Notes for Lifting Techniques *

Paul Vrbik

June 29, 2009

Contents

1 Preliminaries

We will be working with power series that have coefficients in $\mathbb{Q}$, denoted

$$\mathbb{Q}[[t]] = \{\sum_{i\geq 0} c_i t^i \; | c_i \in \mathbb{Q}\}.$$

Let $\mathbb{Q}[[t]]^{n\times n}$ be the $n \times n$ matrices with entries from $\mathbb{Q}[[t]]$. Our development will be done in $\mathbb{Q}[[t]]$ but our results will be valid for the more general case (i.e. replacing $\mathbb{Q}$ with any ring).

*Adapted from a lecture given by Dr. Éric Schost May 2009.

2 Introduction

Newton Iteration and Hensel lifting are iterative methods for finding a solution, $x(t) \in \mathbb{Q}[[t]]$, to some equation $F(x(t), t) = 0$ where:

1. $x(t)$ is a power series in t, i.e. $x(t) = x_0 + x_1 t + \cdots$.
2. x_0 is known.

We would like to adapt this to do:

1. Inverse of power series, i.e. for $1 - t \in \mathbb{Q}[[t]]$ calculate
$$(1-t)^{-1} = 1 + t + t^2 + \cdots .$$
2. Inverse of matrices of power series, i.e. for
$$\mathbf{A} = \begin{bmatrix} \frac{1}{1-t} & 2+t \\ \frac{1}{1+t} & \frac{-3}{1+t^2+t^3} \end{bmatrix}$$
find $\mathbf{A}^{-1} \in \mathbb{Q}[[t]]^{n\times n}$ such that $\mathbf{A}\cdot\mathbf{A}^{-1} = \mathrm{Id}$.
3. Power series roots of univariate and multivariate equations, i.e.
$$y^2 - 1 - t = 0 \Rightarrow y = 1 + \frac{t}{2} - \frac{t^2}{2} + \cdots .$$
4. "Triangular sets" with power series coefficients.

We will study the development these methods.

3 Power Series Inversion

It is worth noting what constitutes an inverse of an element from $\mathbb{Q}[[t]]$. First year calculus teaches us that $\frac{1}{1-t} = 1 + t + t^2 + \cdots$ only when $|t| < 1$ which can lead to some confusion. Reminding ourselves that the inverse of f (denoted f^{-1}) uniquely satisfies $ff^{-1} = 1$ we see that $1 + t + t^2 + \cdots$ is indeed the inverse of $1 + t$. Notice:

$$\begin{aligned}(1-t)(1+t+t^2+\cdots) &= (1-t) + (1-t)t + (1-t)t^2 + \cdots \\ &= 1 - t + t - t^2 + t^2 - t^3 + \cdots \\ &= 1\end{aligned}$$

We may also ask for the inverse of $(1-t) \in \mathbb{Q}[[t]]$ modulo t^k. In this case the inverse is $1 + t + t^2 + \cdots + t^{k-1}$ as:

$$\begin{aligned}(1-t)(1+t+t^2+\cdots+t^{k-1}) &\equiv 1 - t + t - t^2 + t^2 - t^3 + \cdots - t^{k-1} + t^{k-1} + t^k \bmod t^k \\ &\equiv 1 \bmod t^k\end{aligned}$$

Our interest is devising algorithms that calculate these types of inverses up to some arbitrary k (usually a power of 2). In particular we are building an algorithm that has the following specification.

Input A series $f(t) = f_0 + f_1 t + f_2 t^2 + \cdots + f_n t^n \in \mathbb{Q}[[t]]$, $f_0 \neq 0$ (otherwise $f(t)$ has no inverse).

Ouput $x(t) = x_0 + x_1 t + x_2 t^2 + \cdots + x_n t^m \in \mathbb{Q}[[t]]$ such that $x(t)\cdot f(t) = 1$. (Note, we assume that $\exists f_0^{-1}$ so $x_0 = 1/f_0$. This is a special case.)

