in Berlekamp algebras. For $\alpha \in B(f, \mathbb{F}_q)$ let

$$\mathrm{Ind}(\alpha) = (\mathrm{Ind}(\alpha_1), \ldots, \mathrm{Ind}(\alpha_k))$$

Let $\alpha, \beta \in B(f, \mathbb{F}_q)$ then

$$\mathrm{Ind}(\alpha) = (\mathrm{Ind}(\alpha_1) + \mathrm{Ind}(\beta_1), \ldots, \mathrm{Ind}(\alpha_k) + \mathrm{Ind}(\beta_k))$$

$\mathrm{Ind}(\alpha^k) = k(\mathrm{Ind}(\alpha_1), \ldots, \mathrm{Ind}(\alpha_k))$ and $\mathrm{Ind}(1) = (0, \ldots, 0)$

Let x be a nonnegative integer, l be a prime, and t be the largest power of l dividing x let

$$|x|_l = \begin{cases} 0 : x = 0 \\ l^{-t} : x \neq 0 \end{cases}$$

and let $d_l(x, y) = |x - y|$.

Definition 15. *For $\alpha \in B(f, \mathbb{F}_q)$, l a prime dividing $q-1$, and $\gamma = Ind(\alpha)$ the diameter of γ is*

$$\sigma_l(\gamma) = \max\{d_l(\gamma_i, \gamma_j)\}$$

.

If $\mathrm{Ind}(\alpha) = m$ then we say that α has index diameter m. For α, l as in Definition 3.2 $\sigma_l(Ind(\alpha)) > 0$ iff $\mathrm{Ind}(\alpha) \neq k(1, \ldots, 1)$ for all $k \in \mathbb{Z}/l^s\mathbb{Z}$.

The following theorem is implicit in the paper of von zur Gathen.

Theorem 1.32. *Let f be a squarefree polynomial in $\mathbb{F}_q[X], \alpha$ an element in $B(f, \mathbb{F}_q), \gamma = \mathrm{Ind}(\alpha)$. If*

$$\sigma_l(\gamma) > 0$$

then f can be factored in deterministic polynomial time in $\log q, \deg(f)$, *and l.*

Proof. Let $\alpha \in B(f, \mathbb{F}_q)$ and $\gcd(\alpha, f) = 1$ then $\sigma_l(\mathrm{Ind}(\alpha)) > 0$ iff $\mathrm{Ind}(\alpha) \neq k(1, \ldots, 1)$ for all $k \in \mathbb{Z}/l^s\mathbb{Z}$. This is equivalent to the existence of a k st $\mathrm{Ind}(\alpha) - k(1, \ldots, 1)$ is divisible by l^s on one component but not every component.

Let ω_{l^s} be an l^s primitive root of unity and for all $0 \leq i \leq s$ let $\omega_{l^i} = \omega_{l^s}^{l^{s-i}}$Note that $\mathrm{Ind}(\alpha) = \mathrm{Ind}_{\chi_{l^s}} \alpha \bmod l^s$ so there exists a k st

$$\gcd(\chi_{l^s}(\alpha)/\omega_{l^s}^k - 1, f) = \gcd(\chi_{l^s}(\alpha) - \omega_{l^s}^k, f)$$

is a nontrivial factor h of f. For any field k if $h, g_1, g_2 \in k[X]$ and $h \mid g_1 - g_2$ then for n a positive integer $h \mid g_1^n - g_2^n$ of f. For n a positive integer

$$\gcd(\chi_{l^s}(\alpha)^{l^n} - \omega_{l^s}^{kl^n}, f) = \gcd(\chi_{l^{s-n}}(\alpha) - \omega_{l^{s-n}}^k, f)$$

is a factor of f for some $0 < k < l^{s-n}$. There exists a least positive integer i st

$$\gcd(\chi_{l^i}(\alpha) - \omega_{l^{s-n}}^k$$

is a nontrivial factor of f for some $0 < k < l^i$. It remains to show that i and k can be found in polynomial time in $\log q, \deg(f)$, and l.

