Lecture 17: Bivariate Polynomial Factoring

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

March 17, 2021

Overview

- Introduction: why multivariate factoring and main idea
- Hensel Lifting
- Main Algorithm
- Conclusion
- Acknowledgements

Why Factor Multivariate Polynomials?

- One of the fundamental algebraic operations
- Widely used in algebraic computation:
    - Primary decomposition of ideals
    - Decoding certain algebraic codes
    - Hardness vs Randomness tradeoffs

Why Factor Multivariate Polynomials?

- One of the fundamental algebraic operations
- Widely used in algebraic computation:
  - Primary decomposition of ideals
  - Decoding certain algebraic codes
  - Hardness vs Randomness tradeoffs
- Today: factoring *bivariate polynomials*

Main Idea

- Given ring $R[y]$, where R is UFD, would like to reduce factoring in $R[y]$ to factoring in R

“if we could factor in R then we can factor in $R[y]$”

Main Idea

- Given ring $R[y]$, where R is UFD, would like to reduce factoring in $R[y]$ to factoring in R

  "if we could factor in R then we can factor in $R[y]$"

- Surely cannot do this in general, as factoring in R could be harder than factoring $R[y]$!

  For instance, $R = \mathbb{Z}$.

Main Idea

- Given ring $R[y]$, where R is UFD, would like to reduce factoring in $R[y]$ to factoring in R

  “if we could factor in R then we can factor in $R[y]$”

- Surely cannot do this in general, as factoring in R could be harder than factoring $R[y]$!

  For instance, $R = \mathbb{Z}$.

- Today: if $R = S[x]$ then we can lift factoring over R to factoring over $R[y](= S[x, y])$!

  If we can factor *univariate* polynomials, then we can also factor *bivariate* ones!

$S = \mathbb{F}$ field

Main Idea

- Given ring $R[y]$, where R is UFD, would like to reduce factoring in $R[y]$ to factoring in R

  "if we could factor in R then we can factor in $R[y]$"

- Surely cannot do this in general, as factoring in R could be harder than factoring $R[y]$!

  For instance, $R = \mathbb{Z}$.

- Today: if $R = S[x]$ then we can lift factoring over R to factoring over $R[y](= S[x, y])$!

  If we can factor *univariate* polynomials, then we can also factor *bivariate* ones!

- Technical tool: Hensel lifting!

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $\underline{f(x, \alpha}) = \underline{g(}x) \cdot \underline{h(x)}$
- Lift this factorization to one of the form $\underline{g(x, y)} \cdot \underline{h(x, y)}$

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

$f(x,y)$ irreducible

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Can any value of $\alpha \in \mathbb{F}$ work?

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Can any value of $\alpha \in \mathbb{F}$ work?
- No. $\alpha = 0$ gives us a reducible univariate polynomial

$$f(x,0) = \underbrace{(x-1)}_{g(x)}\underbrace{x(x+1)}_{h(x)}$$

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Can any value of $\alpha \in \mathbb{F}$ work?
- No. $\alpha = 0$ gives us a reducible univariate polynomial
- Will a random value work? Yes!

Idea: High Level

- Say we are in the ring $R = \mathbb{F}[x, y]$ and we want to factor $f(x, y)$
- We know how to factor over $\mathbb{F}[x]$
- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Can any value of $\alpha \in \mathbb{F}$ work?
- No. $\alpha = 0$ gives us a reducible univariate polynomial
- Will a random value work? Yes!
- Suppose we pick an α (good or bad), now what?

Idea: High Level

- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Suppose we picked $\alpha = 0$, can we still get some information?

Idea: High Level

- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:
$$f(x, y) = y^2 + (x - 1)x(x + 1)$$
- Suppose we picked $\alpha = 0$, can we still get some information?
- $f(x, 0) = (x - 1)x(x + 1)$

Idea: High Level

- Try to substitute random value for y, say α
- Factor $f(x, \alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x, y) \cdot h(x, y)$
- Example:

$$f(x, y) = y^2 + (x - 1)x(x + 1)$$

- Suppose we picked $\alpha = 0$, can we still get some information?
- $f(x, 0) = (x - 1)x(x + 1)$
- Same as

$$f(x, y) \equiv +(x - 1)x(x + 1) \bmod y$$

mod (y)

Idea: High Level

- Try to substitute random value for y, say α
- Factor $f(x,\alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x,y) \cdot h(x,y)$
- Example:

$$f(x,y) = y^2 + (x-1)x(x+1)$$

- Suppose we picked $\alpha = 0$, can we still get some information?
- $f(x,0) = (x-1)x(x+1)$
- Same as

$$f(x,y) \equiv +(x-1)x(x+1) \bmod y$$

- Using Hensel lifting, we can get

$$f(x,y) \equiv g(x,y)h(x,y) \bmod y^2$$

where $\underbrace{g(x,y) \equiv x-1}$ mod y and $\underbrace{h(x,y) \equiv +x^2 + x}$ mod y

consistent with factorization modulo (y)