3.1 By the Naive Algorithm

The basis of a naive algorithm is to extract the coefficients from $xf = 1$ somehow. For $a \in \mathbb{Q}[[t]]$ denote

$$[a]_i := \text{ coefficient of } t^i \text{ in } a$$

so that $[xf]_i = \sum_{j+k=i} x_j f_k$. As $xf = 1$ we have $[xf]_i = \sum_{j+k=i} x_j f_k = 0$ for $i > 0$.

To develop the naive algorithm it is best to just work through an example.

Example 1. At each step we use $[xf]_i$ to solve for x_i (note: $1/f_0 = x_0$);

$$
\begin{array}{lll}
i = 1 & x_0 f_1 + x_1 f_0 = 0 & \Rightarrow x_1 = \dfrac{-x_0 f_1}{f_0} = -x_0 \\
i = 2 & x_0 f_2 + x_1 f_1 + x_2 f_0 = 0 & \Rightarrow x_2 = \dfrac{-x_0 f_2 + x_1 f_1}{f_0} \\
i = 3 & x_0 f_3 + x_1 f_2 + x_2 f_1 + x_3 f_0 = 0 & \Rightarrow x_3 = \dfrac{-x_0 f_3 + x_1 f_2 + x_2 f_1}{f_0}
\end{array}
$$

From Example 1 we see that we can calculate x_i by

$$x_i = \frac{-x_0 f_i + x_1 f_{i-1} + \cdots + x_{i-1} f_1}{f_0},$$

enabling us to generate the desired output. As we are not using information from $x_{i-1}, \ldots, x_0$ we do $O(i)$ operations to get x_i for a total of $O(i^2)$ operations to explicitly build $x(t)$ to i terms which is far from ideal.

3.2 By Newton Iteration

We would like to reuse old information to save computation. So now suppose $x_0, \ldots, x_{i-1}$ (i-coefficients) in $x(t)$ are given so that $x(t)f(t) \equiv 1 \bmod t^i$. Let

$$x(t) = x_0 + x_1 t + \cdots + x_{i-1} t^{i-1} + \delta x$$

where $\delta x = a_i t^i + a_{i+1} t^{i+1} + \cdots$ are the higher order terms of $x(t)$ whose coefficients are unknown. We can interpret this as knowing $x(t) \bmod t^i$. What follows is a method for establishing $\delta x \bmod t^{2i}$ thereby allowing us to double the "accuracy" of $x(t)$ (as we would expect from the quadratically convergent Newton's method).

Define

$$x_{\text{init}} := x_0 + x_1 t + \cdots + x_{i-1} t^{i-1}$$

so that $x = x_{\text{init}} + \delta x$.

We again build coefficients by extracting them from $xf = 1$ except now we have:

$$xf = 1 \Rightarrow (x_{\text{init}} + \delta x)f = 1 \Rightarrow x_{\text{init}} f + \delta x f = 1. \tag{1}$$

where (by our assumption) $x_{\text{init}} f = 1 + 0t + \cdots + 0t^{i-1} + t^i R \equiv 1 \bmod t^i$ for some "remainder" term R. Multiplying (1) by x_{init} on both sides we get

$$x_{\text{init}}^2 f + x_{\text{init}} \delta x f = x_{\text{init}} \tag{2}$$

which allows us to derive an expression for δx as all other values are known.

Rewrite $f x_{\text{init}} \equiv 1 \bmod t^i$ as $x_{\text{init}} f = 1 + t^i R$ for some remainder R and multiply this expression by δx giving:

$$x_{\text{init}} \delta x f = \delta x + \delta x t^i R \tag{3}$$

Recall that $\delta x \equiv 0 \bmod t^i$ so $t^i | \delta x$ and therefore $t^{2i} | \delta x t^i R$ meaning $\delta x t^i R \equiv 0 \bmod t^{2i}$. So, subbing (2) into (3) and taking $\bmod t^{2i}$ we get

$$x_{\text{init}}^2 f + \delta x \equiv x_{\text{init}} \bmod t^{2i}$$

and solving for δx gives

$$\delta x \equiv x_{\text{init}} - x_{\text{init}}^2 f \bmod t^{2i} \tag{4}$$

which is the update formula we desire.