Let $s = v_l(q-1)$. $\chi_{l^s}(\alpha) \notin {\mathbb{F}_q}^*$ by Theorem 3.3 and all components of it are l^ith roots of unity. Hence there exists a least nonnegative integer $j \leq s$ st $\chi_{l^s}(\alpha)^{l^j} = \chi_{l^{s-j}}(\alpha) \in {\mathbb{F}_p}^*$. By Theorem 3.1 the polynomial

$$X^l - \chi_{l^{s-j}}(\alpha)$$

has l roots in ${\mathbb{F}_q}^*$.

Each of these roots is an l^{s-j} root of unity and so the set of roots can be expressed $\{\omega_{l^{s-j+1}}^{k_1}, \ldots, \omega_{l^{s-j+1}}^{k_l}\}$. Then $i = s - j$ and k is one of $k_1, \ldots, k_l$. It is easy to verify that the running time is polynomial time in $\log q$, $\deg(f)$, and l.

□

(Note that size of $\sigma_l(\alpha)$) is a factor in the number of operations used by the algorithm. The smaller $\sigma_l(\alpha)$ the more operations are required)

The following theorem is not needed in the sequel but is somewhat interesting.

Theorem 1.33. *Let f be a squarefree polynomial in $\mathbb{F}_q[X]$, α, β elements in $B(f, \mathbb{F}_q)$, $\gamma = \mathrm{Ind}(\alpha)$, and $\tau = \mathrm{Ind}(\beta)$.*

$$\sigma_l(\gamma + \tau) \leq \max \sigma_l(\gamma), \sigma_l(\tau)$$

Proof.

$$\begin{aligned}\sigma_l(\gamma + \tau) &= \max\{d_l(\gamma_i + \tau_i, \gamma_j + \tau_j) : 1 \leq i, j \leq n\} \\ &\leq \max\{\max\{d(\gamma_i, \gamma_j), d(\tau_i, \tau_j)\} : 1 \leq i, j \leq n\} \\ &\leq \max\{sigma_l(\gamma), sigma_l(\tau)\}\end{aligned}$$

Where the first inequality is by the triangle inequality.

□

Chapter 3 - Previous Results

In this section we review the literature on algorithms for FPFF that are probabilistic, deterministic, and deterministic under certain conjectures.

A probabilistic factorization algorithm was given in Zassenhaus [1969] that uses a number of bit operations polynomial in $\log q$ and $\deg f$. A similar probabalistic algorithm was given in Berlekamp [1970]. A more efficient algorithm was given by Cantor and Zassenhaus [1981]. These probabilistic algorithms are of Las Vegas type, if a solution is produced then it is correct. No unconditional and deterministic algorithm for FPFF is known that runs in subexponential time even for polynomials of degree 2. An algorithm for this problem was given in Berlekamp [1967] which uses $O((\deg(f) + q)(\lg(f))^2)$. Shoup [1991a] gives an algorithm for unconditional deterministic polynomial factorization of a degree n polynomial in $\mathbb{F}_{p^k}[X]$ that uses $(logp)\tilde{O}(nk^2) + (p^{1/2}\log p)\tilde{O}(nk)^{3/2}$ bit operations. Shoup [1990] and Lange and Winterhof [2000] give algorithms for factoring almost all polynomials in $\mathbb{F}_p$ deterministically.

Many results on deterministic FPFF pertain to finding roots of binomials, equations of the form $X^n - a$. In this case a root of the polynomial is called an nth root of a. Deterministic algorithms for computing n roots exist which run in polynomial time in special cases. Schoof [1985] gives an algorithm for computing the square root of x in $\mathbb{F}_p$ that uses $O((x^{1/2+\epsilon}\log p)^9)$ bit operations as an application of an algorithm for counting points on elliptic curves. Using ideas related to Schoof's, Pila [1990] shows that for any odd prime l and prime p st $p \equiv 1 \mod p$ an lth root of unity in $\mathbb{F}_p$ can be computed in $poly(\log p, l)$. Sze [2011] gives a deterministic algorithm to compute square roots in finite fields that runs in polynomial time for some special finite fields.

