Lec16B Univariate Hensel Lifting

March 11, 2021 1:15 PM

Algorithm Univariate Hensel Lifting 6.5

Input $a \in \mathbb{Z}[x]$, p an odd prime s.t. $p \nmid lc(a)$ $cont(a) = 1$.
$u_0, w_0 \in \mathbb{Z}_p[x]$ s.t. $a - u_0 w_0 \equiv 0 \mod p$
and $\gcd(u_0, w_0) = 1$ in $\mathbb{Z}_p[x]$.
$B > \|f\|_\infty$, $f | a$.

Output Either $u, w \in \mathbb{Z}[x]$ s.t. $a - u \cdot w = 0$
OR FAIL $\Rightarrow \nexists\, u, w \in \mathbb{Z}[x]$ s.t. $a - uw = 0$
with $u \equiv u_0 \mod p$, $w \equiv w_0 \mod p$

$\alpha \leftarrow lc(a)$ $a \leftarrow \alpha \cdot a$ $B \leftarrow \alpha B$.
$u_0 \leftarrow \alpha \cdot (u_0 / lc(u_0)) \mod p$
$w_0 \leftarrow \alpha \cdot (w_0 / lc(w_0)) \mod p$ } $a - u^0 \cdot w^0 \equiv 0 \pmod p$.

Solve $s w_0 + t u_0 = 1$ for $s, t \in \mathbb{Z}_p[x]$: $\deg(s) < \deg(u_0)$.
$u^{(1)} \leftarrow u_0$, $w^{(1)} \leftarrow w_0$, $k \leftarrow 1$
do
  $e_k \leftarrow a - u^{(k)} \cdot w^{(k)} \in \mathbb{Z}[x]$
  if $e_k = 0$ then output $u^{(k)}, w^{(k)}$ $\leftarrow pp(u^{(k)}), pp(w^{(k)})$.
  if $p^k > 2B$ then output FAIL
  $c_k \leftarrow (e_k / p^k) \mod p$
  # Solve $u_k w_0 + w_k u_0 = c_k$ for $u_k, w_k \in \mathbb{Z}_p[x]$
  $(r, q) \leftarrow rem(c_k \cdot s, u_0), quo(c_k \cdot s, u_0)$
  $u_k, w_k \leftarrow r,\ w_0 q + c_k t$
  $u^{(k+1)} \leftarrow u^{(k)} + u_k p^k$ $u^{(k+1)} \leftarrow \alpha \cdot u^{(k+1)} / lc\, u^{(k+1)} \mod p^{k+1}$
  $w^{(k+1)} \leftarrow w^{(k)} + w_k p^k$ $w^{(k+1)} \leftarrow \alpha \cdot w^{(k+1)} / lc\, w^{(k+1)} \mod p^{k+1}$.
  $k \leftarrow k+1$

Hensel lifting example : monic case

```
> a := x^5-19*x^3+9*x^2+84*x-108;
```

$$a := x^5 - 19\,x^3 + 9\,x^2 + 84\,x - 108$$

Let us try to factor a over ℤ.

```
> Factor(a) mod 5;
```

$$\left(x^2 + 3\right)\left(x + 1\right)\left(x + 2\right)^2$$

```
> Factor(a) mod 7;
```

$$\left(x^3 + 2\right)\left(x^2 + 2\right)$$

Perhaps a has a quadratic and cubic factor.

```
> p := 7;
  `mod` := mods;
```

$$p := 7$$

$$mod := mods$$

```
> u0 := x^3+2;
```

$$u0 := x^3 + 2$$

```
> w0 := x^2+2;
```

$$w0 := x^2 + 2$$

Now, to perform Hensel lifting modulo , we need to ensure that u0 and w0 are relatively prime modulo p.

```
> Gcd(u0,w0) mod p;
```

$$1$$

The first order approximations are just

```
> u := u0; w := w0;
```

$$u := x^3 + 2$$

$$w := x^2 + 2$$

```
> e1 := expand( a - u*w );
```

$$e1 := -21\,x^3 + 7\,x^2 + 84\,x - 112$$

```
> c1 := e1/p;
```

$$c1 := -3\,x^3 + x^2 + 12\,x - 16$$

Solve mod using the extended Euclidean algorithm.

```
> Gcdex( w0, u0, x, 's', 't' ) mod p;
```