Example 2. By letting $t = p$ for p some prime we can use this update formula to calculate inverses modulo p^n. If we let $p = 3$ then we can calculate $-1/2 \bmod (3^8 = 6561)$ as follows:

1. $\frac{-1}{2} = \frac{1}{1-3} = 1 \bmod 3$
2. $\delta x \equiv (1 - (1)^2(1-3)) \bmod 3^2 = 3$ which implies $1 + 3 = 4 \equiv \frac{-1}{2} \bmod 3^2$
3. $\delta x \equiv (4 - (4)^2(1-3)) \bmod 3^4 = 36$ which implies $4 + 36 = 40 \equiv \frac{-1}{2} \bmod 3^4$
4. $\delta x \equiv (40 - (40)^2(1-3)) \bmod 3^8 = 3240$ which implies $40 + 3240 = 3280 \equiv \frac{-1}{2} \bmod 3^8$

where this process could be repeated up to any 3^{2^k}.

To simplify the complexity analysis for this method we will assume that we can multiply polynomials in linear time (which is absurd as the best method is $O(n \log n)$). Making this assumption means we will only be off by some log factors which is not a big deal.

Assuming that $x_0 = 1/f_0$ is given it takes one operation to calculate x_1, two operations to calculate x_2, x_3, four operations to calculate $x_4, \ldots, x_7$, and so on. Generalizing this we find that it takes $O(1 + 2 + 4 + 8 + \cdots + 2^k) = O(2^{k+1}) = O(2^k)$ operations to calculate $O(2^k)$ terms.

Remark 1. An optimization to calculate $x_{\text{init}}^2 f$ can be done. Observe

$$x_{\text{init}}^2 f = x_{\text{init}}(x_{\text{init}} f) = x_{\text{init}}(1 + 0t + \cdots + 0t^{i-1} + t^i R) = x_{\text{init}} + t^i x_{\text{init}} R.$$

This means (3) can be rewritten as:

$$\delta x \equiv -t^i x_{\text{init}} R \bmod t^{2i}.$$

and using a trick called "middle product" it *is* possible to compute *only* R (see []).

4 Inversion of Matrices in $\mathbb{Q}[[t]]^{n\times n}$

Let $\mathbf{F}(t) \in \mathbb{Q}[[t]]^{n\times n}$, e.g. letting $n = 2$ we have

$$\mathbf{F}(t) = \begin{bmatrix} f_{0,0}(t) & f_{0,1}(t) \\ f_{1,0}(t) & f_{1,1}(t) \end{bmatrix}$$

which we can express as a series of matrices (i.e. as an element from $\mathbb{Q}^{2\times 2}[[t]]$):

$$\mathbf{F}(t) = \mathbf{F}_0 + \mathbf{F}_1 t + \mathbf{F}_2 t^2 + \cdots$$

where $\mathbf{F}_i \in \mathbb{Q}^{2\times 2}$. What we would like to find is $\mathbf{X}(t) = \mathbf{X}_0 + \mathbf{X}_1 t + \mathbf{X}_2 t^2 + \cdots \in \mathbb{Q}^{n\times n}[[t]] \cong \mathbb{Q}[[t]]^{n\times n}$ such that $\mathbf{F}\mathbf{X} = \mathrm{Id}$.

To do this:

1. Compute $\mathbf{X}_0 = \mathbf{F}_0^{-1}$ (assume this is possible).
2. Repeat the newton iteration scheme from §3.2 replacing the series $f(t), x(t)$ with the series of matrices $\mathbf{F}(t), \mathbf{X}(t)$. Namely update $\mathbf{X} = \mathbf{X}_{\text{init}} + \delta\mathbf{X}$ using

$$\delta\mathbf{X} = \mathbf{X}_{\text{init}} - \mathbf{X}_{\text{init}}\mathbf{F}\mathbf{X}_{\text{init}} \bmod t^{2i}, \tag{5}$$

   where the products are matrix multiplications.