There are a large number of deterministic results under generalizations of the Riemann hypothesis. Typically these results make use of the following two theorems on the construction of nonresidues in $\mathbb{F}_p$ and certain extensions of $\mathbb{F}_p$ respectively. Specifically they deterministically reduce some instance of the FPFF to the problem of construction of a nonresidue and then they apply one of the following theorems to solve the latter problem in deterministic polynomial time under some version of the Riemann Hypothesis. These results are stated in Theorem 5.2 and 5.3 in the appendix. As with the case for the unconditionally deterministic results, a number of the results depending on the Riemann Hypothesis pertain to binomial equations. A polynomial time reduction from finding a root of $X^2 - a$ to computing quadratic nonresidues in $\mathbb{F}_q$ was given in Tonelli [1891]. This algorithm is sometimes attributed to Shanks [1972] or Adleman et al. [1977]. Another method of finding a root of $X^2 - a$ in $\mathbb{F}_q$ was given by Cipolla [1903]. Both of these algorithms were later generalized to solving $X^n - a$.

Evdokimov [1989] gives a deterministic polynomial time algorithm for factoring polynomials over $\mathbb{F}_p$ with solvable Galois group over $\mathbb{Q}$ generalizing a result of Huang [1991]. von zur Gathen [1987] von zur Gathen [1987] gives an algorithm for FPFF some special finite fields. For $\mathbb{F}_q$ a finite field of characteristic p the algorithm

runs in polynomial time when $p-1$ is smooth. This algorithm is generalized to apply when $\Phi_n(p)$ is smooth in Bach et al. [2001]. The complexity of Gathen's algorithm was improved in Shoup [1991b].

Rónyai [1988] gives a poly$(n^r, \log q)$ algorithm for factoring polynomials in $\mathbb{F}_q[X]$ for any $r|\deg(f)$. An implication is that if f has a constant number of irreducible factors then it can be factored. Generalizing this result, Evdokimov [1989] gives a deterministic algorithm for factoring polynomials over $\mathbb{F}_q$ that uses $O((n^{\log n}\log q)^{O(1)})$ bit operations under GRH. This remains the best algorithm for the general problem. Ivanyos et al. [2012] further generalizes the framework of Evdokimov [1989] to give algorithms which allows a factor to be constructed in some cases and avoids the assumption of GRH. When a factor is not a recovered an automorphism of a certain algebra is found.

Ivanyos et al. [2009] and Arora et al. [2012] use an algebraic-combinatorial approach and give results that are deterministic polynomial time under GRH for some polynomials of prime degree.

Chapter 4 - New Definitions, Lemmas, Theorems

We give a new partial result that is deterministic under a generalization of the Riemann hypothesis. The tool we make use of is the following. If f is a product of n linear factors, $\mathbb{F}_q$ a finite field containing nth primitive roots of unity, and there is an element α in $R = \mathbb{F}_q[X]/(f)$, there is a relationship between the index of the norm of α into $\mathbb{F}_q$ and the index of the components of α. This relationship gives α structure that a randomly chosen element in R does not have.

Definition 16. *Let $\mathbb{F}_q$ be a finite field. A set T of elements in $\mathbb{F}_q$ is index balanced with respect to a natural number n if there exists $0 \le k < n$ st*

$$\mathrm{Ind}(t) \equiv k \bmod n$$

for every $t \in T$

A notable set of polynomials over $\mathbb{F}_q$ are those with roots that are not balanced wrt to some prime l dividing $q-1$. These polynomials are easy to factor by 1.32.

We will see later that polynomials that split into products of linear factors over $\mathbb{F}_q$ and satisfy $v_l(\mathrm{Ind}f(0)) > v_l(n)$ are easy to factor. Factoring a polynomial st $v_l(\mathrm{Ind}f(0)) < v_l(n)$ reduces to factoring another polynomial st $v_l(\mathrm{Ind}f(0)) = v_l(n)$.