$$1$$

Now we want to find the solution to where we have .

```
> u1 := Rem(c1*s,u0,x,'q') mod p;
```

$$u1 := -x + 1$$

```
> w1 := Expand( w0*q+c1*t ) mod p;
```

$$w1 := -2$$

```
> expand(u1*w0 + w1*u0 = c1) mod p;
```

$$-3\,x^3 + x^2 - 2\,x - 2 = -3\,x^3 + x^2 - 2\,x - 2$$

Now we want the new th order p-adic approximations

```
> u := u + u1*p;
```

$$u := x^3 - 7\,x + 9$$

```
> w := w + w1*p;
```

$$w := x^2 - 12$$

```
> e2 := expand( a - u*w );
```

$$e2 := 0$$

Since the error is zero we are done.

```
> factor(a);
```

$$\left(x^3 - 7\,x + 9\right)\left(x^2 - 12\right)$$

Hensel lifting example

This procedure solves $\sigma\, a + \tau\, b = c$ for σ and τ in Zp[x]

```
> DiophantSolve := proc(a,b,c,x,p)
  local g,sigma,tau,q,s,t;
      g := Gcdex(a,b,x,'s','t') mod p;
      if g <> 1 then error "a and b are not relatively prime!" fi;
      sigma := Rem(c*s,b,x,'q') mod p;
      # c s a = b (aq) + sigma a
      tau := Expand(c*t+q*a) mod p;
      return( sigma,tau );
  end:
```

```
> p := 5;
```

$$p := 5$$

```
> `mod` := mods;
```

$$mod := mods$$

```
> a := 16*x^2+58*x+7;
```

$$a := 16\,x^2 + 58\,x + 7$$

```
> u0,w0 := x+1, x+2;
```

$$u0, w0 := x + 1, x + 2$$

Check that the conditions required for Hensel lifting to work

```
> Expand( a-u0*w0 ) mod p;
```

$$0$$

```
> Gcd(u0,w0) mod p;
```

$$1$$

```
> alpha := lcoeff(a,x);
```

$$\alpha := 16$$

```
> a := alpha*a;
```

$$a := 256\,x^2 + 928\,x + 112$$

```
> u,w := u0,w0;
```

$$u, w := x + 1, x + 2$$

```
> u,w := (alpha*u mod p, 16*w mod p);
```

$$u, w := x + 1, x + 2$$

```
> e1 := expand( a-u*w );
```

$$e1 := 255\,x^2 + 925\,x + 110$$

```
> c1 := e1/p mod p;
```

$$c1 := x^2 + 2$$

```
> u1,w1 := DiophantSolve(w0,u0,c1,x,p);
```

$$u1, w1 := -2, x + 1$$

```
> Expand( u1*w0+w1*u0 - c1 ) mod p;
```

$$0$$

```
> u,w := (u0 + u1*p, w0 + w1*p);
```

$$u, w := -9 + x, 6\,x + 7$$

```
> u,w := (alpha*u mod p^2, alpha/6*w mod p^2);
```

$$u, w := 6 - 9\,x, -9\,x + 2$$

```
> e2 := expand( a-u*w );
```

$$e2 := 175\,x^2 + 1000\,x + 100$$

```
> c2 := e2/25 mod p;
```

$$c2 := 2\,x^2 - 1$$

```
> u2,w2 := DiophantSolve(w0,u0,c2,x,p);
```

$$u2, w2 := 1, 2\,x + 2$$

```
> u,w := (u+u2*p^2,w+w2*p^2);
```

$$u, w := 31 - 9\,x, 41\,x + 52$$

```
> u,w := (u/(-9)*alpha mod p^3, w/(41)*alpha mod p^3);
```

$$u, w := 56 + 16\,x, 16\,x + 2$$

```
> e3 := expand( a-u*w );
```

$$e3 := 0$$

```
> u := primpart(u,x);
  w := primpart(w,x);
```

$$u := 7 + 2\,x$$

$$w := 8\,x + 1$$

Hensel lifting example.

