8-2009

Factoring Polynomials and Groebner Bases

Genhua (yinhua) Guan
Clemson University, gguan@clemson.edu

FACTORING POLYNOMIALS AND GRÖBNER BASES

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematics

---

by
Yinhua Guan
August 2009

Accepted by:
Dr. Shuhong Gao, Committee Chair
Dr. Hiren Maharaj
Dr. Gretchel L Matthews
Dr. Elena S Dimitriova

Abstract

Factoring polynomials is a central problem in computational algebra and number theory and is a basic routine in most computer algebra systems (e.g. Maple, Mathematica, Magma, etc). It has been extensively studied in the last few decades by many mathematicians and computer scientists. The main approaches include Berlekamp's method (1967) based on the kernel of Frobenius map, Niederreiter's method (1993) via an ordinary differential equation, Zassenhaus's modular approach (1969), Lenstra, Lenstra and Lovasz's lattice reduction (1982), and Gao's method via a partial differential equation (2003). These methods and their recent improvements due to van Hoeij (2002) and Lecerf et al (2006–2007) provide efficient algorithms that are widely used in practice today.

This thesis studies two issues on polynomial factorization. One is to improve the efficiency of modular approach for factoring bivariate polynomials over finite fields. The usual modular approach first solves a modular linear equation (from Berlekamp's equation or Niederreiter's differential equation), then performs Hensel lifting of modular factors, and finally finds right combinations. An alternative method is presented in this thesis that performs Hensel lifting at the linear algebra stage instead of lifting modular factors. In this way, there is no need to find the right combinations of modular factors, and it finds instead the right linear space from which the irreducible factors can be computed via gcd. The main advantage of this method is that extra solutions can be eliminated at the early stage of computation, so improving on previous Hensel lifting methods.

Another issue is about whether random numbers are essential in designing efficient algorithms for factoring polynomials. Although polynomials can be quickly factored by randomized polynomial time algorithms in practice, it is still an open problem whether there exists any deterministic polynomial time algorithm, even if generalized Riemann hypothesis (GRH) is assumed. The deterministic complexity of factoring polynomials is studied here from a different point of view that is more geometric and combinatorial in nature. Tools used include Gröbner basis structure theory and graphs, with connections to combinatorial designs. It is shown how to compute deterministically new Gröbner bases from given Göbner bases when new polynomials are added, with running time polynomial in the degree of the original ideals. Also, a new upper bound is given on the number of ring extensions needed for finding proper factors, improving on previous results of Evdokimov (1994) and Ivanyos, Karpinski and Saxena (2008).

Dedication

This work is dedicated to my family.

Acknowledgments

I am truly grateful for all the instruction, encouragement, infinite patience and inspiring ideas from my advisor Professor Shuhong Gao during my studies as a Ph.D candidate in Clemson University. It has been a great pleasure to discuss problems with him who is very knowledgeable, very friendly, working hard and with sense of humor. I also want to thank the financial support that I have received from the National Science Foundation and from mathematical department.

I would like to thank my committee, Prof. H. Maharaj, Prof. Gretchen L Matthews, Prof. Hui Xue, Prof. Elena S Dimitrova for their advice, instruction of classes, encouragement and support. I have learned a lot from them. Additional thanks is due to Prof. Beth Novick, Prof. Peter C Kiessler and Prof. Hyesuk K Lee for their support, Prof. Robert Taylor for the teaching opportunity, and Prof. Joel Brawley for great teaching and support. And I want to thank Susan Zhang for her care and encouragement.

I would also like to thank Mingfu Zhu, Yunwei Cui, Raymond A Heindl, Jang-Woo Park, Qi Zheng for inspiring talks and friendship. Also I should thank Artur Gorka, Yang Yang, Zhe Sun, Hua Zhang, Ping Yan, Qing Xu, Zendong Wan, Ru Chen, Jun Gao, Hong Dong, Guang Zeng, Rui Wang, who have been great friends through my years in Clemson, also friends from badminton team and chinese soccer team.

I owe much to my parents, Xingying He and Faen Guan, my older sister Yuhua Yang and older brother Honghua Guan, and my lovely nephew and niece. They always

have faith in me with unconditional love, especially my sister. My honor belongs to them as well.

Contents

List of Figures

Chapter 1

Introduction

1.1 Factoring polynomials

Factoring polynomials is a central problem in computer algebra with applications in mathematics and engineerings. For univariate polynomial factorization, we have probabilistic methods by Berlekamp (1967) and Neiderreiter (1993). Hensel lifting method was first presented by Zassenhaus (1969) for factoring in $\mathbb{Q}[x]$. A.K. Lenstra, H.W. Lenstra and Lovász (1982) introduced lattice reduction and gave the first polynomial time algorithm for factoring in $\mathbb{Q}[x]$. Then Chistov (1984), A. K. Lenstra (1984) and Kaltofen (1982) showed that multivariate polynomials over fintie fields can be factored in polynomial time. Gao and Lauder (2002) proved that Hensel lifting method for polynomial time in $\mathbb{F}_q[x, y]$ is fast on average (almost linear). Van Hoeij (2002) improved the LLL lattice reduction method for factoring in $\mathbb{Q}[x]$ whose key idea is to recombine the logarithmic derivatives of lifted factors and use a small lattice. And Belabas, von Hoeij and Kluners (2002) generalized Hoeij's method from $\mathbb{Q}$ to more general global fields including $\mathbb{K}(y)[x]$. Gao (2003) gave a PDE approach to factor $f \in \mathbb{K}[x, y]$ requiring that $p > 2n^2 - 1$, where $char = p$ and n is the total degree of f and also works for absolute factorization and mumerical factor-

ing over $\mathbb{R}$ or $\mathbb{C}$ (coefficients of f are approximate). Lecerf (2006) presented, when the field characterisitc is zero or sufficiently large, recombination algorithms which only cost subquadratic time in term of the total degree, and Lecerf (2007) gave a new recombination algorithm that works for fields of any characteristic and lifts only to the total degree.

We are interested in two aspects, efficient bivariate polynomial factorization and deterministic algorithms for univariate polynomial factorization over finite fields.

Suppose $\mathbb{K}$ is a commutative field containing $\mathbb{F}_q$ with characteristic p. Let $f \in \mathbb{K}[x, y]$ be square free. Suppose

$$f = f_1 f_2 \cdots f_r, \tag{1.1}$$

where $f_i \in \mathbb{K}[x, y]$ are irreducible and distinct. We want to find these irreducible factors. The basic idea of current approaches can be summarized by the following diagram:

$$\begin{array}{c} f \in \mathbb{K}[x,y] \\ \downarrow \quad \mathrm{mod}\phi(y) \\ f \in \mathbb{K}[y]/(\phi(y))[x] \\ \downarrow \quad \text{factoring} \\ f \equiv f_1^{(1)} f_2^{(1)} \cdots f_s^{(1)} \bmod \phi(y) \\ \downarrow \quad \text{Hensel lifting} \\ f \equiv f_1^{(m)} f_2^{(m)} \cdots f_s^{(m)} \bmod \phi(y)^m \\ \downarrow \quad \text{Combination} \\ f_1, f_2, \cdots, f_r \end{array}$$

It is possible that f is irreducible but $f \pmod{\phi(y)}$ has many factors for all $\phi(y)$. Thus the combination stage could have exponential running time. For example, the follow-

ing polynomial is irreducible

$$f(x,y) = \prod_{i=1}^{n}(x-i) + y \cdot g(x,y).$$

But, if $\phi(y) = y$, we have

$$f(x,y) \equiv \prod_{i=1}^{n}(x-i) \pmod{\phi(y)}.$$

For another example, the following polynomial is irreducible

$$f(x,y) = \prod (x \pm \sqrt{y} \pm \sqrt{y+1} \pm \cdots \pm \sqrt{y+t-1}) \in \mathbb{F}_q[x,y],$$

where the product is over all choices of $+$ and $-$. However, for every irreducible $\phi(y) \in \mathbb{F}_q[y]$, the irreducible factors of f mod $\phi(y)$ all have degrees ≤ 2.

In the worst case, it needs to try 2^n combinations. In practice, however most polynomials have only a small number of modular irreducible factors. So the above approach is efficient for most polynomials.

In our approach, we want to use a solution basis for modified Berlekamp equation (1.4) or Neiderreiter equation (1.5) to find factors. The question is how to find a solution space (1.8) for any of these two equations. When $\mathbb{K} = \mathbb{F}_q$, each of the equations is a linear system over $\mathbb{F}_q$, with the coefficients of h as unknowns. The system can be solved by any fast algorithms in the literature. In the case when $\mathbb{K}$ is a function field, say $\mathbb{K} = \mathbb{F}_q(x)$. We show how to find the solutions via Hensel lifting. The details will be presented in chapter 2.

We are also interested in the deterministic complexity of factoring polynomials over finite fields. Given any polynomial $f \in \mathbb{F}_q[x]$ of degree n, we want to find a proper factor of f. There exist several randomized algorithms to factor f over $\mathbb{F}_q$ with complexity

in polynomial time $(\log q, \deg f)^{O(1)}$, see for examples, Berlekamp (1970), Cantor and Zassenhaus (1981), von zur Gathen and Shoup (1992), Kaltofen and Shoup (1998). Nevertheless, it is still an open problem whether there exist any deterministic algorithm running in polynomial time in n and $\log p$.

It is a major open problem in computer science whether $P = RP$. Recall that P is the collection of problems that can be solved by deterministic algorithms in polynomial time, RP is the collection of problems that can be solved by randomized algorithms in polynomial time. The main issue is whether random numbers are necessary in efficient computing. For a simple example, consider the following problem. Given a prime p, find a quadratic nonresidue $a \in \mathbb{F}_p$ ($a \neq b^2 \pmod p$ for all $b \in \mathbb{F}_p$). This can be solved by the following algorithm.

Randomized algorithm: Find a quadratic nonresidue

Input: p a prime

Output: "Failure" or $a \in \mathbb{F}_p$ a quadratic nonresidue

Step1: Pick $a \in \mathbb{F}_p \backslash \{0\}$ at random

Step2: Compute $b := a^{\frac{p-1}{2}} \pmod p$

Step3: If $b = 1$ then output "Failure", otherwise output a

The algorithm outputs a quadratic nonresidue $a \in \mathbb{F}_p$ with probability $1/2$. Run the algorithm 100 times to get a quadratic nonresidue in $\mathbb{F}_p$ with probability $1 - 2^{-100}$.

However, we don't know any deterministic algorithm for this problem. A simple approach is to test $a = 1, 2, 3, \cdots$ until a quadratic nonresidue is found. The problem is to find a good bound for the smallest quadratic nonresidue mod p. Under extended Riemann Hypothesis (ERH), N.C. Ankeny (1952), Y. Wang (1959), E. Bach (1990) gave a upper bound $2 \log^2 p$. Hence, under GRH, there exists a deterministic polynomial time algorithm to find a quadratic nonresidue.

Berlekamp algorithm reduces general polynomials in $\mathbb{F}_q[x]$ deterministically to poly-

nomials that are separable and split completely. It can be shown that factoring quadratic polynomials is equivalent to finding a quadratic nonresidue in $\mathbb{F}_p$. We do not know any deterministic polynomial time algorithm for factoring quadratic polynomials without assuming GRH. Bach, von zur Gathen and Lenstra (2001) proved that it is polynomial time if $\phi_K(p)$ is smooth for some k where $\phi_k(x)$ is the k-th cyclotomic polynomial. Ronyai [Ronyai92] proved that under GRH f can be factord in polynomial time modulo p in deterniminstic polynomial time except for finitely many primes p if $\mathbb{Q}[x]/f$ is a Galois extension. This result extends previous work of Huang (1991), Evdokimov (1989) and Adleman, Manders and Miller (1977). Evdokimov (1994) gave a subexponential-time algorithms in $n^{\log n}$ and $\log q$ under GRH. Gao (1996) showed that hard-to-factor polynomials must be square balanced. Recently, Ivanyos, Karpinski and Saxena (2008) demonstrate the level r in Evdokimov's algorithm (1994) can be reduced to $\frac{\log n}{1.5}$ and gave the first deterministic polynomial time algorithm to find a nontrivial factor of a polynomial of prime degree n where $(n-1)$ is a smooth number.

Evdokimov (1992) gave an exponential deterministic polynomial time algorithm with complexity $(n^{\log_2 n} \log q)^{O(1)}$ to factor f into irreducible factors over k, assuming GRH (generalized Riemann Hypothesis) and f of degree n over an explicitly given finite field k of cardinality q. Ivanyos, Karpinski and Saxena (2008) showed it only needs to extend $\frac{\log_2 n}{\log_4 8}$ levels instead of $\log_2 n$ in Evdokimov (1992). We continue this line of research for deterministic polynomial time algorithms under GRH and reduce the levels by a constant as stated in the following theorem 3.5.13 in Chapter 3.

Theorem 1.1.1. *Let $\ell(n)$ be the extension needed to find a factor of polynomial of degree n, then $\ell(n) \leq \frac{\log_2 n}{\log_4 12}$.*

1.2 Basic theory for factoring univariate polynomials

In this section, we give a brief survey of results that are essential for factoring univariate polynomials. In chapter 2, we shall show how to use these results for factoring bivariate polynomials.

Let $\mathbb{K}$ be a commutative field containing $\mathbb{F}_q$ with characteristic p. Let $f \in \mathbb{K}[x]$ be squarefree and suppose it factors as

$$f = f_1 f_2 \cdots f_r, \tag{1.2}$$

where $f_i \in \mathbb{K}[x]$ are irreducible and distinct, which we want to find. There are several methods to do this, each of them reduces the problem to a linear algebra problem. More precisely, Berlekamp's method finds all $g \in \mathbb{K}[x]$ satisfying $\deg(g) \leq \deg(f)$,

$$g^q \equiv g \pmod{f}, \tag{1.3}$$

which is equivalent to

$$h^q \equiv (f')^{q-1} h \pmod{f}. \tag{1.4}$$

Note that (1.3) and (1.4) are equivalent only if f is squarefree, in fact

$$h = g \cdot f' \pmod{f}.$$

Niederreiter's method considers the differential equation

$$H^{(q-1)}\left(\frac{h}{f}\right) = \left(\frac{h}{f}\right)^q, \tag{1.5}$$

where $H^{(q-1)}$ is the $(q-1)$-th Hasse derivative on $\mathbb{F}_q[x]$ defined by

$$H^{(q-1)}(x^i) = \binom{i}{q-1} x^{i-(q-1)}.$$

Also, Wan considers the equation

$$\psi_q(f^{q-1}xh) = (xh)^{[q]}, \tag{1.6}$$

where

$$g^{[q]} = \sum a_i^q x^i,$$

if $g = \sum a_i x^i \in \overline{K}((x))$, and ψ_q is the $\mathbb{K}$-linear operator on $\mathbb{K}((x))$ defined by

$$\psi_q(x^u) = \begin{cases} x^{u/q}, & if \quad q|u, \\ 0, & otherwise. \end{cases}$$

Theorem 1.2.1 (Niederreiter 1993)**.** *Let $f \in \mathbb{K}[x]$ be squarefree with r distinct irreducible factors as in (1.2). Then $\dim_{\mathbb{F}_q}(N_f) = r$, and every h to (1.5) is of the form:*

$$h = \sum_{i=1}^{r} \lambda_i E_i,$$

where $\lambda_i \in \mathbb{F}_q$ and $E_i = \frac{f}{f_i} f_i'$ for $1 \leq i \leq r$.

Proof. Each irreducible factors f_i can be written as

$$f_i = \prod_{j=1}^{\ell} (x - \beta_{ij}), \quad \beta_{ij} \in \overline{\mathbb{K}}, \quad 1 \leq i \leq r.$$

We order the elements β_{ij}'s as $(\beta_1, \beta_2, \cdots, \beta_n)$. Then $\beta_1, \beta_2, \ldots, \beta_n$ are distinct and are all

the roots of f in the algebraic closure of $\mathbb{K}$. Hence

$$f = c\prod_{i=1}^{n}(x-\beta_i),$$

where $c \in \mathbb{K}$ is the leading coefficient of f. Since $\deg_x(h) < \deg_x(f)$, we have

$$\frac{h}{f} = \sum_{i=1}^{n} \frac{b_i}{x-\beta_i}\,, \tag{1.7}$$

where $b_i = \frac{h(\beta_i)}{f'(\beta_i)} \in \overline{\mathbb{K}}$, $1 \le i \le n$. Hence

$$H^{(q-1)}\left(\frac{h}{f}\right) = \sum_{i=1}^{n} H^{(q-1)}\left(\frac{b_i}{x-\beta_i}\right) = \sum_{i=1}^{n} \frac{-b_i}{x^q-\beta_i^q},$$

So (1.4) becomes

$$\sum_{i=1}^{n} \frac{-b_i}{x^q-\beta_i^q} + \sum_{i=1}^{n} \frac{b_i^q}{x^q-\beta_i^q} = 0\,,$$

which implies that $b_i = b_i^q$, i.e. $b_i \in \mathbb{F}_q$ for $1 \le i \le n$.

If β_i and β_j are conjugates over $\mathbb{K}$, i.e. if they are roots of the same irreducible factor of $f \in \mathbb{K}[x]$, then there exists an $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ such that $\sigma(\beta_i) = \beta_j$. Hence

$$b_i = \sigma(b_i) = \sigma\left(\frac{h(\beta_i)}{f'(\beta_i)}\right) = \frac{h(\sigma(\beta_i))}{f'(\sigma(\beta_i))} = \frac{h(\beta_i)}{f'(\beta_i)} = b_j\,,$$

Thus $b_i = b_j$ whenever β_i and β_j are roots of the same irreducible factor of f.