Remark 2. The development of the above method can be done in the same manner as §3.2. Special care needs to be taken with regards to commutativity. However, it is true that

$$\mathbf{F}\mathbf{X}_{\text{init}} = \mathbf{X}_{\text{init}}\mathbf{F} \equiv 0 \bmod t^i,$$

which is easily proved and useful for working out (5).

5 Series Roots of Univariate Polynomials

We now consider univariate polynomials with power series coefficients, i.e. $F \in \mathbb{Q}[[t]][u]$ where

$$F(t, u) = u^2 - 1 - t - t^2 - t^3 - t^4 - \cdots .$$

Our goal is to compute a point $x(t) \in \mathbb{Q}[[t]]$ such that $F(t, x(t))|_{t=0} = 0$ (which will just write as $F(0, x) = 0$). The point $x = 1$ satisfies this property for F defined above.

For reasons that will become clear later we require

$$\frac{\partial F}{\partial u}(0, x) \neq 0.$$

We can interpret this geometrically as helping us avoid double roots (but more to the point we must eventually divide by this quantity).

For the algorithm assume we know $x_0, x_1, \ldots, x_{i-1}$ such that

$$F(t, x_0 + x_1 t + \cdots + x_{i-1}t^{i-1}) \equiv 0 \bmod t^i.$$

We want to compute x_i such that

$$F(t, x_0 + x_1 t + \cdots + x_i t^i) \equiv 0 \bmod t^{i+1} \tag{6}$$

Definition 1 (Taylor formula)**.** For a polynomial P we have

$$P(A+B) = P(A) + \frac{\partial P}{\partial u}(A)B + B^2 R \tag{7}$$

for R some polynomial remainder term.

Applying Taylor's formula to (6) with $A = x_1 + \cdots + x_{i-1}t^{i-1}$ and $B = x_i t^i$ we get

$$0 \equiv F(A) + \frac{\partial F}{\partial u}(A)B + B^2 R \mod t^{i+1} \tag{8}$$

$$\equiv F(t, x_0 + \cdots + x_{i-1}t^{i-1}) + \frac{\partial F}{\partial u}(t, x_0 + \ldots + x_{i-1}t^{i-1})x_i t^i + t^{2i} R \mod t^{i+1} \tag{9}$$

The coefficient of t^i in (9) is

$$[F(t, x_o + x_1 t + \cdots + x_{i-1}t^{i-1})]_i + \left[\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1})x_i t_i\right]_i$$

where

$$\left[\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1})x_i t^i\right]_i = x_i \left[\frac{\partial F}{\partial u}(t, x_0 \cdots + x_{i-1}t^{i-1})\right]_0 = x_i \frac{\partial F}{\partial u}(0, x_0)$$

yielding the update formula

$$x_i = -\frac{[F(t, x_0 + \cdots + x_{i-1}t^{i-1}]_i}{\frac{\partial F}{\partial u}(0, x_0)} \mod t^{i+1}. \tag{10}$$

To instead lift a solution modulo t^i to modulo t^{2i} we apply the Taylor's formula to (9) using $A = x_1 + \cdots + x_{i-1}t^{i-1}$ and $B = \delta x$:

$$F(t, x_0 + \cdots + x_{i-1}t^{i-1}) + \frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1})\delta x + \delta x^2 R. \tag{11}$$

Recall that $\delta x \equiv 0 \mod t^i$ and $\delta x^2 \equiv 0 \mod t^{2i}$ so taking (11) mod t^{2i} and solving for x_i gives:

$$\delta x = -\frac{F(t, x_0 + \cdots + x_{i-1}t^{i-1})}{\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1})} \mod t^{2i}. \tag{12}$$

If we implement this we will have to:

1. compute $F(t, x_0 + \cdots + x_{i-1}t^{i-1}) \bmod t^{2i}$
2. compute $\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1}) \bmod t^{2i}$
3. invert and multiply $\mod t^{2i}$.

