June 9, 2016

Algorithm 1 Gram-Schmidt algorithm

Input: A basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a full-rank lattice $L \subset \mathbb{R}^m$.

Output: The GSO $\mathbf{B}^\star$ of $\mathbf{B}$

- **for** $i = 1$ to n **do**
  - $\mathbf{b}_i^\star \leftarrow \mathbf{b}_i$
  - **for** $j = 1$ to $i-1$ **do**
    - $\mathbf{b}_i^\star \leftarrow \mathbf{b}_i^\star - \frac{\langle \mathbf{b}_i^\star, \mathbf{b}_j^\star \rangle}{\|\mathbf{b}_j^\star\|^2} \cdot \mathbf{b}_j^\star$
- return $\mathbf{B}^\star = [\mathbf{b}_1^\star, \ldots, \mathbf{b}_n^\star]$

Algorithm 2 Round'off algorithm

Input: A basis $\mathbf{B}$ of a full-rank lattice $L \subset \mathbb{R}^n$, a target point $\mathbf{t} \in \mathbb{R}^n$.

Output: A decomposition $\mathbf{t} = \mathbf{v} + \mathbf{f}$ where $\mathbf{v} \in L$ and $\mathbf{w} \in \mathcal{P}(\mathbf{B})$

- $\mathbf{x} \leftarrow \mathbf{B}^{-1}\mathbf{t}$
- $\mathbf{y} \leftarrow (\lfloor x_1 \rceil, \ldots, \lfloor x_n \rceil)$
- $\mathbf{v} \leftarrow \mathbf{B}\mathbf{y}$
- $\mathbf{f} = \mathbf{t} - \mathbf{v}$
- return $(\mathbf{v}, \mathbf{f})$

Algorithm 3 Nearest Plane Algorithm

Input: A basis $\mathbf{B}$ of a full-rank lattice $L \subset \mathbb{R}^n$, its GSO $\mathbf{B}^\star$, and a target point $\mathbf{t} \in \mathbb{R}^n$.

Output: A decomposition $\mathbf{t} = (\mathbf{v} + \mathbf{f})$ where $\mathbf{v} \in L$ and $\mathbf{w} \in \mathcal{P}(\mathbf{B}^\star)$

- $\mathbf{f} \leftarrow \mathbf{t}$
- $\mathbf{v} \leftarrow \mathbf{0}$
- **for** $i = n$ downto 1 **do**
  - $y \leftarrow \langle \mathbf{t}, \mathbf{b}_i^\star \rangle / \|\mathbf{b}_i^\star\|^2$
  - $z_i = \lfloor y \rceil$
  - $\mathbf{f} \leftarrow \mathbf{f} - z_i \mathbf{b}_i$
  - $\mathbf{v} \leftarrow \mathbf{v} + z_i \mathbf{b}_i$
- return $(\mathbf{v}, \mathbf{f})$