6.885 Algebra and Computation October 5, 2005

Lecture 8

Lecturer: Madhu Sudan *Scribe: Guy Rothblum*

Today we will complete the description of Berlekump's deterministic algorithm for efficiently factorizing polynomials over $\mathbb{F}_q$ (where $q = p^t$ for a prime p) in time polynomial in $\deg(f)$, t, p.

We will then begin laying the groundwork for algorithms that factor polynomials over $\mathbb{Z}[x]$ and for factoring bivariate polynomials. We will see these two problems are related and introduce Hensel's Lifting, a useful tool for solving them.

1 A deterministic Algorithm—Continued

Recall that we saw in the last lecture that for any reducible polynomial $f(x) \in \mathbb{F}_q$ of degree $2d$, there exists a polynomial $g(x) \in \mathbb{F}_q$ s.t. $f(x)|g(x)^p - g(x)$ and the degree of $g(x)$ is at most $2d - 1$. We also saw that if we could find this $g(x)$ efficiently then we could factor efficiently. We will proceed to show how to find g efficiently.
Recall also that the field $\mathbb{F}_q$ is isomorphic to the t-dimentional (additive) vector space $\mathbb{F}_p^t$, where the isomorphism maps every element $\alpha \in \mathbb{F}_q$ to a vector $v_\alpha \in \mathbb{F}_p^t$.

Claim 1 *The map $A : v_\alpha \rightarrowtail v_{\alpha^p}$ is a linear map.*

Proof
We only need to verify that:

1. $A(v_{\alpha+\beta}) = v_{(\alpha+\beta)^p} = v_{\alpha^p+\beta^p (\text{mod } p)} = v_{\alpha^p} + v_{\beta^p} = A(v_\alpha) + A(v_\beta)$
2. $A(v_{a\cdot\alpha}) = a \cdot A(v_\alpha)$

■

Since A is a linear map, it can be represented by a $t \times t$ matrix $A \in \mathbb{F}_p^{t\times t}$

Fact 2 *Given one of the "nice" representations of $\mathbb{F}_q$ (e.g. $\mathbb{F}_q$ represented as a vector space or using an irreducible polynomial), the matrix A can be computed efficiently.*

How does this fact help us? We want to find $g(x)$ s.t. $f(x)|g(x)^p - g(x)$, where $f(x)$ is known but $g(x)$ is unknown. We will use the linear map A to find $g(x)$! We view $g(x)$ as $g(x) = \sum_{i=0}^{2d-1} c_i \cdot x^i$, where the c_i's are unknowns, and get that:

$$g(x)^p = (\sum_{i=0}^{2d-1} c_i \cdot x^i)^p = \sum_{i=0}^{2d-1} c_i^p \cdot x^{i\cdot p}$$

To find $g(x)$ we will construct a system of linear equations. Towards this end we define two new polynomials $h(x), a(x)$ where $h(x) = g(x)^p$ and $a(x) \cdot f(x) = g(x)^p - g(x) = h(x) - g(x)$.

Let $\{e_i\}_{i=0}^{p\cdot(2d-1)}$ and $\{a_i\}_{i=0}^{p\cdot(2d-1)-2d}$ be the coefficients of $h(x)$ and $a(x)$ respectively. We get that:

$$h(x) = \sum_{j=0}^{p\cdot(2d-1)} e_j \cdot x^j = \sum_{i=0}^{2d-1} c_i^p \cdot x^{i\cdot p} = g(x)^p$$

1. The first system of constraints will reflect the equality $h(x) = g(x)^p$:
   (a) For any integer j that is not a multiple of p: $e_j = 0$.
   (b) For any integer i: $e_{i\cdot p} = c_i^p = A \times c_i$.
2. The second constraint specifies that $f(x) \cdot a(x) = h(x) - g(x)$. Looking at the coefficients on both sides and at $f(x)$ as $\sum_{i=0}^{2d} f_i \cdot x^i$, for the j-th coefficient we get the constraint:
   $$e_j - c_j = \sum_{i=0}^{j} f_i \cdot a_{j-i} = \sum_{i=0}^{j} M_{f_i} \cdot a_{j-i}$$
   Where M_{f_i} is the matrix representation of f_i (recall this matrix representation supports multiplication).
3. Finally, we would like for the solution to be non-trivial, and thus we add the constraint $(c_1, \ldots c_{2d-1}) \neq (0, \ldots 0)$. Note that while this is not a linear equation per se, it can be incorporated into the algorithm for solving the other linear equations, so that the algroithm returns a non-zero solution when one exists.