However, we can reduce the complexity by some constant factors by making the following observation:

Remark 3. Since $F(t, x_0 + \cdots + x_{i-1}t^{i-1}) \equiv 0 \bmod t^i$ we may express it as $t^i R_i$ with $R_i \in \mathbb{Q}[[t]][u]$ and instead do:

$$\begin{aligned} &\equiv \frac{F(t, x_0 + \cdots + x_{i-1}t^{i-1})}{\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1})} \bmod t^{2i} \\ &\equiv \frac{t^i R_i}{\frac{\partial F}{\partial u}} \bmod t^{2i} \\ &= t^i \left(\frac{R_i}{\frac{\partial F}{\partial u}} \bmod t^i \right). \end{aligned}$$

Therefore we need only calculate $\frac{\partial F}{\partial u}(t, x_0 + \cdots + x_{i-1}t^{i-1}) \bmod t^i$ (instead of $\bmod t^{2i}$).

Remark 4 (Representation of F)**.** F is in $k[[t]][u]$ so $F = \sum_i F_i u^i$ for $F_i \in k[[t]]$. We need a data structure that can accommodate the evaluation of F (and it's derivatives) at some arbitrary point. A DAG (directed acyclic graph) representation is a good choice. [PICTURE HERE]

6 Series Roots of Multivariate Polynomials

Let $F_1, \ldots, F_N$ be multivariate polynomials in $\mathbb{Q}[[t]][u_1, \ldots, u_n]$. Our goal is to solve the system $\langle F_1, \ldots, F_n \rangle$ by finding $x^{(1)}, \ldots, x^{(n)} \in \mathbb{Q}[[t]]$ ($x^{(i)} = x_0^{(i)} + x_1^{(i)} t + \cdots$) such that

$$\begin{aligned} F_1(x^{(1)}, \ldots, x^{(n)}, t)\big|_{t=0} &= 0 \\ &\vdots \\ F_n(x^{(1)}, \ldots, x^{(n)}, t)\big|_{t=0} &= 0 \end{aligned}$$

We require a point $(x_0^{(1)}, \ldots, x_0^{(n)})$ satisfying

$$F_i(x_0^{(1)}, \ldots, x_0^{(n)}) \text{ for } i = 1 \ldots n$$

and that,

$$\mathbf{J} := \left[\begin{array}{ccc} \frac{\partial F_1}{\partial u_1} & \cdots & \frac{\partial F_1}{\partial u_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial u_1} & \cdots & \frac{\partial F_n}{\partial u_n} \end{array} \right] \Bigg|_{(u_1, \ldots, u_n) = (x^{(1)}, \ldots, x^{(n)})}$$

is invertible $\bmod t$ (i.e. the Jacobian of $\mathbf{F} = \langle F_1, \ldots, F_n \rangle$ evaluated at the initial point is invertible)

Definition 2 (Generalized Taylor Formula)**.** For a multivariate polynomial P we have

$$P(A^{(1)} + B^{(1)}, \ldots, A^{(n)} + B^{(n)}) = P(A^{(1)}, \ldots, A^{(n)}) + \sum \frac{\partial F}{\partial A^{(i)}} B^i + \left\langle B^{(1)}, \ldots, B^{(n)} \right\rangle^2$$

Now, assume we have a solution for the system modulo t. Namely suppose that we are given

$$\begin{aligned} x^{(1)} &= x_0^{(1)} + x_1^{(1)} t + \cdots + x_{i-1}^{(1)} t^i \\ &\vdots \\ x^{(n)} &= x_0^{(n)} + x_1^{(n)} t + \cdots + x_{i-1}^{(n)} t^i \end{aligned}$$

such that

$$F_j(x^{(1)},\ldots,x^{(n)}) \equiv 0 \bmod t^i \text{ for } j = 1\ldots n.$$

To proceed with Newton iteration to find $\delta x^{(1)},\ldots,\delta x^{(n)}$ such that

$$F_j(x^{(1)}+\delta x^{(1)},\ldots,x^{(n)}+\delta x^{(n)}) = 0 \text{ for } j = 1\ldots n.$$