For each irreducible factor f_i of f, we group the terms in (1.7) where β_j is a root of f_i and let λ_i be the common value of these b_j. Then

$$\frac{h}{f} = \sum_{i=1}^{r} \lambda_i \sum_{\beta\text{: root of } f_i} \frac{1}{x-\beta} = \sum_{i=1}^{r} \lambda_i \frac{1}{f_i}\frac{\partial f_i}{\partial x}.$$

Therefore

$$h = \sum_{i=1}^{r} \lambda_i \frac{f}{f_i} \frac{\partial f_i}{\partial x}$$

as claimed by the theorem.

Since f_i's are distinct, we see that E_i's are linearly independent over $\mathbb{F}_q$. This proves that $E_1, E_2, \cdots, E_r$ form a basis over $\mathbb{F}_q$ for the solution space. □

Theorem 1.2.2. *Let $f \in \mathbb{K}[x]$ be squarefree with r distinct irreducible factors. Then (1.4), (1.5) and (1.6) have the same solution space.*

$$H = \{h \in \mathbb{K}[x] : h \text{ satisfies } (1.4)\}. \tag{1.8}$$

1.3 Geometric structure of Gröbner bases

We assume f is squarefree that splits completely over finite fields. Let S be the set of roots of f. We construct ideals extended from $\langle f(x) \rangle$ and varieties extended from S. We show how to use Gröbner bases structure theorem to decompose these ideals and varieties, and how those might lead to proper factors of f which is to be factored.

In the following, we describe a correspondence between the geometric structure of the variety of a zero-dimensional radical ideal and its Gröbner basis under elimination order . This will be one of the main tools to split polynomial system.

Let $\mathbb{F}$ be any field. For any ideal $I \subset \mathbb{F}[x_1, x_2, \cdots, x_n]$, let $V(I)$ be the set of common solutions of I in $\bar{\mathbb{F}}^n$. We call $V(I)$ the variety of I. For an ideal I, we are interested in the structure of its variety $V(I)$. In particular, we want to know the number of extensions of particular solutions.

For a set of points $V \in \bar{\mathbb{F}}^n$, we say $(a_1, a_2, \cdots, a_{i-1})$ is a partial point of V, for any $2 \leq i \leq n$, if there exist $a_i, \cdots, a_n$ such that $(a_1, a_2, \cdots, a_{i-1}, a_i, \cdots, a_n)$ is a point in V.

Definition 1.3.1. *Let $V \subset \bar{\mathbb{F}}^n$ and $(a_1, a_2, \cdots, a_{i-1})$ is a partial point in V. We define the fiber size of above $(a_1, a_2, \cdots, a_{i-1})$ to be*

$$\#\left\{b \in \bar{\mathbb{F}} : (a_1, \cdots, a_{i-1}, b) \text{ is a partial point in } V\right\}.$$

We say fibre sizes of V at level i to be the fibre sizes above all partial points $(a_1, a_2, \cdots, a_{i-1})$ of V.

We define a projection map π as follows. Let a set of points $V \subset \bar{\mathbb{F}}^n$.

$$\begin{aligned} \pi : \quad & V \to \bar{\mathbb{F}}^{n-1} \\ & (a_1, a_2, \cdots, a_{n-1}, a_n) \mapsto (a_1, a_2, \cdots, a_{n-1}) \end{aligned}$$

Let $W = \pi(V)$. Given first $n-1$ coordinates of a point from V, we denote

$$\pi^{-1}(a_1, \cdots, a_{n-1}) = \left\{b \in \bar{\mathbb{F}} : (a_1, \cdots, a_{n-1}, b) \in V\right\}.$$

According to distinct fibre sizes above $n-1$ level, V can be partitioned by one to one correspondence as

$$V = P_1 \cup \cdots \cup P_r,$$

where any two points $u, v \in P_i$ have the property that $\pi(u)$ and $\pi(v)$ share a common fibre size m_i, $1 \leq i \leq r$.

Example 1.3.2. *Suppose we have the following points:* $P = \{(0,0,1), (0,0,4), (0,0,2)$ $, (0,4,0), (2,2,3), (2,3,1), (3,1,2), (3,1,3)\}$. *The fiber sizes are* $(0,0)$, $|\pi^{-1}(0,0)| = 3$, $\pi^{-1}(3,1) = 2$, $\pi^{-1}(0,4) = 1$, $\pi^{-1}(2,2) = 1$, $\pi^{-1}(2,3) = 1$. *So* $P_2 = \pi(P) = \{(0,0)\} \cup \{(3,1)\} \cup \{(0,4), (2,2), (2,3)\}$.

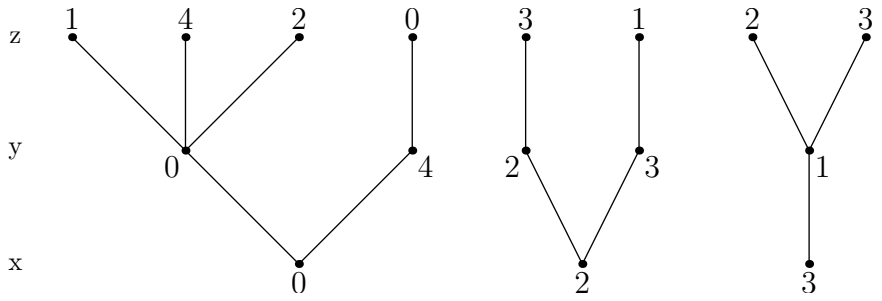

Figure 1.1: Points Structure

Definition 1.3.3. *(Uniform).*

We say that the set V is uniform at level i or above level $i-1$, if the fibre size of any partial point $(a_1, \cdots, a_{i-1})$ in V is a constant.

If it is uniform for each level to the next, we say the points are totally uniform.

Now we give an example that all fiber sizes are the same as follows.

Example 1.3.4. *Points are* $\{(1,2),(1,3),(2,3),(2,4),(3,4),(3,5),(4,1),(4,5),(5,1),(5,2)\}$. *All fiber sizes of* $\pi(s), s \in P_2$ *are 2. We say that it is uniform from level 1 to level 2 in this case.*

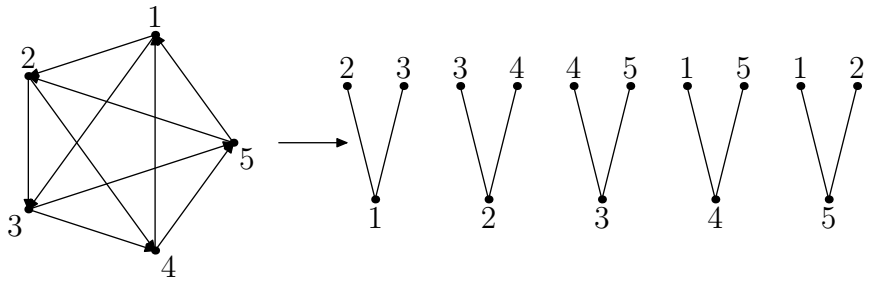

Figure 1.2: Regular graph

The variety of a radical zero-dimensional ideal I, $V(I)$ has an partition according to fiber sizes. Can we tell about Gröbner basis of I from the information of fibre sizes of $V(I)$, or vice verse? The main theorem of Gao, Rodrigues, and Stroomer (2003) answered this question.

Theorem 1.3.5 (Gao, Rodrigues, and Stroomer 2003)**.** *Let $\mathbb{F}$ be a perfect field, I a zero-dimensional radical ideal in $\mathbb{F}[x_1, x_2, \cdots, x_n]$, and P_n the set of points of $V(I)$ in $\bar{\mathbb{F}}^n$. Assume the fibre sizes in P_n are $0 < m_1 < m_2 < \cdots < m_r$. Let G be any minimal Gröbner basis for I under an elimination order for x_n, i.e. $x_n > x_1, x_2, \cdots, x_{n-1}$. View the elements of G as polynomials in x_n with coefficients in $\mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$, and group polynomials in G by their degrees in x_n as follows.*

$$G = G_0 \cup G_1 \cup G_2 \cdots \cup G_t,$$

where G_i denotes all polynomials in G with a common degree in x_n. Then

(1). $t = r$, and the degree of x_n in G_i is m_i, $1 \leq i \leq r$.

(2). For $1 \leq i \leq r$, let $Lc_{<m_i}(G) \subset \mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$ denote the leading coefficients of the polynomials in

$$G_0 \cup G_{m_1} \cup G_{m_2} \cdots \cup G_{m_{i-1}}.$$

Let $P_{n-1} = \pi(P_n)$, $P_{n-1,i} = \{A \in P_{n-1} |\ |\pi^{-1}(A) = m_i\}$, and

$$P_{n-1,\geq i} = P_{n-1,i} \cup P_{n-1,i+1} \cdots \cup P_{n-1,r}.$$

Then $Lc_{<m_i}(G)$ is a Gröbner basis for I s.t. $V(I) = P_{n-1,\geq m_i}$ for $1 \leq i \leq r$.

Remark 1: One simple conclusion made from the theorem is that points projected with fibre size $\geq m_i$ vanish all of those leading coefficients of terms with $\deg_{x_n} < m_i$ in the Groeber Basis G. The coefficient of the polynomial in G with highest degree in x_n is 1.

Remark 2: Under the elimination order on x_n, the degree in x_n of the items in the minimal Gröbner basis are exactly the fibre sizes of $\pi(V(I))$.

Example 1.3.6. *Let $P = \{(1,3,1), (1,3,2), (1,1,1), (2,1,3), (2,1,2), (2,4,1)\}$.*

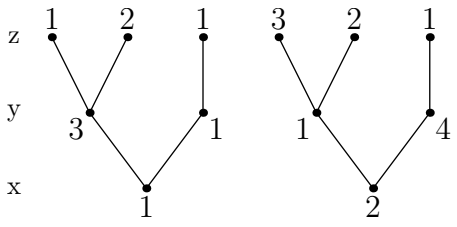

Figure 1.3: An example

$P_2 = \pi_3(P) = \{(1,3),(1,1),(2,1),(2,4)\}$. *Then* $P_2 = S_1 \cup S_2$. $S_1 = \{(1,3),(2,1)\}$, m_1=*2;* $S_2 = \{(1,1),(2,4)\}$, $m_2 = 1$. *So fiber sizes from 2-level to 3-level of* P *are 1 and 2. Let* $I = I(P)$. *Under elimination order* $x_1 < x_2 < x_3$, *the Gröbner Basis consists of the following polynomials:*

$$\begin{aligned} g_0 &= x^2 - 3x + 2 \\ g_1 &= y^2 - xy - 3y + x + 2 \\ g_2 &= (2x + y - 5)z - y - 2x + 5 \\ g_3 &= 3z^2 - 6xz - 3z - 2xy + 2y + 14x - 8 \end{aligned}$$

So the leading terms are $\{x^2, y^2, z, z^2\}$. z *and* z^2 *'s degree are 1 and 2, exactly the fiber sizes of* P_2. *And* $I_0 = \{g_0, g_1\}$ *is a Gröbner basis for* P_2, $I_1 = \{g_0, g_1, 2x + y - 5\}$ *is a Gröbner basis for* $I(S_1)$ *according to the theorem 1.3.5. By using quotient operation, we can compute a Gröbner basis for The ideal generated by* S_2, *since* $I(S_2) = I_0 : I_1$.

Example 1.3.7. *Suppose* I *has the following Gröbner basis* $\{(x-1)(x-2), (x-2)y + 1, y^2 - 1\}$ *under lex order* $x < y$. *And fibre sizes of* x *are 1 and 2 because the degree of* y *is 1 and 2.*

Given an ideal I, let $P = V(I)$. If under elimination order on x_n, it is uniform from $\pi_n(P)$ to P, then I has a minimal Gröbner basis of the form, $G = G_0 \cup g$, where $LT(g) = x_n^m$, m is a constant. If P is totally uniform under lex order $x_1 \prec x_2 \prec \cdots, \prec x_n$, then $G = \{g_1(x_1), x_2^{m_2} + g_2(x_1, x_2), \cdots, x_n^{m_n} + g_n(x_1, x_2, \cdots, x_n)\}$ where $x_i^{m_i}$'s is the

leading term of i-th polynomial.

Example 1.3.8. *Let* $P = \{(1,4,1),(1,4,2),(1,4,4),(1,2,1),(1,2,2),(1,2,5),$
$(2,3,1),(2,3,4),(2,3,3),(2,2,7),(2,2,2),(2,2,3)\}$.

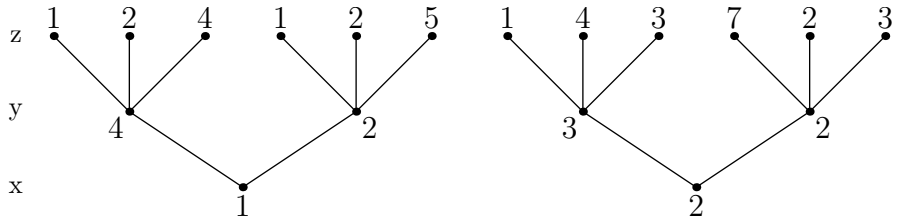

Figure 1.4: An uniform case

Using lex order with $x \leq y \leq z$*, the reduced Gröbner basis G of* $I(P)$ *is given by the polynomials below:*

$$\begin{aligned} g_0 &= x^2 - 3x + 2 \\ g_1 &= y^2 - xy - 2x - 7y + 10 \\ g_2 &= 2z^3 + (7xy - 6y - 22x + 4)z^2 + (-41xy + 38y + 130x - 90)z + 58xy - 56y - 180x + 156 \end{aligned}$$

As stated in theorem 1.3.5 , $Lc_{<m_i}(G)$ is a Gröbner basis for $P_{n-1,\geq m_i}$ for $1 \leq i \leq r$. $I(Lc_{<m_i}(G)) \subset I(Lc_{<m_{i+1}}(G))$. So, we can use quotient to compute the ideal vanished at points with fibre size exactly m_i.

If I is not uniform, by the structure theorem, then not all leading coefficients are constants. In this case, we can refine the ideal. For example, in example 1.3.6 $G_0 = \{x^2 - 3x + 2, y^2 - xy - 3y + x + 2\}$. $G_1 = \{g_0, g_1, 2x + y - 5\} = \{x^2 - 3x + 2, 2x + y - 5\}$ is a Gröbner basis for $I(S_1)$ with fibre sizes bigger than 1.Variety of G_1 is $S_1 = \{(1,3),(2,1)\}$. $J_1 = I_0 : I(S_1) = I(x^2 - 3x + 2, y - 3x + 2)$, which is exactly the ideal vanishes on points set $S_2 = \{(1,1),(2,4)\}$ with fibre size exactly 1. We can write I as an intersection

$$I = I(x^2 - 3x + 2, y - 3x + 2, z - 1) \cap I(x^2 - 3x + 2, 2x + y - 5, z^2 - 2xz - z + 4x - 2).$$

Theorem 1.3.9. *For each $1 \leq i \leq r$, J_i is a Gröbner Basis for the points in $S = \pi(P)$ that are projections of fibres of size exactly m_i. Then*

$$J_i =< G_{i-1} >:< G_i > .$$

We will show this can be computed in deterministic polynomial time in Section 3.2.

Example 1.3.10. *Let's consider the example 1.3.6.* $G_0 = \{x^2 - 3x + 2, y^2 - xy - 3y + x + 2\}$. *Let* $I_0 = I(G_0)$ *with* $V(I_0) = V(P_2) = \{(1,3),(1,1),(2,1),(2,4)\}$.
And $G_1 = \{g_0, g_1, 2x + y - 5\} = \{x^2 - 3x + 2, 2x + y - 5\}$ *is a Gröbner basis for* $I(S_1)$ *with fibre sizes bigger than 1.Variety of* G_1 *is* $S_1 = \{(1,3),(2,1)\}$. $J_1 = I_0 : I(S_1) = I(x^2 - 3x + 2, y - 3x + 2)$, *which is exactly the ideal vanishes on points set* $S_2 = \{(1,1),(2,4)\}$ *with fibre size exactly 1.*

Chapter 2

Factoring bivariate polynomials via lifting linear spaces

We present a new modular approach that does not need any recombination of factors. Instead of lifting modular factors we lift the linear space of solutions and get complete factorization directly from lifted solutions.

2.1 Lifting Berlekamp's linear spaces

From now on, we assume $f \in \mathbb{F}_q[y][x]$. To solve (1.4), let $\phi(y) \in \mathbb{F}_q[y]$ be irreducible, we consider

$$h^q \equiv (f')^{q-1}h \pmod{f, \phi(y)},$$

where

$$h = \sum_{i=0}^{n-1} a_i(y)x^i,\ \deg_y a_i(y) < \deg_y \phi(y).$$

This is a linear system over $\mathbb{F}_q$ with N unknowns and N equations respectively, where $N = n \deg_y \phi(y)$.

Theorem 2.1.1. *let $\phi(y) \in \mathbb{F}_q[y]$ be irreducible such that $f \pmod{\phi}(y)$ is square free. Let*

$m \geq 1$ *and* $h_0 \in \mathbb{F}_q[x,y]$ *such that*

$$h_0^q \equiv (f')^{q-1} h_0 \pmod{f(x,y), \phi^m(y)}.$$

Then there exists a unique $g \in \mathbb{F}_q[y][x]$ *such that* $\deg_y(g) < \deg(\phi)$, $\deg_x(g) < n$, *and*

$$(h_0 + g\phi^m)^q \equiv (f')^{q-1}(h_0 + g\phi^m) \pmod{f(x,y), \phi^{m+1}(y)}.$$

In fact

$$g \equiv \frac{h_0^q - (f')^{q-1} h_0}{\phi^m} \frac{1}{(f')^{q-1}} \pmod{f, \phi(y)}.$$

Remark: Since $h_0^q \equiv (f')^{q-1} h_0 \pmod{f, \phi^m(y)}$, $h_0^q - (f')^{q-1} h_0$ mod $(f, \phi^{m+1})$is divisible by ϕ^m. So it is $h_0^q \equiv (f')^{q-1} h_0$ is computed $\pmod{f, \phi^{m+1}(y)}$ first, then divided by ϕ^m. The quotient is then multiplied with the other term modulo $(f, \phi(y))$. Also $(f')^{q-1}$ only needs to be computed mod $(f, \phi(y))$ once.