This procedure solves $\sigma a + \tau b = c$ for σ and τ in Zp[x]

```
> DiophantSolve := proc(a,b,c,x,p)
  local g,sigma,tau,q,s,t;
      g := Gcdex(a,b,x,'s','t') mod p;
      if g <> 1 then error "a and b are not relatively prime!" fi;
      sigma := Rem(c*s,b,x,'q') mod p;
      # c s a = b (aq) + sigma a
      tau := Expand(c*t+q*a) mod p;
      return( sigma,tau );
  end:
```

```
> a := 10*x^5-59*x^3+45*x^2+84*x-108;
```

$$a := 10\,x^5 - 59\,x^3 + 45\,x^2 + 84\,x - 108$$

```
> b := 2*x^5-3*x^3-5*x^2+4*x^4+4*x+18;
```

$$b := 2\,x^5 - 3\,x^3 - 5\,x^2 + 4\,x^4 + 4\,x + 18$$

```
> gcd(a,b);
```

$$2\,x^3 - 7\,x + 9$$

Use Hensel lifting to find $g = \mathrm{GCD}(a, b)$ where, note, a and b are primitive.

```
> `mod` := mods;
  p := 7;
```

$$mod := mods$$

$$p := 7$$

```
> u0 := Gcd(a,b) mod p;
```

$$u0 := x^3 + 1$$

```
> w0 := Quo(a,u0,x) mod p;
```

$$w0 := 3\,x^2 - 3$$

Hensel lifting modulo p^k. Ensure $GCD(u_0, w_0) = 1$.

```
> Gcd(u0,w0) mod 7;
```

$$x + 1$$

I'll try another prime.

```
> p := 11;
```

$$p := 11$$

```
> u0 := Gcd(a,b) mod p;
```

$$u0 := x^3 + 2\,x - 1$$

```
> w0 := Quo(a,u0,x) mod p;
```

$$w0 := -x^2 - 2$$

```
> Gcd(u0,w0) mod p;
```

$$1$$

```
> alpha := lcoeff(a);
```

$$\alpha := 10$$

```
> a := alpha*a;
```

$$a := 100\,x^5 - 590\,x^3 + 450\,x^2 + 840\,x - 1080$$

```
> u0 := alpha*u0/lcoeff(u0) mod p;
```

$$u0 := -x^3 - 2\,x + 1$$

```
> w0 := alpha*w0/lcoeff(w0) mod p;
```

$$w0 := -x^2 - 2$$

Just to check that the new a and u0, w0 satisfy $a - u0\,w0 = 0 \ \mathbf{mod}\ p$.

```
> expand( a - u0*w0 ) mod p;
```

$$0$$

The first order approximations are just

```
> u := u0; w := w0;
```

$$u := -x^3 - 2\,x + 1$$

$$w := -x^2 - 2$$

```
> e1 := expand( a - u*w );
```

$$e1 := 99\,x^5 - 594\,x^3 + 451\,x^2 + 836\,x - 1078$$

```
> c1 := (e1/p) mod p;
```

$$c1 := x^3 - x - 3\,x^2 + 1 - 2\,x^5$$

```
> u1,w1 := DiophantSolve(w0,u0,c1,x,p);
```

$$u1, w1 := -5\,x + 5, 2\,x^2$$

```
> Expand( u1*w0 + w1*u0 - c1 ) mod p;
```

$$0$$

Now we want the new $k + 1$ th order p-adic approximations

```
> u := u + u1*p;
```

$$u := -x^3 - 57\,x + 56$$

```
> w := w + w1*p;
```

$$w := 21\,x^2 - 2$$

```
> u := alpha * u/lcoeff(u) mod p^2;
```

$$u := 10\,x^3 - 35\,x + 45$$

```
> w := alpha * w/lcoeff(w) mod p^2;
```

$$w := 10\,x^2 - 24$$

A check that they really are 2nd order approximations

```
> expand( a - u*w ) mod p^2;
```

$$0$$

Computer the new error. Since it's zero we are done.

```
> e2 := expand( a - u*w );
```

$$e2 := 0$$

```
> u,w := primpart(u),primpart(w);
```

$$u, w := 2\,x^3 - 7\,x + 9, 5\,x^2 - 12$$