Lattices and Homomorphic Encryption, Spring 2013 Instructors: Shai Halevi, Tal Malkin

Problem Set #4

March 12, 2013 Due March 26, 2013

1 Sampling Discrete Gaussians over $\mathbb{Z}^n$

In this question we show how to sample from the discrete Gaussian distribution over the integer lattice $\mathbb{Z}^n$.

1. Let $\mathcal{D}$ be an arbitrary distribution with a finite support set X, and denote by $p_{\max}$ the probability mass of the most likely element, $p_{\max} = \max\{\mathcal{D}(x) : x \in X\}$. Consider the following process (called *rejection sampling*):

   (a) Draw a uniform element from the support $x \in_R X$,

   (b) Toss a biased coin with head probability exactly $\mathcal{D}(x)/p_{\max} \in [0,1]$,

   (c) If the coin comes out head then output x, else goto (a).

   Prove that the output distribution of this rejection sampling process is exactly $\mathcal{D}$.

   Hint. For any $x \in X$, analyze the conditional probability $\Pr[\text{output } x|\text{stop after 1st sample}]$. Use the identity $\Pr[A|B] = \Pr[A\&B]/\Pr[B]$.

2. Show that the number of samples taken by the rejection sampling procedure above is distributed according to a geometric distribution with parameter $p = 1/(p_{\max} \cdot |X|)$.

3. For any $s \geq \eta_{2^{-k}}(\mathbb{Z})$, describe an efficient procedure that on input $c \in \mathbb{R}$ samples from a distribution statistically close to $D_{\mathbb{Z},s,c}$, the one-dimensional discrete Gaussian with center c (upto statistical distance $< 2^{-k}$).

   Hint. Consider the distribution $D_{\mathbb{Z},s,c}$ conditioned on the outcome being closer to c than $s\sqrt{k}$. Namely $\mathcal{D}(x)$ is proportional to $D_{\mathbb{Z},s,c}(x)$ if $|x-c| < s\sqrt{k}$, and $\mathcal{D}(x) = 0$ otherwise. To show that $\mathcal{D}$ is close to $D_{\mathbb{Z},s,c}$, you can use the fact that for $s \geq \eta_\epsilon(\mathbb{Z})$ we have

   $$\Pr_{x \sim D_{\mathbb{Z},s,c}}[|x-c| > s\sqrt{k}] < 2e^{-\pi k} \cdot \frac{1+\epsilon}{1-\epsilon}$$

   (no need to prove that fact). Then analyze the number of samples taken by rejection sampling for $\mathcal{D}$, showing that the probability of taking more than (say) $s \cdot k^2$ samples is smaller than 2^{-k}.

4. For any $s > \eta_{2^{-k}}(\mathbb{Z})$ and $n > 0$, describe an efficient procedure that on input $\vec{c} \in \mathbb{R}^n$ samples from a distribution statistically close to $D_{\mathbb{Z}^n,s,\vec{c}}$, the n-dimensional discrete Gaussian with center $\vec{c}$ (upto statistical distance $< n \cdot 2^{-k}$).

Note that $\eta_{2^{-k}}(\mathbb{Z}) < \sqrt{k}$, so the procedure from this problem can be used to sample elements that are closer to $\vec{c}$ than $k\sqrt{n}$ (with overwhelming probability).

2 Reduction Modulo $\mathcal{L}_A^\perp$

Fix parameters $n, q \geq \text{poly}(n), m \geq 2n \log q$, and a matrix $A \in \mathbb{Z}_q^{n \times m}$. Recall that we define

$$\mathcal{L}_A^\perp \stackrel{\text{def}}{=} \{\vec{x} \in \mathbb{Z}^m : A\vec{x} = 0 \pmod{q}\},$$

and that $\mathcal{L}_A^\perp$ is a rank-m lattice. We assume that A has rank n modulo q (i.e., its columns linearly span the entire $\mathbb{Z}_q^n$). Let $B = (b_1 b_2 \dots b_m)$ be an arbitrary basis for $\mathcal{L}_A^\perp$.

1. Prove that for any two distinct points in the basic cell of B, $\vec{v}_1, \vec{v}_2 \in \mathcal{P}(B)$, $\vec{v}_1 \neq \vec{v}_2$, it holds that $A\vec{v}_1 \neq A\vec{v}_2 \pmod{q}$.

2. Prove that if $\mathcal{D}$ is the uniform distribution over the integer vectors in $\mathcal{P}(B)$, then drawing $\vec{x} \leftarrow \mathcal{D}$ and computing the syndrome $\vec{y} = A\vec{x} \bmod q$ yields a uniform distribution over $\mathbb{Z}_q^n$.

3. Let $s \geq \eta_{2^{-k}}(\mathcal{L}_A^\perp)$. Prove that drawing from a discrete Gaussian $\vec{x} \leftarrow D_{\mathbb{Z}^m, s}$ and computing the syndrome $\vec{y} = A\vec{x} \bmod q$, yields a distribution which is close to uniform over $\mathbb{Z}_q^n$ upto statistical distance at most 2^{-k}.