Electronic Colloquium on Computational Complexity, Report No. 8 (2005)

Recognizing permutation functions in polynomial time

Neeraj Kayal [*]

Indian Institute of Technology, Kanpur
and *National University of Singapore*

December 11, 2004

Abstract

Let $\mathbb{F}_q$ be a finite field and $f(x) \in \mathbb{F}_q(x)$ be a rational function over $\mathbb{F}_q$. The decision problem **PermFunction** consists of deciding whether $f(x)$ induces a permutation on the elements of $\mathbb{F}_q$. That is, we want to decide whether the corresponding map $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ defined by $a \mapsto f(a)$ is a bijective mapping or not. This problem was known to be in $\mathcal{ZPP}$ but not known to be in $\mathcal{P}$. We resolve the complexity of **PermFunction** by giving a deterministic polynomial-time algorithm for this problem.

1 Introduction

1.1 The general problem statement

Let q be a prime-power and $\mathbb{F}_q$ a finite field with q elements. $f(x) = g(x)/h(x) \in \mathbb{F}_q(x)$ is an arbitary rational function with $g(x)$, $h(x) \in \mathbb{F}_q[x]$ and gcd(g, h)=1. Then $f(x)$ induces a partial mapping $\mathbb{F}_q \mapsto \mathbb{F}_q$ via $a \mapsto f(a)$ for $a \in \mathbb{F}_q$. If $f(x)$ is total and bijective then $f(x)$ is called a permutation function over $\mathbb{F}_q$. In the special case that $h = 1$, so that $f(x) = g(x) \in \mathbb{F}_q[x]$, it is called a permutation polynomial over $\mathbb{F}_q$.

1.2 Previous work

Shparlinski [Shp92] has given a deterministic superpolynomial algorithm for this problem. Ma and Gathen [MG94] show that this problem is in $\mathcal{ZPP}$ and have

[*] Part of this work was done while the author was Princeton University, Princeton, NJ, USA in 2003-04. This research was partially supported by a fellowship from Infosys Technologies Limied, Bangalore.

ISSN 1433-8092

also devised a fast random polynomial time test for this problem [MG93] which requires almost linear number of operations over $\mathbb{F}_q$.

A survey of permutation functions and their potential applications in public-key cryptography along with further references can be found in the articles by Lidl and Mullen [LM88], [LM93] and Mullen [Mul93]. Being algebraic objects having the nice combinatorial property of inducing a permutation on the set of elements in $\mathbb{F}_q$, they have been well studied in mathematics. The aim of this research was to derive a necessary and sufficient criterion for a rational function to be able to induce a permutation on $\mathbb{F}_q$. MacCluer [Mac67] and then Williams [Wil68] obtained a sufficient condition for polynomials over finite fields. Davenport and Lewis [DL63], Bombieri and Davenport [BD66] and Hayes [Hay67] obtained a necessary condition as well for polynomials. The general version for rational functions over finite fields shown by Cohen [Coh70] and Ma and Gathen [MG94] can be summarized in the theorem given below. But first we introduce the concept of an absolutely irreducible polynomial.

Definition 1.1. A bivariate polynomial $h(x, y) \in \mathbb{F}[x, y]$ is said to be *absolutely irreducible* if it is irreducible over $\mathbb{F}$ and remains irreducible over the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$.

For example $(y^2 - x^3) \in \mathbb{F}_7[x, y]$ is absolutely irreducible whereas $(y^2 + x^2) \in \mathbb{F}_7[x, y]$ is irreducible over $\mathbb{F}_7$ but factors into $(y + \sqrt{-1}x)(y - \sqrt{-1}x)$ over the extension $\mathbb{F}_{7^2} = \mathbb{F}_7(\sqrt{-1})$ and hence is not absolutely irreducible over $\mathbb{F}_7$.

Theorem 1.2. *Let $f(x) = \frac{g(x)}{h(x)} \in \mathbb{F}_q(x)$ and $n = deg(g) + deg(h)$. Also let $q \geq 16n^4$. Then f is a permutation function if and only if f is total and $f^*(x, y) := \frac{g(x)h(y)-h(x)g(y)}{x-y}$ does not have any absolutely irreducible factors over $\mathbb{F}_q$.*

We extend this line of work to show that permutation functions can be recognized in polynomial time.

Theorem 1.3. *There exists a deterministic polynomial-time algorithm that given a rational function $f(x) = \frac{g(x)}{h(x)} \in \mathbb{F}_q(x)$ determines whether it is a permutation function in time $poly((deg(g) + deg(h)) \log q)$.*

In doing this, we build upon the work of Gao, Kaltofen and Lauder [GKL04] and come up with an extension of their algorithm for distinct degree factorization of multivariate polynomials over finite fields.

