Geometry of Numbers
Foundations and Algorithmic Aspects

University of Sydney, Department of Mathematics and Statistics
Damien Stehlé

Second assignment, due 10/10/2008

This assignment will represent 20% of the overall mark.

1 Small questions on LLL

1. Consider the LLL-reduction with parameter $\delta = 0.99$. Give an LLL-reduced basis which is not Minkowski-reduced. Same question with $\delta = 1$.
2. Let $\alpha \in (0, 3/4)$. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a basis of a lattice L. We say it is α-Siegel reduced if for any i we have $\alpha \|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$. Give some properties of LLL-reduced bases that are still satisfied by Siegel-reduced bases and some that are not anymore. Hint: Siegel-reduced bases are not necessarily size-reduced.
3. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a lattice basis and $(\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_d)$ be its dual basis. Show that if $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is Siegel-reduced, then $(\hat{\mathbf{b}}_d, \ldots, \hat{\mathbf{b}}_1)$ is also Siegel-reduced (with that ordering of the vectors). Does it also hold if we replace the Siegel-reduction by the LLL-reduction?

2 Hermite normal form

Let $B \in \mathbb{Z}^{n \times n}$. Then there exists a unimodular matrix U such that the matrix H defined by $H = B \cdot U$ satisfies the three following properties:

(a) The matrix H is upper triangular.

(b) The diagonal coefficients of H are positive.

(c) If $j > i$, then $H_{i,j} \in (-H_{i,i}/2, H_{i,i}/2]$.

The decomposition $A = H \cdot U^{-1}$ is unique and is called the Hermite normal form.

1. Explain how to make all three conditions satisfied when condition (a) already holds.

2. By using the LLL algorithm, show that one can find a matrix U such that $A \cdot U$ has exactly one non-zero entry in its last row. Hint: multiply the last row of A by a large constant, and use the fact that if $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is an LLL-reduced basis of a d-dimensional lattice L, then $\prod_i \|\mathbf{b}_i\| \leq 2^{d^2/4} \cdot \det(L)$.

3. Using the two questions above, describe an algorithm that computes the Hermite normal form. Does this algorithm run in polynomial time?

3 RSA with a small decryption exponent

Let $N = p \cdot q$ be the product of two primes such that $p > q > p/2$. Let e and d be such that $ed = 1 \mod (p-1)(q-1)$. In the RSA cryptosystem, the public key is (N, e) and the private key is (p, q, d). The encryption of an integer $m \in [0, N-1]$ is the operation $m \mapsto m^e \mod N$ and the decryption of an encrypted message c is the operation $c \mapsto c^d \mod N$. Fermat's little theorem ensures that $(m^e)^d = m \mod N$, allowing the receiver to recover the message that was sent to him. The integer d is called the decryption exponent. The smaller d, the faster the decryption. The goal of this exercise is to show that when d is too small, then one can factor N in polynomial time, thus breaking the system.

In the following, we suppose that e belongs to $[N/2, N]$ and that N and e are known, while p, q and d are unknown. We suppose that $d \leq e^\delta$ for some $\delta < 1$.

1. Let $P(x, y) = x(N + 1 + y) - 1$. Show that P has a root (x_0, y_0) modulo e with $y_0 = -(p + q)$, and
$$|x_0| \leq c_1 \cdot e^\delta \text{ and } |x_1| \leq c_2 \cdot e^{1/2},$$
for some constants c_1 and c_2. Show that if we could find that root (x_0, y_0) in polynomial time, then we could factor N in polynomial time.

2. Let $\alpha \geq 1$ be an integer. Consider the polynomials:
$$\begin{aligned} g_{i,k} &= x^i P^k(x, y) e^{\alpha - k} \quad \text{for} \quad k \in [0, \alpha] \text{ and } i \in [0, \alpha - k] \\ h_{j,k} &= y^j P^k(x, y) e^{\alpha - k} \quad \text{for} \quad k \in [0, \alpha] \text{ and } j \in [1, t], \end{aligned}$$
where t will be determined later on. Show that for any polynomial Q in that family, we have $Q(x_0, y_0) = 0 \mod e^\alpha$.

3. Let $\epsilon > 0$. By using the LLL algorithm on a lattice related to the above polynomials, and by optimizing t, show that if $\delta < 0.284 - \epsilon$, then one can find a polynomial Q such that $Q(x_0, y_0) = 0$ holds over the integers.

4. A single bivariate polynomial is not sufficient to recover the desired y_0 in polynomial time. Suggest a way to work around that difficulty. Hint: use the fact that if $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is an LLL-reduced basis of a d-dimensional integral lattice, then $\prod_i \|\mathbf{b}_i\| \leq 2^{d^2/4} \det(L)$ and $\|\mathbf{b}_1\| \geq 1$.

4 A transference theorem

Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a Hermite-Korkine-Zolotarev-reduced basis of a lattice L. For any $i \leq d$, we define $L^{(i)}$ as the projection of L orthogonally to the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$. Let $\hat{L}$ be the dual of L. The goal of this exercise is to obtain a bound on each quantity $\lambda_i(L)\lambda_{d-i+1}(\hat{L})$ that depends only on the dimension d.

1. Show that for any i and any $j \leq d-i+1$, we have $\lambda_j(\hat{L}) \leq \lambda_j(\widehat{L^{(i)}})$.
2. Show that for any i, we have $\|\mathbf{b}_i\|^2 \leq \sum_{j \leq i} \lambda_1(L^{(j)})^2$.
3. Show that for any i, we have $\lambda_i(L)^2 \lambda_1(\hat{L})^2 \leq d\widetilde{\gamma_d}^2$, where $\widetilde{\gamma_d} = \max_{i \leq d} \gamma_i$ and γ_i is the i-th dimensional Hermite constant.
4. Show that for any i we have $\lambda_i(L)\lambda_{d-i+1}(\hat{L}) \leq d\widetilde{\gamma_d}$.