Idea: High Level

- Try to substitute random value for y, say α
- Factor $f(x,\alpha) = g(x) \cdot h(x)$
- Lift this factorization to one of the form $g(x,y) \cdot h(x,y)$
- Example:

$$f(x,y) = y^2 + (x-1)x(x+1)$$

- Suppose we picked $\alpha = 0$, can we still get some information?
- $f(x,0) = (x-1)x(x+1)$
- Same as

$$f(x,y) \equiv -(x-1)x(x+1) \bmod y$$

- Using Hensel lifting, we can get

$$f(x,y) \equiv g(x,y)h(x,y) \bmod y^2$$

  where $g(x,y) \equiv x - 1 \bmod y$ and $h(x,y) \equiv -x^2 - x \bmod y$
- Doing this many times will give us information whether our *base factorization* was good or not

Strategy

- On input $f(x,y) \in \mathbb{F}[x,y]$
- Do some preprocessing to know that we have a "nice polynomial"
  1. the restriction of f should be square free

$$f(x,\alpha) = \underbrace{p_1(x)\,p_2(x)\cdots p_b(x)}_{\text{irreducible distinct}}$$

will be able to take α to be zero

$$f(x,y) \rightarrow \boxed{f_\alpha(x,y)} := \underline{f(x,y+\alpha)}$$

$f_\alpha(x,0)$ nice

Strategy

- On input $f(x, y) \in \mathbb{F}[x, y]$
- Do some preprocessing to know that we have a “nice polynomial”
  1. the restriction of f should be square free
- Factor

$$f(x, y) \equiv g(x, y) \cdot h(x, y) \bmod y$$

  using the univariate factoring algorithm

$$f(x,0) = g(x,0) \cdot h(x,0)$$

univariate polynomials

Strategy

- On input $f(x,y) \in \mathbb{F}[x,y]$
- Do some preprocessing to know that we have a “nice polynomial”
  1. the restriction of f should be square free
- Factor
$$f(x,y) \equiv g(x,y) \cdot h(x,y) \bmod y$$
  using the univariate factoring algorithm
- Lift factorization above to
$$f(x,y) \equiv g_k(x,y) \cdot h_k(x,y) \bmod y^{2^k}$$
  for some value of k (large enough)

Strategy

- On input $f(x,y) \in \mathbb{F}[x,y]$
- Do some preprocessing to know that we have a "nice polynomial"
  1. the restriction of f should be square free
- Factor
$$f(x,y) \equiv g(x,y) \cdot h(x,y) \bmod y$$
  using the univariate factoring algorithm
- Lift factorization above to
$$f(x,y) \equiv g_k(x,y) \cdot h_k(x,y) \bmod y^{2^k}$$
  for some value of k
- From factorization above, extract factors of $f(x,y)$

Just like in the univariate case!

- Introduction: why multivariate factoring and main idea
- Hensel Lifting
- Main Algorithm
- Conclusion
- Acknowledgements

Hensel Lifting - General Setting

- Let R be a ring, $I \subset R$ ideal, and we have

$$f \equiv gh \mod I$$

where there are $a, b \in R$ such that

$$ag + bh \equiv 1 \mod I$$

"pseudo-GCD"

"$\gcd(g, h) \equiv 1 \mod I$"

Hensel Lifting - General Setting

- Let R be a ring, $I \subset R$ ideal, and we have

  $$f \equiv gh \mod I$$

  where there are $a, b \in R$ such that

  $$ag + bh \equiv 1 \mod I$$

  "pseudo-GCD"

- In our setting, $R = \mathbb{F}[x, y]$, $I = (y)$, f is our input polynomial and $g, h \in \mathbb{F}[x, y]$ is the coprime factorization.

$$f(x,0) \equiv \underbrace{g(x,0)\, h(x,0)}_{\text{coprime}} \mod (y)$$

coprime $\Rightarrow \exists\, a, b$ s.t.

$$a\, g(x,0) + b\, h(x,0) = 1.$$

$\mathbb{F}[x]$ Euclidean Domain (PID)

Hensel Lifting - General Setting

- Let R be a ring, $I \subset R$ ideal, and we have

$$f \equiv gh \mod I$$

where there are $a, b \in R$ such that

$$ag + bh \equiv 1 \mod I$$

“pseudo-GCD”

- In our setting, $R = \mathbb{F}[x, y]$, $I = (y)$, f is our input polynomial and $g, h \in \mathbb{F}[x, y]$ is the coprime factorization.
- If f, g, h satisfy the conditions above, then there exist $g^*, h^* \in R$ such that

$$f \equiv g^* h^* \bmod I^2 \quad \left\{ \text{lift of factorization} \right.$$

consistency

“downward compatibility”

$$\left\{ \begin{array}{l} g^* \equiv g \bmod I \\ h^* \equiv h \bmod I \end{array} \right.$$