Definition 17. *Let q be a prime power, $\mathbb{F}_q$ be a finite field, $f \in \mathbb{F}_q[X]$ of degree n, and l be a prime dividing $q-1$ then f is*
1) low index wrt l if $v_l(\mathrm{Ind}f(0)) < v_l(n)$,
2) intermediate index wrt l if $v_l(\mathrm{Ind}f(0)) = v_l(n)$,
3) high index wrt l if $v_l(\mathrm{Ind}f(0)) > v_l(n)$,

To Do: examples of these types.

Lemma 1.34. *Let $\mathbb{F}_q$ be a finite field, l a prime dividing $q-1$, and f a polynomial of degree n that splits into a product of linear factors over $\mathbb{F}_q$ st $v_l(\mathrm{Ind}f(0)) < v_l(n)$ then for any l nonresidue $a \in \mathbb{F}_q$ the polynomial $g = \frac{1}{a^n}f(aX)$ satisfies $v_l(\mathrm{Ind}g(0)) = v_l(n)$ and if h is a factor of g then $a^n h(X/a)$ is a factor of f.*

Proof. Since a is an lth nonresidue $\mathrm{Ind}(a)$ is coprime to l. Therefore $v_l(\mathrm{Ind}(a^n)) = v_l(n\mathrm{Ind}(a)) = v_l(n)$

$$\mathrm{Ind}g(0) = \mathrm{Ind}(f(0)/a^n) = \mathrm{Ind}(f(0)) - \mathrm{Ind}(a^n)$$

$$v_l(\mathrm{Ind}g(0)) = v_l(\mathrm{Ind}(f(0)) - \mathrm{Ind}(a^n)) = \max\{v_l(\mathrm{Ind}(f(0))), v_l(\mathrm{Ind}(a^n))\} = v_l(n)$$

□

Definition 18. *Let q be a prime power, $\mathbb{F}_q$ a finite field, l a prime dividing $q-1$,*

$$f = \sum_{i=0}^{n} c_i X^i$$

a monic polynomial with coefficients in $\mathbb{F}_q$ st $v_l(\mathrm{Ind}(f(0))) = v_l(n)$, and ω an element of $\mathbb{F}_q$ st $v_l(\mathrm{Ind}(\omega)) = v_l(n)+1$
Then
1) The coefficient c_k of f is Type 1 wrt l if $v_l(\mathrm{Ind}(c_k\omega^k)) = v_l(n)$.
2) The polynomial f is Type 1 wrt l if every coefficient except c_n is Type 1.
3) The polynomial f is balanced wrt l if every nonzero coefficient except c_n is Type 1.
4) The polynomial f is unbalanced wrt l if it is not balanced.

Letting ω be a root of the polynomial $X^{l^{v_l(n)}} - f(0)$ would work which is what I was doing before. A root of $X^{l^{v_l(n)}} - f(0)$ exists because of the restriction on the index of the constant term $v_l(\text{Ind}(f(0))) = v_l(n)$ (intermediate index polynomials) and it can be found using Tonelli's algorithm. But this way of constructing ω isn't conceptually clear. It is much simpler to take an lth nonresidue in $\mathbb{F}_q$ and raise it to the power l repeatedly until an element with the property is found.

Note that f is not Type 1 iff it has a coefficient other than c_n that is not Type 1 and f is balanced iff it has a nonzero coefficient other than c_n that is not Type 1
To Do: Better name for Type 1?

The next lemma shows that the certain terms can be removed from a balanced or unbalanced polynomial without making it unbalanced or balanced respectively.

Lemma 1.35. *Let $\mathbb{F}_q$ be a finite field, l a prime dividing $q-1$, and*

$$f = \sum_{i=0}^{n} c_i X^i$$

then
1) If f is a balanced polynomial $f - c_k X^k$ is also a balanced polynomial for any $0 < k < n$. 2) If f is an unbalanced polynomial and c_k is Type 1 for some $0 < k < n$ then $f - c_k X^k$ is also an unbalanced polynomial.

