Chapter 4

Lattices

In the context of interest to us, lattices mean discrete subgroups of the finite-dimensional vector spaces $\mathbf{R}^n$. They appear in many settings in both mathematics and applications. Closer to the topics of this subject, lattices play an important role in number theory and in cryptography.

4.1 Basic properties of lattices

A *lattice* in $\mathbf{R}^n$ is a *discrete subgroup* L of $(\mathbf{R}^n, +)$, that is a subgroup such that there exists $\varepsilon > 0$ with

$$\mathbf{B}_\varepsilon(0) \cap L = \{0\}.$$

Equivalently, we could ask that for every $R \in \mathbf{R}_{>0}$ the set $\{v \in L : \|v\| \leqslant R\}$ is finite.

We have chosen to give this definition using the concrete vector spaces $\mathbf{R}^n$, but occasionally it is useful to consider it in an arbitrary real vector space V equipped with an inner product.

Example 4.1. Consider $\mathbf{Z}^n \subset \mathbf{R}^n$. This is clearly a subgroup of the additive group $\mathbf{R}^n$. The shortest nonzero vectors in $\mathbf{Z}^n$ are $\pm e_i$, of unit length, so if we take $\varepsilon = 1/2$ we get $\mathbf{B}_\varepsilon(0) \cap \mathbf{Z}^n = \{0\}$.

Note that we could have introduced this lattice as

$$\mathsf{Span}_{\mathbf{Z}}\{e_1, \dots, e_n\}.$$

More generally, we can get a lattice L in $\mathbf{R}^n$ by choosing linearly independent vectors $v_1, \dots, v_m \in \mathbf{R}^n$ and letting

$$L = \mathsf{Span}_{\mathbf{Z}}\{v_1, \dots, v_m\}.$$

In fact, this last construction gives all the lattices:

Proposition 4.2. *A subset $L \subseteq \mathbf{R}^n$ is a lattice if and only if there exist $\mathbf{R}$-linearly independent vectors $v_1, \dots, v_m \in \mathbf{R}^n$ such that*

$$L = \mathsf{Span}_{\mathbf{Z}}\{v_1, \dots, v_m\}.$$

A set of linearly independent vectors $\{v_1, \dots, v_m\}$ as in Proposition 4.2 is called a $\mathbf{Z}$-*basis* of L. The number m is called the *rank* of L. We say that a lattice L is *full* (or *has full rank*) if $\dim L = \dim \mathbf{R}^n = n$.

Proposition 4.3. *The rank of a lattice is well-defined: if L is a lattice, then any two $\mathbf{Z}$-bases of L have the same number of elements.*

Proof. Let B and C be $\mathbf{Z}$-bases of $L \subset \mathbf{R}^n$.

Let $W = \mathsf{Span}_{\mathbf{R}}(L) = \mathsf{Span}_{\mathbf{R}}(B) = \mathsf{Span}_{\mathbf{R}}(C)$. Then B and C are $\mathbf{R}$-bases of the vector subspace W of $\mathbf{R}^n$. Therefore they have the same number of elements. □

A $\mathbf{Z}$-basis $\{v_1, \dots, v_m\}$ of L gives rise to a *basis matrix* $M = [v_1 \dots v_m] \in \mathsf{M}_{n\times m}(\mathbf{R})$. Then $L = \{Mx : x \in \mathbf{Z}^m\}$.

A choice of ordered $\mathbf{Z}$-basis $B = (v_1, \dots, v_n)$ for L defines an invertible $\mathbf{Z}$-linear transformation $[\cdot]_B : L \longrightarrow \mathbf{Z}^n$ mapping the basis vector v_j to the standard basis vector e_j, and an arbitrary $v \in L$ to its coordinate vector $[v]_B$ with respect to the basis B.

Example 4.4. Given $A \in \mathsf{M}_{m\times n}(\mathbf{Z})$, $\mathsf{ker}\,(A) = \{x \in \mathbf{Z}^n : Ax = 0\} \subset \mathbf{R}^n$ is a lattice of rank $n - \mathsf{rank}\,(A)$.