apply Taylor's formula

$$F_j(x^{(1)},\ldots,x_n^{(n)}) + \sum_{k=1}^{n} \frac{\partial F_j}{\partial u_k}(x^{(1)},\ldots,x^{(n)})\delta x^{(k)} + \left\langle \delta x^{(1)},\ldots,\delta x^{(n)} \right\rangle^2 = 0 \tag{13}$$

for $j = 1\ldots n$ and reduce $\bmod t^{2i}$ to get

$$F_j(x^{(1)},\ldots,x_n^{(n)}) + \sum_{k=1}^{n} \frac{\partial F_j}{\partial u_k}(x^{(1)},\ldots,x_n^{(n)})\delta x^{(k)} + 0 \equiv 0 \mod t^{2i} \tag{14}$$

$$\Rightarrow \left[\frac{\partial F_j}{\partial u_1}(x^{(1)},\ldots,x_n^{(n)}),\ldots,\frac{\partial F_j}{\partial u_n}(x^{(1)},\ldots,x_n^{(n)})\right] \begin{bmatrix} \delta x^{(1)} \\ \vdots \\ \delta x^{(n)} \end{bmatrix} \equiv 0 \bmod t^{2i}$$

(note $\delta x^{(j)}\delta x^{(j)} \equiv 0 \bmod t^{2i}$). This gives an expression for (13) in matrix form:

$$\mathbf{J} \begin{bmatrix} \delta x^{(1)} \\ \vdots \\ \delta x^{(n)} \end{bmatrix} \equiv - \begin{bmatrix} F_1(x^{(1)},\ldots,x_n^{(n)}) \\ \vdots \\ F_n(x^{(1)},\ldots,x_n^{(n)}) \end{bmatrix} \bmod t^{2i}$$

and solving gives an update formula for the $\delta x^{(i)}$'s:

$$\begin{bmatrix} \delta x^{(1)} \\ \vdots \\ \delta x^{(n)} \end{bmatrix} \equiv -\mathbf{J}^{-1} \begin{bmatrix} F_1(x^{(1)},\ldots,x_n^{(n)}) \\ \vdots \\ F_n(x^{(1)},\ldots,x_n^{(n)}) \end{bmatrix} \bmod t^{2i} \tag{15}$$

which has nontrivial implementation.

Remark 5. If we are in a lifting loop we reuse old $\mathbf{J}^{-1}$'s to update. Namely suppose that $\mathbf{J} \bmod t$ is known, we compute $\mathbf{J}^{-1} \bmod t^{2i}$ by computing $\mathbf{J}^{-1} \bmod t^2, t^4, \ldots, t^{2i}$ incrementally using lifting.

7 Lifting a Factor of a Univariate Polynomial

Let $G(x,t), H(x,t), F(x,t) \in \mathbb{Q}[[t]][x]$. Suppose $G(x,t)\cdot H(x,t) \equiv F(x,t) \bmod t^n$, $G, H \neq 1$ we call G and H the "factors" of F modulo t^n

Example 3. Let

$$\begin{aligned} F(x,t) = x^4(1+t+t^2+t^3+\cdots) + 2x^3(1+4t+t^2+\cdots) \\ + x^2(3+3t+\cdots) + 2x(1+4t+\cdots) + (2+2t+\cdots) + \cdots \end{aligned}$$

then $G(x,t) = (x^2+1)(x^2+2x+2)$ is a factor of $F(x,0)$.

Assume a factor $G_{\text{init}} = G_0 + tG_1 + \cdots + t^{i-1}G_{i-1}$ of F mod t^n is known (we also require that $\frac{\partial F}{\partial x}(x,0)$ is invertible modulo G and that $\deg_x G_k < \deg_x G_0$ for all $k > 0$). We wish to find an update formula for δG so that

$$F = (G_{\text{init}} + \delta G)H. \tag{16}$$

(i.e., so that $G = G_{\text{init}} + \delta G$ is a factor of F in the base field).