2 Reformulating our goal

By the degree of a bivariate polynomial $h(x, y) \in \mathbb{F}[x, y]$ we will mean the total degree of $h(x, y)$. Moreover $h(x, y)$ has a unique factorization over the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$. Now collect all the elements of $\bar{\mathbb{F}}$ that occur as the coefficient of some term $x^i y^j$ in some irreducible factor of $h(x, y)$ over $\bar{\mathbb{F}}$. Since this is a finite set, all these coefficients lie in some finite extension $\mathbb{K}$ of $\mathbb{F}$. We will call the smallest such extension field $\mathbb{K}$ the splitting field of $h(x, y)$. We will denote by $dim_{\mathbb{F}}(h(x, y))$ the dimension of the splitting field of $h(x, y)$ over $\mathbb{F}$.

We will call a polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ a *uniform polynomial* if all its irreducible factors over $\mathbb{F}_q$ have the same degree and the same splitting field $\mathbb{K}$.

Definition 2.1. Let $h(x, y) \in \mathbb{F}_q[x, y]$ with $h(x, y) = h_1(x, y)h_2(x, y) \cdots h_k(x, y)$ where the $h_i(x, y)$'s are irreducible polynomials over $\mathbb{F}_q$. We will say that $h(x, y)$ is *uniform* iff

$$dim_{\mathbb{F}_q}(h_i(x, y)) = dim_{\mathbb{F}_q}(h(x, y)) \ \ \forall\, 1 \leq i \leq k$$

and

$$deg(h_i(x, y)) = deg(h_j(x, y)) \ \ \forall\, 1 \leq i, j \leq k$$

We extend the distinct degree factorization algorithm of Gao, Kaltofen and Lauder [GKL04] to split a given polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ into a product of uniform polynomials.

Theorem 2.2. *[Uniform factoring] There exists a deterministic algorithm that on input a polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ outputs*

$$\langle (h_1(x, y), n_1, d_1), (h_2(x, y), n_2, d_2), \cdots (h_k(x, y), n_k, d_k) \rangle$$

such that

$$h(x, y) = h_1(x, y)h_2(x, y) \cdots h_k(x, y)$$

where each $h_i(x, y) \in \mathbb{F}_q[x, y]$ is a uniform polynomi-al consisting of irreducible (over $\mathbb{F}_q$) factors of degree n_i and $d_i = dim_{\mathbb{F}_q}(h_i(x, y))$.

Moreover the algorithm runs in time $poly(deg(h) \log q)$.

Note that the output of the algorithm of Theorem 2.2 is a refinement of the distinct degree factorization of $h(x, y)$ over $\mathbb{F}_q$. It also tells us about the irreducibility and the absolute irreducibility of $h(x, y)$ over $\mathbb{F}_q$.

It is easy to see how we can use the algorithm of Theorem 2.2 together with the criterion from Theorem 1.2 to get a deterministic polynomial time algorithm for recognizing a permutation function. If the size of the underlying field is small ($\leq 16n^4$), we can decide whether $f(x) = \frac{g(x)}{h(x)}$ is a permutation function by just simple enumeration. For large fields, Theorem 1.2 implies that testing the permutation property of a rational function is equivalent to testing whether the related difference polynomial has any absolutely irreducible factors or not. For such fields, we invoke our uniform factoring algorithm on the difference polynomial $f^*(x, y) := \frac{g(x)h(y) - h(x)g(y)}{x - y}$ and get back a list of uniform divisors of $f^*(x, y)$ and then check whether the dimension of the splitting field over $\mathbb{F}_q$ of any such uniform factor of $f^*(x, y)$ is 1 or not. Now $f^*(x, y)$ has no absolutely irreducible factor if and only if the dimension of each uniform divisor is greater than 1.

The discussion above shows that Theorem 2.2 implies Theorem 1.3. The rest of this article is devoted to a proof of Theorem 2.2.

3 Nice bivariate polynomials

Definition 3.1. A bivariate polynomial $f(x,y) \in \mathbb{F}_q[x,y]$ of total degree n is *nice* if $f(x,0)$ is squarefree and of degree n.

Note that the coefficient of x^i of a nice polynomial $f(x,y)$ as a polynomial in y has degree no more than $n-i$, in particular the leading coefficient of $f(x,y)$ with respect to x is in $\mathbb{F}_q$.

Also observe that a nice polynomial $f(x,y) \in \mathbb{F}_q[x,y]$ remains nice over any extension field $\mathbb{K}$ of $\mathbb{F}_q$ and that any factor of a nice polynomial is also a nice polynomial. We will see that the problem of general bivariate factoring can be reduced to factoring a nice bivariate polynomial.