If $n > m$ we can project the lattice L inside $\mathbf{R}^m$ so that it becomes a full lattice:

Proposition 4.5. *Let L be a lattice with basis matrix $M \in \mathsf{M}_{n\times m}(\mathbf{R})$. There is a length-preserving linear map $\pi : \mathbf{R}^n \longrightarrow \mathbf{R}^m$ such that $\pi(L)$ is a full rank lattice in $\mathbf{R}^m$. Moreover, if $v_1, \dots v_m$ are the columns of M then*

$$\langle v_i, v_j\rangle = \langle \pi(v_i), \pi(v_j)\rangle \qquad \text{for all } i, j.$$

A basis matrix for the lattice $\pi(L)$ is given by $PM \in \mathsf{M}_m(\mathbf{R})$, where P is the standard matrix representation of π.

Sketch: Let $V = \mathsf{Span}_{\mathbf{R}}\{v_1, \dots, v_m\} \subseteq \mathbf{R}^n$. Use Gram–Schmidt orthonormalisation to construct a basis $u_1, \dots, u_m$ of V that is orthonormal with respect to the standard inner product on $\mathbf{R}^n$.

Define $\pi : \mathbf{R}^n \longrightarrow \mathbf{R}^m$ by setting $\pi(u_i) = e_i$ and $\pi(V^\perp) = 0$.

The claims follow by standard linear algebra. □

Corollary 4.6. *Two matrices M and M' define the same lattice L if and only if $M' = MU$ for some unimodular matrix U, that is an $m \times m$ matrix with integer entries and determinant ± 1.*

Proof. Write $v_1, \dots, v_m$ for the columns of M and $v'_1, \dots, v'_m$ for the columns of M'.

If M and M' define the same lattice L then we can write for $i = 1, \dots, m$:

$$v'_i = \sum_{j=1}^{m} u_{ji} v_j \qquad u_{ji} \in \mathbf{Z}.$$

In other words, we have $M' = MU$ for $U = (u_{ij}) \in \mathsf{M}_m(\mathbf{Z})$.

Similarly, $M = M'U'$ for some $U' \in \mathsf{M}_m(\mathbf{Z})$. Therefore $M = MUU'$. We apply the projection from Proposition 4.5 on both sides and get $PM = PMUU'$. But the matrix PM is invertible, therefore $UU' = I$. Since both U and U' are integer matrices, $\mathsf{det}\, U, \mathsf{det}\, U' \in \mathbf{Z}$, and $(\mathsf{det}\, U)(\mathsf{det}\, U') = 1$, so $\mathsf{det}\, U = \pm 1$.

Conversely, suppose $M' = MU$ for some unimodular matrix U. Multiplication by U is a bijective map $\mathbf{Z}^m \longrightarrow \mathbf{Z}^m$, $x \mapsto y = Ux$, so

$$\{M'x : x \in \mathbf{Z}^m\} = \{MUx : x \in \mathbf{Z}^m\} = \{My : y \in \mathbf{Z}^m\} = L.$$ □

Let L be a lattice in $\mathbf{R}^n$ and let $B = \{v_1, \dots, v_m\}$ be a $\mathbf{Z}$-basis for L. The *fundamental domain* for L with respect to B is the subset of $\mathbf{R}^n$ defined by

$$\mathcal{F}(B) = \{t_1 v_1 + \cdots + t_m v_m : 0 \leqslant t_j < 1 \text{ for all } j = 1, \dots, m\}.$$

Draw this for a rank 2 lattice in $\mathbf{R}^2$.

Say something about the geometry of $\mathcal{F}(B)$: its closure $\overline{\mathcal{F}(B)}$ is a parallelepiped in $\mathbf{R}^n$.

Proposition 4.7. *Let L be a full lattice in $\mathbf{R}^n$ and let $\mathcal{F}$ be a fundamental domain for L. Then for every $v \in \mathbf{R}^n$ there exist unique vectors $v_0 \in \mathcal{F}$ and $w \in L$ such that $v = v_0 + w$.*

You get to prove this in the tutorial.

Proposition 4.8. *Let L be a lattice in $\mathbf{R}^n$ and $\mathcal{F}$ the fundamental domain with respect to a basis matrix M. Then the volume of $\mathcal{F}$, viewed as a subset of $\mathsf{Span}_{\mathbf{R}}(L)$, is equal to $|\det(PM)|$, where P is the projection matrix from Proposition 4.5.*

In particular, any two fundamental domains for L have the same volume.

Proof. Since the projection represented by P preserves the inner product, the volume of $\mathcal{F}$ is the same as the volume of $P\mathcal{F}$, which is given by $|\det(PM)|$.