Definition 19. *For p a prime and k a positive integer, $\mathbb{F}_{p^k}$ a finite field, let $S(\mathbb{F}_{p^k})$ be the subset of $\mathbb{F}_{p^k}[X]$ of polynomials that are squarefree, are products of linear factors, and have degree less than p.*

Definition 20. *Let $\mathbb{F}_q$ be a finite field, and l a prime dividing $q-1$. Then $T(\mathbb{F}_q, l)$ is the subset of $S(\mathbb{F}_q)$ st $f \in T(\mathbb{F}_q, l)$ iff l divides $\deg(f)$ and f is not Type 1 wrt l.*

The next result is the main theorem. Note that while it only treats polynomials in $f \in T(\mathbb{F}_q, l)$, which are required to have intermediate index, the polynomials in $S(\mathbb{F}_q)$ of high and low index are easy to factor or can be reduced to factoring a polynomial of intermediate index respectively. The main restriction made by the theorem is that the polynomial f is not balanced. Equivalently, f has at least one nonzero coefficient other than the leading coefficient that is not Type 1.

Theorem 1.36. *Let q be a power of a prime p, $\mathbb{F}_q$ a finite field, l an odd prime, and let $f \in T(\mathbb{F}_q, l)$. Under GRH factoring f is deterministic polynomial time reducible to factoring a polynomial $g \in \mathbb{F}_q[X]$ st $\deg(g) \leq \deg(f)$ and g has fewer nonzero terms than f.*

2 Below this point needs to have definitions updated to the new ones.

In Theorem 3.5 the principle used in the Cantor Zassenhaus algorithm is generalized. The theorem is a useful tool for factoring polynomials deterministically under GRH. It is a fairly standard result. For example, it is implicit in the exposition of von zur Gathen [1987] in Bach and Shallit [1996] Theorem 7.8.8 [probably von zur Gathen [1987] as well]. We present it in slightly different terms to better motivate the main result of this section, Theorem 3.9. The Cantor Zassenhaus algorithm is given for reference in Algorithm 1. (The statement of the algorithm is essentially that of Bach and Shallit [1996].)

Whenever $\chi_2(\alpha)$ is equal to 1 on one component but not equal to 1 on all components then $\gcd(\chi_2(\alpha)-1, f) = 1$ gives a nontrivial factor of f. This approach to factorization should be contrasted with Berlekamp's 1967 algorithm. Berlekamp's algorithm splits $f \in S(\mathbb{F}_p)$ (factoring any polynomial in $S(\mathbb{F}_q)$ reduces to factoring a polynomial in $S(\mathbb{F}_p)$) by constructing a single $\alpha \in B(f, \mathbb{F}_p)$ and then trying $x = 1, 2, \cdots \in \mathbb{F}_p$ until x and α are equal on at least one component but not every component.

Definition 21. *Let $x \in Fq^*$ and l a prime dividing $q-1$ then $\text{ord}_l x = l v_l(\text{ord}(x))$.*

Note that $\text{ord}_p(x)$ is often defined as the multiplicative order of x in $\mathbb{F}_p$ or as the largest power of a prime p dividing an integer x, whereas here these concepts are both being used together in a single definition. The gcd of $\text{Ind}(x)$ and $q-1$ is independent of the choice of generator used to compute $\text{Ind}(x)$. $\text{ord}(x)$ and $\text{Ind}(x)$ are related by

$$\text{ord}(x) = \text{lcm}(q-1, \text{Ind}(x))$$

Theorem 2.1. *Let q be a prime power, $\mathbb{F}_q$ be a finite field, l a prime dividing $q-1$, $f \in \mathbb{F}_q[X]$ be a squarefree polynomial with k irreducible factors and degree n, $\alpha \in B(f, \mathbb{F}_q)$ then*
(1) $\mathrm{Ind}(N(\alpha)) = \sum_{j=1}^{k} \mathrm{Ind}(\alpha_j)$
(2) $\mathrm{ord}_l(N(\alpha)) \leq \max\{\mathrm{ord}_l(\alpha_j) : j = 1, \ldots, k\}$
(3) $\chi_l(N(\alpha)) = \sum_{j=1}^{k} \chi_l(\alpha_j)$

