CS681	Computational Number Theory

Lecture 26 : Hensel Lifting

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

We first saw two algorithms to factor univariate polynomials over finite fields. We shall now get into bivariate factoring over finite fields. Before that, we need to look at a very important and powerful tool called Hensel Lifting.

1 Hensel Lifting

The intuition behind Hensel Lifting is the following - you have a function for which you need to find some root. Suppose you have an x very close to a root x_0 in the sense that there is a small error. The question is how can you use x and the polynomial to get a closer approximation?

Recall the Newton Rhapson Method you might have done in calculus to find roots of certain polynomials. Let us say f is the polynomial and x_0 is our first approximation of a root. We would like to get a better approximation. For this, we just set $x_1 = x_0 + \varepsilon$. And by the Taylor Series,

$$\begin{aligned} f(x_1) = f(x_0 + \varepsilon) &= f(x_0) + \varepsilon f'(x_0) + \varepsilon^2 \frac{f''(x)}{2!} + \cdots \\ &= f(x_0) + \varepsilon f'(x_0) + O(\varepsilon^2) \end{aligned}$$

Ignoring the quadratic error terms, we want a better approximation. Thus, in a sense, we would want $f(x_1)$ to be very close to 0. To find the right ε that would to the trick, we just set $f(x_1) = 0$ and solve for ε. With just some term shuffling, we get

$$\epsilon = -\frac{f(x_0)}{f'(x_0)} \implies x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

But one crucial property we need here is that $f'(x_0)$ is not zero for otherwise division doesn't make sense. In the same spirit, we shall look at version 1 of the Hensel Lifting.

1.1 Hensel Lifting: Version 1

Theorem 1. *Let p be a prime and c and positive integer, and let f any polynomial. Suppose we have a solution x that satisfies*

$$f(x) = 0 \bmod p^c \qquad , \qquad f'(x) \neq 0 \bmod p$$

then we can "lift" x to a better solution $x^\star$ that satisfies

$$f(x^\star) = 0 \bmod p^{2c} \qquad , \qquad x^\star = x \bmod p^c$$

It is of course clear that if $f(x^\star) = 0 \bmod p^{2c}$ then $f(x^\star) = 0 \bmod p^c$ but the converse needn't be true. Therefore, $x^\star$ is a more accurate root of f. The proof of this is entirely like the proof of the Newton Rhapson Method.

Proof. Set $x^\star = x + hp^c$. We need to find out what h is. Just as in newton rhapson,

$$\begin{aligned} f(x^\star) = f(x + hp^c) &= f(h) + hp^c f'(x) + (hp^c)^2 \frac{f''(x)}{2!} + \cdots \\ &= f(h) + hp^c f'(x) + O((hp^c)^2) \\ &= f(h) + hp^c f'(x) \bmod p^{2c} \end{aligned}$$

Since we want $f(x^\star) = 0 \bmod p^{2c}$, we just set the LHS as zero and we get

$$h = \frac{f(x)}{p^c f'(x)}$$

Note that $f(x) = 0 \bmod p^c$ and therefore it makes sense to divide $f(x)$ by p^c. Thus our $x^\star = x + hp^c$ where h is defined as above and by definition $x^\star = x \bmod p^c$. ☐

Another point to note here is that since $x^\star = x \bmod p^c$, $f(x^\star) \neq 0 \bmod p$ as well. Therefore, we could lift even further. And since the accurace doubles each time, starting with $f(x) = 0 \bmod p$, i lifts will take us to an $x^\star$ such that $f(x^\star) = 0 \bmod p^{2^i}$.

Hensel Lifting allows us to get very good approximations to roots of polynomials. The more general version of Hensel Lifting plays a very central role in Bivariate Polynomial Factoring.

1.2 Hensel Lifting: Version 2

In the first version of the Hensel Lifting, we wanted to find a root of f. Finding an α such that $f(\alpha) = 0 \bmod p$ is as good as saying that we find a factorization $f(x) = (x-\alpha)g(x) \bmod p$. And also, the additional constraint that $f'(\alpha) \neq 0 \bmod p$ is just saying that α is not a repeated root of f or in other words $(x-\alpha)$ does not divide g. With this in mind, we can give the more general version of the Hensel Lifting.

Theorem 2. *Let R be a UFD and $\mathfrak{a}$ any ideal of R. Suppose we have a factorization $f = gh \bmod \mathfrak{a}$ with the additional property that there exists $s,t \in R$ such that $sg + th = 1 \bmod \mathfrak{a}$. Then, we can lift this factorization to construct $g^\star, h^\star, s^\star, t^\star$ such that*

$$\begin{aligned} g^\star &= g \bmod \mathfrak{a} \\ h^\star &= h \bmod \mathfrak{a} \\ f &= g^\star h^\star \bmod \mathfrak{a}^2 \\ s^\star g^\star + t^\star h^\star &= 1 \bmod \mathfrak{a}^2 \end{aligned}$$

Further, for any other g', h' that satisfy the above four properties, there exists a $u \in \mathfrak{a}$ such that

$$\begin{aligned} g' &= g^\star(1+u) \bmod \mathfrak{a}^2 \\ h' &= h^\star(1-u) \bmod \mathfrak{a}^2 \end{aligned}$$

Therefore, the lifted factorization in some sense is unique.

Proof. (sketch) Set $g^\star = g + te$ and $h^\star = h + se$. Now solve for e and that should do it. Finding $s^\star, t^\star$ is also similar. (painful!) $\square$

Here is a more natural way is to look at this. What we want is a solution to the curve $XY = f$ where f is the function we want to factorize. Let us call $F(X,Y) = f - XY$. We have X, Y as solutions such that $F(X,Y) = f - XY = e$. Now

$$\begin{aligned} F(X+\Delta X, Y+\Delta Y) &= f - (X+\Delta X)(Y+\Delta Y) \\ &= f - XY - (X\Delta Y + Y\Delta X) + O(\Delta^2) \\ &= F(X,Y) - (X\Delta Y + Y\Delta X) \\ &= e - (X\Delta Y + Y\Delta X) \end{aligned}$$

Further, we also know that $sX + tY = 1$ and therefore, if we just set $\Delta X = se$ and $\Delta Y = te$, we have

$$F(X+\Delta X, Y+\Delta Y) = e - e(sX+tY) = 0 \bmod \Delta^2$$

One should also be able to look at the lifts of s and t as solving appropriate equations. In the next class, we shall look at this technique put to use in Bivariate Factorization.