Another fundamental domain would be given by another basis matrix M', which we have seen can be written as $M' = MU$ with $\det U = \pm 1$. So $|\det(PM')| = |\det(PM)\det(U)| = |\det(PM)|$. □

The volume in $\mathsf{Span}_{\mathbf{R}}(L)$ of a fundamental domain for L is called the *determinant* of L.

Proposition 4.9 (Hadamard's Inequality)**.** *Let $L \subset \mathbf{R}^n$ be a full lattice with basis $\{v_1, \dots, v_n\}$. Then*

$$\det L \leqslant \|v_1\| \, \|v_2\| \, \dots \, \|v_n\|.$$

Given a basis $B = \{v_1, \dots, v_n\}$ for L, the *Hadamard ratio* of B is defined to be

$$\mathcal{H}(B) = \left(\frac{\det L}{\|v_1\| \dots \|v_n\|} \right)^{1/n}.$$

We have $0 < \mathcal{H}(B) \leqslant 1$. In the extremal case $\mathcal{H}(B) = 1$, the basis B is orthogonal.

4.2 Hard lattice problems: shortest/closest vector

There are many questions of a computational nature involving lattices. Some of them are generalisations of linear algebra problems and have fairly efficient algorithms: lattice membership (given a lattice L and a $\mathbf{Z}$-basis, determine whether some vector $v \in \mathbf{R}^n$ is in L), lattice basis (given a finite set of vectors not known to be linearly independent, find a $\mathbf{Z}$-basis for the lattice they generate), kernel lattice basis (given an integer matrix A, find a basis for the lattice $\ker A$).

Other lattice problems appear to be genuinely difficult.

If W is a subspace of $\mathbf{R}^n$, there is no such thing as a shortest nonzero vector in W: this is trivially true if $W = \{0\}$, and otherwise, we can take any nonzero vector in W and scale it by a real scalar to an arbitrarily small (but nonzero) length.

By contrast, the very definition of a (nonzero) lattice L means that there is a positive lower bound $\varepsilon > 0$ for the length of any nonzero vector. This suggests the following

Shortest Vector Problem. *Given a nonzero lattice $L \subset \mathbf{R}^n$, find a shortest nonzero vector in L, i.e. $v \in L \setminus \{0\}$ that minimises $\|v\|$.*

Theorem 4.10 (Hermite)**.** *If $L \subset \mathbf{R}^n$ is a full lattice, there exists a vector $v \in L \setminus \{0\}$ such that*

$$\|v\| \leqslant \sqrt{n} \det(L)^{1/n}.$$

We derive Hermite's Theorem from the following result that plays an important role in algebraic number theory:

Theorem 4.11 (Minkowski)**.** *Let $L \subseteq \mathbf{R}^n$ be a full lattice and let $S \subseteq \mathbf{R}^n$ be a symmetric convex set such that*

$$\mathsf{vol}(S) > 2^n \det(L).$$

Then there exists a nonzero vector in $S \cap L$.

Moreover, if S is also closed in $\mathbf{R}^n$, the same conclusion holds under the slightly weaker hypothesis $\mathsf{vol}(S) \geqslant 2^n \det(L)$.

Proof of Hermite's Theorem. Fix a positive real number M and let S_M be the n-cube with centre 0 and side length $2M$:

$$S_M = \{(x_1, \dots, x_n) \in \mathbf{R}^n : \ -M \leqslant x_i \leqslant M \text{ for all i}\}.$$

Then S_M is symmetric, closed, bounded, of volume $\mathsf{vol}\,(S_M) = (2M)^n$. An arbitrary element $x \in S_M$ satisfies

$$\|x\| = \sqrt{x_1^2 + \cdots + x_n^2} \leqslant \sqrt{n}\, M.$$

Now take $M = \mathsf{det}\,(L)^{1/n}$ and let $S = S_M$. Since $\mathsf{vol}\,(S) = 2^n \mathsf{det}\,(L)$, by Minkowski's Theorem we get a nonzero vector $x \in S \cap L$, which by the above has $\|x\| \leqslant \sqrt{n}\, M = \sqrt{n}\, \mathsf{det}\,(L)^{1/n}$. □

Extension of Hermite's Theorem: given a full lattice $L \subset \mathbf{R}^n$, there exists a basis $v_1, \dots, v_n$ such that

$$\|v_1\|\, \|v_2\| \dots \|v_n\| \leqslant n^{n/2} \mathsf{det}\, L.$$

Another fundamental lattice problem is

Closest Vector Problem. *Given a nonzero lattice L in V and a vector $w \in V \setminus L$, find a vector $v \in L$ that is closest to w, in other words such that the distance $\|w - v\|$ is minimised.*

There are versions of SVP and CVP that ask for approximate solutions, that is vectors that are close to being optimal.

