TUTORIAL ON ENUMERATION AND BKZ ALGORITHMS

1 Enumeration

1. Prove that the size of the enumeration tree in the algorithm described in the class is of order $2^{\mathcal{O}(n^2)}$when given on input an LLL-reduced basis.

   Use the facts that for an LLL-reduced bases the following holds:

   1. $\frac{r_{1,1}}{r_{i,i}} < \alpha^{i-1}$, where you can take $\alpha = 2$ (it is the upper bound on α);
   2. $r_{1,1} = \|\mathbf{b}_1\| \leq \alpha^{\frac{n-1}{2}} (\det L)^{1/n}$.

2 BKZ

Let B be a basis given on input to the BKZ algorithm and let $B_{[i,j]}$ for $i < j$ be the (projected) basis formed by the basis vectors $\mathbf{b}_i, \ldots \mathbf{b}_j$ projected orthogonally to the first $i-1$ basis vectors.

1. What is the memory complexity of the BKZ algorithm described in class?

2. Apply Minkowski theorem to the projected lattice $B_{[i,i+\beta-1]}$ to obtain an upper bound on $\|\tilde{\mathbf{b}}_i\|$. Conclude that

$$\|\tilde{\mathbf{b}}_i\|^\beta \leq \beta^{\beta/2} \prod_{j=i}^{i+\beta-1} \|\tilde{\mathbf{b}}_j\| \tag{1}$$

3. With the obtained upper bounds for all $1 \leq i \leq n - \beta + 1$'s, show that

$$\|\tilde{\mathbf{b}}_1\|^{\beta-1} \cdot \|\tilde{\mathbf{b}}_2\|^{\beta-2} \cdot \ldots \cdot \|\tilde{\mathbf{b}}_{\beta-1}\| \leq \beta^{\frac{\beta(n-\beta+1)}{2}} \|\tilde{\mathbf{b}}_{n-\beta+2}\|^{\beta-1} \|\tilde{\mathbf{b}}_{n-\beta+3}\|^{\beta-2} \cdot \ldots \cdot \|\tilde{\mathbf{b}}_n\|. \tag{2}$$

   In order to do that, apply Inequality (1) to $\prod_{i=1}^{n-\beta+1} \|\tilde{\mathbf{b}}_i\|^\beta$.

4. Using the fact that not only $B_{[1,\beta]}$ is SVP reduced, but also $B_{[1,i]}$ for $i \leq \beta$ are SVP reduced (think why this is true), conclude that (compare with Inequality (1)):

$$\|\tilde{\mathbf{b}}_1\|^i \leq i^{i/2} \prod_{j=1}^{i} \|\tilde{\mathbf{b}}_j\| \quad \forall i \leq \beta \tag{3}$$

5. Multiply Inequalities (3) for $1 \leq i \leq \beta - 1$ and use Inequality (2) to obtain

$$\|\tilde{\mathbf{b}}_1\|^{\frac{\beta(\beta-1)}{2}} \leq \beta^{\frac{\beta(n-1)}{2}} \cdot \|\tilde{\mathbf{b}}_{n-\beta+2}\|^{\beta-1} \|\tilde{\mathbf{b}}_{n-\beta+3}\|^{\beta-2} \cdot \ldots \cdot \|\tilde{\mathbf{b}}_n\| \tag{4}$$

6. Assume that there exist a shortest vector $\mathbf{v}_{\texttt{shortest}}$ whose projection orthogonal to the first $n-1$ basis vectors is non-zero (otherwise, if all shortest vector project to zero onto the span of $\tilde{\mathbf{b}}_n$, then we know that all of them live in a lattice of dimension at most $n-1$ and we can remove $\mathbf{b}_n$).

   This implies that $\lambda_1 = \|\mathbf{v}_{\texttt{shortest}}\| \geq \|\tilde{\mathbf{b}}_i\|$ for $n - \beta + 2 \leq i \leq n$ (think why). Plugging this inequality into the right-hand side of Inequality (4) conclude that

$$\|\mathbf{b}_1\| \leq \beta^{\frac{n-1}{\beta-1}} \lambda_1.$$