Let $\mathbb{K}$ be a field extension of the finite field $\mathbb{F}_q$. Let $\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}$ be an automorphism of $\mathbb{K}$. We extend ϕ to $\mathbb{K}[x,y]$ as follows

Definition 3.2. Let $\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}$ be an automorphism of $\mathbb{K}$. Define the map $\phi : \mathbb{K}[x,y] \mapsto \mathbb{K}[x,y]$ as

$$\phi(f(x,y)) = \sum_{1 \le k,l \le n} \phi(a_{kl}) x^k y^l$$

where

$$f(x,y) = \sum_{1 \le k,l \le n} a_{kl} x^k y^l$$

Observe that the map $\phi : \mathbb{K}[x,y] \mapsto \mathbb{K}[x,y]$ is an automorphism of the ring $\mathbb{K}[x,y]$ that fixes the subring $\mathbb{F}_q[x,y]$. In particular,

- $\phi(f(x,y) + g(x,y)) = \phi(f(x,y)) + \phi(g(x,y))$
- $\phi(f(x,y)g(x,y)) = \phi(f(x,y))\phi(g(x,y))$

We now define an equivalence relation on $\mathbb{K}[x,y]$ induced by such automorphisms of $\mathbb{K}[x,y]$.

Definition 3.3. Let $f(x,y) \in \mathbb{K}[x,y]$ be any bivariate polynomial. Then $\phi(f(x,y))$ for any $\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}$ is said to be a *conjugate* of $f(x,y)$ over $\mathbb{F}_q$. When the underlying field $\mathbb{F}_q$ is clear from context, we will simply say that $\phi(f(x,y))$ is a conjugate of $f(x,y)$.

Observe that conjugacy is an equivalence relation on $\mathbb{K}[x,y]$.

Now consider a nice polynomial $h(x,y) \in \mathbb{F}_q[x,y]$ that is irreducible over $\mathbb{F}_q$. Let $\mathbb{K} \supseteq \mathbb{F}_q$ be a finite field extension of $\mathbb{F}_q[x,y]$. How does $h(x,y)$ factor over $\mathbb{K}$? We claim that all the irreducible factors of $h(x,y)$ in $\mathbb{K}$ are in fact conjugates of each other. In particular, all the factors of $h(x,y)$ in $\mathbb{K}[x,y]$ that are irreducible over $\mathbb{K}$ are of equal degree.

Claim 3.3.1. *Let $h(x,y) \in \mathbb{F}_q[x,y]$ be a nice irreducible polynomial of total degree n. Let $\mathbb{K}$ be any finite field extension of $\mathbb{F}_q$. If $f_1(x,y) \in \mathbb{K}[x,y]$ and $f_2(x,y) \in \mathbb{K}[x,y]$ are any two factors of $h(x,y)$ that are irreducible over the extension field $\mathbb{K}$, then $f_1(x,y)$ and $f_2(x,y)$ are conjugates over the base field $\mathbb{F}_q$.*

Proof. For a polynomial $f(x,y) \in \mathbb{K}[x,y]$, define $H_f \leq Gal_{\mathbb{K}/\mathbb{F}_q}$ to be the subgroup of $Gal_{\mathbb{K}/\mathbb{F}_q}$ consisting of automorphisms in $Gal_{\mathbb{K}/\mathbb{F}_q}$ that fix $f(x,y)$. Since the galois groups of finite extensions of finite fields are cyclic groups, H_f must be a normal subgroup of $Gal_{\mathbb{K}/\mathbb{F}_q}$.

Let $f(x,y) \in \mathbb{K}[x,y]$ be a factor of $h(x,y)$ which is irreducible over $\mathbb{K}$. Let the set of distinct cosets of H_f in $Gal_{\mathbb{K}/\mathbb{F}_q}$ be

$$Gal_{\mathbb{K}/\mathbb{F}_q}/H_f = \{H_f\phi_1, H_f\phi_2, \cdots, H_f\phi_t\}$$

Then $\phi_1(f(x,y)), \phi_2(f(x,y)), \cdots \phi_t(f(x,y))$ are all the distinct conjugates of $f(x,y)$. We claim that the unique factorization of $h(x,y)$ into irreducible polynomials over $\mathbb{K}$ is simply the product of all these distinct conjugates of $f(x,y)$. That is,

$$h(x,y) = \prod_{H_f\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}/H_f} \phi(f(x,y)) \tag{1}$$

Let ϕ be any automorphism in $Gal_{\mathbb{K}/\mathbb{F}_q}$. Now

$$f(x,y)|h(x,y) \Rightarrow \exists g(x,y) \in \mathbb{K}[x,y] \text{ such that } h(x,y) = f(x,y)g(x,y)$$

$$\text{Applying } \phi \text{ to both sides, } \phi(h(x,y)) = \phi(f(x,y))\phi(g(x,y))$$
$$\text{or, } h(x,y) = \phi(f(x,y))\phi(g(x,y))$$
$$\Rightarrow \phi(f(x,y))|h(x,y)$$

