Monash University
FIT 5124: Advanced Topics in Security
Week 3 Tutorial Sheet

Ron Steinfeld, 17 March 2015

This week's tutorial will cover the LLL lattice reduction algorithm and applications of it (and its variants) to cryptanalysis of and selecting secure parameters for Ajtai's lattice-based hash function.

Problems

1 **GSO.** Let

$$\boldsymbol{b}_1 = \begin{bmatrix} 12 \\ 5 \end{bmatrix}, \boldsymbol{b}_2 = \begin{bmatrix} 3 \\ 8 \end{bmatrix}.$$

- a Find the angle between $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$.
- b Find the component $\boldsymbol{b}_2^{par}$ (aka projection) of $\boldsymbol{b}_2$ parallel to $\boldsymbol{b}_1$ and the component $\boldsymbol{b}_2^*$ of $\boldsymbol{b}_2$ orthogonal to $\boldsymbol{b}_1$.
- c Verify that for any n vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$, the corresponding GSO vectors $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*$ (as defined in the lecture) are pairwise orthogonal.

2 **LLL.** Use LLL properties 1 and 2 of an LLL reduced basis $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ (with $\delta = 3/4$) to deduce that the Hermite Factor $\gamma_{HF} = \frac{\|\boldsymbol{b}_1\|}{\det L(B)^{1/n}}$ of an LLL reduced basis is at most $2^{(n-1)/4}$.

3 **LLL in cryptanalysis.** This problem continues last week's question on Ajtai's cryptographic hash function with parameters $n = 5, q = 31, m = 30$.

- a Use the 'Gaussian Heuristic' approximation $\lambda_1(L) \approx \sqrt{\frac{m}{2\pi \mathrm{e}}} \cdot \det(L)^{1/m}$ for an m-dimensional lattice L, to estimate the length of the shortest vector in the Ajtai hash SIS lattice $L_q^\perp(A)$ with $n = 5, q = 31, m = 30$. Then use this to estimate the length of the first vector in an LLL reduced basis for $L_q^\perp(A)$, using the 'average' LLL Hermite Factor estimate $\gamma_{HF} \approx 1.02^{m-1}$. Compare it to the theoretical upper bound on this length using $\gamma_{HF} \leq 2^{(m-1)/4}$. Do you expect LLL to give a solution to $2\sqrt{m}$-SIS problem for these parameters?
- b Use Sage to run LLL on the basis B for the SIS lattice $L_q^\perp(A)$ (corresponding to the Ajtai hash matrix A with parameters $n = 4, q = 31, m = 30$) you generated for problem 4 of the week 2 tutorial. What is the Euclidean norm of the shortest non-zero lattice vector you get from the LLL reduced basis B'? How does it compare to the estimate of this length in (a)? Does it reveal a collision for Ajtai's hash with $d = 1$? If so, compute the two colliding inputs $\boldsymbol{x} \neq \boldsymbol{x}'$ with $A \cdot \boldsymbol{x} = A \cdot \boldsymbol{x}' \bmod q$.