Parallelepipeds and Gaussian sampling

For any vectors $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{R}^m$, we define the centered parallelepiped spanned by them as:

$$P(\vec{b}_1, \ldots, \vec{b}_n) = \left\{ \sum_{i=1}^n x_i \vec{b}_i, -1/2 \leq x_i < 1/2 \right\}.$$

If the $\vec{b}_i$’s are the rows of a matrix $B$, we let $P(B) = P(\vec{b}_1, \ldots, \vec{b}_n)$. As usual, the $\vec{b}_i^*$’s denote the corresponding Gram-Schmidt vectors.

1. Babai’s Round-Off Algorithm. \hspace{1cm} (*)

Let $B = (\vec{b}_1, \ldots, \vec{b}_n)$ be a basis of a lattice $L$. We are going to show that $P(B)$ is a so-called fundamental domain of $L$. Let $\vec{t}$ be in the linear span of $L$.

1. Show that there exists a unique $\vec{v} \in L$ such that $\vec{t} - \vec{v} \in P(\vec{b}_1, \ldots, \vec{b}_n)$.
2. If $L \subseteq \mathbb{Z}^n$, show that the group $\mathbb{Z}^n/L$ is finite.
3. Let $f_B$ be the function mapping any $\vec{t}$ in the linear span of $L$ to $\vec{t} - \vec{v}$. Show that $f_B(\vec{a}) = f_B(\vec{b})$ if and only if $\vec{a} - \vec{b} \in L$. Assume that $\vec{t}$ is of the form $\vec{t} = \vec{u} + \vec{e}$ where $\vec{u} \in L$ and $\vec{e} \in P(\vec{b}_1, \ldots, \vec{b}_n)$. Show that $f_B(\vec{t}) = \vec{e}$: thus, one can solve BDD with any noise within $P(\vec{b}_1, \ldots, \vec{b}_n)$.
4. If the $\vec{b}_i$’s and $\vec{t}$ belong to $\mathbb{Z}^m$, show that there exists a polynomial-time algorithm which, given as input the $\vec{b}_i$’s and $\vec{t}$, output this $\vec{v} \in L$. You can assume that you can compute the inverse of a square non-singular integral matrix in polynomial time.

2. Babai’s Nearest Plane Algorithm. \hspace{1cm} (**) 

We take the same notation as in Babai’s round-off algorithm. Here, we show that $P(B^*)$ is a fundamental domain of $L$. Let $\vec{t}$ be in the linear span of $L$.

1. Show that there exists a unique $\vec{v} \in L$ such that $\vec{t} - \vec{v} \in P(\vec{b}_1^*, \ldots, \vec{b}_n^*)$, where the $\vec{b}_i^*$’s are the Gram-Schmidt vectors of the $\vec{b}_i$’s. Hint: use an induction over $n$.
2. If the $\vec{b}_i$’s and $\vec{t}$ belong to $\mathbb{Z}^m$, show that there exists a polynomial-time algorithm which, given as input the $\vec{b}_i$’s and $\vec{t}$, output this $\vec{v} \in L$. You may assume that you know the Gram-Schmidt orthogonalization of the $\vec{b}_i$’s.
3. Let $f_{B^*}$ be the function mapping any $\vec{t}$ in the linear span of $L$ to $\vec{t} - \vec{v}$. Show that this function has the same properties as $f_B : f_{B^*}(\vec{a}) = f_{B^*}(\vec{b})$ if and only if $\vec{a} - \vec{b} \in L$.
4. If $\vec{t} = \vec{u} + \vec{e}$ where $\vec{u} \in L$ and $\|\vec{e}\| < \frac{1}{2} \min_i \|\vec{b}_i^*\|$, show that $\vec{v} = \vec{u}$. Thus, Babai’s nearest plane algorithm $f_{B^*}$ solves Bounded Distance Decoding if the noise has norm $< \frac{1}{2} \min_i \|\vec{b}_i^*\|$. 

1
3. Discrete Gaussian sampling.

Let $B = (\vec{b}_1, \ldots, \vec{b}_n)$ be a basis of an $n$-rank lattice $L$ and $s > 0$ be a parameter. At SODA ’00, Klein introduced the following randomized variant of Babai’s nearest plane algorithm:

1. $\vec{c} \leftarrow \vec{0}$;
2. For $i = n$ downto 1:
   (a) Sample $z_i \in \mathbb{Z}$ from the discrete Gaussian distribution over $\mathbb{Z}$ with center $c_i$ and width $s_i$, where $s_i = s/\|\vec{b}_i\|$ and $c_i$ is the $i$-th coordinate of $\vec{c}$.
   (b) $\vec{c} \leftarrow \vec{c} - z_i \cdot \vec{u}_i$ where $\vec{u}_i = (\mu_{i,1}, \ldots, \mu_{i,i-1}, 1, 0, \ldots, 0)$ and $\mu_{i,j} = \langle \vec{b}_i, \vec{b}_j \rangle / \|\vec{b}_j\|^2$.
3. return $\vec{v} = \sum_{i=1}^{n} z_i \vec{b}_i$

1. Show that a vector $\vec{v} \in L$ is output by Klein’s algorithm with probability $p_B(\vec{v}) = \rho_s(\vec{v}) \times \prod_{i=1}^{n} \frac{1}{\rho_{s,c_i}(\mathbb{Z})}$, where $\rho_{s,c}(\cdot)$ is the Gaussian function of parameter $s$ and center $c$.

2. Show that if $s > \|B^*\|\eta_e(\mathbb{Z})$ where $\|B^*\| = \max_{1 \leq i \leq n} \|\vec{b}_i\|$ and $\eta_e(\mathbb{Z})$ is the smoothing parameter of $\mathbb{Z}$, then for all $\vec{v} \in L$:

$$|p_B(\vec{v}) - p(\vec{v})| \leq \frac{1}{2} \left( \left( \frac{1 + \varepsilon}{1 - \varepsilon} \right)^n - 1 \right),$$

where $p(\vec{v})$ is the mass of $\vec{v}$ with respect to the discrete Gaussian distribution over $L$ with width $s$.

Thus, we can sample from the discrete Gaussian distribution over $L$ in polynomial time, as while as the width $s$ is sufficiently large: the smaller $\|B^*\|$ is, the smaller $s$ can be chosen.