Now, to find $g(x)$ all that remains is to solve this system of (linear) equations! Note that this is *not* a proof of existence of a non-trivial $g(x)$, we proved $g(x)$'s existence in the previous lecture, this is simply an efficient procedure for finding $g(x)$.

2 Framework for the Next Talks

In the next talks we see how to factor bivariate polynomials and polynomials over the rational numbers $\mathbb{Q}[x]$. We begin by laying out the framework that we will follow in these (surprisingly) related results.

Factoring Bivariate Polynomials We will see how to go from factoring polynomials to factoring bivariate polynomials, we will go from factoring $\mathbb{R}[x]$ to factoring $\mathbb{R}[x, y]$. Given $f(x, y) \in \mathbb{R}[x, y]$, we will factor it using an algorithm for factoring in $\mathbb{R}[x]$. We proceed in several steps:

1. Somehow (the details will follow) "perturb" $f(x, y)$ into $\tilde{f}(x, y)$.
2. Begin by factoring $\tilde{f}(x, y) (\mathrm{mod}\ y)$ using the algorithm for factoring in $\mathbb{R}[x]$.
3. Proceed in Hensel iterations, and progressively go from factoring $\tilde{f}(x, y) (\mathrm{mod}\ y^i)$ to factoring $\tilde{f}(x, y) (\mathrm{mod}\ y^{2i})$.
4. From factoring over $\mathbb{R}[x, y] (\mathrm{mod}\ \ y^t)$, go to factoring over $\mathbb{R}[x, y]$.

Factoring over $\mathbb{Q}[x]$: To factor polynomials over integers $\mathbb{Z}[x]$, we actually factor over $\mathbb{Q}[x]$ (we couldn't really expect to factor over $\mathbb{Z}[x]$, since the polynomials of degree 0 there are integers...). We proceed similarly to the bivariate case:

1. Somehow pick a "nice" prime p.
2. Begin by factoring $f(x)(\text{mod } p)$.
3. Proceed in Hensel iterations, and progressively go from factoring $f(x)(\text{mod } p^i)$ to factoring $f(x)(\text{mod } p^{2i})$.
4. From factors over $\mathbb{Z}[x](\text{mod } p^t)$, go to factoring over $\mathbb{Z}[x]$.

As can be seen, the two seemingly unrelated problems of factoring integers and bivariate polynomials, are actually closely tied together by our plan of action and its use of Hensel iterations.

3 Hensel's Lifting Lemma

We want to go from a factorization $f(x) = g(x) \cdot h(x) \pmod p$ to $f(x) = \tilde{g}(x) \cdot \tilde{h}(x) \pmod{p^2}$. One appealing idea is to take $\tilde{g}(x) = g(x) \pmod p$ and $\tilde{h}(x) = h(x) \pmod p$. Unfortunately, this natural idea fails, as can be seen in the simple case:

$$f(x) = x^2 - 2x + 6 = (x-1) \cdot (x-1) \pmod 5$$

We want $\tilde{g}(x) = (x-1) + 5 \cdot a(x)$ and $\tilde{h}(x) = (x-1) + 5 \cdot b(x)$, which implies that modulo 25 we should get: $f(x) = (x-1)^2 + 5 \cdot (x-1) \cdot (a(x) + b(x)) + 25a(x) \cdot b(x)$. Unfortunately, $f(x)$ isn't of this form modulo 25!
To overcome this obstacle, we observe that our natural idea may have failed in the example above simply because the factors $g(x), h(x)$ were not relatively prime. Before stating the Lemma itself, note that by J^2 we refer to the collection of linear combinations of products of pairs of items in J.

