Lattices and Homomorphic Encryption, Spring 2013	Instructors: Shai Halevi, Tal Malkin
Problem Set #3	
February 19, 2013	Due March 12, 2013

1 Intersection of Spheres

Let $\mathbf{B}(\vec{c}, r) \subset \mathbb{R}^n$ denote the n-dimensional sphere of radius r and center $\vec{c}$, and let $\mathcal{U}(\mathbf{B}(\vec{c}, r))$ denote the uniform distribution over this sphere. In this question you can use the following fact:

Fact. The volume of an n-dimensional unit sphere is $\mathrm{vol}(\mathbf{B}(\vec{c}, 1)) = \frac{\pi^{n/2}}{\Gamma(n/2)}$ where the function $\Gamma(x)$ satisfies $\Gamma(x+1) = x \cdot \Gamma(x)$, $\Gamma(1) = 1$, $\Gamma(1/2) = \sqrt{\pi}$, and

$$\lim_{x\to\infty} \frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)} \;=\; \lim_{x\to\infty} \frac{\Gamma(x+1)}{\Gamma(x+\frac{1}{2})} \;=\; \sqrt{x}.$$

(a) Prove that for any $\epsilon \in (0, 1)$, the intersection between two n-dimensional unit spheres whose centers are ϵ apart has volume at least

$$\mathrm{vol}\big(\ \mathbf{B}(\vec{0}, 1) \cap \mathbf{B}(\vec{c}, 1)\ \big) \;\geq\; \mathrm{vol}\big(\ \mathbf{B}(\vec{0}, 1)\ \big) \;\cdot\; \frac{\epsilon(1-\epsilon^2)^{\frac{n-1}{2}}}{3} \cdot \sqrt{n} \cdot (1 - o(1))$$

(where $\vec{c} \in \mathbb{R}^n$ is any vector of Euclidean norm $\|\vec{c}\| = \epsilon$).

Hint. Show that the intersection contains a cylinder of radius $\sqrt{1-\epsilon^2}$ and height ϵ.

(b) Use Part (a) to conclude that there exists an absolute constant ϵ (independent of n) such that at any large enough dimension n and for any distance $d > 0$, the uniform distributions over two radius-$(\frac{1}{2}d\sqrt{n})$ spheres whose centers are $\leq d$ apart, are close upto statistical distance $\leq \epsilon$. Namely

$$\Big|\mathcal{U}\big(\mathbf{B}(\vec{c}, \tfrac{1}{2}d\sqrt{n})\big) \;-\; \mathcal{U}\big(\mathbf{B}(\vec{0}, \tfrac{1}{2}d\sqrt{n})\big)\Big| \;\leq\; \epsilon$$

for any vector $\vec{c} \in \mathbb{R}^n$ of Euclidean norm $\|\vec{c}\| \leq d$.

2 Using the Leftover Hash Lemma

Let G be a finite additive group, denote the size of G by $|G|$, and let $\ell \geq 3\log|G|$. For any fixed ℓ-vector of group elements, $\vec{x} = \langle x_1, \ldots, x_\ell \rangle$, denote by $\mathcal{S}_{\vec{x}}$ the distribution of random subset-sums of the x_i's. Namely

$$\mathcal{S}_{\vec{x}} \;\stackrel{\text{def}}{=}\; \left\{ \sum_{i=1}^{\ell} \sigma_i x_i \;:\; \text{the } \sigma_i\text{'s are uniform and independent in } \{0, 1\} \right\}$$

Also denote by $\mathcal{U}_G$ the uniform distribution over G and by $SD(\mathcal{D}_1, \mathcal{D}_2)$ the statistical distance between the two distributions $\mathcal{D}_1, \mathcal{D}_2$.

Prove the following lemma, asserting that for most vectors $\vec{x}$, the distribution $\mathcal{S}_{\vec{x}}$ is close to uniform.

Lemma 1. *For any finite group G (and $\ell \geq 3\log|G|$), it holds for almost all vectors $\vec{x} \in G^\ell$, except at most a $(1/\sqrt{|G|})$-fraction of them, that $\mathcal{S}_{\vec{x}}$ is at most $(1/\sqrt{|G|})$-away from the uniform distribution on G (in statistical distance). Namely,*

$$\Pr_{\vec{x}\in G^\ell}\left[SD(\mathcal{S}_{\vec{x}},\ \mathcal{U}_G) > \frac{1}{\sqrt{|G|}} \right] \leq \frac{1}{\sqrt{|G|}}$$

Hint. Consider the family of hash functions $\mathcal{H} = \{H_{\vec{x}} : \vec{x} \in G^\ell\}$ from $\{0,1\}^\ell$ to G, which are defined by $H_{\vec{x}}(\sigma_1, \ldots, \sigma_\ell) = \sum_i \sigma_i x_i$. Show that this is a 2-universal family of hash functions, and use the leftover-hash-lemma to show that the statistical distance between the distributions $\{(\vec{x}, H_{\vec{x}}(\vec{\sigma}))\}$ and $\{(\vec{x}, y)\}$ is at most $\frac{1}{2}\sqrt{\frac{|G|}{2^\ell}}$ (where $\vec{x} \in G^\ell$, $\vec{\sigma} \in \{0,1\}^\ell$, and $y \in G$ are all chosen uniformly at random). Use the above to prove the lemma.

3 A Partial Trapdoor

Fix the parameters n, m, q as in the SIS problem, with n the security parameter, $q = \text{poly}(n)$ (say), and $m > 3n \log q$. Describe an efficient algorithm for generating a nearly-uniform $n \times m$ matrix A over $\mathbb{Z}_q$, together with a 0-1 vector $\vec{v}$ such that $A\vec{v} = 0 \pmod{q}$. The statistical distance between the distribution of A output by your algorithm and the uniform distribution over $\mathbb{Z}_q^{n \times m}$ should be exponentially small in n (i.e., $2^{-\Omega(n)}$). *Hint.* Use Lemma 1 above.