Hensel Lifting - Full Statement

- Let R be a ring, $I \subset R$ ideal, and we have $f \equiv gh \mod I$ where there are $a, b \in R$ such that $ag + bh \equiv 1 \mod I$.
  Then, there are g^*, h^* such that

$$\begin{aligned} f &\equiv g^* h^* \text{ mod } I^2 \\ g^* &\equiv g \text{ mod } I \\ h^* &\equiv h \text{ mod } I \end{aligned}$$

Hensel Lifting - Full Statement

- Let R be a ring, $I \subset R$ ideal, and we have $f \equiv gh \mod I$ where there are $a, b \in R$ such that $ag + bh \equiv 1 \mod I$.
  Then, there are g^*, h^* such that

$$\begin{aligned} f &\equiv g^* h^* \text{ mod } I^2 \\ g^* &\equiv g \text{ mod } I \\ h^* &\equiv h \text{ mod } I \end{aligned}$$

1. There are a^*, b^* such that

$$a^* g^* + b^* h^* \equiv 1 \mod I^2$$

allows us to iterate the lift!

Hensel Lifting - Full Statement

- Let R be a ring, $I \subset R$ ideal, and we have $f \equiv gh \mod I$ where there are $a, b \in R$ such that $ag + bh \equiv 1 \mod I$.

  Then, there are g^*, h^* such that

$$\begin{aligned} f &\equiv g^* h^* \bmod I^2 \\ g^* &\equiv g \bmod I \\ h^* &\equiv h \bmod I \end{aligned}$$

1. There are a^*, b^* such that

$$a^* g^* + b^* h^* \equiv 1 \mod I^2$$

iterate

2. given a, b, g, h, one can easily compute a^*, b^*, g^*, h^*

computationally efficient!

Hensel Lifting - Full Statement

- Let R be a ring, $I \subset R$ ideal, and we have $f \equiv gh \mod I$ where there are $a, b \in R$ such that $ag + bh \equiv 1 \mod I$.
  Then, there are g^*, h^* such that

$$\left.\begin{aligned} f &\equiv g^* h^* \bmod I^2 \\ g^* &\equiv g \bmod I \\ h^* &\equiv h \bmod I \end{aligned}\right\} (i)$$

1. There are a^*, b^* such that

$$a^* g^* + b^* h^* \equiv 1 \mod I^2$$

2. given a, b, g, h, one can easily compute a^*, b^*, g^*, h^*
3. solution g^*, h^* is unique. That is, any other solution g', h' is such that

"up to first order terms"

$$h^* \equiv h'(1 + u) \mod I^2$$

$$g^* \equiv g'(1 - u) \mod I^2$$

for some $u \in I$.

Hensel Lifting - Proof

- Let $m = f - gh$. Thus, $m \in I$

$f \equiv g \cdot h \mod I$

Hensel Lifting - Proof

- Let $m = f - gh$. Thus, $m \in I$
- Set

$$\boxed{\text{computing } g^* \text{ and } h^*}$$

$$g^* = g + bm$$
$$h^* = h + am$$

$ag + bh \equiv 1 \mod I$

Hensel Lifting - Proof

- Let $m = f - gh$. Thus, $\boxed{m \in I}$
- Set computing g^* and h^*

$$g^* = g + bm$$
$$h^* = h + am$$

- Notice that:

$$\begin{aligned} f - g^*h^* &= f - gh - \overset{I \ni}{m}\overbrace{(bh + ag)}^{\equiv 1 \bmod I} \overset{-}{+} \overset{0 \bmod I^2}{\cancel{abm^2}} \\ &\equiv f - gh - m \bmod I^2 \\ &\equiv 0 \bmod I^2 \end{aligned}$$

$$g^* h^* = (g + bm)(h + am) = gh + m(ag + bh) + abm^2$$

$$m \cdot \underbrace{(bh + ag)}_{1 + x} \equiv m \bmod I^2$$

$$= m + \cancel{xm}^{0}$$

Hensel Lifting - Proof

- Let $m = f - gh$. Thus, $m \in I$
- Set

computing g^* and h^*

$$\begin{aligned} g^* &= g + bm \\ h^* &= h + am \end{aligned}$$

- Notice that:

$f \equiv g^*h^* \bmod I^2$

$$\begin{aligned} f - g^*h^* &= f - gh - m(bh + ag) + abm^2 \\ &\equiv f - gh - m \bmod I^2 \\ &\equiv 0 \bmod I^2 \end{aligned}$$

- Let $q = ag^* + bh^* - 1$. $\boxed{q \in I}$

$\boxed{\text{computing } a^* \text{ and } b^*}$

First guess

$a^* = a$

$b^* = b$

$$\begin{aligned} a^* &= a(1 - q) \\ b^* &= b(1 - q) \end{aligned}$$

$q = ag^* + bh^* - 1 \equiv ag + bh - 1 \equiv 1 - 1 \equiv 0 \bmod I$

Hensel Lifting - Proof

- Let $q = ag^* + bh^* - 1$. $q \in I$

computing a^* and b^*

$$\boxed{\begin{aligned} a^* &= a(1-q) \\ b^* &= b(1-q) \end{aligned}}$$

$$q \in I \Rightarrow q^2 \in I^2$$

$$ag^* + bh^* = 1 + q$$

$$\underbrace{(1-q)\left(ag^* + bh^*\right)}_{a^*g^* + b^*h^*} = (1+q)(1-q) = 1 - q^2 \equiv 1 \mod I^2$$

