Lattice algorithms – Exercises

June 20th, 2017

Throughout we will consider the two-dimensional lattice generated by $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ with:

$$\boldsymbol{b}_1 = \begin{pmatrix} 144 \\ 0 \end{pmatrix}, \qquad \boldsymbol{b}_2 = \begin{pmatrix} 89 \\ 1 \end{pmatrix}. \tag{1}$$

The corresponding lattice is defined as $\mathcal{L} = \mathcal{L}(\mathbf{B}) = \{\lambda_1 \boldsymbol{b}_1 + \lambda_2 \boldsymbol{b}_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\}$. Observe that these basis vectors are not very short or orthogonal. For instance $\boldsymbol{b}_1 - \boldsymbol{b}_2$ is also a lattice vector, and has a smaller Euclidean norm than $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$.

1. Gauss reduction

In two dimensions, Gauss reduction provides an efficient way to find the "best" basis of a lattice. Given a basis $\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$, this algorithm repeatedly applies the following two steps:

- **Swap**: If $\|\boldsymbol{b}_1\| > \|\boldsymbol{b}_2\|$, then swap $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$.
- **Reduce**: While $\|\boldsymbol{b}_2 \pm \boldsymbol{b}_1\| < \|\boldsymbol{b}_2\|$, replace $\boldsymbol{b}_2 \leftarrow \boldsymbol{b}_2 \pm \boldsymbol{b}_1$.

Gauss reduction repeats the above two steps until no more progress can be made. A Gauss-reduced basis contains a shortest (non-zero) vector as one of its basis vectors.

a) Perform Gauss-reduction on the basis $\mathbf{B}$ above to find a reduced basis $\mathbf{B}'$.

b) Find a shortest non-zero vector in this lattice.

c) Find a lattice vector at Euclidean distance at most 12 from the target $\boldsymbol{t} = (7, 21)$.

d) Explain why a Gauss-reduced basis generates the same lattice as the input basis.

2. Lattice enumeration

Lattice enumeration is a way to find all short vectors in a lattice, by exhausting the space of all possible solutions. This method uses the Gram-Schmidt orthogonalization of a basis:

$$\boldsymbol{b}_1^* = \boldsymbol{b}_1, \qquad \boldsymbol{b}_2^* = \boldsymbol{b}_2 - \frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1. \tag{2}$$

Here $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_i x_i y_i$ denotes the standard inner product.

a) Compute the Gram-Schmidt orthogonalization of the reduced basis $\mathbf{B}'$ from 1a.

b) Show that if $\boldsymbol{v} = \lambda_1 \boldsymbol{b}_1 + \lambda_2 \boldsymbol{b}_2$, then $\|\boldsymbol{v}\| \geq |\lambda_2| \cdot \|\boldsymbol{b}_2^*\|$.

c) Find all lattice vectors of norm at most 24.
(Hint: Find a bound on λ_2, and then find all solutions for each choice of λ_2.)

d) Describe what happens if we try the approach from 2a-c with the original basis $\mathbf{B}$.

e) Suppose $\boldsymbol{t} \in \mathbb{R}^2$ with $\|\boldsymbol{t}\| \leq 12$. Argue that one of the vectors found in 2c must be a closest lattice vector to $\boldsymbol{t}$.

f) Find the exact closest lattice vector to $\boldsymbol{t} = (7, 21)$.
(Hint: Use 1c to construct a vector $\boldsymbol{t}' = \boldsymbol{t} - \boldsymbol{v}$, with $\boldsymbol{v} \in \mathcal{L}$, of norm at most 12.)

3. The Voronoi cell of a lattice

The Voronoi cell of a lattice $\mathcal{L} \subset \mathbb{R}^n$ is defined as the region $\mathcal{V} \subset \mathbb{R}^n$ of points closer to the origin than to any other lattice point:

$$\mathcal{V} = \left\{ \boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\| \leq \|\boldsymbol{x} - \boldsymbol{v}\| \text{ for all } \boldsymbol{v} \in \mathcal{L} \right\}. \tag{3}$$

The Voronoi relevant vectors are defined as those lattice vectors $\boldsymbol{r} \in \mathcal{L}$ for which $\mathcal{V}$ and the shifted Voronoi cell $\mathcal{V} + \boldsymbol{r}$ share a non-empty boundary[1]. For the 2D lattice from the previous exercises, the six relevant vectors are $\pm(8, -8), \pm(13, 5), \pm(5, 13)$.

a) Given a vector $\boldsymbol{t} \in \mathcal{V}$, what is the closest lattice vector to $\boldsymbol{t}$?

b) Given a vector $\boldsymbol{t} \in \mathbb{R}^2$, describe an algorithm for finding a closest lattice vector to $\boldsymbol{t}$ using the Voronoi relevant vectors, and prove this algorithm terminates.
(Hint: "Reduce" $\boldsymbol{t}$ with the relevant vectors.)

c) Use this method to verify your answer from 2f.

4. Lattice basis reduction and relation finding

Lattice basis reduction can also be used for other purposes, such as obtaining (approximate) relations between numbers of a given form. As an example, using Gauss reduction we have reduced the basis $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ to $\mathbf{B}' = \{\boldsymbol{b}_1', \boldsymbol{b}_2'\}$ with $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_1', \boldsymbol{b}_2'$ given below.

$$\boldsymbol{b}_1 = \begin{pmatrix} 100000 \\ 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{b}_2 = \begin{pmatrix} 314159 \\ 0 \\ 1 \end{pmatrix}, \qquad \boldsymbol{b}_1' = \begin{pmatrix} -33 \\ -355 \\ 113 \end{pmatrix}, \quad \boldsymbol{b}_2' = \begin{pmatrix} 887 \\ 22 \\ -7 \end{pmatrix}. \tag{4}$$

a) Express $\boldsymbol{b}_1'$ and $\boldsymbol{b}_2'$ in terms of the basis $\mathbf{B}$, and use this to construct two equations of the form $\lambda_1 \cdot 100000 + \lambda_2 \cdot 314159 = \lambda_3$ with "small" $\lambda_1, \lambda_2, \lambda_3$.

b) Rewrite these equations to obtain rational approximations of π.

c) Perform Gauss reduction on the basis $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ given by

$$\boldsymbol{b}_1 = \begin{pmatrix} 100000 \\ 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{b}_2 = \begin{pmatrix} 9740909 \\ 0 \\ 1 \end{pmatrix}. \tag{5}$$

d) Use the previous reduced basis to obtain Ramanujan's approximation of π^4.

[1] Formally, $\mathcal{V} + \boldsymbol{r} = \left\{ \boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x} - \boldsymbol{r}\| \leq \|\boldsymbol{x} - \boldsymbol{v}\| \text{ for all } \boldsymbol{v} \in \mathcal{L} \right\}$.