2.2 Lifting Niederreiter's linear spaces

Lifting via Niederreiter's equation is much more complicated, we will show how this can be done in polynomial time.. We consider Niederreiter' differential equation (1.5) Let

$$h = \sum_{i=0}^{n-1} a_i x^i, \quad f^{q-1} = \sum_{j=0}^{(q-1)n} b_j x^j,$$

where $a_i, b_j \in \mathbb{F}_q[y]$. We can rewrite (1.5) as

$$\sum_{i=0}^{n-1} b_{lq+q-1-i} \cdot a_i = a_l^q, \ \ 0 \leq l \leq n-1,$$

or equivalently,

$$\begin{pmatrix} b_{q-1} & b_{q-2} & \cdots & b_{q-n} \\ b_{2q-1} & b_{2q-2} & \cdots & b_{2q-n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{(n-1)q-1} & b_{(n-1)q-2} & \cdots & b_{(n-1)q-n} \\ b_{nq-1} & b_{nq-2} & \cdots & b_{nq-n} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-2} \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0^q \\ a_1^q \\ \vdots \\ a_{n-2}^q \\ a_{n-1}^q \end{pmatrix}.$$

We show how to compute this matrix in the appendix.

Lemma 2.2.1. *Let $\mathbb{K}$ be any field containing $\mathbb{F}_q$ and $g \in K[x]$ such that $\gcd(g, g') = 1$. Then, for any $w \in K[x]$ with $\deg w < \deg g = n$, there exists a unique $h \in K[x]$ with $\deg h < n$ such that*

$$H^{(q-1)}\left(\frac{h}{g}\right) = \left(\frac{w}{g}\right)^q. \tag{2.1}$$

Proof. Since $\gcd(g, g') = 1$, g is separable. Let K_g be the splitting field of g over K. Let $\beta_1, \cdots, \beta_n$ be the n distinct roots of g in K_g. Then

$$\frac{w}{g} = \sum_{i=1}^{n} \frac{w_i}{x - \beta_i},$$

where $w_i = \frac{w(\beta_i)}{g'(\beta_i)}$. So

$$\left(\frac{w}{g}\right)^q = \sum_{i=1}^{n} \frac{w_i^q}{x^q - \beta_i^q}.$$

By interpolation, there is an $h \in K_g[x]$ such that $\deg h < n$ and $h(\beta_i) = w_i^q g'(\beta_i), 1 \leq i \leq n$. Then

$$\frac{h}{g} = \sum_{i=1}^{n} \frac{h_i}{x - \beta_i}, \text{ where } h_i = \frac{h(\beta_i)}{g'(\beta_i)} = w_i^q \quad 1 \leq i \leq n.$$

Note that

$$H^{(q-1)}\left(\frac{h}{g}\right) = \sum_{i=1}^{n} H^{(q-1)}\left(\frac{h_i}{x-\beta_i}\right) = \sum_{i=1}^{n} \frac{w_i^q}{(x-\beta_i)^q} = \left(\frac{w}{g}\right)^q.$$

i.e. h satisfies (2.1).

We need to show that $h \in K[x]$. Since $\gcd(g, g') = 1$, K_g is Galois over K. Hence, for any $\beta \in K_g$, we have $\beta \in K$ iff $\sigma(\beta) = \beta$ for all $\sigma \in \text{Gal}(K_g/K)$. Now each $\sigma \in \text{Gal}(K_g/K)$ extends to a unique a ring isomorphism of $K_g[x]$ that fixes all polynomials in $K[x]$. Applying σ to (2.1), we see that $\sigma(h)$ is another solution in $K_g[x]$. The uniqueness argument below shows that $\sigma(h) = h$ for all $\sigma \in \text{Gal}(K_g/K)$, hence $h \in K[x]$.

It remains to prove the uniqueness of h. In fact, we prove the uniqueness for $h \in K_g[x]$. Let $u, v \in K_g[x]$ be any two solutions to (2.1) with $\deg(u) < n$ and $\deg(v) < n$. Then

$$H^{(q-1)}\left(\frac{u}{g}\right) = H^{(q-1)}\left(\frac{v}{g}\right).$$

Expanding u/g and v/g into partial fractions (similar to h/g above), we see that $u(\beta_i) = v(\beta_i)$ for $1 \leq i \leq n$. Since both u and v have degrees less than n, it follows that $u = v$. This completes the proof. □

Theorem 2.2.2. *For any $m \geq 1$, and $h_0 \in \mathbb{F}_q[y][x]$ such that*

$$H^{(q-1)}\left(\frac{h_0}{f}\right) \equiv \left(\frac{h_0}{f}\right)^q \pmod{\phi^m}. \tag{2.2}$$

There exists a unique $h_1 \in \mathbb{F}_q[y][x]$ such that $\deg_y(h_1) < \deg(\phi)$, $\deg_x(h_1) < n$, and

$$H^{(q-1)}\left(\frac{h_0 + h_1\phi^m}{f}\right) \equiv \left(\frac{h_0 + h_1\phi^m}{f}\right)^q \pmod{\phi^{m+1}}. \tag{2.3}$$

Furthermore, let

$$u(x) = \frac{1}{\phi^m}(h_0^q - H^{(q-1)}(h_0 f^{q-1})) \in \mathbb{F}_q[y][x^q]. \tag{2.4}$$

Then

$$h_1(x) = \frac{u(x)}{f'(x)^{q-1}} \pmod{f(x), \phi(y)}. \tag{2.5}$$

Proof. Expanding (2.3), gives

$$H^{(q-1)}\left(\frac{h_0}{f}\right) + \phi^m H^{(q-1)}\left(\frac{h_1}{f}\right) \equiv \left(\frac{h_0}{f}\right)^q + \phi^{qm}\left(\frac{h_1}{f}\right)^q \pmod{\phi^{m+1}}.$$

So

$$\frac{1}{\phi^m}\left(\left(\frac{h_0}{f}\right)^q - H^{(q-1)}\left(\frac{h_0}{f}\right)\right) \equiv H^{(q-1)}\left(\frac{h_1}{f}\right) \pmod{\phi},$$

which we write as

$$\frac{u}{f^q} \equiv H^{(q-1)}\left(\frac{h_1}{f}\right) \pmod{\phi}, \tag{2.6}$$

where

$$u(x) = \frac{1}{\phi^m}(h_0^q - H^{(q-1)}(h_0 f^{q-1})) \in \mathbb{F}_q[y][x^q]. \tag{2.7}$$

Now there exists unique $w \in \mathbb{F}_q[y]/(\phi(y))[x]$ such that $w^q \equiv u \pmod{\phi}$, hence (2.6) is equivalent to

$$H^{(q-1)}\left(\frac{h_1}{f}\right) \equiv \left(\frac{w}{f}\right)^q \pmod{\phi}.$$

By Lemma 2.2.1 where $K = \mathbb{F}_q[y]/(\phi(y))$, there exists a unique $h_1 \in \mathbb{F}_q[y]/(\phi(y))[x]$ that satisfying (2.3). In fact $h = h_1$ is the unique polynomial such that

$$\frac{h}{f} = \sum_{i=1}^{n} \frac{h_i}{x - \beta_i},$$

where $h_i = \frac{h(\beta_i)}{f'(\beta_i)} = w_i^q$ and $w_i = \frac{w(\beta_i)}{f'(\beta_i)}$. This means that

$$h(\beta_i) = \frac{w(\beta_i)^q}{f'(\beta_i)^{q-1}} = \frac{u(\beta_i)}{f'(\beta_i)^{q-1}}.$$

Therefore, we have

$$h_1(x) = \frac{u(x)}{f'(x)^{q-1}} \pmod{f(x), \phi(y)}.$$

□

Theorem 2.2.3. *For any $m \geq 1$, and $h_0 \in \mathbb{F}_q[y][x]$ such that*

$$H^{(q-1)}\left(\frac{h_0}{f}\right) \equiv \left(\frac{h_0}{f}\right)^q \pmod{\phi^m}. \tag{2.8}$$

There exists a unique $g_m \in \mathbb{F}_q[y][x]$ such that $\deg_y(g_m) < \deg(\phi)$, $\deg_x(g_m) < n$, and

$$H^{(q-1)}\left(\frac{h_0 + g_m\phi^m}{f}\right) \equiv \left(\frac{h_0 + g_m\phi^m}{f}\right)^q \pmod{\phi^{m+1}}.$$

Furthermore, let

$$u(x) = \frac{1}{\phi^m}(h_0^q - H^{(q-1)}(h_0 f^{q-1})) \in \mathbb{F}_q[y][x^q]. \tag{2.9}$$

Then

$$g_m(x) = \frac{u(x)}{f'(x)^{q-1}} \pmod{f(x), \phi(y)}. \tag{2.10}$$

2.3 Lifting bound

In [Lecerf, 2007], Lecerf proved that it only needs to lift the solutions to degree at most $d_y + 1$ in y, where d_y is the degree of y, with differentiation with respect to x. Let

$$\frac{h}{f} = \sum_{i=1}^{n} \frac{\rho_i}{x - \phi_i},$$

where ϕ_i are the distinct roots of f in $\bar{\mathbb{F}}_q[[y]]$. If h is a solution, then

$$\frac{\partial}{\partial y}\rho_i = 0, \quad \forall i.$$

It is equivalent with the condition that h satisfies $D(h) = 0$, i.e. $h \in \ker(D)$, where D is defined as

$$D \quad : \quad \mathbb{K}[y,x]_{d_y, d_x - 1} \longrightarrow \mathbb{K}[y,x]_{3d_y, 3d_x - 3}$$

$$g \mapsto \left(\frac{\partial g}{\partial y}\frac{\partial f}{\partial x} - \frac{\partial g}{\partial x}\frac{\partial f}{\partial y}\right)\frac{\partial f}{\partial x} - \left(\frac{\partial^2 f}{\partial xy}\frac{\partial f}{\partial x} - \frac{\partial^2 f}{\partial x^2}\frac{\partial f}{\partial y}\right) g.$$

And if $h \in \ker D$, then $\mathcal{N}_f(h) \in \mathbb{K}[x^p, y^p]_{d_x - 1, d_y}$, where $\mathcal{N}_f$ is defined as follows.

$$\mathcal{N}_f \quad : \quad \mathbb{K}[x,y]_{d_x - 1, d_y} \longrightarrow \mathbb{K}[x^p, y]_{d_x - 1, p d_x},$$

$$g \mapsto g^p - H^{(p-1)}\left(f^{p-1} g\right).$$

For $h \in \mathbb{F}_q[x,y]$ with $\deg_x h < d_x$, $\deg_y h \leq d_y$ and $h \in \ker D$. If

$$h^p - H^{(p-1)}\left(f^{q-1} h\right) \equiv 0 \pmod{\psi(y)},$$

where $\psi(y)$ is any polynomial have $d_y + 1$ distinct roots in K, then h is a true solution.

Theorem 2.3.1 (Lecerf 2007)**.** *Let the characteristic of* $\mathbb{K}$ *be* $p > 0$ *and* $g \in \ker(D)$*. Let* S

be an arbitrary set of size $d_y + 1$. *For all* $a \in S$, *if* $Res_x(f, \frac{\partial f}{\partial x}) \neq 0$ *and* $\mathcal{N}_f(g)(x, a) = 0$, *then* g *is a solution to (1.5).*

2.4 The algorithm of finding a solution basis

Define Berlekamp map as:

$$\mathcal{B}_f \quad : \quad \mathbb{K}[x, y]_{d_x-1,d_y} \longrightarrow \mathbb{K}(x)[y]/(f)$$

$$h \mapsto h^q - (f')^{q-1}h,$$

that is, for $h \in \mathbb{K}[x, y]_{d_x-1,d_y}$,

$$\mathcal{B}_f(h) = h^q - (f')^{q-1}h \pmod{f}.$$

In the following algorithm, we mean bad solutions by those with total degree higher than f.

Algorithm 1: Find a solution basis

Input: $f \in \mathbb{K}[x][y]$, $\phi(y) \in \mathbb{K}[y]$ such that $(Res_x(f, \frac{\partial f}{\partial x})(x, a) \neq 0 \pmod{\phi(y)}$, and m s.t. $\deg(\phi^m) \geq d_y + 1$

Output: A solution basis for N_f

1. Find a basis of solutions of g of $\mathcal{B}_f(g) = 0 \pmod{f, \phi(y)}$, say $G = \{g_1, \cdots, g_r\}$;

2. **For** $i = 1, 2 \cdots, m-1$ **do**

   2.1. Lift each g_i in G to a solution $\hat{g}$ in $\mathbb{K}[x, y]/ < f, \phi^{i+1} >$;

   2.2. Use total degree to get rid of bad solutions via Gauss elimination ;

   2.3. Update G, suppose $G = \{\hat{g_1}, \cdots, \hat{g_t}\}$;

   End do ;

3. Check $D(g) = 0, \forall g \in G$. Get rid of bad solutions via Gauss elimination ; Suppose a good basis is $H = \{h_1, \cdots, h_r\}$;

4. Find a squarefree polynomial $\psi(y)$ of degree $d_y + 1$ in y satisfying $Res_x(f, f') \neq 0 \pmod{\psi(y)}$;

5. Check $\mathcal{B}_f(g) \equiv 0 \pmod{f, \psi}$, $g \in H$. Get rid of bad solutions via Gauss elimination and find a basis as output.

Proposition 2.4.1. *The algorithm (1) gives correct solution space N.*

Proof. After we lift to (y^{d_y+1}) and check with the map D, we have solutions of N_f, also belong to $\mathbb{K}[x^p, y^p]$. Then we choose $d_y + 1$ many value for y to check the solutions. By theorem 2.3.1, g s a true solution. □

Since solutions modulo ϕ^{m+1} can be obtained uniquely by lifting solutions modulo ϕ^m for each $m \geq 1$. And we don't need to lift each solution, but instead lifting any basis

of solutions to high powers of ϕ. In each level of lifting, if there are some elements in the basis whose total degree is greater than that of f, we eliminate them and update the basis by getting rid of those ones with high degree. We lift m many times and obtain a basis $\{b_1, b_2, \cdots, b_s\}$. Compute for each $i \in \{1, 2, \cdots, s\}$,

$$t_i = b_i^q - H^{(q-1)}(b_i f^{q-1}) \pmod{f(x), \phi_1(y)}. \tag{2.11}$$

If b_i is a solution for (1.5), then (2.11) should be 0. Thus we eliminate $\{t_1, t_2, \cdots, t_s\}$ by linear combination to find a set of coefficients $l_i = \{l_{i1}, \cdots, l_{is}\}$ such that $\sum_{k=1}^{s} l_{ik} t_k = 0$. Then from the proposition, we claim that

$$\left\{ \sum_{k=1}^{s} l_{1k} b_k, \cdots, \sum_{k=1}^{s} l_{rk} b_k \right\}$$

is the right basis for (1.5).

Remark: Lecerf's method uses the map D to do recombination and $\mathcal{N}_f$ or $\mathcal{B}_f$ to check. When characteristic is not high enough or zero, he uses $\mathcal{N}_f$ to do more combination. Our way is to use modified berlekamp's equation to solve solution space without recombination and lift the solution basis, but use the map D to check solutions.

2.5 Finding factors from a solution basis

Let $h(x, y)$ be any solution of (1.5), then

$$f = \prod_{\lambda \in \mathbb{F}_q} \gcd(f, h - \lambda f').$$

Use all h from a solution basis for (1.5), we can find all factors of f.

Algorithm 2: Find factors

Input: $f \in \mathbb{K}[x][y]$, solutions $h_1, \cdots, h_r$ and $\phi(y)$,

Output: factors of f.

Let $S = \{f\}$;

foreach $1 \leq i \leq r$ **do**

    Solve λ from $Res_x(f, h_i - \lambda f') \equiv 0 \pmod{\phi}$, for each h_i ;

    foreach *root* λ *of* h_i *and each* $g \in S$ **do**

        compute $\gcd(g, h_i - \lambda f')$;

        Update S by replace g by g's factors from $\gcd(g, h_i - \lambda f')$;

    end

end

Let $f = \prod_{i=1}^{r} s_i$, for all $s_i \in S$;

Suppose $\deg_x \phi^m > d_x + 1$;

Lift the factorization $f \equiv \prod_{s_i \in S} s_i$, to degree of ϕ^m ;

2.6 An example

We consider the following polynomials

$$f = x^p - x + y^{p-1} \in \mathbb{F}_p[x, y]$$

with total degree $d = p$. This polynomial, also can be written as $y^{p-1} - x(x-1)\cdots(x-p+1)$, is irreducible, but splits completely mod y.

Our example below shows that we only need to lift up to y^{d+1} to get the right linear space.

Let $p = 5$.

$$f = x^5 - x + y^4 \in \mathbb{F}_p[x, y].$$

The solutions basis mod y^m, $1 \leq m \leq 6$, are as follows:

$\bmod y$	$\bmod y^2$	$\bmod y^3$	$\bmod y^4$	$\bmod y^5$	$\bmod y^6$
$-x$	$-x$	$-x$	$-x$	$y^4 - x$	$y^4 - x$
$2x^2$	$2x^2$	$2x^2$	$2x^2$	$y^4x + 2x^2$	$y^4x + 2x^2$
$3x^3$	$3x^3$	$3x^3$	$3x^3$	$y^4x^2 + 3x^3$	$y^4x^2 + 3x^3$
x^4	x^4	x^4	x^4	$y^4x^3 + x^4$	$y^4x^3 + x^4$
1	1	1	1	1	1

The last row indicates that $h = 1$ is a true solution, and we can get rid of $\{y^4x + 2x^2, y^4x^2 + 3x^3, y^4x^3 +$ - because their total degree is bigger than that of f. Next we check with maps D and $\mathcal{B}_f$.