By the same reasoning $\phi(f(x,y)) \in \mathbb{K}[x,y]$ is irreducible over $\mathbb{K}$ for if any $g(x,y) \in \mathbb{K}[x,y]$, $deg(g(x,y)) < deg(\phi(f(x,y)) = deg(f(x,y))$ divides $\phi(f(x,y))$ then $\phi^{-1}(g(x,y))$ divides $f(x,y)$, contradicting the irreducibility of $f(x,y)$ over $\mathbb{K}$. Thus any conjugate of $f(x,y)$ is also an irreducible factor of $h(x,y)$. Moreover, $f(x,y)$ being irreducible over $\mathbb{K}$, is coprime to all conjugates distinct from itself. Thus the rhs of equation (1) divides $h(x,y)$. Moreover the rhs of equation (1) is fixed by all the automorphisms in $Gal_{\mathbb{K}/\mathbb{F}_q}$. Since finite extensions of finite fields are normal extensions, so any polynomial in $\mathbb{K}[x,y]$ that is fixed by all the automorphisms in $Gal_{\mathbb{K}/\mathbb{F}_q}$ is in fact a polynomial in $\mathbb{F}_q[x,y]$. Hence the rhs of equation (1) is in fact a polynomial in $\mathbb{F}_q[x,y]$ that divides $h(x,y)$. By the irreducibility of $h(x,y)$ over $\mathbb{F}_q$, we deduce that equation (1) is indeed the unique factorization of $h(x,y)$. Thus all the irreducible factors of $h(x,y)$ over $\mathbb{K}$ are precisely all the distinct conjugates of $f(x,y)$.

□

Now consider an irreducible polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ that factors in the algebraic closure of $\mathbb{F}_q$. What is the splitting field of $h(x, y)$? Can we put a bound on the dimension of the splitting field over $\mathbb{F}_q$? Assuming that $h(x, y)$ is a nice polynomial, the following proposition shows that if $t(x)$ is an irreducible factor of $h(x, 0)$, then the splitting field of $h(x, y)$ is a subfield of the finite field $\mathbb{F}_q[z]/\langle t(z)\rangle$. In particular, if $h(x, 0)$ has a root $\alpha \in \mathbb{F}_q$, then $h(x, y)$ must be absolutely irreducible.

Proposition 3.4. *Let $h(x, y) \in \mathbb{F}_q[x, y]$ be a nice irreducible polynomial of total degree n. Let $dim_{\mathbb{F}_q}(h(x, y)) = d$. Also let $t(z) \in \mathbb{F}_q[z]$ be an irreducible factor of $h(z, 0)$. Then $d|deg(t(z))$ and $h(x, y)$ breaks into absolutely irreducible factors over $\mathbb{K} := \mathbb{F}_q[z]/\langle t(z)\rangle$, each irreducible factor over $\mathbb{K}$ being of degree $m = \frac{n}{d}$.*

Proof. Let $f(x, y) \in \mathbb{K}[x, y]$ be an irreducible factor of $h(x, y)$ in $\mathbb{K}[x, y]$. Suppose if possible that $f(x, y)$ is not absolutely irreducible but breaks further over some finite extension $\mathbb{L} \supset \mathbb{K}$.

Let H_f be as in claim 3.3.1. By Claim 3.3.1

$$h(x, y) = \prod_{H_f\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}/H_f} \phi(f(x, y)) \tag{2}$$

Let $\alpha \in \mathbb{K}$ be a root of the polynomial $t(z)$. Now

$$(x - \alpha) \mid (h(x, 0) = \prod_{H_f\phi \in Gal_{\mathbb{K}/\mathbb{F}_q}/H_f} \phi(f(x, 0)))$$

$$\Rightarrow \exists \phi \in Gal_{\mathbb{K}/\mathbb{F}_q} \text{ such that } (x - \alpha)|\phi(f(x, 0))$$

$$\Rightarrow (x - \beta)|f(x, 0) \text{ where } \beta = \phi^{-1}(\alpha)$$

Note that $\beta = \phi^{-1}(\alpha) \in \mathbb{K}$ is also a root of the polynomial $t(z)$.

By Claim 3.3.1 the irreducible factors of $f(x, y)$ over $\mathbb{L}$ are all conjugates. Let $f_1(x, y)$ be an irreducible factor of $f(x, y)$ over $\mathbb{L}$ such that $(x - \beta)$ divides $f_1(x, 0)$. Let $\psi \in Gal_{\mathbb{L}/\mathbb{K}}$ be such that $\psi(f_1(x, y))$ is another irreducible (over $\mathbb{L}$) factor of $f(x, y)$ distinct from $f_1(x, y)$. Now since $(x - \beta)|f_1(x, 0)$, we must also have $(x - \psi(\beta)) = (x - \beta)|\psi(f_1(x, 0))$. This implies that $(x - \beta)^2$ divides $f(x, 0)$ which is a contradiction since $h(x, 0)$ and hence $f(x, 0)$ are squarefree.

