6.885 Algebra and Computation October 26, 2005

Lecture 13

Lecturer: Madhu Sudan *Scribe: Michael Manapat*

In today's lecture, we'll complete the analysis of the LLL algorithm and finish factoring over $\mathcal{Q}[X]$ (details will be left to the exercises).

1 LLL Analysis

Let $b_1, \ldots, b_n \in \mathbb{Z}^n$ be lattice points and let $\text{Ł}(b_1, \ldots, b_n)$ be the lattice generated by $b_1, \ldots, b_n$, i.e., the set of all $\mathbb{Z}$-linear combinations of $b_1, \ldots, b_n$:

$$\text{Ł}(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} \lambda_i b_i : \lambda_i \in \mathbb{Z} \right\}.$$

Our goal is to find a short vector in Ł.

Before continuing, we recall some notational conventions:

- b_i^* will denote the projection of b_i in the direction orthogonal to the subspace generated by $b_1, \ldots, b_{i-1}$, and
- $b_i(j)$ will denote the projection of b_i to the subspace orthogonal to the one generated by $b_1, \ldots, b_{i-1}$.

Note that the by the way the Gram-Schmidt orthogonalization procedure works, each b_i is a linear combination (over $\mathbb{R}$) of the b_j^*, $j \leq i$:

$$b_i = \sum_{j=1}^{i} \mu_{ij} b_j^*.$$

The matrix $\{\mu_{ij}\}$ is then a lower-triangular matrix with 1s on the diagonal.

Now we can describe the LLL algorithm:

Step 1: Gram-Schmidt Reduction
for $i = 1$ to n **do**
    for $j = i - 1$ to 1 **do**
        $m \leftarrow \text{round}(\mu_{ij})$
        $b_i \leftarrow b_i - m b_j$
    end for
end for
Step 2: Swap
if there is an i such that $\|b_i(i-2)\| \leq \frac{3}{4}\|b_{i-1}(i-2)\|$ **then**
    swap b_i and b_{i-1}
    go to Step 1
else
    stop and output b_1
end if

1.1 LLL Potential Function

Let $\text{Vol}_i(b_1, \ldots, b_i)$ denote the volume of the parallelpiped formed by the vectors $b_1, \ldots, b_i$ in Euclidean space. In the case of n vectors in n-space, this volume is just the determinant of the matrix whose columns are the coefficients of the b_j. Equivalently, this volume is the product of the lengths of the b_j^*:

$$\mathrm{Vol}_i(b_1, \ldots, b_i)) = \prod_{j=1}^{i} \|b_j^*\|.$$

Now we define a potential function Φ by

$$\Phi = \prod_{i=1}^{n} \mathrm{Vol}_i(b_1, \ldots, b_i).$$

We can get a sense of the running time of the LLL algorithm by making the following observations:

- Φ is always an integer (each Vol_i is clearly an integer, being the determinant of an integer matrix).
- Φ remains unchanged in step 1 of the algorithm.
- Φ decreases by a factor of $3/4$ in step 2 if a swap is made (Vol_{i-1} decreases by $3/4$, but all other volumes remain unchanged).
- At the start, $\|b_i^*\| \leq n2^l$, so initially $\Phi \leq (n2^l)^{n^2}$, i.e., $\Phi \leq 2^{\mathrm{poly}(l,n)}$.

Since the potential function is decreasing exponentially fast, and initially has a value that is exponential in a polynomial of l and n, we can conclude that the number of repeated loops (i.e., the number of times steps 1 and 2 are executed) is polynomial in l and n.

Now we turn to the correctness of the algorithm.

Lemma 1 *If $b_1, \ldots, b_n$, $b_1^*, \ldots, b_n^*$, and $\{\mu_{ij}\}$ as earlier satisfy*

1. *for all $i > j$, $|\mu_{ij}| \leq 1/2$, and*
2. *for all i, $\|b_i(i-2)\| > \frac{3}{4}\|b_{i-1}(i-2)\|$,*

then for all nonzero vectors $v \in L(b_1, \ldots, b_n)$, $\|b_1\| \leq 2^n\|v\|$.

