Lattice algorithms – Exercises + Solutions

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 $\mathbf{B}'$.
Solution: Using Gauss reduction we obtain the basis $\mathbf{B}' = \{(8, -8), (13, 5)\}$.

b) Find a shortest non-zero vector in this lattice.
Solution: From $\mathbf{B}'$ we can extract a shortest vector $\boldsymbol{s} = (8, -8)$.

c) Find a lattice vector at Euclidean distance at most 12 from the target $\boldsymbol{t} = (7, 21)$.
Solution: Trial and error should suffice to find a sufficiently close vector here. For instance $(5, 13)$ is a lattice vector, and lies at distance $\sqrt{4 + 64} < 12$ from $\boldsymbol{t}$.

d) Explain why a Gauss-reduced basis generates the same lattice as the input basis.
Solution: One way to do this is to prove that $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathbf{B}')$, whenever $\mathbf{B}'$ is obtained from $\mathbf{B}$ through swaps and reductions. To prove this, it suffices to show that a single swap leads to a basis for the same lattice, and a single reduction does not change the generated lattice either.

Recall that a lattice vector can be represented in a basis by a pair (λ_1, λ_2) of coefficients. After a swap, the coefficients become $(\lambda_1, \lambda_2) \mapsto (\lambda_2, \lambda_1)$, and so any vector representable in $\mathbf{B}$ with integer coefficients is also representable in $\mathbf{B}'$ with integer coefficients, and vice versa. Similarly a reduction corresponds to a mapping $(\lambda_1, \lambda_2) \mapsto (\lambda_1, \lambda_2 \pm \lambda_1)$, and again $(\lambda_1, \lambda_2) \in \mathbb{Z}^2$ if and only if $(\lambda_1, \lambda_2 \pm \lambda_1) \in \mathbb{Z}^2$.

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.
Solution: Starting from the reduced basis $\boldsymbol{b}_1 = (8, -8)$ and $\boldsymbol{b}_2 = (13, 5)$, we find $\boldsymbol{b}_1^* = \boldsymbol{b}_1 = (8, -8)$ and $\boldsymbol{b}_2^* = \boldsymbol{b}_2 - \frac{\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1 = (13, 5) - \frac{64}{128}(8, -8) = (9, 9)$.

b) Show that if $\boldsymbol{v} = \lambda_1 \boldsymbol{b}_1 + \lambda_2 \boldsymbol{b}_2$, then $\|\boldsymbol{v}\| \geq |\lambda_2| \cdot \|\boldsymbol{b}_2^*\|$.
Solution: If $\boldsymbol{v} = \lambda_1 \boldsymbol{b}_1 + \lambda_2 \boldsymbol{b}_2$ then also $\boldsymbol{v} = \lambda_1^* \boldsymbol{b}_1^* + \lambda_2 \boldsymbol{b}_2^*$: the coefficient λ_1 may be different when representing $\boldsymbol{v}$ in this orthogonalized basis, but the coefficient for $\boldsymbol{b}_2^*$ remains the same. Since $\boldsymbol{b}_1^*$ and $\boldsymbol{b}_2^*$ are orthogonal, we obtain a bound on $\|\boldsymbol{v}\|$ as $\|\boldsymbol{v}\| = \sqrt{(\lambda_1^*)^2 \cdot \|\boldsymbol{b}_1^*\|^2 + \lambda_2^2 \cdot \|\boldsymbol{b}_2^*\|^2} \geq \sqrt{\lambda_2^2 \cdot \|\boldsymbol{b}_2^*\|^2} = |\lambda_2| \cdot \|\boldsymbol{b}_2^*\|$.

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.)
Solution: We know that $|\lambda_2| \cdot \|\boldsymbol{b}_2^*\| \leq \|\boldsymbol{v}\| \leq 24$. Since $\|\boldsymbol{b}_2^*\| = \sqrt{9^2 + 9^2} > 12$, this leads to $|\lambda_2| < 2$. Since λ_2 is integer, this leads to $\lambda_2 \in \{-1, 0, 1\}$, and due to symmetry of the lattice, we only need to consider the cases $\lambda_2 = 0$ and $\lambda_2 = 1$.

For $\lambda_2 = 0$, we are looking for points $\boldsymbol{v} = \lambda_1 \cdot (8, -8)$ with norm at most 24. Since $(8, -8)$ has norm approximately 11.31, we find solutions for $|\lambda_1| \leq 2$, namely the five vectors $\{(0, 0), \pm(8, -8), \pm(16, -16)\}$.