Thus the irreducible factors of $h(x, y)$ over $\mathbb{K}$ are absolutely irreducible. Hence there exists a subfield $\mathbb{F} \subseteq \mathbb{K}$ which is the splitting field of $h(x, y)$. Therefore $d = [\mathbb{F} : \mathbb{F}_q]$ divides $deg(t(z)) = [\mathbb{K} : \mathbb{F}_q] = [\mathbb{K} : \mathbb{F}][\mathbb{F} : \mathbb{F}_q]$.

By the definition of the splitting field of $h(x, y)$, the coefficients occuring in $f(x, y)$ lie in the field $\mathbb{F}$ and do not all lie in some proper subfield of $\mathbb{F}$. Hence $\mathbb{F}$ is precisely the subfield of $\mathbb{K}$ which is fixed by every automorphism in H_f. So

$$d = [\mathbb{F} : \mathbb{F}_q] = ord(Gal_{\mathbb{K}/\mathbb{F}_q}/H_f)$$

Further $ord(Gal_{\mathbb{K}/\mathbb{F}_q}/H_f)$ is the number of distinct absolutely irreducible factors of $h(x,y)$. Since all the irreducible factors of $h(x,y)$ are of the same degree, say m, we have

$$m.ord(Gal_{\mathbb{K}/\mathbb{F}_q}/H_f) = deg(h(x,y))$$

$$\Rightarrow \ m.d = n$$

$$\Rightarrow \ m = \frac{n}{d}$$

□

In summary, if $h(x,y) \in \mathbb{F}_q[x,y]$ is a nice polynomial that is irreducible over $\mathbb{F}_q$ and $t_1(z), t_2(z) \in \mathbb{F}_q[z]$ are any two factors of $h(z,0)$ that are irreducible over $\mathbb{F}_q$, then the degree of an irreducible factor of $h(x,y)$ over $\mathbb{K}_1 := \mathbb{F}_q[z]/\langle t_1(z)\rangle$ is the same as the degree of an irreducible factor of $h(x,y)$ over $\mathbb{K}_2 := \mathbb{F}_q[z]/\langle t_2(z)\rangle$. This observation will be the key to our uniform-factoring algorithm.

4 Lifting roots of $h(x,0)$ to factors of $h(x,y)$.

Let $h(x,y) \in \mathbb{F}_q[x,y]$ be a nice bivariate polynomial that we wish to factor. Let $\alpha_0 \in \mathbb{F}_q$ be a root of $h(x,0)$. Then there exists a unique (upto scalar multiples) irreducible (over $\mathbb{F}_q$) factor $h_0(x,y)$ of $h(x,y)$ such that α_0 is a root of $h_0(x,0)$. The following proposition shows how to construct a linear system over $\mathbb{F}_q$ whose solutions correspond to multiples of $h_0(x,y)$.

Proposition 4.1. *Let $h(x,y) \in \mathbb{K}[x,y]$ be a nice polynomial of degree n. Moreover $\alpha_0 \in \mathbb{K}$ is a root of the squarefree univariate polynomial $h(x,0)$. Let $k = 2n(n-1)$ and $m \leq n$ be an integer. Then there exists a unique $\alpha(y) = \alpha_0 + \alpha_1 y + \cdots \alpha_k y^k$ such that*

$$h(\alpha(y), y) = 0 \ \ (mod\ y^{k+1})$$

Let $h_0(x,y)$ be the unique irreducible factor of $h(x,y)$ such that $h_0(\alpha_0, 0) = 0$. Then the linear system

$$\sum_{i=0}^{m} u_i(y)\alpha(y)^i = 0 \ \ (mod\ y^{k+1}) \tag{3}$$

with unknowns

$$u_i(y) \in \mathbb{K}[y], deg(u_i(y)) \leq (m-i)$$

has a non-zero solution if and only if $deg(h_0(x,y)) \leq m$

Proof. The uniqueness of $\alpha(y)$ follows from the squarefreenes of $h(x,0)$ and the well-known Hensel Lifting lemma. Moreover since $h_0(\alpha_0, y) = 0$, by hensel lifting again there exists a unique $\bar{\alpha}(y) = \alpha_0 + \bar{\alpha_1} y + \cdots + \bar{\alpha_k} y^k$ such that $h_0(\bar{\alpha(y)}, y) = 0$.