Hensel Lifting - Proof

- Let $q = ag^* + bh^* - 1$. $q \in I$ computing a^* and b^*

$$\begin{aligned} a^* &= a(1-q) \\ b^* &= b(1-q) \end{aligned}$$

- Note that

$$\begin{aligned} a^*g^* + b^*h^* - 1 &= ag^* + bh^* - 1 - q(ag^* + bh^*) \\ &= q(1 - ag^* + bh^*) = -q^2 \in I^2 \end{aligned}$$

Hensel Lifting - Proof

- Let $q = ag^* + bh^* - 1$. $q \in I$ computing a^* and b^*

$$a^* = a(1-q)$$
$$b^* = b(1-q)$$

- Note that

$$\begin{aligned} a^*g^* + b^*h^* - 1 &= ag^* + bh^* - 1 - q(ag^* + bh^*) \\ &= q(1 - ag^* + bh^*) = -q^2 \in I^2 \end{aligned}$$

- Uniqueness of solution:
  Let g', h' be another solution to the lifting problem.

$$\underline{g_1} = g' - g^* \quad \text{and} \quad \underline{h_1} = h' - h^*$$

both in I.

$g' \equiv g^* \equiv g \mod I$

Uniqueness of Solution

- Let g', h' be another solution to the lifting problem.
- $g_1 = g' - g^*$ and $h_1 = h' - h^*$ both in I

Uniqueness of Solution

- Let g', h' be another solution to the lifting problem.
- $g_1 = g' - g^*$ and $h_1 = h' - h^*$ both in I
- from $f - g'h' \equiv 0 \equiv f - g^*h^* \mod I^2$

$$\begin{aligned} \underline{g^*h^*} &\equiv g'h' \mod I^2 \\ &\equiv (g^*+g_1)(h^*+h_1) = g^*h^* + g^*h_1 + g_1h^* + \overset{\in I^2}{\cancel{g_1h_1}} \\ &\equiv \underline{g^*h^* + g^*h_1 + g_1h^*} \mod I^2 \end{aligned}$$

$$g'h' = (g^* + g_1)(h^* + h_1) = g^*h^* + g^*h_1 + g_1h^* + g_1h_1$$

$$0 \equiv g^*h_1 + g_1h^* \mod I^2$$

$$g^*h_1 \equiv -h^* \cdot g_1 \mod I^2 \Rightarrow g^2 b^* h_1 \equiv (-b^*h^*) g_1$$

$\underline{a^*g^* + b^*h^* \equiv 1}$ $\qquad$ mod I^2

$$g^*(b^*h_1) \equiv (-b^*h^*)\cdot g_1$$

$$\equiv (a^*g^*-1)\cdot g_1$$

$$\Rightarrow \quad g' - g^* = g_1 \equiv g^*(a^*g_1 - b^*h_1)$$

$$\Rightarrow \quad g' \equiv g^*\left(1 + (\underbrace{a^*g_1} - \underbrace{b^*h_1})\right)$$

$\in I$

$u = a^*g_1 - b^*h_1 \quad \therefore u \in I$

$$g' = g^*(1 + u)$$

Uniqueness of Solution

- Let g', h' be another solution to the lifting problem.
- $g_1 = g' - g^*$ and $h_1 = h' - h^*$ both in I
- from $f - g'h' \equiv 0 \equiv f - g^*h^* \mod I^2$

$$\begin{aligned} g^*h^* &\equiv g'h' \mod I^2 \\ &\equiv (g^* + g_1)(h^* + h_1) = g^*h^* + g^*h_1 + g_1h^* + g_1h_1 \\ &\equiv g^*h^* + g^*h_1 + g_1h^* \mod I^2 \end{aligned}$$

- Using $a^*g^* + b^*h^* \equiv 1 \mod I^2$

$$\begin{aligned} b^*g^*h_1 &\equiv -g_1b^*h^* \mod I^2 \\ &\equiv g_1(a^*g^* - 1) \mod I^2 \\ \Rightarrow g_1 &\equiv g^*(a^*g_1 - b^*h_1) \quad \mod I^2 \\ \Rightarrow g' &\equiv g^*(1 + a^*g_1 - b^*h_1) \quad \mod I^2 \end{aligned}$$

Uniqueness of Solution

- Let g', h' be another solution to the lifting problem.
- $g_1 = g' - g^* \quad \text{and} \quad h_1 = h' - h^*$ both in I
- from $f - g'h' \equiv 0 \equiv f - g^*h^* \bmod I^2$

$$\begin{aligned} g^*h^* &\equiv g'h' \bmod I^2 \\ &\equiv (g^* + g_1)(h^* + h_1) = g^*h^* + g^*h_1 + g_1h^* + g_1h_1 \\ &\equiv g^*h^* + g^*h_1 + g_1h^* \bmod I^2 \end{aligned}$$