Proof. 1) follows from the linearity property of Ind 2) from Theorem 3.4 [fix], 3) from the multiplicativity of χ_d for any positive integer d. □

The value of Theorem 3.8 is that the order of the norm constrains the possible orders of the elements. For example, in the contex of the Cantor Zassehaus algorithm this relation allows us to give conditions on f, q and α st $\gcd(\chi_2(\alpha) - 1)$ is guaranteed to be a nontrivial factor of f in $\mathbb{F}_q$. Suppose the number of irreducible factors of f is even, $2 \mid q-1$, and a nonconstant $\alpha \in B(f, \mathbb{F}_q)$ is chosen st the product of the components of $\chi_2(\alpha)$ is -1. Then by Theorem 3.8 (3) not every component of α can be 1 or -1 and so $\gcd(\chi_2(\alpha) - 1, f)$ gives a nontrivial factor of f. Equivalently this can be stated terms of indexs. If $\mathrm{Ind}(N(\alpha)) \equiv 1 \bmod 2$ then by Theorem 3.8 (1) not every component of $\mathrm{Ind}(\alpha)$ can be 1. The next theorem generalizes this idea.

Theorem 2.2. *Let f be a squarefree polynomial with k irreducible factors, and l a prime st $l \mid k$ and $l \mid q-1$. If $v_l(\mathrm{Ind}(N(\alpha))) < v_l(k)$ then $\sigma_l(\mathrm{Ind}(\alpha)) > 0$:*

Proof. $\sigma_l(\mathrm{Ind}(\alpha)) > 0$ is equivalent to the statement that $\mathrm{Ind}(\alpha) \neq a(1, \ldots, 1)$ for all $a \in \mathbb{Z}/l^s\mathbb{Z}$. □

[Draft note: Let $s = v_l(q-1)$ then $\mathrm{Ind}(N(\alpha)) = l^j$ for $j < v_l(n)$ is equivalent to $\mathrm{ord}_l(N(\alpha)) = l^j$ for $j > \max\{f, s - v_l(k)\}$]

We give an example of Theorem 3.9. Let $f(X) = \Phi_4(X) = X4 + 1$, the minimal polynomial of the primitive 8th roots of unity, and $p = 17$. $p \equiv 1 \bmod 8$ so $f \in S(p)$. Let $\alpha = 1 - X$ then $N(\alpha) = 2$ (by Theorem 3.7) which is easily checked to have order 8 and so $v_2(\mathrm{Ind}(\alpha)) = 1$. This is less than $v_2(\deg f) = v_2(4) = 2$ so Theorem 3.9 states that $\sigma_2(Ind(\alpha)) > 0$. We now provide details for checking this statement. The roots of f are (2, 8, 9, 15). The corresponding components of α are (16, 10, 9, 3). We compute $\mathrm{Ind}(\alpha) = (8, 3, 2, 1)$ wrt the primitive root 3. $\mathrm{Ind}(\alpha) = (0, 1, 0, 1) \bmod 2$ and from this it is easily checked that $\sigma_2(\mathrm{Ind}(\alpha)) > 0$.

The next theorem relates properties of the index of the roots of a polynomial that splits to the index of its constant term.

Corollary 2.3. *Let f be a squarefree polynomial in $\mathbb{F}_q[X]$ that splits with roots $r_1, \ldots, r_n$ and constant term $c0$, and l be a prime st $l \mid n$ and $l \mid q-1$. (a) If f is l-high then f can be factored in deterministic polynomial time. (b) If $\mathrm{Ind}(r_i) \equiv \mathrm{Ind}(r_j) \bmod l^k$ for all $1 \leq i, j \leq n$ then $\mathrm{Ind}(r_i) \equiv \mathrm{Ind}(c0)/l^{v_l(n)} \bmod l^k$*

Proof. Let f be a degree n polynomial in $\mathbb{F}_q[X]$ that splits linearly, $\alpha = -X$ an element of the algebra $R = \mathbb{F}_q[X]/(f)$. $N(\alpha) = c0$ by Theorem 3.7. Hence (a) follows from Theorem 3.9 and (b) from the linearity property of Ind. Algorithm 2 makes use Theorem 3.9 to factor f given a certain $\alpha \in B(f, \mathbb{F}_q)$.