If $h_i(x,y) \in \mathbb{K}[x,y], i \geq 1$ is any irreducible factor of $h(x,y)$ over $\mathbb{K}$, then since $h_i(\alpha_0, 0) \in \mathbb{K}^*$, therefore $h_i(\alpha(y), y)$ is a unit of the ring $\mathbb{K}[y]/\langle y^{k+1}\rangle$. Since $h(\alpha(y), y) = 0$ in this ring, we must have $h_0(\alpha(y), y) = 0 \pmod{y^{k+1}}$. Now sqauerfreeness of $h(x,0)$ implies squarefreeness of $h_0(x,0)$ and hence by uniqueness of Hensel lifting, we have $\alpha(y) = \bar{\alpha(y)}$.

Let $h_0(x,y) = v_0(y) + v_1(y)x + \cdots v_l(y)x^l$. Now if $l \leq m$ then

$$(v_0(y), v_1(y), \cdots, v_l(y), 0, \cdots, 0)$$

is clearly a non-zero solution of the linear system defined by equation (3).

Conversely suppose that the system 3 has a nontrivial solution. Let

$$g(x,y) := \sum_{i=0}^{m} u_i(y)x^i \in \mathbb{K}[x,y]$$

Let

$$\rho(y) := \mathit{Resultant}_x(h_0(x,y), g(x,y)) \in \mathbb{K}[y]$$

Then $deg(\rho(y)) \leq (2n-1)n = k$.

Then there exist polynomials $a(x,y), b(x,y) \in \mathbb{K}[x,y]$ such that

$$\rho(y) = a(x,y)h_0(x,y) + b(x,y)g(x,y) \tag{4}$$

Now substituting $x := \alpha(y)$ in equation (4), we have

$$\rho(y) = 0 \pmod{y^{k+1}}$$

But $deg(\rho(y)) \leq k$ and hence we must have that $\rho(y)$ is identically zero. Thus $gcd_x(h_0(x,y), g(x,y))$ is nontrivial and whence by the irreducibility of $h_0(x,y)$ we deduce that $g(x,y)$ is a multiple of $h_0(x,y)$ and the degree of $h_0(x,y)$ must be less than or equal to m.

□

5 Linear systems over a ring

Let $w(z) \in \mathbb{F}_q[z]$ be a squarefree polynomial of degree n with irreducible factors $w_j(z) \in \mathbb{F}_q[z], 1 \leq j \leq r$. We consider homogeneous linear systems over the ring

$$R_w := \mathbb{F}_q[z]/\langle w(z)\rangle \cong \oplus_{j=1}^{r} \mathbb{F}_q[z]/\langle w_j(z)\rangle$$

We will denote by π_{w_j} the projection of R_w onto the jth component. Thus for $u(z) \in R_w$,

$$\pi_{w_j}(u(z)) := u(z) \pmod{w_j(z)}$$

Let $\mathcal{L}$ be a linear system over R_w given by

$$Lv = 0$$

where L is a matrix with entries in R_w and v is a vector of unknowns.

Proposition 5.1. *Let $\mathcal{L}$ be any linear system over R_w. Let $S \subseteq \{1, 2, \cdots r\}$ with the following properties: The dimension over $\mathbb{F}_q$ of the solution space of the projected system $\mathcal{L}_{w_j}$ is non-zero if and only if $j \in S$. Then the gcd of all the entries of all the basis elements of the solution space of $\mathcal{L}$, thought of as polynomials in $\mathbb{F}_q[z]$ is exactly $(\prod_{j \notin S} w_j(z))$.*

Proof. See [GKL04]. □

6 The Algorithm and its proof of correctness.

We will use the preprocessing step described in [GKL04] to reduce the general uniform factoring problem to factoring nice bivariate polynomials. Henceforth, will assume that the input to our algorithm is a nice bivariate polynomial.

We can also use the distinct degree factoring algorithm of [GKL04] to obtain factors $h^{[1]}(x, y), h^{[2]}(x, y), \cdots h^{[n]}(x, y)$ of a given polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ such that

$$h(x, y) = \prod_{1 \leq i \leq n} h^{[i]}(x, y)$$

and $h^{[i]}(x, y)$ has the property that every factor of $h^{[i]}(x, y)$ that is irreducible over $\mathbb{F}_q$ has degree i. We now iteratively factor each $h^{[i]}(x, y)$ into a product of uniform polynomials.

So now we can assume that the input to our algorithm is a nice bivariate polynomial $h(x, y)$ and an integer n, such that each irreducible factor of $h(x, y)$ has the same degree n. Let

$$1 = d_0 \leq d_1 \leq d_2 \leq \cdots \leq d_{m-1} \leq d_m = n$$

be the sequence of divisors of n. Let $h^{[d_i]}(x, y)$ be the product of those irreducible factors of $h(x, y)$ that have dimension d_i. Using the subroutine described below, our algorithm first extracts $h^{[d_m]}(x, y)$ then invokes the subroutine on $\frac{h(x,y)}{h^{[d_m]}(x,y)}$ to obtain $h^{[d_{m-1}]}(x, y)$ and then invokes the subroutine again on $\frac{h(x,y)}{h^{[d_m]}(x,y)h^{[d_{m-1}]}(x,y)}$ to obtain $h^{[d_{m-2}]}(x, y)$ and so on until we obtain the complete the uniform factorization of $h(x, y)$.