- Using $a^*g^* + b^*h^* \equiv 1 \mod I^2$

$$\begin{aligned} b^*g^*h_1 &\equiv -g_1b^*h^* \bmod I^2 \\ &\equiv g_1(a^*g^* - 1) \bmod I^2 \\ \Rightarrow g_1 &\equiv g^*(a^*g_1 - b^*h_1) \quad \bmod I^2 \\ \Rightarrow g' &\equiv g^*(1 + a^*g_1 - b^*h_1) \quad \bmod I^2 \end{aligned}$$

- Set $u = a^*g_1 - b^*h_1$. Thus $u \in I$.

Analogous for h

Example

- $f(x, y) = y^2 + (x - 1)x(x + 1)$ over $\mathbb{Z}_5[x, y]$

Example

- $f(x,y) = y^2 + (x-1)x(x+1)$ over $\mathbb{Z}_5[x,y]$
- $f(x,y) \equiv (x-1)x(x+1) \mod (y)$

$$g = x - 1 \quad \text{and} \quad h = x(x+1)$$

$$\begin{array}{l|l} x^2+x & x-1 \\ \hline \underline{x^2-x} & x+2 \\ 2x & \\ & \\ 2 & \end{array}$$

$$(x^2+x) - (x+2)(x-1) = 2$$

$$\boxed{\underbrace{3}_{b}\cdot(x^2+x) - \underbrace{3(x+2)}_{a}(x-1) = 1}$$

Example

- $f(x,y) = y^2 + (x-1)x(x+1)$ over $\mathbb{Z}_5[x,y]$
- $f(x,y) \equiv (x-1)x(x+1) \mod (y)$

$$g = x - 1 \quad \text{and} \quad h = x(x+1)$$

- $a = 3(x+2),\ b = 3$

Example

- $f(x,y) = y^2 + (x-1)x(x+1)$ over $\mathbb{Z}_5[x,y]$
- $f(x,y) \equiv (x-1)x(x+1) \mod (y)$

$$g = x - 1 \quad \text{and} \quad h = x(x+1)$$

- $a = 3(x+2),\ b = 3$
- $m = f - gh = y^2$

$$g^* = (x-1) + by^2 \quad \text{and} \quad h^* = x(x+1) + ay^2$$

$$(x-1) + 3y^2 \qquad\qquad x^2 + x + 3(x+2)y^2$$

$$g^* \cdot h^* = (x-1)(x)(x+1) + [\underbrace{3(x+2)(x-1) + 3(x^2+x)}_{1}]y^2 + y^4(\cdots)$$

$$\equiv f + y^4(\cdots) \equiv f \mod (y^2)$$

Example

- $f(x,y) = y^2 + (x-1)x(x+1)$ over $\mathbb{Z}_5[x,y]$
- $f(x,y) \equiv (x-1)x(x+1) \mod (y)$

$$g = x - 1 \quad \text{and} \quad h = x(x+1)$$

- $a = 3(x+2),\ b = 3$
- $m = f - gh = y^2$

$$g^* = (x-1) + by^2 \quad \text{and} \quad h^* = x(x+1) + ay^2$$

- $q = ag^* + bh^* - 1$ and

$$a^* = a(1-q) \quad \text{and} \quad b^* = b(1-q)$$

Example

- Introduction: why multivariate factoring and main idea
- Hensel Lifting
- Main Algorithm
- Conclusion
- Acknowledgements

Main Algorithm

- **Input:** $f \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \leq d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.

Main Algorithm

- **Input:** $f \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \le d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.
- Pick $\alpha \in \mathbb{F}$ such that $\mathrm{disc}_x(f)(\alpha) \neq 0$ and set

$$\boxed{f(x, y) \leftarrow f(x, y + \alpha)}$$

$$\big\downarrow$$

makes $\mathrm{disc}_x(f)(0) \neq 0$

Q: what if $\nexists\ \alpha \in \overline{\mathbb{F}}$ s.t. $\mathrm{disc}_x(f)(\alpha) \neq 0$

$\Rightarrow \mathrm{disc}_x(f) = 0 \Rightarrow \gcd(f, \partial_x f)$ nontrivial

$\Rightarrow$ return factorization

Main Algorithm

- **Input:** $f \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \le d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.
- Pick $\alpha \in \mathbb{F}$ such that $\text{disc}_x(f)(\alpha) \neq 0$ and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

- Factor $f_0(x) := f(x, 0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor. $\}$ $a_0 g_0 + b_0 h_0 = 1$

($\mathbb{F}[x]$ is PID)

go over this later

intuition:

$f = g(x,y)\, h(x,y)$

$$f(x,0) = \underbrace{\prod_{i=1}^{t} \boxed{p_i(x)}} \cdot \underbrace{\prod_{i=1}^{k} q_i(x)}$$

don't know which grouping of the factors work

Main Algorithm

- **Input:** $f \in \mathbb{F}[x,y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \leq d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.
- Pick $\alpha \in \mathbb{F}$ such that $\text{disc}_x(f)(\alpha) \neq 0$ and set

$$f(x,y) \leftarrow f(x, y+\alpha)$$

- Factor $f_0(x) := f(x,0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Apply Hensel lifting for $k \geq \underline{2\log d + 2}$ times and find

large enough

$$f(x,y) \equiv \underline{g_k(x,y)} \cdot \underline{h_k(x,y)} \bmod (y^{2^k})$$

$$2^k \geq 2^{2\log d + 2} \geq 4 \cdot d^2$$

Main Algorithm

- **Input:** $f \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \leq d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.
- Pick $\alpha \in \mathbb{F}$ such that $\mathrm{disc}_x(f)(\alpha) \neq 0$ and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

- Factor $f_0(x) := f(x, 0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Apply Hensel lifting for $k \geq 2 \log d + 2$ times and find

$$f(x, y) \equiv g_k(x, y) \cdot h_k(x, y) \bmod (y^{2^k})$$

- Solve linear system and find $\underline{G}, \underline{L} \in \mathbb{F}[x, y]$ with $\underline{\deg_x(G) < \deg_x(f)}$, $\deg_y(G) \leq \deg_y(f)$ and

$$\underline{G} \equiv \underline{g_k} \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

Main Algorithm

- **Input:** $f \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is a field, where $\deg_x(f), \deg_y(f) \leq d$
- **Output:** if f factors, output nontrivial factor of f. Else, output f.
- Pick $\alpha \in \mathbb{F}$ such that $\mathrm{disc}_x(f)(\alpha) \neq 0$ and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

- Factor $f_0(x) := f(x, 0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Apply Hensel lifting for $k \geq 2 \log d + 2$ times and find

$$f(x, y) \equiv g_k(x, y) \cdot h_k(x, y) \bmod (y^{2^k})$$

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\underline{\deg_x(G) < \deg_x(f)}$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

- Output $\gcd(G, f)$

Intuition about G

$\deg_x(p) < \deg_x(f)$

$\deg_y(p) \leq \deg_y(f)$

$$f = \underbrace{p(x,y)}_{\leq \deg_x f - 1} \underbrace{q(x,y)}_{\geq 1}$$

$$f(x,0) = \underbrace{\prod p_i(x)} \cdot \underline{\prod q_j(x)}$$

$$p_1(x) = g_0(x)$$

G

$$p(x,y) \equiv g_k(x,y) \cdot l_k(x,y) \mod (y^{2^k})$$

one of the factors of f is multiple of $g_k(x,y)$ modulo (y^{2^k})

$\therefore$ G is multiple of $p(x,y)$

$p \mid \gcd(G, f)$

Analysis

- Pick $\alpha \in \mathbb{F}$ "at random" and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

- Why would a random shift work with high probability?

Analysis

- Pick $\alpha \in \mathbb{F}$ at random and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

- Why would a random shift work with high probability?
- If
  1. $|\mathbb{F}| > 4d^2$,
  2. $f(x, y)$ is *square-free*,

  then there is $\alpha \in \mathbb{F}$ such that $f(x, \alpha)$ *does not have repeated factors*

Analysis

- Pick $\alpha \in \mathbb{F}$ at random and set

$$f(x, y) \leftarrow f(x, y + \alpha)$$

$\operatorname{disc}_x(f) \neq 0$ in $\mathbb{F}[y]$ has at most $2d^2$ roots in $\mathbb{F}$ $\therefore$ $|\mathbb{F}| > 2d^2$ $\Rightarrow$ $\exists\, \alpha \in \mathbb{F}$ s.t. $\operatorname{disc}_x(f)(\alpha) \neq 0$

- Why would a random shift work with high probability?
- If
  1. $|\mathbb{F}| > 4d^2$,
  2. $f(x, y)$ is *square-free*,

  then there is $\alpha \in \mathbb{F}$ such that $f(x, \alpha)$ *does not have repeated factors*
- $\operatorname{disc}_x(f) \in \mathbb{F}[y]$ has degree $\leq 4d^2$

$\deg_y(f) \leq d$ $\quad$ $\deg_y(\partial_x f) \leq d$

$$\operatorname{disc}_x(f) = \operatorname{Res}_x(f, \partial_x f) = \det \left(\overbrace{\qquad\quad}^{d-1} \overbrace{\qquad}^{d} \;\; \square \qquad \right)$$

$\in \mathbb{F}[y]$

polynomial in $\mathbb{F}[y]$ of deg $\leq d$

Analysis

- Factor $f_0(x) := f(x, 0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Why can we do this?