Consider the basis mod y^6, $H_5 = \{y^4 - x, y^4x + 2x^2, y^4x^2 + 3x^3, y^4x^3 + x^4, 1\}$.

$$\begin{aligned}
h_{51} = y^4 - x \quad &\Rightarrow \quad D(h_{51}) = 0, \\
h_{52} = y^4x + 2x^2 \quad &\Rightarrow \quad D(h_{52}) = -y^7, \\
h_{53} = y^4x^2 + 3x^3 \quad &\Rightarrow \quad D(h_{53}) = -2xy^7, \\
h_{54} = y^4x^3 + x^4 \quad &\Rightarrow \quad D(h_{54}) = -3x^2y^7, \\
h_{55} = 1 \quad &\Rightarrow \quad D(h_{55}) = 0,
\end{aligned}$$

So the new basis is $\{y^4 - x, 1\}$. $\mathcal{B}(y^4 - x) = (y^4 - x)^5 - (y^4 - x) = y^{40} = y^{4 \cdot 5} \neq 0$. So 1 is the only factor, hence f is irreducible.

2.7 Appendix: Computing coefficient matrix

The Niederreiter equation (1.5) is equivalent with

$$H^{(q-1)}\left(f^{q-1}h\right) = h^q.$$

Since

$$H^{(q-1)}(x^i) = \begin{cases} x^{i-q+1} & \text{if } i \equiv q-1 \pmod{q} \\ 0 & \text{otherwise.} \end{cases}$$

(1.5) and (1.6) turn out to be the same linear system over $\mathbb{F}_q$, so they are equivalent.

To write the equation (1.6) into a matrix form, suppose

$$h = \sum_{i=0}^{n-1} a_i x^i, \quad f^{q-1} = \sum_{j=0}^{(q-1)n} b_j x^j,$$

where $a_i, b_j \in \mathbb{F}_q[y]$. Then for $0 \le k \le n-1$, since $h^{[q]} = \sum_{i=0}^{n-1} a_i^q x^i$, we have

$$\psi_q\left(f^{q-1}xh\right) = \psi_q\left(\sum_{i=0}^{n(q-1)} b_i x^i \cdot x \cdot \sum_{k=0}^{n-1} a_k x^k\right) = \sum_{l=0}^{n-1} \psi_q\left(\sum_{i=0}^{n-1} b_{lq+q-1-i} x^{lq+q-1-i} \cdot x \cdot a_i x^i\right).$$

Since

$$\psi_q\left(f^{q-1}xh\right) = xh(x),$$

$$\psi_q\left(\sum_{i=0}^{n-1} b_{lq+q-1-i} x^{lq+q-1-i} \cdot x \cdot a_i x^i\right) = \sum_{i=0}^{n-1} b_{lq+q-1-i} \cdot a_i \cdot x^{l+1} = x \cdot a_l^q x^l,$$

which we can write as:

$$\sum_{i=0}^{n-1} b_{lq+q-1-i} \cdot a_i = a_l^q, \ 0 \le l \le n-1.$$

$$\begin{pmatrix} b_{q-1} & b_{q-2} & \cdots & b_{q-n} \\ b_{2q-1} & b_{2q-2} & \cdots & b_{2q-n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{(n-1)q-1} & b_{(n-1)q-2} & \cdots & b_{(n-1)q-n} \\ b_{nq-1} & b_{nq-2} & \cdots & b_{nq-n} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-2} \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0^q \\ a_1^q \\ \vdots \\ a_{n-2}^q \\ a_{n-1}^q \end{pmatrix} \tag{2.12}$$

We will show how to solve this system in the implementation section.

Note that, for any $g \in \mathbb{K}[x]$, we have $(g/f^p)' = g'/f^p$. By induction, it follows that

$$\left(\frac{h}{f}\right)^{(p-1)} = \left(\frac{hf^{p-1}}{f^p}\right)^{(p-1)} = \frac{(hf^{p-1})^{(p-1)}}{f^p}. \tag{2.13}$$

Then the equation (1.5) is equivalent to

$$(hf^{p-1})^{(p-1)} + h^p = 0\,. \tag{2.14}$$

To write the equation (2.14) into a matrix form, suppose

$$h = \sum_{i=0}^{n-1} a_i x^i, \quad f^{p-1} = \sum_{j=0}^{(p-1)n} b_j x^j,$$

where $a_i, b_j \in \mathbb{F}$. Then

$$g = hf^{p-1} = \sum_{k=0}^{m} c_k x^k \in \mathbb{F}[x]$$

where

$$c_k = \sum_{i+j=k} a_i b_j\,.$$

For any k,

$$\left(x^k\right)^{(p-1)} = k(k-1)\cdots(k-(p-1)+1)x^{k-(p-1)}.$$

If $k \not\equiv -1 \pmod{p}$, then $\left(x^k\right)^{(p-1)} = 0$ in $\mathbb{F}[x]$. Otherwise when $k \equiv -1 \pmod{p}$,

$$\left(x^k\right)^{(p-1)} = -x^{k-(p-1)} = -x^{dp}, \text{ where } d = (k-(p-1))/p\,.$$

So

$$g^{(p-1)} = \left(\sum_{k=0}^{m} c_k x^k\right)^{(p-1)} = \sum_{\ell=0}^{\lfloor \frac{m-(p-1)}{p} \rfloor} -c_{\ell p+p-1} x^{\ell p}.$$

Therefore the equation (2.14) is equivalent to the following system of equations:

$$c_{kp+p-1} = a_k^p, \quad 0 \le k \le n-1,$$

namely,

$$\sum_{i=0}^{n-1} a_i b_{kp+p-1-i} = a_k^p, \quad 0 \le k \le n-1$$

where $b_i = 0$, if $i > n(p-1)$, or $i < 0$. Then the above equation can be written as :

$$\begin{pmatrix} b_{q-1} & b_{q-2} & \cdots & b_{q-n} \\ b_{2q-1} & b_{2q-2} & \cdots & b_{2q-n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{(n-1)q-1} & b_{(n-1)q-2} & \cdots & b_{(n-1)q-n} \\ b_{nq-1} & b_{nq-2} & \cdots & b_{nq-n} \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} a_0^p \\ a_1^p \\ \vdots \\ a_{n-2}^p \\ a_{n-1}^p \end{pmatrix}$$

For a given $f \in \mathbb{K}[x]$, one can expand f^{q-1} to get the coefficients b_i in (2.12). This is fine for small q, but too expensive for large q. We now show a faster algorithm for computing the required n^2 coefficients for the matrix without computing all the $n(q-1)+1$ coefficients of f^{q-1}.

We first introduce a **convolution product** of vectors. Let $u = (u_{n-1}, u_{n-2}, \cdots, u_0)$,

$v = (v_0, v_1, \cdots, v_{n-1})$. We define

$$u * v^T = (u_{n-1}, u_{n-2}, \cdots, u_0) * \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = c^T, \quad (*)$$

where

$$c_i = u_i v_0 + u_{i-1} v_1 + \cdots + u_0 v_i. \quad 0 \le i \le n-1.$$

Equivalently, if we denote $u(x) = \sum_{i=0}^{n-1} u_i x^i$, $v(x) = \sum_{j=0}^{n-1} v_j x^j$, and $c(x) = \sum_{i=0}^{\infty} c_i x^i$, then $(*)$ is equivalent to

$$c(x) \equiv u(x)v(x) \pmod{x^n}.$$

This means that the convolution $u * v^T$ is equivalent to one polynomial multiplication.

Suppose $f = f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{F}[x]$. We compute the b_i's by using the inverse of f. Suppose

$$\frac{1}{f} = \sum_{i=0}^{\infty} w_i \cdot x^i, \quad w_i \in \mathbb{K}.$$

We assume $w_i = 0$, if $i < 0$. Then

$$f^{q-1} = f^q \cdot \frac{1}{f} = \left(\sum_{i=0}^{n} f_i^q x^{iq} \right) \left(\sum_{i=0}^{\infty} w_i \cdot x^i \right) = \sum_{i=0}^{n(q-1)} \left(\sum_{t=0}^{\lfloor \frac{i}{q} \rfloor} f_t^q \cdot w_{i-tq} \right) \cdot x^i.$$

So, the coefficient b_{kq-j} of x^{kq-j} in f^{q-1} can be written as:

$$b_{kq-j} = w_{kq-j} \cdot f_0^q + w_{(k-1)q-j} \cdot f_1^q + \cdots + w_{q-j} \cdot f_{k-1}^q, \quad 1 \le k \le n, \quad 1 \le j \le n,$$

that is,

$$\begin{pmatrix} b_{q-j} \\ b_{2q-j} \\ \vdots \\ b_{nq-j} \end{pmatrix} = (f^q_{n-1}, f^q_{n-2}, \cdots, f^q_0) * \begin{pmatrix} w_{q-j} \\ w_{2q-j} \\ \vdots \\ w_{nq-j} \end{pmatrix}.$$

Denote $V(f^q)$ by $(f^q_{n-1}, f^q_{n-2}, \cdots, f^q_0)$, and

$$B = \begin{pmatrix} b_{q-1} & b_{q-2} & \cdots & b_{q-n} \\ b_{2q-1} & b_{2q-2} & \cdots & b_{2q-n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{(n-1)q-1} & b_{(n-1)q-2} & \cdots & b_{(n-1)q-n} \\ b_{nq-1} & b_{nq-2} & \cdots & b_{nq-n} \end{pmatrix},$$

and let

$$W = \begin{pmatrix} w_{q-1} & w_{q-2} & \cdots & w_{q-n} \\ w_{2q-1} & w_{2q-2} & \cdots & w_{2q-n} \\ \vdots & \vdots & \vdots & \vdots \\ w_{(n-1)q-1} & w_{(n-1)q-2} & \cdots & w_{(n-1)q-n} \\ w_{nq-1} & w_{nq-2} & \cdots & w_{nq-n} \end{pmatrix}.$$

Then

$$B = V(f^q) * W. \tag{2.15}$$

We next show how to compute the matrix

$$W^\star = \begin{pmatrix} w_{q-n} & w_{q-n+1} & \cdots & w_{q-1} \\ w_{2q-n} & w_{2q-n+1} & \cdots & w_{2q-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{nq-n} & w_{nq-n+1} & \cdots & w_{nq-1} \end{pmatrix}.$$

Since $\frac{1}{f} = \sum_{i=0}^{\infty} w_i \cdot x^i$, $f \cdot \sum_{i=0}^{\infty} w_i \cdot x^i = 1$. We can set $f_0 = 1$. The coefficient of x^k of 1, $(k > 0)$, is zero, so

$$\sum_{i=0}^{min(n,k)} w_{k-i} f_i = 0,$$

equivalently

$$w_k = - \sum_{i=max(0,k-n)}^{k-1} w_i f_{k-i}.$$

When $k \geq n$,

$$w_k = - \sum_{i=k-n}^{k-1} w_i f_{k-i}. \tag{2.16}$$

For $k \geq 0$, let $W_k = (w_k, w_{k+1}, \cdots, w_{k+n-1})$. and let

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & -f_n \\ 1 & 0 & 0 & 0 & \cdots & -f_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -f_{n-2} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -f_2 \\ 0 & 0 & 0 & \cdots & 1 & -f_1 \end{pmatrix}$$

Then (2.16) gives us a recursion relation:

$$W_{k+1} = W_k \cdot M, \quad k \geq 0.$$

By induction, we see that

$$W_{k+q} = W_k \cdot M^q, \quad k \geq 0.$$

It remains to show how to compute M^q. Let f^* be the reciprocal of f, i.e. $f^*(x) = \sum_{i=0}^{n} f_{n-i}x^i$. Define a map $\psi : \mathbb{F}[x] \to \mathbb{F}^n$ as follows. For any $h(x) \in \mathbb{F}[x]$, suppose $h(x) \equiv h_0 + h_1 x + \cdots + h_{n-1}x^{n-1} \pmod{f^*}$. Then

$$\rho(h(x)) = (h_0, h_1, \cdots, h_{n-1})^T.$$

Theorem 2.7.1.

$$M^j = \left(\rho(x^j), \rho(x^{j+1}), \cdots, \rho(x^{j+n-1})\right).$$

Proof. For any $h(x) \in \mathbb{F}[x]$ and suppose $\rho(h(x)) = (h_0, h_1, \cdots, h_{n-1})^T$. We first show that

$$\rho(h(x) \cdot x) = M \cdot \rho(h(x)).$$

Let $X = (1, x, \cdots, x^{n-1})$. Note that

$$\begin{aligned} h(x) \cdot x &= \sum_{i=0}^{n-1} h_i \cdot x^{i+1} \\ &\equiv \sum_{i=0}^{n-2} h_i \cdot x^{i+1} - h_{n-1} \cdot \sum_{i=0}^{n-1} f_{n-i}x^i \pmod{f^*(x)} \\ &\equiv [(0, h_0, \cdots, h_{n-3}, h_{n-2}) - h_{n-1}(f_n, f_{n-1}, \cdots, f_1)] \cdot X^T \\ &\equiv X \cdot M \cdot h \pmod{f^*(x)}. \end{aligned}$$

That is, for any $h \in \mathbb{F}[x]$,

$$\rho(h(x) \cdot x) = M \cdot h = M \cdot \rho(h(x)).$$

By induction,

$$\rho(h(x) \cdot x^j) = M^j \rho(h(x)), \quad \forall j \geq 1. \tag{2.17}$$

Particularly, for $h(x) = x^i$, $0 \leq i \leq n-1$, then $\rho(h(x)) = (0, \cdots, 0, 1, 0, \cdots)$.

$$\rho(x^{i+j}) = M^j \cdot \rho(x^i) = M^j \cdot (0, 0, \cdots, 1, 0, \cdots)^T,$$

which means $\rho(x^{i+j})$ is the $(i+j+1)st$ row of M^j, $0 \leq i+j \leq n-1$. □

Remark: Let $j = q$, then

$$M^q = \left(\rho(x^q), \rho(x^{q+1}), \cdots, \rho(x^{q+n-1})\right).$$

Consider the matrix W^*. First compute the first row of W^*,

$$(w_{q-n}, w_{q-n+1}, \cdots, w_{q-1})$$

by the equation

$$(w_{q-n}, w_{q-n+1}, \cdots, w_{q-1}) = (w_0, w_1, \cdots, w_{n-1}) M^{q-n}.$$

Each row of W can be obtained by multiplying the previous row in W by M^q. The complexity for computing $x^q \pmod{f^*}$ is $\tilde{O}(n \log q)$, for $x^i \cdot x^q \pmod{f^*}$ is $O(n^2)$. So the complexity for M^q is $\tilde{O}(n \log q + n^2)$.

After W^* is obtained, we can compute B by (2.15) in polynomial time.

Chapter 3

Deterministic factoring via Gröbner bases

3.1 Introduction

In this chapter, we concentrate on the deterministic complexity of factoring univariate polynomials over finite fields with help of Gröbner bases and combinatorics. In Chapter 1, we have defined fibre size which measures the geometric structure of point sets, and we described the structure theorem of Gröbner bases. This gives us a deterministic algorithm to decompose ideals when fibre sizes are not constant. In the following sections, we use Gröbner basis structure theorem to design deterministic algorithms for factoring univariate polynomials.

The chapter is organized as follows. In Section 3.2, we show how to compute Göbner bases of certain ideals in deterministic polynomial time. More precisely, suppose we are given a Göbner basis of a zero-dimensional ideal I in $\mathbb{F}_q[x_1, x_2, \cdots, x_m]$. For any polynomial h, we show that there is a deterministic polynomial time algorithm for computing Göbner bases for $\langle I, h\rangle$ and $(I : h)$ in deterministic polynomial time. We will use this algorithm to compute Göbner bases for all the ideals rising in our method. This result is interesting as it might be useful for general Göbner basis computation.

In Section 3.3, we describe an algorithm to compute r-th roots of elements in extension rings of $\mathbb{F}_q$, provided we are given an r-th nonresidue η in $\mathbb{F}_q$ which can be found in deterministic polynomial time under ERH.

In Section 3.4, we use this deterministic algorithm for computing square roots to introduce a tool called *square selector* and show how it splits ideals.

In Section 3.5, we describe how to use square selectors to decompose various ideals. More precisely, let $f \in \mathbb{F}_p[x]$ be a squarefree polynomial of degree n with all roots lying in $\mathbb{F}_p$. Let $S \subset \mathbb{F}_p$ be the set of roots of f. Define

$$S^{[m]} = \{(a_1, \cdots, a_m) : a_i \in S, a_i \neq a_j, \text{ if } i \neq j\}.$$

We asocciate a *tournament graph* to each point in $S^{[m]}$ and partition S^m according tournament graphs. We study the symmetry of this partition and show how it is related to combinatorial designs and the factorization of f. In particular, when $m = 2$, we can decompose f if S is *not square balanced*, and for when $m = 3$, we show how a connection with Hadamard designs. As a consequence, we obtain a bound on the number of extensions needed to get a proper factor of f, thus improve a previous result of Ivanyos, karpinski and Saxena (2008).

3.2 Computing Gröbner bases

Let I be a 0-dimensional radical ideal in $R = \mathbb{F}[x_1, \cdots, x_m]$. Suppose we know a Gröbner basis for I with respect to some term order. If we join a polynomial $h \in R$ to I, then the Gröbner basis of the new ideal $\langle I, h \rangle$ may be dramatically different. Is it possible to take advantage of this extra information (i.e. the Gröbner basis of I) to get a polynomial

time algorithm for the new ideal? Also, how to compute a Gröbner basis for the colon ideal

$$(I : h) = \{g \in R : gh \in I\}.$$

We show below that the Gröbner bases for both ideals can indeed be computed efficiently. More precisely, we prove the following theorem and the desired algorithms will be clear from the proof.