So now our problem boils down to the following problem: given a nice bivariate polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ and positive integers n and d such that each factor of $h(x, y)$ that is irreducible over $\mathbb{F}_q$ has degree n and dimension at most d, compute in deterministic polynomial time $h^{[d]}(x, y)$, $h^{[d]}(x, y)$ being the product of those irreducible (over $\mathbb{F}_q$) factors of $h(x, y)$ that have dimension d over $\mathbb{F}_q$.

6.1 Outline of the algorithm

The key idea behind our algorithm is to work over the ring $R := \mathbb{F}_q[z]/\langle h(z,0)\rangle$. Now $\alpha_0 = z \in R$ is a root of the polynomial $h(x,0) \in R[x]$. We pretend that R is a field and proceed as in Proposition 4.1, thereby constructing a linear system over R whose solutions correspond to factors of $h(x,y)$ of degree $m = \frac{n}{d}$ in the algebraic closure $\mathbb{A}$ of $\mathbb{F}_q$. Unfortunately, we cannot recover these individual factors without knowing a complete *factorization* of the ring R. But all is not lost. By the discussion above, we can assume that every factor of $h(x,y)$ that is irreducible over $\mathbb{F}_q$ has dimension at most d and hence $h(x,y)$ has no factor of degree less than m over $\mathbb{A}$. Now think of $h(x,y)$ as a polynomial in $\mathbb{A}[x,y]$. Then $h^{[d]}(x,y)$ is the product of irreducible factors of degree m of $h(x,y)$ in $\mathbb{A}[x,y]$, irreduciblity being over the algebraic closure $\mathbb{A}$. By Proposition 5.1, we can recover $h^{[d]}(x,0) \in \mathbb{F}_q[x]$ using the solutions to the linear system that we had devised. Finally, knowing $h^{[d]}(x,0) \in \mathbb{F}_q[x]$, we recover $h^{[d]}(x,y)$ by using the well-known algorithm that reduces bivariate factoring to univariate factoring over a field.

6.2 Algorithm description

Algorithm. (Deterministic distinct dimension factoring) .

Input. A finite field $\mathbb{F}_q$, a nice polynomial $h(x,y) \in \mathbb{F}_q$. An integer $n \geq 1$ such that all the irreducible factors of $h(x,y)$ over $\mathbb{F}_q$ have degree n. An integer $d|n$ such that the dimension of all irreducible factors of $h(x,y)$ over $\mathbb{F}_q$ is less than or equal to d.

Output. $g(x,y) \in \mathbb{F}_q[x,y]$ such that $g(x,y)$ is the product of all irreducible factors of $h(x,y)$ which have dimension d, *if such a* $g(x,y)$ *exists.*

Step 1. (Approximate a root of $h(x,y)$) Let $k := (2n-1)n$. $w(z) := h(z,0)$. $m := \frac{n}{d}$. $R_w := \mathbb{F}_q[z]/\langle w(z)\rangle$ and $a_0 := z \in R_w$. By Newton iteration compute $a_1, a_2, \cdots, a_k \in R_w$ such that

$$f(a_0 + a_1 y + a_2 y^2 + \cdots + a_k y^k, y) \equiv 0 \pmod{y^{k+1}}$$

Let

$$\alpha := a_0 + a_1 y + a_2 y^2 + \cdots + a_k y^k \in R_w[y]/\langle y^{k+1}\rangle$$

For $1 \leq i \leq m$, compute

$$\alpha^i := (a_0 + a_1 y + \cdots + a_k y^k)^i \pmod{y^{k+1}}$$

Step 2. (Try to find a polynomial of degree $\leq m$ one of whose approximate roots is α.) Compute a basis over $\mathbb{F}_q$ of solutions over R_w of the homogeneous linear system $\mathcal{L}$ over R_w given by,

$$\sum_{i=0}^{m} u_i(y)\alpha^i \equiv 0 \pmod{y^{k+1}} \tag{5}$$

where $u_i(y) \in R_w[y]$, $deg_y(u_i) \leq (m-i)$ are the unknowns. If the dimension is zero then output "No such $g(x,y)$ exists and halt.

Step 3. Compute the gcd of $w(z)$ and the entries of all basis elements of the solution space of $\mathcal{L}$ thought of as polynomials in $\mathbb{F}_q[z]$. This gives a factor, $l_0(z)$ of $w(z) = h(z,0)$. Let $g_0(z) := \frac{w(z)}{l_0(z)}$.

Using Hensel lifting compute a factorization $h(x,y) = g(x,y).l(x,y)$ with $g(x,0) = g_0(x)$ and $l(x,0) = l_0(x)$. Output $g(x,y)$.