$\mathrm{disc}_x(f)(0) \neq 0 \Rightarrow f_0(x)$ doesn't have repeated factors

$$f_0(x) = \underbrace{p_1(x)}_{\substack{g_0 \\ \text{irreducible}}} \underbrace{p_2(x) \cdots p_n(x)}_{h_0}$$

Analysis

- Factor $f_0(x) := f(x,0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Why can we do this?
- After we shifted $y \leftarrow y + \alpha$, we know that $f(x,0)$ does not have square factors

Analysis

- Factor $f_0(x) := f(x, 0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Why can we do this?
- After we shifted $y \leftarrow y + \alpha$, we know that $f(x, 0)$ does not have square factors
- Take any irreducible factor of $f(x, 0)$

Analysis

- Factor $f_0(x) := f(x,0)$ as $f_0(x) = g_0(x) \cdot h_0(x)$ where
  1. g_0 is irreducible
  2. g_0 and h_0 do not have a common factor.
- Why can we do this?
- After we shifted $y \leftarrow y + \alpha$, we know that $f(x,0)$ does not have square factors
- Take any irreducible factor of $f(x,0)$
- Because $\mathbb{F}[x]$ is an Euclidean Domain, we can also find a_0, b_0 such that

$$a_0 g_0 + b_0 h_0 = 1$$

$\therefore$ satisfy Hensel lifting assumptions!

Analysis

- Apply Hensel lifting for $k \geq 2\log d + 2$ times and find

$$f(x, y) \equiv g_k(x, y) \cdot h_k(x, y) \bmod (y^{2^k})$$

Analysis

- Apply Hensel lifting for $k \geq 2\log d + 2$ times and find

$$f(x,y) \equiv g_k(x,y) \cdot h_k(x,y) \bmod (y^{2^k})$$

- Can do this since we have

$$f(x,y) = g_0(x) \cdot h_0(x) \mod (y)$$

and

$$a_0 g_0 + b_0 g_0 = 1$$

Analysis

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

Analysis

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

- Intuition: by finding G, we are finding the factor of f which is divisible by g_0 modulo (y)

Analysis

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \text{ and } G \neq 0$$

- Intuition: by finding G, we are finding the factor of f which is divisible by g_0 modulo (y)
- If $f(x, y) = g(x, y) \cdot h(x, y)$, such that $g(x, y) \equiv g_0 \cdot \ell_0 \bmod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \bmod (y^{2^k})$

Analysis

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

- Intuition: by finding G, we are finding the factor of f which is divisible by g_0 modulo (y)
- If $f(x, y) = g(x, y) \cdot h(x, y)$, such that $g(x, y) \equiv \underbrace{g_0 \cdot \ell_0}_{\text{factors of } f_0} \mod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \mod (y^{2^k})$
  2. g_0, ℓ_0 coprime

$$g \equiv g_0 \ell_0 \mod (y) \underset{\text{Hensel lifting}}{\Rightarrow} g \equiv \hat{g}_k \cdot \ell_k \mod (y^{2^k})$$

Analysis

- Solve linear system and find $G, L \in \mathbb{F}[x, y]$ with $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \text{ and } G \neq 0$$

- Intuition: by finding G, we are finding the factor of f which is divisible by g_0 modulo (y)
- If $f(x, y) = g(x, y) \cdot h(x, y)$, such that $g(x, y) \equiv g_0 \cdot \ell_0 \mod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \mod (y^{2^k})$
  2. g_0, ℓ_0 coprime

  $$g \equiv g_0\ell_0 \mod (y) \Rightarrow g \equiv \hat{g}_k \cdot \ell_k \mod (y^{2^k})$$

  3. Now we have two solutions:

  $$f - \underline{g_k h_k} \equiv f - gh \equiv f - \underline{\hat{g}_k \cdot \ell_k h} \mod (y^{2^k})$$

  and we know $\hat{g}_k \equiv g_0 \mod (y)$ and $\ell_k h \equiv h_0 \mod (y)$

Analysis

- If $f(x,y) = g(x,y) \cdot h(x,y)$, such that $g(x,y) \equiv g_0 \cdot \ell_0 \bmod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \bmod (y^{2^k})$, and g_0, ℓ_0 coprime

$$\boxed{g \equiv g_0 \ell_0 \bmod (y) \;\Rightarrow\; g \equiv \hat{g}_k \cdot \ell_k \bmod (y^{2^k})}$$

Analysis

- If $f(x,y) = g(x,y) \cdot h(x,y)$, such that $g(x,y) \equiv g_0 \cdot \ell_0 \mod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \mod (y^{2^k})$, and g_0, ℓ_0 coprime

$$g \equiv g_0 \ell_0 \mod (y) \;\Rightarrow\; \underline{g \equiv \hat{g}_k \cdot \ell_k \mod (y^{2^k})}$$

  2. By induction and uniqueness of Hensel Lifting, can make

$$\hat{g}_k = g_k \mod (y^{2^k})$$

$$g_1 \equiv \hat{g}_1 \equiv g_0 \mod (y)$$

$$f \equiv g_1 h_1 \equiv gh \mod (y^2)$$

$$\equiv \hat{g}_1 \cdot \ell_1 h$$

h_1 $\ell_1 h$

g_1 $\hat{g}_1$ solutions to Hensel lifting problem for f

uniqueness of Hensel lifting $\Rightarrow$ $g_1 \equiv \hat{g}_1 (1+u) \mod (y^2)$