For $\lambda_2 = 1$, we are looking for lattice points of the form $\boldsymbol{v} = (13, 5) + \lambda_1(8, -8)$, which leads to sufficiently short vectors for $\lambda_1 \in \{-2, -1, 0, 1\}$ corresponding to the four short vectors $\{(-3, 21), (5, 13), (13, 5), (21, -3)\}$. For $\lambda_2 = -1$ we find these solutions with a minus sign, i.e. $\{(3, -21), (-5, -13), (-13, -5), (-21, 3)\}$. Altogether, this leads to the 13 short vectors mentioned above.

d) Describe what happens if we try the approach from 2a-c with the original basis $\mathbf{B}$.
Solution: Since the original basis was longer and less orthogonal, enumeration becomes more expensive as described during the lecture. In this particular case, the vector $\boldsymbol{b}_2^*$ would be equal to $(0, 1)$ of norm 1, and so the bound on the coefficient λ_2 in terms of this non-reduced basis would be $|\lambda_2| \leq 24$. If we tried the same approach, we would have spent much more time checking each possible choice λ_2 for solutions.

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 $\boldsymbol{t}$.
Solution: Any vector not in this list has norm larger than 24, and therefore due to the triangle inequality has distance more than 12 from $\boldsymbol{t}$. Since $\mathbf{0}$ is a lattice vector at distance at most 12 from $\boldsymbol{t}$, such a long vector cannot be a closest vector.

f) Find the exact closest lattice vector to $\boldsymbol{t} = (7, 21)$.
Solution: From 1c we had a close vector $(5, 13)$. Considering $\boldsymbol{t}' = (7, 21) - (5, 13) = (2, 8)$, this vector has norm less than 12, and has a closest vector in the list from 2c. Checking all vectors, we find $(5, 13)$ to be the closest to $(2, 8)$, at distance $\sqrt{34} < 6$. The closest vector to $(7, 21)$ is therefore our initial guess $(5, 13)$ plus the exact closest vector to $\boldsymbol{t}'$, $(5, 13)$ leading to $(10, 26)$ at distance $\sqrt{34}$.

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:

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

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 $\boldsymbol{t}$?
Solution: By definition, the Voronoi cell $\mathcal{V}$ contains all vectors which are closer to the origin than to any other lattice vector, so the origin is the closest lattice vector.

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.
Solution: Given the list of the relevant vectors, we can iteratively "reduce" a target vector $\boldsymbol{t}$ with the relevant vectors (replacing $\boldsymbol{t}$ by $\boldsymbol{t}' = \boldsymbol{t} \pm \boldsymbol{r}$ if $\boldsymbol{t} \pm \boldsymbol{r}$ is shorter than $\boldsymbol{t}$) until the reduced target cannot be further reduced with any of the relevant vectors. From this one can then trace back to the closest vector of the original vector.

To prove that this algorithm terminates, note that since everything is discrete, the number of intermediate values the norm of the target can take is finite (assuming reductions are only done with a strict inequality). The algorithm therefore has to terminate at some point, at which point no more reductions can be done.

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" $\lambda_1, \lambda_2, \lambda_3$.
Solution: The easiest way to extract the coordinates of $\mathbf{B}'$ in terms of $\mathbf{B}$ is to look at the second and third coordinates, which for $\mathbf{B}$ are unit vectors. It immediately follows that $\boldsymbol{b}'_1 = -355 \cdot \boldsymbol{b}_1 + 113 \cdot \boldsymbol{b}_2$ and $\boldsymbol{b}'_2 = 22 \cdot \boldsymbol{b}_1 - 7 \cdot \boldsymbol{b}_2$. Looking at the first coordinates of $\mathbf{B}'$ expressed in terms of $\mathbf{B}$ we then find:

$$-33 = -355 \cdot 100000 + 113 \cdot 314159 \tag{5}$$
$$887 = 22 \cdot 100000 - 7 \cdot 314159 \tag{6}$$

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

b) Rewrite these equations to obtain rational approximations of π.
Solution: Dividing both equations by 100000 and the coefficient of 314159, and rewriting the terms, we obtain the two equations

$$3.14159 - \frac{355}{113} = \frac{-33}{11300000} \tag{7}$$

$$3.14159 - \frac{22}{7} = \frac{-887}{700000} \tag{8}$$

Since $\pi \approx 3.14159$, and the right hand sides are (relatively) small, we obtain the rational approximations $\pi \approx \frac{355}{113}$ and $\pi \approx \frac{22}{7}$.

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

$$\boldsymbol{b}_1 = \begin{pmatrix} 100000 \\ 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{b}_2 = \begin{pmatrix} 9740909 \\ 0 \\ 1 \end{pmatrix}. \tag{9}$$

Solution: Applying Gauss reduction, we find the reduced basis $\mathbf{B}' = \{\boldsymbol{b}'_1, \boldsymbol{b}'_2\}$ with $\boldsymbol{b}'_1 = (2, 2143, -22)$ and $\boldsymbol{b}'_2 = (4545, -487, 5)$. The first vector $\boldsymbol{b}'_1$ is a shortest vector in this lattice.

d) Use the previous reduced basis to obtain Ramanujan's approximation of π^4.
Solution: Using similar techniques as above, this can ultimately be rewritten as $97.40909 \approx \frac{2143}{22}$ (with an explicit error term). Since $\pi^4 \approx 97.40909$, we obtain the rational approximation $\pi^4 \approx \frac{2143}{22}$ previously obtained by Ramanujan.