Theorem 3.2.1. *Let $I \subset R = \mathbb{F}[x_1, \cdots, x_m]$ be a 0-dimensional ideal with a Gröbner basis $G = \{g_1, g_2, \cdots, g_t\}$ under some term order. For any $h \in R$, we have*

(1). $\dim_{\mathbb{F}} R/I = \dim_{\mathbb{F}} R/\langle I, h\rangle + \dim_{\mathbb{F}} R/(I : h)$*; and*

(2). if h is given reduced modulo G, then Gröbner bases for $\langle I, h\rangle$ and $(I : h)$ can be computed deterministically in time polynomial in mN where $N = \dim_{\mathbb{F}} R/I$ is the degree of I.

Proof. Since we know a Gröbner basis for I, we can find the standard monomial basis for R/I:

$$B(I) = \{X^{\alpha_1}, X^{\alpha_2}, \cdots, X^{\alpha_N} = 1\}$$

where we assume the monomials are in decreasing order (under the given term order). Then $B(I)$ is a linear basis for R/I over $\mathbb{F}$. Suppose

$$h \cdot X^{\alpha_i} \equiv \sum_{j=1}^{N} a_{ij} X^{\alpha_j} \pmod{G}, \tag{3.1}$$

where $a_{ij} \in \mathbb{F}$, that is,

$$h \cdot \begin{pmatrix} X^{\alpha_1} \\ X^{\alpha_2} \\ \cdots \\ X^{\alpha_N} \end{pmatrix} \equiv A \begin{pmatrix} X^{\alpha_1} \\ X^{\alpha_2} \\ \cdots \\ X^{\alpha_N} \end{pmatrix} \pmod{G},$$

where $A = (a_{ij})_{N \times N}$ over $\mathbb{F}$. It is important to note that, in the congruence equations above and below as well, when we say "$a \equiv b \pmod{G}$" we mean a can be reduced to b by long division under the given term order. We know from Gröbner basis theory that G is a Gröbner basis for I iff every polynomial in I can be reduced to 0 by G.

Apply Gauss elimination to rows of A with elimination in order starting from the last column to the first column. Then we get an $N \times N$ matrix M such that MA is of the following row echelon form

$$MA = \begin{pmatrix} 0 & u_{1n_1} & * & * & \cdots & u_{1N} \\ 0 & 0 & u_{2n_2} & * & \cdots & u_{2N} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & u_{\ell n_\ell} & \cdots & u_{\ell N} \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

where ℓ is the rank of A and $1 \leq n_1 < n_2 < \cdots < n_\ell \leq N$. Let M_1 be the first ℓ rows of

M and let

$$M_1 \begin{pmatrix} h_1 \\ h_2 \\ \cdots \\ h_N \end{pmatrix} = M_1 A \begin{pmatrix} X^{\alpha_1} \\ X^{\alpha_2} \\ \cdots \\ X^{\alpha_N} \end{pmatrix} = \begin{pmatrix} u_1(x) \\ u_2(x) \\ \cdots \\ u_\ell(x) \end{pmatrix},$$

where $u_i(x) = \sum_{j=n_i}^{N} u_{ij} X^{\alpha_j}$. We claim that

$$G_1 = G \cup \{u_1(x), \cdots, u_\ell(x)\}$$

form a Gröbner basis for $\langle I, h\rangle$ and $\dim_{\mathbb{F}}(R/\langle G_1\rangle) = N - \ell$. In fact, for any $g \in \langle I, h\rangle$, we have

$$g = g_0 + g_1 h, \quad \text{for some } g_0 \in I, g_1 \in \mathbb{F}[x_1, \cdots, x_m].$$

By using G to reduce g, we may assume that

$$g \equiv V \cdot h \pmod{G},$$

where $V = \sum_{i=1}^{N} v_i X^{\alpha_i}$ for some $v_i \in \mathbb{F}$. Then

$$\begin{aligned} g &\equiv (v_1, v_2, \cdots, v_N) h (X^{\alpha_1}, \cdots, X^{\alpha_N})^T \pmod{G} \\ &\equiv (v_1, v_2, \cdots, v_N) A (X^{\alpha_1}, \cdots, X^{\alpha_N})^T \\ &\equiv (v_1, v_2, \cdots, v_N) M^{-1} \cdot MA (X^{\alpha_1}, \cdots, X^{\alpha_N})^T \\ &\equiv (v_1, v_2, \cdots, v_N) M^{-1} \cdot (u_1, \cdots, u_\ell, 0, \cdots, 0)^T \end{aligned}$$

Let $(v_1, v_2, \cdots, v_N) M^{-1} = (c_1, c_2, \cdots, c_\ell, \cdots, c_N) \in \mathbb{F}^N$. Then

$$g \equiv \sum_{i=1}^{\ell} c_i u_i(x) \pmod{G}. \tag{3.2}$$

This shows that every $g \in \langle I, h\rangle$ can be reduced to zero by G_1. Therefore G_1 is a Gröbner basis for $\langle I, h\rangle$.

Next we prove that $\dim_{\mathbb{F}}(R/\langle I, h\rangle) = N - \ell$. Since G_1 is a Gröbner basis for $\langle I, h\rangle$, we have

$$\dim_{\mathbb{F}}(R/\langle I, h\rangle) = \#B(G_1),$$

where $B(G_1)$ denotes the set of monomials not divisible by any leading term of polynomials in G_1. Note that the leading term of u_i is $X^{\alpha_{n_i}}$, which belongs to $B(I) = \{X^{\alpha_1}, \cdots, X^{\alpha_N}\}$. It suffices to prove that, for each $j \in \{1, 2, \cdots, N\} \setminus \{n_1, \cdots, n_\ell\}$, the term X^{α_j} is not the leading term of any polynomial $g \in \langle I, h\rangle$. Suppose otherwise, that is, there is a polynomial $g \in \langle I, h\rangle$ with $\mathrm{lt}(g) = X^{\alpha_j}$. By reducing g modulo G, we may assume that g is linear combination of terms in $B(I)$. However, by (3.2), g should be a linear combination of $u_1, \ldots, u_\ell$. This is impossible, as the leading term of g is different from those of u_i's and the u_i's are in echelon form.

It remains to show how to get a Gröbner basis for $(I : h)$. Let M_2 be the last $t = N - \ell$ rows of M and let

$$M_2 \begin{pmatrix} X^{\alpha_1} \\ \cdots \\ X^{\alpha_N} \end{pmatrix} = \begin{pmatrix} w_1(x) \\ \cdots \\ w_t(x) \end{pmatrix}.$$

We claim that

$$G_2 = G \cup \{w_1(x), \cdots, w_t(x)\}$$

generates $(I : h)$. In fact, we know from the row echelon from of MA that $M_2 A = 0_{\ell \times N}$.

Hence

$$h\begin{pmatrix} w_1(x) \\ \dots \\ w_t(x) \end{pmatrix} \equiv M_2 h \begin{pmatrix} X^{\alpha_1} \\ \dots \\ X^{\alpha_N} \end{pmatrix} \equiv M_2 A \begin{pmatrix} X^{\alpha_1} \\ \dots \\ X^{\alpha_N} \end{pmatrix} = 0 \pmod{G}.$$

We see that $G_2 \subset (I : h)$. To show G_2 is a generating set for $(I : h)$, we only need to show that, for any $g \in R$ such that $gh \in I$, we have $g \in \langle G_2 \rangle$. Suppose

$$g \equiv g_1 X^{\alpha_1} + g_2 X^{\alpha_2} + \cdots + g_N X^{\alpha_N} \pmod{G}.$$

Let $(b_1, \cdots, b_N) = (g_1, \cdots, g_N) M^{-1}$. Then

$$gh \equiv (b_1, \cdots, b_N)\, M X^{\alpha} h \equiv (b_1, \cdots, b_N)\, MAX^{\alpha} = (b_1, \cdots, b_N)\, (u_1, \cdots, u_\ell, 0_{1\times t})^T \pmod{G}.$$

Since $gh \in I$, we have $gh \equiv 0 \pmod{G}$, that is, $\sum_{i=1}^{\ell} b_i u_i \equiv 0 \pmod{G}$. As $u_1, \cdots, u_\ell$ are linearly independent mod G, we see that $b_1 = \cdots = b_\ell = 0$. Hence

$$\begin{aligned} g &\equiv (g_1, \cdots, g_N) X^{\alpha} \\ &\equiv (b_1, \cdots, b_N) M X^{\alpha} \\ &\equiv (b_{\ell+1}, \cdots, b_N) M_2 X^{\alpha} \\ &\equiv \textstyle\sum_{i=1}^{t} b_{\ell+i} w_i(x) \pmod{G}. \end{aligned}$$

Therefore, each$g \in (I : h)$ is congruent to a linear combination of $w_i(x)$'s modulo G. We can use row operations to reduce M_2 to a row echelon form M_2^* such that $M_2^* X^{\alpha}$ has m distinct leading terms in $B(I)$. So $\{G, M_2^* X^{\alpha}\}$ is a Gröbner basis for $(I : h)$. Also, we have $\dim_{\mathbb{F}} R/\,(I : h) = \ell$, since it is impossible that a polynomial $g \in (I : h)$ is linear combination of $M_2^* X^{\alpha}$ and at the same time have leading term different from those of $M_2^* X^{\alpha}$.

Finally, note that the matrix $A = (a_{ij})$ in (3.1) can be computed deterministically in time polynomial in m and N, using border basis. As Gauss eliminations can done in polynomial time in N, (2) follows. □

3.3 Computing η-square roots

In this section, we introduce an algorithm in [Gao 2001] how to compute an r-th root of an arbitrary element, say A, in R for any prime r. If r is coprime to $q-1$ then A^s is an r-th root of A where $sr \equiv 1 \pmod{q-1}$. So it is suffices to show that r is prime and can divide $q-1$. Suppose $q-1 = r^e w$ where $r \nmid w$. Let η be a given r^e-th root of unity in $\mathbb{F}_q$. And under GRH, we can compute η in polynomial time, see in [wang 1959] and [Bach 1997]. Note that r-th root of A exists only if $A = 0$ or $A^{\frac{(q-1)}{r}} = 1$. We write $A = \eta^u B$ for some $u \leq r^e$ and $B \in \mathbb{F}_q$. Suppose $B^w = 1$. Then $A^{1/r}$ exists iff $r \mid u$.

We want to find an r-th root of A. If A is not invertible in R, we can decompose R to be two parts, one of them is $R_A = \{CA : C \in R\}$. Let I be the identity element of R_1, then $A\dot{I}$ is invertible in R_1. An r-th root of $A\dot{I}$ in R_1 is an r-th root of A in R. Thus we can assume that A is invertible in R.

Find t and s such that $sr^e + tw = 1$. Then

$$A = A^{tw} A^{sr^e}.$$

We only need to find an r-th root of A^{tw}. Denote $A^{tw} = A_1$. Since $A_1^{r^e} = 1$, we can use Pohlig and Hellman's algorithm to find k, u such that

$$A_1^{r^k} = \eta^u.$$

If $k = 0$, then $\eta^{u/r}$ is an r-th root of A_1. Otherwise, we can find a zero divisor of R and decompose R as follows. Since $A_1^{r^{k-1}}\eta^{-u/r} \notin \mathbb{F}_q$ but $(A_1^{r^{k-1}}\eta^{-u/r})^r = 1$, $A_1^{r^{k-1}}\eta^{-u/r}$ is an r-th root of unity. So there are $r+1$ distinct r-th roots of unity in R, i.e. $1, \zeta, \cdots, \zeta^{r-1}$, where $\zeta = \eta^{r^{e-1}}$. So there exists some $1 \leq i \leq r$ such that $A_1^{r^{k-1}}\eta^{-u/r} - \zeta^i$ is a zero divisor in R. We find this i by checking. Let $D = A_1^{r^{k-1}}\eta^{-u/r} - \zeta^i$, and R can be decomposed to the direct sum of two subrings

$$R_1 = RD = \{DC : C \in R\},\ R_2 = \{C \in R : DC = 0\}.$$

Then $A_1 = A_{11} + A_{12}$, where $A_{11} \in R_1$ and $A_{12} \in R_2$. And proceed recursively in R_1 and R_2 to compute r-th roots of A_{11} and A_{12}. The whole process can be done in time polynomial in $r, nand \log q$.

We denote this algorithm as σ_r. Then σ_r has properties as belows.

Proposition 3.3.1 (Gao 2001)**.** *Given a primitive r^l-th root η of unity in $\mathbb{F}_q$ where $q - 1 = r^l Q$, $l \geq 1$ and $\gcd(r, Q) = 1$, the algorithm σ_r runs in polynomial time in $r, \log q$ and $n = \dim R$. Furthermore, σ_r has the following properties:*

(a) $\sigma_r(aA) = \sigma_r(a)A$, *if $A \in R$ is idempotent, i.e. $A^2 = A$.*

(b) $\sigma_r(A + B) = \sigma_r(A) + \sigma_r(B)$, *if $A, B \in R$ are orthogonal, i.e. $AB = 0$.*

(c) Let $\mu_1, \cdots, \mu_n$ be primitive idempotents in R and $A = \sum_{i=1}^n a_i\mu_i$, where $a_i \in \mathbb{F}_q$, then

$$\sigma_r(A) = \sum_{i=1}^{n} \sigma_r(a_i)\mu_i.$$

(d) Let $a = \eta^c\theta$ where $\theta \in \mathbb{F}_q$ with $\theta^Q = 1$ and $1 \leq c < r^l$. Then $\sigma_r(a^r) = a$ iff $c < r^{l-1}$.

An element $a \in \mathbb{F}_q$ is called an *η-square* if $\sigma_2(a^2) = a$.

Lemma 3.3.2. *Let $\eta \in \mathbb{F}_q$ of order 2^l where 2^l is the highest power of 2 dividing $q-1$. Then, for any $a \in \mathbb{F}_q$,*

$$\sigma_2(a^2) = \begin{cases} a, & \textit{if } a \textit{ is a } \eta\textit{-square} \\ -a, & \textit{otherwise.} \end{cases}$$

Proof. Suppose $a = \eta^m a_1$, where a_1 has odd order and $m < 2^l$ has binary representation as

$$m = 2^{l-1}m_{l-1} + 2^{l-2}m_{l-2} + \cdots + 2m_1 + m_0,$$

where $m_i \in \{0,1\}, 0 \le i \le l-1$. Then

$$a^2 = \eta^{2m}a_1^2 = \eta^{2^{l-1}m_{l-2}+\cdots+2^2m_1+2m_0}a_1^2,$$

thus

$$\sigma_2(a^2) = \eta^{2^{l-2}m_{l-2}+\cdots+2m_1+m_0}a_1 = \begin{cases} a, & \text{if } m_{l-1} = 0, \\ -a, & \text{if } m_{l-1} = 1. \end{cases}$$

where we used the fact that $\eta^{2^{l-1}} = -1$. □

Example 3.3.3. *In $R = \mathbb{F}_p$ where $p \equiv 3 \pmod 4$, we have $\sigma_2(b) = b^{\frac{p+1}{4}}$, if $b \in \mathbb{F}_p$ is a square. Here the nonresidue η is -1. One can check that*

$$\sigma_2(a^2) = \begin{cases} a, & \textit{if } a \textit{ is a square in} \mathbb{F}_p, \\ -a, & \textit{otherwise.} \end{cases}$$

Lemma 3.3.4. *Let $f = \prod_{i=1}^n (x - a_i)$ where $a_i \in \mathbb{F}_p$ are distinct. Let*

$$\xi_i = \frac{f(x)}{(x-a_i)f'(a_i)} \in \mathbb{F}_p[x],\ 1 \le i \le n.$$

Let $R_1 = \mathbb{F}_p[x,y]/ < f(x), f(y) >$. *Then*

$$\sigma((x-y)^2) \equiv \sum_{1\le i,j\le n} \sigma((a_i-a_j)^2)\xi_i(x)\xi_j(y) \pmod{\langle f(x), f(y)\rangle}.$$

Proof. Note that

$$\xi_i(a_j) = \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

We see that ξ_i are primitive idempotents modulo $f(x)$, and

$$x \equiv a_1\xi_1 + \cdots + a_n\xi_n \pmod{f(x)}.$$

Then R_1 has a basis consists of $\{\xi_i(x)\xi_j(y) : 1 \le i,j \le n\}$ and

$$\begin{aligned} x &\equiv a_1\xi_1(x) + \cdots + a_n\xi_n(x) = \sum_{1\le i,j\le n} a_i\xi_i(x)\xi_j(y) \pmod{\langle f(x), f(y)\rangle}, \\ y &\equiv a_1\xi_1(y) + \cdots + a_n\xi_n(y) = \sum_{1\le i,j\le n} a_i\xi_i(x)\xi_j(y) \pmod{\langle f(x), f(y)\rangle}. \end{aligned}$$

By using the property of primitive idempotent, we can write in R_1,

$$x - y = \sum_{1\le i,j\le n} (a_i - a_j)\xi_i(x)\xi_j(y).$$

So

$$\sigma((x-y)^2) = \sum_{1\le i,j\le n} \sigma((a_i-a_j)^2)\xi_i(x)\xi_j(y).$$

□

The coefficients $\sigma((a_i-a_j)^2)$ are computed implicitly without knowing the basis $\xi_i(x), \xi_j(y)$.