Clearly the second condition in the lemma is satisfied after the algorithm terminates (step 2 clearly ensures this). We leave it as an easy exercise to show that the reduction procedure in step 1 results in a matrix $\{\mu_{ij}\}$ all of whose entries are bounded in magnitude by $1/2$. We will prove the claim in two steps.

Claim 2 *For all b_i, b_j^*, and $v \in L(b_1, \ldots, b_n) \setminus \{0\}$, $\|v\| \geq \min\{\|b_i^*\|\}$.*

Proof We can write

$$v = \sum \lambda_i b_i = \sum \lambda_i^* b_i^*,$$

where the $\lambda_i \in \mathbb{Z}$ and the $\lambda_i^* \in \mathbb{R}$. Since the b_j^* are orthogonal, we have

$$\|v\|^2 = \sum |\lambda_i^*|^2 \|b_i^*\|^2,$$

so it is enough to show that some λ_i^* has magnitude at least 1.

Now $b_i = \sum_j \mu_{ij} b_j^*$, so

$$v = \sum_i \lambda_i \left(\sum_j \mu_{ij} b_j^* \right),$$

and thus

$$\lambda_i^* = \sum_{j \geq i} \mu_{ji} \lambda_j.$$

Let k be the largest index such that $\lambda_k \neq 0$. Then

$$\lambda_k^* = \sum_{j \geq k} \mu_{jk} \lambda_j = \mu_{kk} \lambda_k = \lambda_k.$$

Since $\lambda_k \in \mathbb{Z}$, we conclue that $|\lambda_k^*| \geq 1$, whence the desired conclusion follows. ■

Claim 3 *For all i, $\|b_i^*\| \leq 2\|b_{i+1}^*\|$.*

Proof This follows from the inequality

$$\|b_i^*\| \geq \sqrt{\left(\frac{3}{4}\right)^2 - \left(\frac{1}{2}\right)^2} \|b_{i-1}(i-2)\| \geq \frac{1}{2}\|b_{i-1}^*\|,$$

which one can deduce by drawing a picture of the vectors b_i^* and b_{i-1}^* in the plane. ■

Given the preceding claims, the conclusion of the lemma, and thus the correctness of the LLL algorithm, follows easily.

2 Factoring

Given a polynomial $f \in \mathbb{Z}[X]$ of degree at most d and coefficients bounded in magnitude by 2^n, we find a factor of f as follows:

1. If the greatest common divisor of f and its derivative f' is nontrivial, output that factor and stop.
2. Find a prime p such that the gcd of the images of f and f' in $\mathbb{F}_p[X]$ is also trivial.
3. Factor f as $f = gh \pmod{p^t}$ in $\mathbb{F}_p[X]$, where g and h are monic and relatively prime and g is irreducible in $\mathbb{F}_p[X]$.
4. Use Hensel Lifting to find monic polynomials G and H such that $f = GH \pmod{p^t}$.
5. Find $\bar{g}$ and $\bar{G}$ of appropriate degree such that $\bar{g}(X) = G(X)\bar{G}(X) \pmod{p^t}$.
6. If $\bar{g}$ and f have a nontrivial gcd, output that gcd; otherwise, output "f is irreducible."

2.1 Exercises

We conclude with a series of exercises that address the details of the above procedure:

1. If f and g are relatively prime polynomials of degree d, with coefficients in the range $-c, \ldots, c$, then the resultant is bounded by $O(dc)^{O(d)}$.
2. If$f = g^* h^*$ over the integers and g^* factors into irreducible polynomials in the form $g(x)g_1(x)\cdots g_k(x) \pmod{p}$, then g^* is a candidate polynomial for the $\bar{g}$ of step 5.
3. If $f = gh$ over $\mathbb{Z}[X]$, with the degree of f at most d and the coefficients of f bounded by 2^n, then the coefficients of g are bounded by $O(d)^{O(d)}2^n$.
4. Prove that the g^* of exercise 2 divides any $\bar{g}$ reported in step 5.