Lemma 3 *Hensel's Lifing Lemma:*
For a ring R and an ideal $J \subseteq R$:
***If** there exist $f, g, h, a, b \in R$ such that:*

1. *$f - g \cdot h \in J$ ($f = g \cdot h \pmod J$).*
2. *$a \cdot g + b \cdot h = 1 \pmod J$ (f and g are relatively prime).*

***Then** there exists a lifting: there exist $\tilde{g}, \tilde{h} \in R$ such that:*

1. *$\tilde{g} = g \pmod J$.*
2. *$\tilde{h} = h \pmod J$.*
3. *$f = \tilde{g} \cdot \tilde{h} \pmod{J^2}$.*

We refer to the set of conditions satisfied by $\tilde{g}$ and $\tilde{h}$ as $(*)$.
The lift is ***unique****: for any g^*, h^* satisfying $(*)$, there exists $u \in J$, such that $g^* = \tilde{g} \cdot (1+u)$ and $h^* = \tilde{h} \cdot (1-u)$.*
Furthermore, for any $\tilde{g}, \tilde{h}$ that satisfy $(*)$, there exist $\tilde{a}, \tilde{b} \in R$, such that $\tilde{a} \cdot \tilde{g} + \tilde{b} \cdot \tilde{h} = 1 \pmod{J^2}$. Thus the new factors are also relatively prime and we can continue to activate Hensel's Lemma.

Proof
We prove each of the guaranteed properties separately:

The existence of a lifting: We proceed as before (but with relatively prime factors!).
$f = g \cdot h + q$ for some $q \in J$, $\tilde{g} = g + g_1$, $\tilde{h} = h + h_1$, where $g_1, h_1 \in J$.
We get that: $\tilde{g} \cdot \tilde{h} = g \cdot h + g_1 \cdot h + h_1 \cdot g + h_1 \cdot g_1$.
Since $h_1 \cdot g_1 \in J^2$, it remains to show that $q = g_1 \cdot h + h_1 \cdot g + h_1$.
We still haven't specified g_1, h_1, so to satisfy this condition we take $g_1 = b \cdot q$, $h_1 = a \cdot q$, and get that $g_1 \cdot h + h_1 \cdot g + h_1 = q \cdot (b \cdot h + a \cdot g) = q$, as required!

$\tilde{g}$ and $\tilde{h}$ are relatively prime: Observe that: $a \cdot \tilde{g} + b \cdot \tilde{h} = a \cdot g + b \cdot h + r' = 1 + r$, for some $r', r \in J$. Now we can take $\tilde{a} = a \cdot (1-r)$ and $\tilde{b} = b \cdot (1-r)$, and get that:

$$\tilde{a} \cdot \tilde{g} + \tilde{b} \cdot \tilde{h} = (1-r) \cdot (a \cdot \tilde{g} + b \cdot \tilde{h}) = (1-r)(1+r) = 1 - r^2 = 1 \pmod{J^2}$$

Uniqueness: Let $g^* = \tilde{g} + g_2$ and $h^* = \tilde{h} + h_2$ for some $g_2, h_2 \in J$ (because, modulo J, we know that $g^* = g = \tilde{g}$ and $h^* = h = \tilde{h}$). Furthermore, modulo J^2, we know that $g^* \cdot h^* = f = \tilde{g} \cdot \tilde{h}$.
Now we get that: $g^* \cdot h^* = \tilde{g} \cdot \tilde{h} + g_2 \cdot \tilde{h} + h_2 \cdot \tilde{g} + g_2 \cdot h_2$. This implies that $g_2 \cdot \tilde{h} + h_2 \cdot \tilde{g} \in J^2$ (because $g_2 \cdot h_2 \in J^2$ and $g^* \cdot h^* = \tilde{g} \cdot \tilde{h} \pmod{J^2}$).

Claim 4 *The only way to get that $g_2 \cdot \tilde{h} + h_2 \cdot \tilde{g} \in J^2$ is by setting $g_2 = u \cdot \tilde{g}$ and $h_2 = -u \cdot \tilde{h}$ for some $u \in J$.*

■

Note that in class it was pointed out that these are existence results. We did not reach a definitive conclusion about whether there is a problem in actually finding r, q etc.
In the next talk we will complete the procedure for factorizing bivariate polynomials.