$u \in (y)$

$$\boxed{g_1 = \hat{g}_1(1-u)} \mod (y^2) \qquad u \in (y)$$

$$l_1 h \equiv h_1(1+u) \mod (y^2)$$

$$g \equiv \hat{g}_1 \cdot l_1 \mod (y^2)$$

$$\equiv \underbrace{\overbrace{\hat{g}_1(1-u)} \cdot \overbrace{(1+u) \cdot l_1}}_{\hat{g}_1 l_1 (1-\underset{\in (y^2)}{\underset{\uparrow}{u^2}})} \equiv g_1 \hat{l}_1 \mod (y^2)$$

$$g \equiv g_1 \cdot \hat{l}_1 \mod (y^2)$$ is another solution to the Hensel lifting

Analysis

- If $f(x,y) = g(x,y) \cdot h(x,y)$, such that $g(x,y) \equiv g_0 \cdot \ell_0 \bmod (y)$, we know such a G must exist
    1. $f - gh \equiv 0 \bmod (y^{2^k})$, and g_0, ℓ_0 coprime

    $$g \equiv g_0 \ell_0 \bmod (y) \;\Rightarrow\; g \equiv \hat{g}_k \cdot \ell_k \bmod (y^{2^k})$$

    2. By induction and uniqueness of Hensel Lifting, can make

    $$\boxed{\hat{g}_k = g_k \bmod (y^{2^k})}$$

    3. Thus, the system

    $$\boxed{G \equiv g_k \cdot L \quad \bmod (y^{2^k}) \quad \text{and} \quad G \neq 0}$$

    will have a solution such that

    factor of f $\deg_x(G) < \deg_x(f),\; \deg_y(G) \le \deg_y(f)$

    $$G = \overset{\downarrow}{g} \qquad L = \hat{\ell}_k \text{ from Hensel lifting}$$

Analysis

- If $f(x,y) = g(x,y) \cdot h(x,y)$, such that $g(x,y) \equiv g_0 \cdot \ell_0 \bmod (y)$, we know such a G must exist
  1. $f - gh \equiv 0 \bmod (y^{2^k})$, and g_0, ℓ_0 coprime
  $$g \equiv g_0\ell_0 \bmod (y) \;\Rightarrow\; g \equiv \hat{g}_k \cdot \ell_k \bmod (y^{2^k})$$
  2. By induction and uniqueness of Hensel Lifting, can make
  $$\hat{g}_k = g_k \bmod (y^{2^k})$$
  3. Thus, the system
  $$G \equiv g_k \cdot L \quad \bmod (y^{2^k}) \;\text{ and }\; G \neq 0$$
  will have a solution such that
  $$\deg_x(G) < \deg_x(f),\; \deg_y(G) \leq \deg_y(f)$$
  4. If it does not, then we can return that f is irreducible!

Analysis

- Now we need to prove that $\gcd(G, f)$ is non-trivial, where $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \text{ and } G \neq 0$$

Analysis

- Now we need to prove that $\gcd(G, f)$ is non-trivial, where $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \le \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

1. Note that $\operatorname{Res}_x(f, G)$ is a polynomial in $\mathbb{F}[y]$ of degree $< 2d^2 \le 2^k$, by our choice of k.

$$\underset{\mathbb{F}[y]}{\underset{\cap}{\operatorname{Res}_x(f, G)}} = u(x, y) \cdot f + v(x, y) \cdot G$$

Analysis

$\mathrm{Res}_x(f,G)=0 \iff \gcd(f,G)$ nontrivial

- Now we need to prove that $\gcd(G,f)$ is non-trivial, where $\deg_x(G) < \deg_x(f)$, $\deg_y(G) \leq \deg_y(f)$ and

$$G \equiv g_k \cdot L \mod (y^{2^k}) \quad \text{and} \quad G \neq 0$$

1. Note that $\mathrm{Res}_x(f,G)$ is a polynomial in $\mathbb{F}[y]$ of degree $< 2d^2 \leq 2^k$, by our choice of k.

$$\mathrm{Res}_x(f,G) = u(x,y) \cdot f + v(x,y) \cdot G \quad \bmod (y^{2^k})$$

2. Modulo y^{2^k}, we have

$\deg_y(R) < \underline{2^k}$

$$\boxed{0 \neq} \mathrm{Res}_x(f,G) = \underline{R(y)} \equiv uf + vG \equiv u g_k h_k + v g_k L$$

$$\equiv g_k (u h_k + v L)$$

depends on x

contradiction.

Conclusion

- Today we learned to factor bivariate polynomials
- Widely used in practice
    - Decoding Reed-Solomon Codes (next lecture)

Acknowledgement

- Lecture based largely on:
  - Madhu's notes - lectures 7 and 8

    `http://people.csail.mit.edu/madhu/FT98/`