□

Algorithm 2 makes use Theorem 3.9 to factor f given a certain $\alpha \in B(f, \mathbb{F}_q)$.

Algorithm 2: Algorithm 2: Deterministic Factorization

Input: $\mathbb{F}_q$ a finite field, f in $S(\mathbb{F}_q)$, a prime l st $l \mid \deg f$ and $l \mid q-1$, and α st $v_l(\mathrm{Ind}_{\mathbb{F}_q}(N(\alpha))) < v_l(n)$
Output: a nontrivial factor of f in $\mathbb{F}_q$ $\beta = \chi_{l^s}(\alpha)$;
while $\beta \notin \mathbb{F}_q$ **do**
    $\beta = \beta^l$;
end
$\tau = \chi_l^{s-k}(\alpha)$;
$\omega = \beta^{1/l}$;
while $0 \leq i < \deg f$ **do**
    if $\gcd(\tau - \omega^i, f) > 1$ **then**
        return $\gcd(\tau - \omega^i, f)$;
    end
end

Chapter 5 - Conclusion

To Do

References

Leonard Adleman, Kenneth Manders, and Gary Miller. On taking roots in finite fields. *18th Annual Symposium on Foundations of Computer Science*, pages 175–178, 1977.

Manuel Arora, Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial factoring and association schemes. *arXiv preprint arXiv:1205.5653*, 2012.

Eric Bach, Joachim Von Zur Gathen, and Hendrik W Lenstra Jr. Factoring polynomials over special finite fields. *Finite Fields and Their Applications*, 7(1):5–28, 2001.

Elwyn R. Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, (46):1853–1859, 1967.

Elwyn R Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111): 713–735, 1970.

David G Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, pages 587–592, 1981.

Sergei Alekseevich Evdokimov. Factoring a solvable polynomial over a finite field and generalized riemann hypothesis. *Zapiski Nauchnykh Seminarov POMI*, 176:104–117, 1989.

Ming-Deh A Huang. Generalized riemann hypothesis and factoring polynomials over finite fields. *Journal of Algorithms*, 12(3):464–481, 1991.

Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Schemes for deterministic polynomial factoring. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 191–198. ACM, 2009.

Gábor Ivanyos, Marek Karpinski, Lajos Rónyai, and Nitin Saxena. Trading grh for algebra: Algorithms for factoring polynomials and related structures. *Mathematics of Computation*, 81(277):493–531, 2012.

Tanja Lange and Arne Winterhof. Factoring polynomials over arbitrary finite fields. *Theoretical computer science*, 234(1):301–308, 2000.

Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

Lajos Rónyai. Factoring polynomials over finite fields. *Journal of Algorithms*, 9(3):391–400, 1988.

René Schoof. Elliptic curves over finite fields and the computation of square roots mod . *Mathematics of computation*, 44(170):483–494, 1985.

Daniel Shanks. Five number-theoretic algorithms. In *Proceedings of the second Manitoba conference on numerical mathematics*, volume 5170, 1972.

Victor Shoup. On the deterministic complexity of factoring polynomials over finite fields. *Information Processing Letters*, 33(5):261–267, 1990.

Victor Shoup. A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pages 14–21. ACM, 1991a.

Victor Shoup. Smoothness and factoring polynomials over finite fields. *Information processing letters*, 38(1): 39–42, 1991b.

Tsz-Wo Sze. On taking square roots without quadratic nonresidues over finite fields. *Mathematics of Computation*, 80(275):1797–1811, 2011.

A. Tonelli. Bemerkung uber die au osung quadratischer congruenzen. *Gottinger Nachrichten*, 32:344–46, 1891.

Joachim von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52(1):77–89, 1987.

Hans Zassenhaus. On hensel factorization, i. *Journal of Number Theory*, 1(3):291–311, 1969.