3.4 The square selector

We now introduce a useful tool for splitting ideals. In the following proof, we shall use the following property: For any radical ideal I and any $f, g \in \mathbb{F}_p[x_1, x_2, \cdots, x_m]$, we have

$$f \equiv g \pmod{I} \text{ iff } f(A) = g(A), \forall A \in V(I).$$

Lemma 3.4.1. *Let $I \subseteq \mathbb{F}_p[x_1, x_2, \cdots, x_m]$ be a 0-dimensional radical ideal with all solutions lying in $\mathbb{F}_p^m$. Fix any $1 \leq i \neq j \leq m$. Let*

$$h(x_i, x_j) = \frac{1}{2}(x_i + x_j + \sigma((x_i - x_j)^2)) \in R = \mathbb{F}_p[x_1, x_2, \cdots, x_m]/I, \tag{3.3}$$

where σ is the deterministic algorithm described in the previous section for computing square root in R, with a given quadratic nonresidue $\eta \in \mathbb{F}_p$. Let $J = \langle I, x_i - h \rangle$. Then

$$V(J) = \{(a_1, \cdots, a_m) \in V(I) |\ a_i - a_j \text{ is } \eta\text{-square}\}.$$

That is, $V(J)$ is the subset of points $A = (a_1, \cdots, a_m) \in V(I)$ such that $a_i - a_j$ is η-square in $\mathbb{F}_p$.

Proof. Let $V(I) = \{A_1, \cdots, A_t\} \subset \mathbb{F}_p^m$. There exist polynomials $\xi_1, \cdots, \xi_t \in \mathbb{F}_p[x_1, \cdots, x_n]$ such that

$$\xi_i(A_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Then ξ_i's are the primitive idempotents in R satisfying the properties:

$$\xi_i \xi_j = \begin{cases} \xi_i, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Let $A_i = (a_{i1}, a_{i2}, \cdots, a_{im}) \in \mathbb{F}_p^m$, $1 \leq i \leq t$. By the condition for two polynomials to be congruent modulo I, we have

$$x_j \equiv \sum_{k=1}^{t} a_{kj}\xi_k \pmod{I}, \quad 1 \leq j \leq m.$$

By Proposition 3.3.1, we have

$$h(x_i, x_j) \equiv \sum_{k=1}^{t} h(a_{ki}, a_{kj})\xi_k \pmod{I}.$$

So

$$x_i - h(x_i, x_j) \equiv \sum_{k=1}^{t} (a_{ki} - h(a_{ki}, a_{kj}))\xi_k \pmod{I}.$$

Note that, for any η-square c in $\mathbb{F}_p$, we have $(\sigma(c))^2 = c$. Hence, for $a, b\mathbb{F}_p$,

$$h(a,b) = \begin{cases} a, & \text{if } a-b \text{ is an } \eta\text{-square,} \\ b, & \text{if } b-a \text{ is an } \eta\text{-square.} \end{cases}$$

It follows that the value of $x_i - h(x_i, x_j)$ at A_k is

$$(x_i - h(x_i, x_j))(A_k) = a_{ki} - h(a_{ki}, a_{kj}) = \begin{cases} 0, & \text{if } a_{ki} - a_{kj} \text{ is an } \eta - square, \\ a_{ki} - a_{kj} \neq 0, & otherwise. \end{cases}$$

That is, $A_k \in V(J)$ iff $a_{ki} - a_{kj}$ is an η-square. □

Corollary 3.4.2. *With the same assumption as in Lemma 3.4.1. Let* $J_1 =< I, x_i - h >$ *and* $J_2 =< I, x_j - h >$ *Then* $I = J_1 \cap J_2$.

The above corollary does not give a proper decomposition of I only when either all $a_{ki} - a_{kj}$ are η-squares or all $a_{ki} - a_{kj}$ are not η-squares. We call the polynomial $h(x_i, x_j)$ in the equation (3.3) **a square selector**. Note that such a square selector can be computed

deterministically in time polynomial in the dimension of the ring R over $\mathbb{F}_p$ (provided a quadratic nonresidue $\eta \in \mathbb{F}_p$ is given). Also, by Theorem 3.2.1, when a Gröbner basis for I is known, Gröbner bases for J_1 and J_2 can be computed in deterministic polynomial time.

3.5 Geometric structure and factoring

3.5.1 Partition and tournament graphs of points

For any point $A = (a_1, \cdots, a_m) \in \mathbb{F}_p^m$, where a_i's are distinct, we associate it with a directed graph G_A as follows: The vertex set is $\{1, 2, \cdots, m\}$ and, for each $1 \leq i \neq j \leq m$, there is an edge from i to j iff $a_i - a_j$ is an η-square. G_A is called the squareness graph of A. Since $a_i - a_j$ is an η-square iff $a_j - a_i$ is not an η-square, the squareness graph of a point is a tournament graph, that is, there is exactly one directed edge between each pair i and j.

In the following, we represent the squareness graph of a point by a binary string. For $a \in \mathbb{F}_p$, define

$$\delta(a) = \begin{cases} 0, & \text{if } a \text{ is an } \eta\text{-square,} \\ 1, & \text{otherwise.} \end{cases}$$

Then, for any point $A = (a_1, \cdots, a_m) \in \mathbb{F}_p^m$, define

$$\delta(A) = (\delta(a_1 - a_2)\delta(a_1 - a_3)\delta(a_2 - a_3) \cdots \delta(a_1 - a_m)\delta(a_2 - a_m) \cdots \delta(a_{m-1} - a_m)),$$

which has length $\ell = \binom{m}{2}$.

Let $f(x) = \prod_{a \in S}(x - a)$where $S \subset \mathbb{F}_p$ is a subset of cardinality n. For each $a \in S$, define

$$B_a(S) = \{b \in S : a - b \text{ is an } \eta\text{-square and } b \neq a\},$$

and

$$\bar{B}_a(S) = \{b \in S : a - b \text{ is not an } \eta\text{-square}\}.$$

Example 3.5.1. *Let* $A = (a, b, c, d)$ *satisfy*

$$a \in S, b \in B_a, c \in B_a \cap B_b, d \in B_a \cap B_b \cap B_c.$$

Then its squareness graph is depicted as Figure 3.1

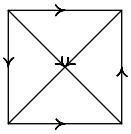

Figure 3.1: $\delta(A) = (000000)$

Example 3.5.2. *Let* $A = (a, b, c, d)$ *satisfy*

$$a \in S, b \in B_a, c \in \bar{B}_a \cap B_b, d \in B_a \cap B_b \cap \bar{B}_c.$$

Then its squareness graph is depicted as Figure 3.2

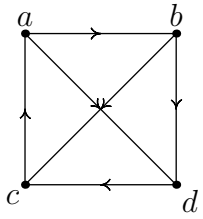

Figure 3.2: $\delta(A) = (010001)$

Define

$$S^{[m]} = \{(a_1, \cdots, a_m) : a_i \in S, a_i \neq a_j \text{ if } i \neq j\}.$$

We partition $S^{[m]}$ into subsets according to their squareness graphs. More precisely, for any

$\tau \in \{0,1\}^{\ell}$, where $\ell = \binom{m}{2}$, define

$$P_\tau = \left\{ A \in S^{[m]} : \delta(A) = \tau \right\}.$$

Then

$$S^{[m]} = \bigcup_{\tau} P_\tau.$$

Let $I_\tau \subseteq \mathbb{F}_p[x_1, \cdots, x_n]$ the vanishing ideal of P_τ. The next lemma shows that we can get a Gröbner basis for I_τ polynomial time.

Lemma 3.5.3. *Given $f(x) = \prod_{a \in S}(x-a)$, where $S \subseteq \mathbb{F}_p$ has size n, and any tournament graph τ on $\{1, 2, \cdots, m\}$, a Gröbner basis for the vanishing ideal of P_τ can be computed deterministically in time polynomial in $\log p$ and n^m.*

Proof. let $I = \langle f(x_1), \cdots, f(x_m) \rangle$ with dimension n^m. Then $\{f(x_1), \cdots, f(x_m)\}$ is Gröbner basis for I under any order. By lemma 3.2.1, we can compute $I : (x_i - x_j)$ for each pair x_i and x_j in polynomial time in $n^m \log p$. So we can compute

$$I : \prod_{1 \le i \ne j \le m} (x_i - x_j),$$

iteratively. Also, we can compute $h(x_i, x_j) \in \mathbb{F}_p[x_1, \cdots, x_n]/I$ in polynomial time by σ-algorithm. For every pair x_i, x_j, if there is an edge from x_i to x_j in τ, we compute

$$I := \langle I, x_i - h(x_i, x_j) \rangle,$$

else

$$I := \langle I, x_j - h(x_i, x_j) \rangle.$$

Thus we get a vanishing ideal of P_τ in deterministic polynomial time in $\{\log p, n^m\}$. $\square$

If P_τ is not uniform, we can decompose it by the structure theorem 1.3.5. In the following, we discuss when all the P_τ can be uniform for small m. Then we talk about the symmetry properties among different P_τ's.

3.5.2 Uniformness and Hadamard design

In this section, we discuss when P_τ are uniform and a connection to combinatorial designs.

3.5.2.1 $m = 2$: Square balanced sets

For $m = 2$, we have $\tau = 0$ or 1. Then

$$S^{[2]} = P_0 \cup P_1, \tag{3.4}$$

where

$$P_0 = \{(a, b) : a \in S, b \in B_a\} \text{ and } P_1 = \left\{(a, b) : a \in S, b \in \bar{B}_a\right\}.$$

Note that the set $S^{[2]}$ corresponds to the ring

$$R = \mathbb{F}_p[x, y] / \left\langle f(x), \frac{f(y) - f(x)}{y - x} \right\rangle.$$

The vanishing ideals of P_0 and P_1 are

$$J_0 = \left\langle f(x), \frac{f(y) - f(x)}{y - x}, x - h(x, y) \right\rangle, \quad J_1 = \left\langle f(x), \frac{f(y) - f(x)}{y - x}, y - h(x, y) \right\rangle.$$

We call S *square balanced* if P_0 is uniform, that is, $|B_a|$ is the same for all $a \in S$.

Lemma 3.5.4. *(a). If S is square balanced, then $|B_a| = \frac{n-1}{2}$ for all $a \in S$; and*

(b). P_0 is uniform iff P_1 is uniform.

Proof. (a). For any $a, b \in S$, either $a \in B_b$ or $b \in B_a$. Since $a \in B_b$ is equivalent to $b \in \bar{B}_a$, that is, either $(a - b)$ or $(b - a)$ is η-square but not both. There are $\binom{n}{2}$ square relations of the form $b \in B_a$. So

$$\sum_{a \in S}^{n} |B_a| = n(n-1)/2.$$

If $|B_a| = \lambda$, for all a, then $|B_a| = \frac{n-1}{2}$.

(b). Note that

$$S = \{B_a\} \cup \left\{\bar{B}_a\right\} \cup \{a\}.$$

If P_0 is uniform, then $|B_a|$=$\frac{n-1}{2}$ for all a, so $|\bar{B}_a|$=$\frac{n-1}{2}$. That is, P_1 is uniform. Similarly for the reverse direction. □

Corollary 3.5.5. *If the size of S is even, then S can not be square balanced. So a factor of f can be found in deterministic polynomial time.*

Now assume S is square balanced. The Gröbner basis of $I_0 = \langle I, x - h(x, y)\rangle$ under elimination order $x \prec y$ is of the form $\langle f(x), g_0(x, y)\rangle$, where the leading term of $g_0(x, y)$ is $y^{(n-1)/2}$. The Gröbner basis of $I_1 = \langle I, y - h(x, y)\rangle$ under elimination order $x \prec y$ is of the form $\langle f(x), g_1(x, y)\rangle$, where the leading term of $g_1(x, y)$ is $y^{(n-1)/2}$ by lemma (3.5.4) as well. Then

$$I = \langle f(x), g_0(x, y)\rangle \cap \langle f(x), g_1(x, y)\rangle. \tag{3.5}$$

3.5.2.2 $m = 3$: Hadamard designs

$S^{[3]}$ can be partitioned into the following union according to the squareness graphs:

$$S^3 = \bigcup_{\tau \in \{0,1\}^3} P_\tau,$$

where

$$P_{000} = \{(a \in S, b \in B_a, c \in B_a \cap B_b)\}, \quad P_{001} = \{(a \in S, b \in B_a, c \in B_a \cap \bar{B}_b)\},$$
$$P_{010} = \{(a \in S, b \in B_a, c \in \bar{B}_a \cap B_b)\}, \quad P_{011} = \{(a \in S, b \in B_a, c \in \bar{B}_a \cap \bar{B}_b)\},$$
$$P_{100} = \{(a \in S, b \in \bar{B}_a, c \in B_a \cap B_b)\}, \quad P_{101} = \{(a \in S, b \in \bar{B}_a, c \in B_a \cap \bar{B}_b)\},$$
$$P_{110} = \{(a \in S, b \in \bar{B}_a, c \in \bar{B}_a \cap B_b)\}, \quad P_{111} = \{(a \in S, b \in \bar{B}_a, c \in \bar{B}_a \cap \bar{B}_b)\}.$$

We discuss below possible symmetry properties of this partition.

Lemma 3.5.6. *Suppose P_{000} is uniform. Then $|B_a \cap B_b| = (n-3)/4$ for $a \in S$ and $b \in B_a$.*

Proof. P_{000} is uniform means that S and B_a are all square balanced for all $a \in S$. By lemma 3.5.4, $|B_a|=\frac{n-1}{2}$, thus

$$|B_a \cap B_b| = \frac{|B_a| - 1}{2} = \frac{n-3}{4},$$

for every $a \in S, b \in B_a$. □

Lemma 3.5.7. *If P_{000} is uniform, then P_τ is uniform for all $\tau \in \{0,1\}^3$.*

Proof. Suppose P_{000} is uniform and $\lambda = \frac{n-3}{4}$. First we show that P_{100} is uniform. Since P_{000} is uniform, we have

$$|B_a \cap B_b| = \lambda, \forall a \in S, b \in B_a,$$

which is the same as

$$|B_b \cap B_a| = \lambda, \forall b \in S, a \in \bar{B}_b.$$

By renaming the variables, we have

$$|B_a \cap B_b| = \lambda, \forall a \in S, b \in \bar{B}_a,$$

which means that P_{100} is uniform. Now we show that P_{001} is uniform. For any $b \in B_a$,

$$|B_a| = |B_a \cap B_b| + |B_a \cap \bar{B}_b| + |\{b\}| = \frac{n-1}{2}.$$

Since $|B_a \cap B_b| = \frac{n-3}{4}$ by lemma 3.5.6, we have $|B_a \cap \bar{B}_b| = \frac{n-3}{4}$. So P_{001} is uniform. It is similar to show P_{011}, P_{101}, P_{111} are uniform. Next we show $P_{010} = \frac{n+1}{4}$. Since $a \notin B_b$, we have

$$|B_b| = |B_a \cap B_b| + |\bar{B}_a \cap B_b| = \frac{n-1}{2},$$

but $|B_a \cap B_b| = \frac{n-3}{4}$, thus

$$|\bar{B}_a \cap B_b| = \frac{n+1}{4}.$$

It is similar to show P_{110} is uniform. □

The correspondence of P_τ and its fibre sizes at each level are listed as follows:

$$\begin{array}{lccc} & a & b & c \\ P_{000} = \{(a \in S, b \in B_a, c \in B_a \cap B_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \\ P_{001} = \{(a \in S, b \in B_a, c \in B_a \cap \bar{B}_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \\ P_{010} = \{(a \in S, b \in B_a, c \in \bar{B}_a \cap B_b)\}: & n & \frac{n-1}{2} & \frac{n+1}{4} \\ P_{011} = \{(a \in S, b \in B_a, c \in \bar{B}_a \cap \bar{B}_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \\ P_{100} = \{(a \in S, b \in \bar{B}_a, c \in B_a \cap B_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \\ P_{101} = \{(a \in S, b \in \bar{B}_a, c \in B_a \cap \bar{B}_b)\}: & n & \frac{n-1}{2} & \frac{n+1}{4} \\ P_{110} = \{(a \in S, b \in \bar{B}_a, c \in \bar{B}_a \cap B_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \\ P_{111} = \{(a \in S, b \in \bar{B}_a, c \in \bar{B}_a \cap \bar{B}_b)\}: & n & \frac{n-1}{2} & \frac{n-3}{4} \end{array}$$

In combinatorial design theory, a system of subsets B_i, $1 \leq i \leq n$, of a set S with cardinality n is called a Hadamard design of order n, if

$$|B_i| = \frac{n-1}{2},\ 1 \leq i \leq n,$$

and

$$|B_i \cap B_j| = \frac{n-3}{4},\ 1 \leq i < j \leq n.$$

For many values of n, there exist Hadamard design of order n. We give two examples.

Example 3.5.8. *Let n be a prime with $m \equiv 3 \pmod 4$, and $S = \mathbb{Z}/(n)$. For $0 \leq a \leq n-1$, define*

$$B_a = \{b \in S : a - b \textit{ is square in } \mathbb{F}_n\}.$$

Then B_a's form an Hadamard design of order n.

Example 3.5.9. *Let $n = 2^\ell - 1$ and $S = \mathbb{F}_2^\ell \backslash \{(0, 0, \cdots, 0)\}$. For each $a = (a_1, \cdots, a_\ell) \in$*

S, define

$$B_a = \{b = (b_1, \cdots, b_\ell) \in S : a_1 b_1 + \cdots + a_\ell b_\ell = 0\}.$$

Then one can check that

$$|B_a| = \frac{n-1}{2}, \text{ and } |B_a \cap B_b| = \frac{n-3}{4} \text{ for all } a \neq b.$$

Since Hadamard designs exist, it is possible that all the eight P_τ are uniform. Here's a concrete example.