6.3 Proof of correctness

For each irreducible factor $t(z)$ of $w(z) = h(z,0)$, the linear system in equation (5) is the projection $\mathcal{L}_t$ of the linear system $\mathcal{L}$ defined by equation (5) under the projection map π_t. Moreover, by the squarefreeness of $h(z,0)$ there exists a **unique** irreducible (over $\mathbb{F}_q$) factor $h_t(x,y)$ of $h(x,y)$ such that $t(z)$ divides $h_t(z,0)$. Let $\mathbb{K}_t$ be the field defined as

$$\mathbb{K}_t := \mathbb{F}_q[z]/\langle t(z)\rangle$$

Moreover z is a root of $h(z,0)$ in the field $\mathbb{K}_t$. Thus we can apply Proposition 4.1 and deduce that the linear system $\mathcal{L}_t$ has a solution over $\mathbb{K}_t$ if and only if $h(x,y)$ has an irreducible factor of degree $\leq m$ over $\mathbb{K}_t$.

Thus $\mathcal{L}_t$ has a solution iff $h_t(x,y)$ has a factor of degree $\leq m$ over $\mathbb{K}_t$. By the corollary to Proposition 3.4 this happens exactly when $dim_{\mathbb{F}_q}(h_t(x,y)) \geq d$. By the input assumption on $h(x,y)$, $h_t(x,y)$ must have dimension exactly d.

Thus we are in the situation of Proposition 5.1 with $w(z) = h(z,0)$. Let $t_1(z), t_2(z) \cdots t_r(z)$ be all the irreducible factors of $w(z)$ over $\mathbb{F}_q$. Also let $h^{[d]}(x,y)$ be the product of all irreducible factors of $h(x,y)$ of dimension d. By Proposition 5.1 we can compute in deterministic polynomial time the factor $g_0(z) = (\prod_{j\in S} t_j(z))$ where S is the set of all indices j such that the polynomial $t_j(z)$ divides $h^{[d]}(z,0)$. Hence using Hensel lifting we may recover this factor $h^{[d]}(x,y)$ in deterministic polynomial time.

Acknowledgement

We thank Manindra Agrawal and Nitin Saxena for many helpful discussions and comments on this work.

References

[BD66] Enrico Bombieri and H. Davenport. *On two problems of Mordell.* Amer. J. Math. 88, 1966. pages 61-70.

[Coh70] S. D. Cohen. *The distribution of polynomials over finite fields.* Acta Arith. 17, 1970. pages 255-271.

[DL63] H. Davenport and D. J. Lewis. *Notes on congruences (I).* Quart. J. Math. Oxford. 14, 1963. pages 51-60.

[Hay67] D. R. Hayes. *A geometric approach to permutation polynomials over a finite field.* Duke Math. J. 34, 1967. pages 293-305.

[GKL04] Shuhong Gao, Erich Kaltofen and Alan Lauder. *Deterministic distinc-degree factorization of polnomials over finite fields.* Journal of Symbolic Computing, Volume 38, Number 6, 2004. pages 1461-70.

[Kal85] E. Kaltofen. *Fast parallel absolute irreducibility testing.* Journal of Symbolic Computing, Volume 1, pages 57-67.

[Kal87] E. Kaltofen. *Deterministic irreducibility testing of polynomials over large finite fields.* Journal of Symbolic Computing, Volume 4, pages 77-82.

[LM88] R. Lidl and G. L. Mullen. *When does a polynomial over a finite field permute the elements of the field?* American Mathematical Monthly 95, 1988. pages 243-246.

[LM93] R. Lidl and G. L. Mullen. *When does a polynomial over a finite field permute the elements of the field?, II* American Mathematical Monthly 100, 1993. pages 71-74.

[Mac67] C. R. MacCluer. *On a conjecture of Davenport and Lewis concerning exceptional polynomials.* Acta Arith. 12, 1967. pages 289-299.

[MG94] Keju Ma and Joachim Von Zur Gathen. *The computational complexity of recognizing permutation functions.* Computational Complexity, Volume 5, Number 1, 1995. pages 76-97.

[MG93] Keju Ma and Joachim Von Zur Gathen. *Tests for permutation functions.* Finite Fields and their applications, Volume 1, Number 1, 1995. pages 31-

[Mul93] G. L. Mullen. *Permutation polynomials.* Proc. Conf. Finite fields and their Applications, vol. 141 of Lecture Notes in Pure and Applied Mathematics. Marcel Dekker, 1993. pages 131-151.

[Shp92] I. E. Shparlinski. *A deterministic test for permutation polynomials.* Computational Complexity 2, 1992. pages 129-132.

[Wil68] K. S. Williams. *On exceptional polynomials.* Canad. Math. Bull. 11, 1968. pages 279-282.