Now to get an update formula for δG recall $\delta G \equiv 0 \bmod t^i$ and $\frac{\partial \delta G}{\partial x} \equiv 0 \bmod t^i$. This allows us to reduce

$$\frac{\partial G_{\text{init}}}{\partial x} F = \frac{\partial G_{\text{init}}}{\partial x} H (G_{\text{init}} + \delta G)$$

modulo t^{2i}, using

$$\begin{aligned} \frac{\partial F}{\partial x} &= \left(\frac{\partial G_{\text{init}}}{\partial x} + \frac{\partial \delta G}{\partial x}\right) H + (G_{\text{init}} + \delta G)\frac{\partial H}{\partial x} \\ \Rightarrow \frac{\partial G_{\text{init}}}{\partial x} H &= -\frac{\partial F}{\partial x} + \frac{\partial \delta G}{\partial x} H + (G_{\text{init}} + \delta G)\frac{\partial H}{\partial x} \end{aligned}$$

to get

$$\frac{\partial G_{\text{init}}}{\partial x} F \equiv \left(\frac{\partial G_{\text{init}}}{\partial x} H\right) G_{\text{init}} - \frac{\partial F}{\partial x}\delta G + \left(\frac{\partial H}{\partial x}\delta G\right) G_{\text{init}} \mod t^{2i} \tag{17}$$

and taking this modulo G_{init} we get

$$\frac{\partial G_{\text{init}}}{\partial x} F \equiv -\frac{\partial F}{\partial x}\delta G \bmod \left\langle t^{2i}, G_{\text{init}} \right\rangle$$

yielding the update formula:

$$\delta G \equiv \left(-\frac{\partial G_{\text{init}}}{\partial x} \cdot F\right) \Big/ \left(\frac{\partial F}{\partial x}\right) \bmod \left\langle t^{2i}, G_{\text{init}} \right\rangle. \tag{18}$$

8 Lifting Triangular Sets

Lifting a triangular set can be interpreted as the generalization of lifting a root or factor of a polynomial.

We wish to devise an algorithm that has the following specification:

Input The system of polynomials $F_1, \ldots, F_n \in \mathbb{Q}[[t]][x_1, \ldots, x_n]$ and triangular sets $T_1, \ldots, T_n$ with $T_i \in \mathbb{Q}[x_i, \ldots, x_n]$ such that

$$\begin{gathered} F_1(x_1, \ldots, x_n, t) \equiv 0 \bmod \langle t, T_1, \ldots, T_n \rangle \\ \vdots \\ F_n(x_1, \ldots, x_n, t) \equiv 0 \bmod \langle t, T_1, \ldots, T_n \rangle \end{gathered}$$

and

$$\begin{bmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial x_1} & \cdots & \frac{\partial F_n}{\partial x_n} \end{bmatrix}$$

is invertible $\bmod \langle T_1(x_1, 0), \ldots, T_n(x_1, \ldots, x_n, 0) \rangle$.

Output The triangular sets

$$\begin{aligned}
T_n(x_1,\dots,x_n,t) &= x_n^{d_n} + T_{n,d_n-1}(x_1,\dots,x_{n-1},t)x_n^{d_n-1} + \cdots + T_{n,0}(x_1,\dots,x_{n-1},t)\\
&\vdots\\
T_2(x_1,x_2,t) &= x_2^{d_2} + T_{2,d_2-1}(x_1,t)x_2^{d_2-1} + \cdots + T_{2,0}(x_1,t)\\
T_1(x_1,t) &= x_1^{d_1} + T_{1,d_1-1}(t)x_1^{d_1-1} + \cdots + T_{1,0}(t)
\end{aligned}$$

such that $F_i \equiv 0 \mod \left\langle t^N, T_n', \dots, T_1' \right\rangle$. That is, a "solution" in the sense that:

$$\begin{aligned}
&x_n - T_{N,0}(t)\\
&\vdots\\
&x_2 - T_{2,0}(t)\\
&x_1 - T_{1,0}(t).
\end{aligned}$$

It is *almost* the case that all roots of $\{T_1,\dots,T_N\}$ are roots of $\{F_1,\dots,F_n\}$ (almost because we may lose isolated roots).