Example 3.5.10. *Let*

$$\begin{aligned} P = \quad & \{[1,2,3],[1,3,4],[1,4,2],[2,3,6],[2,5,3],[2,6,5],[3,4,7], \\ & [3,6,4],[3,7,6],[4,2,5],[4,5,7],[4,7,2],[5,1,3],[5,3,7], \\ & [5,7,1],[6,1,4],[6,4,5],[6,5,1],[7,2,6],[7,1,2],[7,6,1]\}. \end{aligned}$$

Then

$$\begin{aligned} & B_1 = \{2,3,4\}, B_2 = \{3,5,6\}, B_3 = \{4,6,7\}, B_4 = \{2,5,7\}, \\ & B_5 = \{1,3,7\}, B_6 = \{1,4,5\}, B_7 = \{1,2,6\}, \end{aligned}$$

and

$$\begin{array}{lll} B_1 \cap B_2 = \{3\} & B_1 \cap B_3 = \{4\} & B_1 \cap B_4 = \{2\} \\ B_2 \cap B_3 = \{6\} & B_2 \cap B_5 = \{3\} & B_2 \cap B_6 = \{5\} \\ B_3 \cap B_4 = \{7\} & B_3 \cap B_6 = \{4\} & B_3 \cap B_7 = \{6\} \\ B_4 \cap B_2 = \{5\} & B_4 \cap B_5 = \{7\} & B_4 \cap B_7 = \{2\} \\ B_5 \cap B_1 = \{3\} & B_5 \cap B_3 = \{7\} & B_5 \cap B_7 = \{1\} \\ B_6 \cap B_1 = \{4\} & B_6 \cap B_5 = \{1\} & B_6 \cap B_5 = \{2\} \\ B_7 \cap B_1 = \{2\} & B_7 \cap B_2 = \{6\} & B_7 \cap B_6 = \{1\} \end{array}$$

Now we show that it is possible to further partition some of the P_τ via another

symmetry property. Note that P_{010} and P_{101} have an automorphism σ_3 mapping (x, y, z) to (y, z, x). By Ronyai lemma as follows, P_{010} and P_{101} can be decomposed. Consider P_{010}. The squareness graph of P_{010} is a 3-cycle. This means P_{010} is invariant under the map: $(a, b, c) \mapsto (b, c, a)$. This induces an automorphism in $\mathbb{F}_p[x, y, z]/I_3$. We will show P_{010} can be decomposed to at least 3 disjoint parts. First of all, P_{010} can not be empty, otherwise by

$$|B_b| = |B_a \cap B_b| + |\bar{B}_a \cap B_b| = \frac{n-1}{2},$$

if $|\bar{B}_a \cap B_b| = 0$, that means

$$|B_a \cap B_b| = |B_b|.$$

But $a \in B_b$, a is not in B_a, $B_a \cap B_b \subsetneq B_b$, contradiction.

Lemma 3.5.11 (Ronyai 1992)**.** *Let A be an algebra over $\mathbb{F}_p$ with dimension t. Given a nontrivial automorphism of A, we can find in deterministic time $(t + \log p)^{o(1)}$ an ideal $I \subsetneq A$.*

Since P_{010} has an automorphsim, we apply Ronyai lemma to decompose the vanishing ideal of P_{010} to subideals until each corresponding split variety doesn't have an automorphism on itself .

Lemma 3.5.12. *Suppose S is square balanced and P_{010} has a finest partition by applying Ronyai's lemma as*

$$P_{010} = Q_1 \cup Q_2 \cup \cdots \cup Q_t.$$

Then $3|t$.

Proof. If $\exists i$ such that $\sigma_3(Q_i) \cap Q_i \neq \emptyset$, then we can decompose Q_i, contradicts. So for any Q_i, there exist Q_ℓ and Q_k such that

$$\sigma_3(Q_i) = Q_\ell, \ \textit{and} \ \sigma_3^2(Q_i) = Q_k.$$

So $3|t$. $\square$

Suppose P_{010} can be partitioned to at least 3 parts as

$$P_{010} = P_{21} \cup P_{22} \cup P_{23}.$$

For each point $(a, b, c) \in P_{21}$, $(b, c, a) \in P_{22}$ and $(c, a, b) \in P_{23}$. So three parts have the same size. We consider 4 cases of the structure of P_{2i}'s, $1 \leq i \leq 3$.

1, P_{2i} is not uniform at first level, we can factor f.

2, P_{2i} is not uniform at second level or can be decomposed at second level, then we can reduce $\frac{n-1}{2}$ to $\frac{n-1}{4}$.

3, If P_{2i} remains uniform at first and second levels but not in the third level, for some i. And the fibre sizes at first and second levels are $n, \frac{n-1}{2}$ respectively. Then we can also reduce $\frac{n-1}{2}$ to $\frac{n-1}{4}$.

4, If P_{2i} remains uniform at all levels but not in the third level, for some i. And the fibre sizes are $n, \frac{n-1}{2}$ respectively. Then let the third level fibre size be k such that:

$$n\frac{n-1}{2}\frac{n+1}{4} = 3n\frac{n-1}{2}k.$$

So $k = \frac{n+1}{12}$.

To conclude, in all four cases, we can either decompose f, or reduce n to $\frac{n-1}{4}$ by doing one extension, or reduce n to $\frac{n+1}{12}$ by doing two extension. So we can reduce the levels needed to find a factor of f from $\log n$ to $\frac{\log n}{\log_4 12}$.

Compared to the extension needed in Evdokimov (1992), we reduce the levels of extension as follows.

Theorem 3.5.13. *Let $\ell(n)$ be the extension needed to find a factor of polynomial of degree n, then $\ell(n) \leq \frac{\log_2 n}{\log_4 12}$.*

Proof. By previous argument, that $\ell(n) = 1 + \ell(n/4)$ or $\ell(n) = 2 + \ell(n/12)$. So $\ell(n) \leq 2 + \ell(n/12)$.

□

This result reduces the number of extensions $\frac{\log_2 n}{\log_4 8}$ in [Ivanyos, karpinski, and Saxena, 2008].

3.5.2.3 $m = 4$: transitive patterns

For every τ and $\sigma \in S_m$, where S_m is the permutation group on m many elements, define $\sigma(\tau)$ to be a new graph with vertices $\{1, 2, \cdots, m\}$ and edges defined as follows. For two vertices i, j in $\sigma(\tau)$, there is an edge from i to j iff there is an edge from $\sigma^{-1}(i)$ to $\sigma^{-1}(j)$ in τ. $\sigma(\tau)$=$\tau(\sigma(x_1, x_2, \cdots, x_m))$ is a new square relation generated from τ. We call the whole class as $Trans(\tau)$.

Example 3.5.14. *For $\sigma \in S_m$, and any point $A = (a_1, \cdots, a_m)$, $\sigma(A) = (a_{\sigma(1)}, \cdots, a_{\sigma(m)})$.*

Example 3.5.15. *Consider S^4. Let $\tau_1 = (000000)$. Then $Trans(\tau_1)$=*

$$\begin{pmatrix} (000000) & (000001) & (000011) & (000111) \\ (001000) & (001010) & (001011) & (001111) \\ (110000) & (110100) & (110101) & (110111) \\ (111000) & (011010) & (111110) & (111111) \\ (011000) & (100001) & (011110) & (011111) \\ (100000) & (111100) & (100101) & (100111) \end{pmatrix}$$

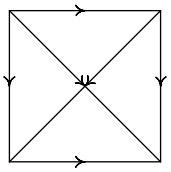

Figure 3.3: Graph all τ's from $Trans(\tau_1)$ which doesn't have cycle

Let $\tau_2 = (010001)$. *Then* $Trans(\tau_2)$=

$$\begin{pmatrix} (010001) & (010011) & (000100) & (000110) \\ (101010) & (101011) & (001100) & (001101) \\ (010100) & (010101) & (110010) & (110011) \\ (101100) & (101110) & (111001) & (111011) \\ (010010) & (010110) & (011001) & (011101) \\ (101001) & (101101) & (100010) & (100110) \end{pmatrix}$$

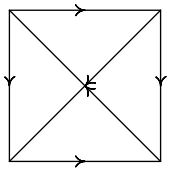

Figure 3.4: Graph for all τ from $Trans(\tau_2)$ which have two cycles

Let τ_3=(000010). *Then* $Trans(\tau_2)$=

$$\begin{pmatrix} (000010) \\ (001001) \\ (110001) \\ (111010) \\ (011100) \\ (100100) \\ (010111) \\ (101111) \end{pmatrix}$$

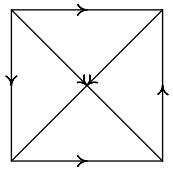

Figure 3.5: Graph for all τ's from $Trans(\tau_3)$ which have one cycle

Let τ_4=(010000). *Then* $Trans(\tau_4)$=

$$\begin{pmatrix} (010000) \\ (000101) \\ (001110) \\ (110110) \\ (111101) \\ (011011) \\ (100011) \\ (101000) \end{pmatrix}$$

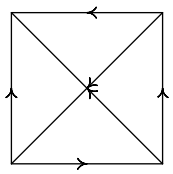

Figure 3.6: Graph for all τ's from $Trans(\tau_4)$ which have one cycle

Then S^4 an be decomposed into 2^6 components. That is

$$S^4 = \bigcup_{\tau \in Trans(\tau_i), 1 \leq i \leq 4} P_\tau,$$

where P_τ=$\{p \in S^4 :$ p satisfies square relation $\tau\}$.

Lemma 3.5.16. *Let G be a tournament graph on n vertices. If $Auto(G) = \{1\}$, then we can get $n!$ graphs by permuting vertices of G.*

We say a point set P_τ is uniform, if it is uniform from i-th coordinator to $i+1$-th coordinator, $1 \leq i \leq m-1$.

Lemma 3.5.17. *If P_{000000} is uniform, then P_{100000} is uniform.*

Proof. We just show the first one. Let τ be uniform. That is, there is a constant C such that

$$|B_a \cap B_b \cap B_c| = C, \forall a \in S, b \in B_a, c \in B_a \cap B_b.$$

By exchanging and rename a and b in $\{b \in S, a \in \bar{B}_b, c \in B_b \cap B_a\}$ to be

$$a \in S, b \in \bar{B}_a, c \in B_a \cap B_b.$$

Then we proved $((0 \text{ or } 1)00000)$ is uniform.

□

Lemma 3.5.18. $P_{\sigma(\tau)} = \sigma(P_\tau) = \{\sigma(p) : A \in P_\tau\}$ *. Let* σ *be a permutation fixing* m*, i.e*

$$\sigma(1, 2, \cdots, m-1, m) = (\sigma(1), \cdots, \sigma(m-1), m).$$

Then P_τ *is uniform at level* m *iff* $P_{\sigma(\tau)}$ *is uniform at level* m*.*

Proof. By definition, $\sigma(A) = (a_{\sigma(1)}, \cdots, a_{\sigma(m-1)}, a_m)$, for any $A \in P_\tau$. Then

$$(a_1, \cdots, a_{m-1}, a_m) \in P_\tau \text{ iff } (a_{\sigma(1)}, \cdots, a_{\sigma(m-1)}, a_m) \in P_{\sigma(\tau)}.$$

This implies that

$$a_m \in \pi^{-1}(a_1, \cdots, a_{m-1}) \text{ iff } a_m \in \pi^{-1}(a_{\sigma(1)}, \cdots, a_{\sigma(m-1)}).$$

So

$$\pi^{-1}(a_1, \cdots, a_{m-1}) = \pi^{-1}(a_{\sigma(1)}, \cdots, a_{\sigma(m-1)}).$$

Hence the same fibre size.

□

Lemma 3.5.19. *If* P_{000000} *is uniform, then* P_τ *is uniform for all* τ*'s* $\in$ *Trans*(τ_1) *are uniform.*

Proof. By lemma 3.5.18, we know all P_τ's where τ's are in the same column in Trans(τ_1) are equivalent to be uniform. So we only need to show that P_τ's, where τ's from the first row, are uniform. They are P_{000001}, P_{000011},P_{000111} are uniform. We first show that if P_{000000} is uniform, then P_{000001} is uniform. Since $c \in B_a \cap B_b$,

$$B_a \cap B_b \cap B_c + B_a \cap B_b \cap \bar{B}_c + \{c\} = B_a \cap B_b,$$

for all $a \in S$, $b \in B_a$, and $c \in B_a \cap B_b$. P_{000000} is uniform implies that

$$|B_a \cap B_b| = \frac{n-3}{4},\ |B_a \cap B_b \cap B_c| = \frac{n-7}{8}.$$

Thus

$$|B_a \cap B_b \cap \bar{B}_c| = \frac{n-7}{8},$$

for all $a \in S$, $b \in B_a$, and $c \in B_a \cap B_b$. Then

$$|B_a \cap B_b \cap \bar{B}_d| = \frac{n-7}{8},$$

for all $a \in S$, $b \in B_a$, and $d \in B_a \cap B_b$. Since $(a, b, d, c) \in P_{000001}$, P_{000001} is uniform.

Next we show that P_{000011} is uniform. $(a, c, d, b) \in P_{000011}$, we need to show that $|B_a \cap \bar{B}_c \cap \bar{B}_d| = \frac{n-7}{8}$.

$$B_a \cap \bar{B}_c \cap B_d + B_a \cap B_c \cap B_d = B_a \cap B_d,$$

since c is not in $B_a \cap B_d$. So

$$B_a \cap \bar{B}_c \cap B_d = \frac{n+1}{8},$$

where $d \in B_a \cap \bar{B}_c$. We apply this to the next equation,

$$B_a \cap \bar{B}_c \cap B_d + B_a \cap \bar{B}_c \cap \bar{B}_d = B_a \cap \bar{B}_c,$$

since d not in $B_a \cap \bar{B}_c$, we get

$$|B_a \cap \bar{B}_c \cap \bar{B}_d| = \frac{n-7}{8},$$

for all $c \in B_a$, $d \in B_a \cap B_c$. Thus we get P_{000011} is uniform and $B_a \cap \bar{B}_d$ is square balanced, for $d \in B_a$.

Finally, we show that P_{000111} is uniform. $(b, c, d, a) \in P_{000111}$. Similarly, we have an equation,

$$\bar{B}_b \cap \bar{B}_c \cap \bar{B}_d + B_b \cap \bar{B}_c \cap \bar{B}_d = \bar{B}_c \cap \bar{B}_d,$$

since $b \in \bar{B}_c \cap \bar{B}_d$. By previous result,

$$|B_b \cap \bar{B}_c \cap \bar{B}_d| = \frac{n-7}{8},$$

we have

$$|\bar{B}_b \cap \bar{B}_c \cap \bar{B}_d| = \frac{n-7}{8},$$

for all $c \in B_b, d \in B_b \cap B_c$. So we proved P_{000111} is uniform.

□

Remark: From this proof, we notice that $B_a \cap B_b$ is square balanced implies that $B_a \cap \bar{B}_b$ and $\bar{B}_a \cap \bar{B}_b$ are both square balanced for all $b \in B_a$.

Remark: It is worth noting that if at second level, all components are uniform, then $\lambda_1 = B_a \cap B_b = \frac{n-3}{4}$, $\lambda_2 = \bar{B}_a \cap B_b = \frac{n+1}{4}$, we have $\lambda_2 = \lambda_1 + 1$. Then one of them must be even number. By Roanyai lemma, either $B_a \cap B_b \cap B_c$ or $\bar{B}_a \cap B_b \cap B_c$, where $a \in S, b \in B_a, c \in B_a \cap B)b$, can not be uniform, so can be further decomposed.

In Cheng, Huang (2000), it is pointed out that $B_a \cap B_b \cap B_c$ can not be uniform for all $a \in S, b \in B_a, c \in B_a \cap B_b$ based on a result in Muller, Pelant (1974). But the result is without the restricted condition $b \in B_a, c \in B_a \cap B_b$, so the number of levels to proceed in Cheng, Huang (2000) $n^{\frac{\log n + O(1)}{3}}$ is not right.

3.5.3 Super square balanced schemes

In Section, we have already get a decomposition of $S^{[m]}$ as

$$S^{[m]} = \bigcup_{\tau} P_{\tau}.$$

In this section, we introduce several splitting tools to further refine this decomposition. More precisely, we have

- **Tool A**: Use Ronyai lemma to decompose if there is an automorphism.
- **Tool B**: Change lex order in Gröbner bases.
- **Tool C**: Self extension.
- **Tool D**: Cross extension.

Tool A. is based on the following lemma.

Lemma 3.5.20 (Ronyai 1992)**.** *Let A be an algebra over $\mathbb{F}_p$ with dimension t. Given a nontrivial automorphism of A, we can find a nontrivial ideal of A in deterministic time $(t + \log p)^{o(1)}$ an ideal $I \subsetneq A$.*

To factor f, we may be able to make different fibre sizes among the points of f. So we need to find ways to change the ideal to be not uniform.

Tool B. uses the fact that an ideal is not necessary to be strong uniform to split ideal. Given a variety in uniform under certain order, say $x_1 < x_2 < \cdots < x_n$. If we change the order to be a new one, say $x_{i_1} < x_{i_2} < \cdots < x_{i_n}$, it is with high possibility that it won't be uniform.

Example 3.5.21. *Consider the example 1.3.8. If we change the term order to be $z < y < x$, then it is not uniform as more as showed as follows.*

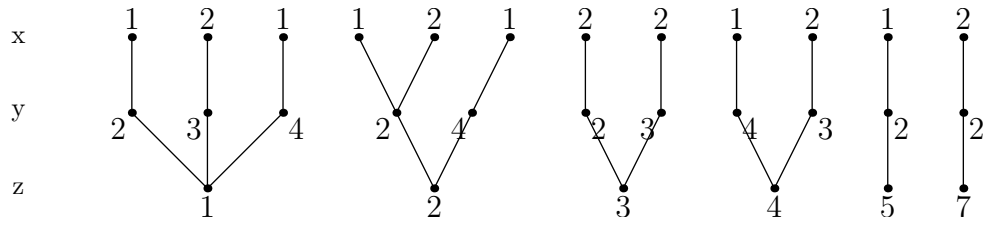

Figure 3.7: An example which is not uniform

And the Gröbner basis is

$$
\begin{aligned}
g_0 &= z^6 - 22z^5 + 190z^4 - 820z^3 + 1849z^2 - 2038z + 840 \\
g_1 &= (z-1)(z-2)(z-3)(z-4)y - 2(z-1)(z-2)(z-3)(z-4) \\
g_2 &= (z-1)(y^2 - 3/2yz^2 + 17/2yz - 17y + 1/3z^4 - 17/3z^3 + 110/3/3z^2 - 248/3z + 100 \\
g_3 &= (y-2)(y-3)(y-4) \\
g_4 &= (z-2)x - y^2 + yz^3 - 13/2yz^2 + 25/2yz - y - 5/18z^5 + 59/12z^4 - 605/18z^3 + \\
&\quad 417/4z^2 - 2585/18z + 184/3 \\
g_5 &= (y-2)(x+y-5) \\
g_6 &= (x-1)(x-2) = x^2 - 3x + 2
\end{aligned}
$$

The leading terms are $\{z^6, yz^4, y^2z, y^3, xz, xy, x^2\}$. *The* $LC(g_1)$ *is* $(z-1)(z-2)(z-3)(z-4)$, *it is a factor of* g_0 *as well as* $LC(g_2) = (z-1)$.

But there may be cases that changing order can not help.

Definition 3.5.22. *(Strong uniform). We say an ideal* I *or its variety is strong uniform, if the points of the ideal is uniform under all lex order* $x_{i_1} < x_{i_2} < \cdots < x_{i_n}$.

Example 3.5.23. *Let*

$$
\begin{aligned}
P = \; & \{[1,2,3],[1,3,4],[1,4,2],[2,3,6],[2,5,3],[2,6,5],[3,4,7], \\
& [3,6,4],[3,7,6],[4,2,5],[4,5,7],[4,7,2],[5,1,3],[5,3,7], \\
& [5,7,1],[6,1,4],[6,4,5],[6,5,1],[7,2,6],[7,1,2],[7,6,1]\}.
\end{aligned}
$$

Computing in $\mathbb{Z}_{103}$ and using lex order $z < y < x$, the reduced Gröbner basis is

$$\begin{aligned}
g_0 &= z^7 - 28z^6 + 13z^5 - 3z^4 - 29z^3 - 51z^2 - 13z + 7 \\
g_1 &= y^3 - 14y^2z^6 - 34y^2z^5 + 7y^2z^4 + y^2z^3 - 15y^2z^2 + 21y^2z + 16y^2 - 49yz^6 + 48yz^5 \\
&\quad -19yz^4 + 38yz^3 - 13yz^2 + 44yz - 45y + 51z^6 - 36z^5 - 5z^4 + 13z^3 + 8z^2 + 2z - 37 \\
g_2 &= x - 41y^2z^6 + y^2z^5 + 14y^2z^3 + 18y^2z^2 + 29y^2z + 32y^2 + 22yz^6 - 23yz^5 - 43yz^4 + \\
&\quad 30yz^3 - 23yz^2 - 44yz + 12y - 2z^6 - 36z^5 - 45z^4 - 33z^3 + 51z^2 - 17z + 23
\end{aligned}$$

And the structure of P is as follows:

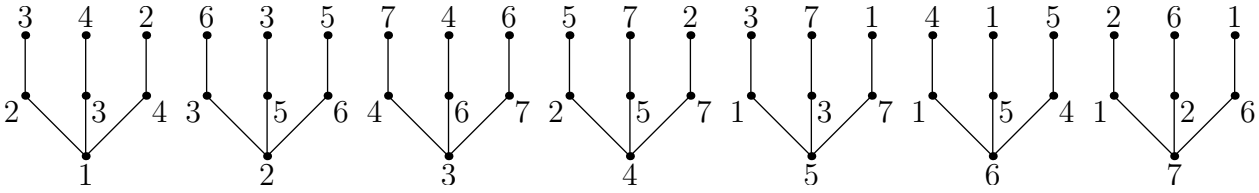

Figure 3.8: A strong uniform case

It is obvious that under different lex order the Gröbner basis remains the same under permutation of variables.

Tool C. is described as follows.

Lemma 3.5.24 (Self-extension)**.** *Let $I_{(X,y)}$ be any radical ideal in $\mathbb{F}_p[X, y]$ where $X = (x_1, \cdots, x_t)$. Define*

$$\hat{I} =< I_{(X,y)}, I_{(X,z)}, y - h(y, z) >: (y - z) \subset \mathbb{F}_p[X, y, z].$$

Then

$$V(\hat{I}) = \{(\alpha, b, c) : (\alpha, b) \in V(I_{(X,y)}), (\alpha, c) \in V(I_{(X,z)}), \text{ and } c \in B_b\}.$$

Hence $V(\hat{I})$ is uniform from (X, y) to z iff $\pi_y^{-1}(\alpha)$ is square balanced for each α.

We describe tool D in the following lemma.

Lemma 3.5.25 (Cross-extension)**.** *Let $I_1(X, y)$ and $I_2(X, y)$ be two radical ideals in $\mathbb{F}_p[X, y]$, where $X = (x_1, \cdots, x_t)$, that are coprime and*

$$I_1 \cap \mathbb{F}_p[X] = I_2 \cap \mathbb{F}_p[X].$$

Define

$$\hat{I} =< I_1((X, y), I_2(X, z), y - h(y, z) > \mathbb{F}_p[X, y, z].$$

Then

$$V(\hat{I}) = \{(\alpha, b, c) : (\alpha, b) \in V(I_1)), (\alpha, c) \in V(I_2), \text{ and } c \in B_b\}.$$

If $V(\hat{I})$ is not uniform at level z, we can decompose $V(I_1(X, y))$ (equivalently $I_1(X, y)$).

For any partition

$$S^{[m]} = P_1 \bigcup P_2 \cdots \bigcup P_t,$$

we say $I(P_i) = \left\langle f^{'}(x), g(x, y), \cdots \right\rangle$ (as a generic position)is homogeneous if $f^{'}(x) = f(x)$. we apply tools A to D to each component or pair of components. We will stop if we find a factor of $f(x)$, that is $\exists P_i$ is not homogeneous.

Definition 3.5.26. *Super square balanced scheme is defined to be any partition*

$$S^{[m]} = P_1 \bigcup P_2 \cdots \bigcup P_t$$

that can not be split further by any of the tools A to D, while all P_i's are homogeneous.

Conjecture 3.5.27. *Super square balanced schemes do not exist for some constant m which implies that we can get a factor of $f(x)$ in deterministic polynomial time.*

Chapter 4

Future work

In this short section, we mention a few major open problems that are related to the topics of the thesis and deserve future studies.

As a bivariate polynomial factorization is a special case for primary decomposition, we are wondering is there any advantage to use Hensel lifting technique on primary decomposition. We have the first problem as follows.

Research problem 1. Can our lifting technique be used for algorithms for primary decomposition?

Jean-Charles Faugére (1999), (2002) (F4, F5) provided efficient algorithms for computing Gröbner bases. Compared to methods used in their algorithms, We can use our method described in the proof of theorem 3.2.1 of computing Gröbner basis for $\langle I, h\rangle$ from Gröbner basis of I by adding one polynomial to speed up algorithms in Jean-Charles Faugére (2002). that is our

Research problem 2. Use our result on $\langle I, h\rangle$ to speed up algorithms for computing Gröbner bases for general ideals (say F4, F5)?

As discussed in Section 3.5.2.3, we are interested in the geometry properties of tournament graphs for $m = 4, 5, \cdots$, which may help to reduce the levels needed to find a proper factor of $f(x)$, even for some constant m. That is the following problem.

Research problem 3. Existence of super square balanced schemes

Bibliography

[1] JEAN-CHARLES FAUGÉRE, "A new efficient algorithm for computing Grbner bases (F4)", *Journal of Pure and Applied Algebra* 139, 1-3 (June 1999), 61-88.

[2] JEAN-CHARLES FAUGÉRE, "A new efficient algorithm for computing Grbner bases without reduction to zero (F5)", *Proceedings of the 2002 international symposium on Symbolic and algebraic computation* ISSAC 2002, Lille France, ACM Press 202, 75 - 83

[3] ERIC BACH, JOACHIM VON ZUR GATHEN AND HENDRIK W. LENSTRA, JR., "Deterministic factorization of polynomials over special finite fields", *Finite Fields and Their Applications*, Volume 7, Issue 1, January (2001),5-28

[4] VLADIMIR MÜLLER, JAN PELANT, "On strongly homogeneous tournaments"*Czechoslovak Mathematical*, Volume 24, (1974), No.3 378-391

[5] THOMAS BECKER AND VOLKER WEISPFENNING *Gröbner bases. A computational approach to commutative algebra*. In cooperation with Heinz Kredel. Graduate Texts in Mathematics, 141. Springer-Verlag, New York, 1993. xxii+574 pp.

[6] ELWYN R. BERLEKAMP, "Factoring polynomials over finite fields", *Bell System Tech. J.*, **46** (1967), 1853-1859.

[7] ELWYN R. BERLEKAMP, "Factoring polynomials over large finite fields", *Math. Comp.*, **24** (1970), 713-735.

[8] P. J. CAMERON AND J. H. VAN LINT, *Designs, Graphs, Codes and Their Links*, London Mathematical Society Student Texts 22, Cambridge University Press, 1991.

[9] D.G. CANTOR AND H. ZASSENHAUS "A new algorithm for factoring polynomials over finite fields," *Math. Comp.* **36** (1981), no. 154, 587–592.

[10] Q. CHENG AND M.D. HUANG, "Factoring polynomials over finite fields and stable colorings of tournaments", in *Algorithmic Number Theory* (W. Bosma, Ed.), Proceedings of 4-th International Symposium, ANTS-4, July, 2000, Springer, 233-246.

[11] A. L. CHISTOV, "An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time" (Russian), *Theory of the complexity of computations, II.*, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **137** (1984), 20–79. [English translation: *J. Sov. Math.* **34** (1986).]

[12] A. L. CHISTOV, "Efficient factorization of polynomials over local fields" (Russian), *Dokl. Akad. Nauk SSSR* **293** (1987), no. 5, 1073–1077. [English translation: *Soviet Math. Dokl.* **35** (1987), no. 2, 434–438.]

[13] A. L. CHISTOV, "Efficient factoring polynomials over local fields and its applications", *Proceedings of the International Congress of Mathematicians*, Vol. I, II (Kyoto, 1990), 1509–1519, Math. Soc. Japan, Tokyo, 1991.

[14] R.M. CORLESS, A. GALLIGO,I.S. KOTSERIAS AND S.M. WATT, "A Symbolic-Geometric Algorithm for Factoring Multivariate Polynomials", *Proc. International Symposium on Symbolic and Algebraic Computation*, ISSAC 2002, July 7-10 2002, Lille France, ACM Press 2002, 37–45.

[15] DAVID COX, JOHN LITTLE AND DONAL O'SHEA, *Using algebraic geometry*, Graduate Texts in Mathematics, 185. Springer-Verlag, New York, 1998.

[16] DOMINIQUE DUVAL, "Absolute factorization of polynomials: a geometric approach," *SIAM J. Comput.* **20** (1991), 1–21.

[17] DAVID EISENBUD, *Commutative algebra*, With a view toward algebraic geometry. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995. xvi+785 pp.

[18] SERGEI EVDOKIMOV, "Factorization of a solvable polynomial over finite fields and the generalized Riemann hypothesis", *Zapiski Nauchnyck Seminarov LOMI*, **176** (1989), 104-117.

[19] SERGEI EVDOKIMOV, "Factorization of polynomials over finite fields in subexponential time under GRH", in *Proc. 1994 Algorithmic Number Theory Symposium* (L. M. Adleman and M.-D. Huang, eds.), LNCS 877, Springer-Verlag, 1994, 209–219.

[20] J. C. FAUGÈRE, P. GIANNI, D. LAZARD, AND T. MORA, "Efficient computation of zerodimensional Grobner bases by change of ordering", *J. Symbolic Comput.*, **16** (1993), 329–344.

[21] SHUHONG GAO, "On the deterministic complexity of polynomial factoring," *Journal of Symbolic Computation* **31** (2001), 19–36.

[22] SHUHONG GAO AND ALAN G.B. LAUDER, "Hensel lifting and bivariate polynomial factorisation over finite fields," *Mathematics of Computation* **71** (2002), 1663-1676.

[23] SHUHONG GAO, "Factoring multivariate polynomials via partial differential equations," *Mathematics of Computation* **72** (2003), 801–822.

[24] SHUHONG GAO, VIRGÍNIA M. RODRIGUES AND JEFF STROOMER, "Gröbner basis structure of finite set of points", submitted to *J. of Symbolic Computation*, (16 pages).

[25] FATIMA ABUSALEM, SHUHONG GAO AND ALAN G.B. LAUDER, "Factoring polynomials via polytopes", in *Proceedings of the 2004 international symposium on Symbolic and algebraic computation (ISSAC 2004)*, pp. 4–11, July 4-7, 2004, University of Cantabria, Santander, Spain.

[26] SHUHONG GAO, ERICH KALTOFEN AND ALAN G.B. LAUDER, "Deterministic distinct degree factorization for polynomials over finite fields," *J. Symbolic Computation*, **38** (2004), 1461-1470.

[27] SHUHONG GAO, ERICH KALTOFEN, JOHN P. MAY, ZHENGFENG YANG AND LIHONG ZHI, "Approximate factorization of multivariate polynomials via differential equations", in em Proceedings of the 2004 international symposium on Symbolic and algebraic computation (ISSAC 2004), pp. 167–174, July 4-7, 2004, University of Cantabria, Santander, Spain.

[28] JEFF FARR AND SHUHONG GAO, "Computing Gröbner Bases for Vanishing Ideals of Finite Sets of Points", Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC16), LNCS 3857, 2006, 118–127.

[29] SHUHONG GAO AND JOACHIM VON ZUR GATHEN, "Berlekamp's and Niederreiter's polynomial factorization algorithms," *Proc. 2nd International Conference on Finite Fields: Theory, Applications, and Algorithms*, Las Vegas, 1993. *Contemporary Mathematics*, vol. 168, 1994, 101–116.

[30] J. VON ZUR GATHEN AND J. GERHARD, "Arithmetic and Factorization of Polynomials over $\mathbb{F}_2$," *Proc. ISSAC 96*, Zurich, Switzerland, ACM press, 1-9.

[31] J. VON ZUR GATHEN AND E. KALTOFEN, "Factorization of multivariate polynomials over finite fields," *Math. Comp.* **45** (1985), no. 171, 251–261.

[32] D. YU GRIGORYEV AND A. L. CHISTOV, "Fast factorization of polynomials into irreducible ones and the solution of systems of algebraic equations" (Russian), *Dokl. Akad. Nauk SSSR* **275** (1984), no. 6, 1302–1306. [English translation: *Soviet Math. Dokl.* **29** (1984), no. 2, 380–383.

[33] MARK VAN HOEIJ, " Factoring polynomials and the knapsack problem", *Journal of Number Theory*, **95** (2002), 167-189.

[34] MING-DEH A. HUANG, "Generalized Riemann Hypothesis and Factoring polynomials over Finite Fields", *J. Algorithms*, **12** (1991), 464–481. (Previous version in *Proc. 17th ACM Symp. Theory of Computing*, pp. 121-130, 1985.)

[35] MING-DEH HUANG AND YIU-CHUNG WONG, "Extended Hilbert irreducibility and its applications", Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 1998). *J. Algorithms* **37** (2000), no. 1, 121–145.

[36] ERICH KALTOFEN, "Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization," *SIAM J. Comput.* **14** (1985), no. 2, 469–489.

[37] E. KALTOFEN AND B. TRAGER, "Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators," *J. Symbolic Comput.* **9** (1990), 301-320.

[38] G. CHÈZE AND G. LECERF, "Lifting and recombination techniques for absolute factorization". Preprint 2005.

[39] G. LECERF " Sharp precision in Hensel lifting for bivariate polynomial factorization", *Mathematics of Computation*, **75** (2006), 921-933.

[40] A. K. LENSTRA, "Factoring multivariate integral polynomials", *Theoret. Comput. Sci.* **34** (1984), no. 1-2, 207–213.

[41] A. K. LENSTRA, "Factoring multivariate polynomials over finite fields", *J. Comput. System Sci.* **30** (1985), no. 2, 235–248.

[42] A. K. LENSTRA, "Factoring multivariate polynomials over algebraic number fields," *SIAM J. Comput.* **16** (1987), no. 3, 591–598.

[43] A. K. LENSTRA, H.W. LENSTRA, JR. AND L. LOVÁSZ, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, **161** (1982), 515–534.

[44] H. NIEDERREITER, "A new efficient factorization algorithm for polynomials over small finite fields," *Appl. Alg. Eng. Comm. Comp.* **4** (1993), 81–87.

[45] H. NIEDERREITER, "New deterministic factorization algorithms for polynomials over finite fields," *Finite fields: theory, applications, and algorithms* (Las Vegas, NV, 1993), 251–268, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.

[46] RONITT RUBINFELD AND RICHARD ZIPPEL "A new modular interpolation algorithm for factoring multivariate polynomials (extended abstract)," in *Proc. 1994 Algorithmic Number Theory Symposium* (L. M. Adleman and M.-D. Huang, eds.), LNCS 877, Springer-Verlag, 1994, 93–107.

[47] W. M. RUPPERT, "Reducibility of polynomials $f(x, y)$ modulo p", *Journal of Number Theory* **77** (1999), 62-70.

[48] WOLMER V. VASCONCELOS, *Computational methods in commutative algebra and algebraic geometry*, With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman. Algorithms and Computation in Mathematics, 2. Springer-Verlag, Berlin, 1998. xii+394 pp.

[49] H. ZASSENHAUS, "On Hensel factorization I", *J. Number Theory* **1** (1969), 291–311.

[50] P. J. CAMERON AND J. H. VAN LINT, *Designs, Graphs, Codes and Their Links*, London Mathematical Society Student Texts 22, Cambridge University Press, 1991.

[51] ERICH KALTOFEN AND VICTOR SHOUP, "Subquadratic-time factoring of polynomials over finite fields," *Math. Comp.* **67** (1998), no. 223, 1179–1197.