Example 4. Let $F_1, F_2 \in \mathbb{Q}[[t]][x_1,x_2]$ be given by:

$$\begin{aligned}
F_1 &= 1 + tx_1x_2 - t^2x_1 - (1+t)x_2 - x_1x_2^2\\
F_2 &= t - (2t-1)x_1 + (1+t)x_1x_2 - tx_1^2x_2
\end{aligned}$$

corresponding to the triangular sets (our input)

$$\begin{aligned}
T_2(x_1,x_2,0) &= x_1 + x_2 - 1\\
T_1(x_1,0) &= x_1^2 + 2x_1.
\end{aligned}$$

Since $\begin{bmatrix} \frac{\partial F_1}{\partial x_1} & \frac{\partial F_1}{\partial x_2} \\ \frac{\partial F_2}{\partial x_2} & \frac{\partial F_2}{\partial x_2} \end{bmatrix}$ invertible $\mod \langle T_2(x_1,x_2,0), T_1(x_1,0), t\rangle$ our algorithm will output:

$$\begin{aligned}
T_2(x_1,x_2,t) &= x_2^2 + (1+t+\cdots)x_1x_2 + (1+t+\cdots)x_1 - (1+t+\cdots)\\
T_1(x_1,t) &= x_1^2 + (1+t+\cdots)x_1.
\end{aligned}$$

such that $F_i \equiv 0 \mod \langle T_2, T_1, t^n\rangle$.

Theorem 1. *Let $F_1,\dots,F_n \in \mathbb{Q}[[t]][x_1,\dots,x_n]$. The number of solutions of $\langle F_1,\dots,F_n\rangle$ is bounded by $\prod_{i=1}^n \deg(F_i)$*

Proof. ? $\square$

Let us now begin to develop the desired algorithm. First recall that F_i is required to reduce to $0 \mod \langle T_1,\dots,T_n\rangle$, we claim this is if and only if there exists $H_{i,1},\dots,H_{i,m}$ such that

$$F_i = H_{i,1}T_1 + \cdots + H_{i,n}T_n.$$

(That is, F_i is a linear combination of elements in $\{T_1, \ldots, T_n\}$.)

We can write the requirement that $F_1, \ldots, F_n$ reduces to 0 mod $\langle T_1, \ldots, T_n \rangle$ as a matrix expression:

$$\begin{bmatrix} F_1 \\ \vdots \\ F_n \end{bmatrix} = \begin{bmatrix} H_{1,1} & \cdots & H_{1,n} \\ \vdots & \ddots & \vdots \\ H_{n,1} & \cdots & H_{n,n} \end{bmatrix} \begin{bmatrix} T_1 \\ \vdots \\ T_n \end{bmatrix}$$

(note the $H_{i,j}$'s aren't necessarily unique, which is problematic).

Suppose we know $(T_{1,\text{init}}, \ldots, T_{n,\text{init}})$ such that $F_1, \ldots, F_n$ reduces to 0 mod $\langle t^i, T_{1,\text{init}}, \ldots, T_{n,\text{init}} \rangle$. We would like to find $\delta_1, \ldots, \delta_n$ (polynomials) such that $\delta_1 \in \mathbb{Q}[[t]][x_1]$, $\delta_2 \in \mathbb{Q}[[t]][x_1, x_2]$, and so on, such that

$$\begin{bmatrix} \delta_1 \\ \vdots \\ \delta_n \end{bmatrix} \equiv \begin{bmatrix} \frac{\partial T_1}{\partial x_1} & \cdots & \frac{\partial T_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial T_n}{\partial x_1} & \cdots & \frac{\partial T_n}{\partial x_n} \end{bmatrix} \begin{bmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial x_1} & \cdots & \frac{\partial F_n}{\partial x_n} \end{bmatrix}^{-1} \begin{bmatrix} F_1 \\ \vdots \\ F_n \end{bmatrix} \mod \left\langle t^{2i}, T_{1,\text{init}}, \ldots, T_{n,\text{init}} \right\rangle$$

(each one of these steps in non-trivial).

We will omit the proof of this development as it is similar enough to the proof given in §7.