4.3 Lattice reduction

If the basis of the lattice is orthogonal, then both SVP and CVP are easily solved.

Example 4.12 (SVP in orthogonal case)**.** Let $v \in L$ and write $v = a_1 v_1 + \cdots + a_n v_n$ with $a_1, \dots, a_n \in \mathbf{Z}$.

If B is orthogonal, then we have

$$\|v\|^2 = \|a_1 v_1 + \cdots + a_n v_n\|^2 = a_1^2 \|v_1\|^2 + \cdots + a_n^2 \|v_n\|^2.$$

Hence the shortest nonzero vectors in L can be found in $\{\pm v_1, \dots, \pm v_n\}$.

(See the tutorial for the solution to CVP in the orthogonal case.)

In the non-orthogonal case, we want a way to produce a "good" basis that is closer to being orthogonal. This process is called reduction; it works particularly well in dimension two.

4.3.1 Two dimensions: Lagrange–Gauss reduction

Let $\{v_1, v_2\}$ be a $\mathbf{Z}$-basis for a lattice L in $\mathbf{R}^2$. WLOG $\|v_1\| \leqslant \|v_2\|$.

We wish to find a $\mathbf{Z}$-basis for L such that the lengths of the vectors are as short as possible. More precisely, we say that a basis (w_1, w_2) of $\mathbf{R}^2$ is *Lagrange–Gauss reduced* if

$$\|w_1\| \leqslant \|w_2\| \leqslant \|w_2 + a w_1\| \qquad \text{for all } a \in \mathbf{Z}.$$

Lemma 4.13. *Let $w_1, w_2 \in \mathbf{R}^2$ and suppose that $\|w_2\| \leqslant \|w_2 \pm w_1\|$. Prove that*

$$|\langle w_1, w_2 \rangle| \leqslant \frac{1}{2} \|w_1\|^2.$$

Proof. By assumption

$$\|w_2\|^2 \leqslant \|w_2 \pm w_1\|^2 = \|w_2\|^2 \pm 2\langle w_1, w_2\rangle + \|w_1\|^2.$$

Therefore

$$\mp 2\langle w_1, w_2\rangle \leqslant \|w_1\|^2 \quad \Rightarrow \quad |\langle w_1, w_2\rangle| \leqslant \frac{1}{2}\|w_1\|^2. \qquad \square$$

Proposition 4.14. *An ordered basis (w_1, w_2) is Lagrange–Gauss reduced if and only if*

$$\|w_1\| \leqslant \|w_2\| \leqslant \|w_2 \pm w_1\|.$$

Proof. One direction is clear.

For the converse, consider the expression

$$\|w_2 + tw_1\|^2 = \|w_2\|^2 + 2t\langle w_1, w_2\rangle + t^2\|w_1\|^2$$

as a function $f(t)$ of the real variable t. This is a quadratic function of t, so it has a unique minimum that can be obtained by differentiating: $t = -\langle w_1, w_2\rangle/\|w_1\|^2$. Therefore using Lemma 4.13

$$|t| = \frac{|\langle w_1, w_2\rangle|}{\|w_1\|^2} \leqslant \frac{\|w_1\|^2/2}{\|w_1\|^2} = \frac{1}{2}.$$

So the minimum of $f(t)$ over $t \in \mathbf{Z}$ occurs at 0, that is

$$\|w_2\|^2 = f(0) < f(a) = \|w_2 + aw_1\|^2 \qquad \text{for all } a \in \mathbf{Z}. \qquad \square$$

Here is the Lagrange–Gauss algorithm for a lattice L given by a basis v_1, v_2:

- If $\|v_2\| < \|v_1\|$, swap v_1 and v_2.
- Let $t = -\langle v_1, v_2\rangle/\|v_1\|^2$.
- If $\lfloor t \rceil = 0$, stop and output v_1, v_2.
- Otherwise, replace v_2 by $v_2 + \lfloor t \rceil v_1$ and go back to the first step.

Example 4.15. Take $v_1 = (1,5)^\mathsf{T}$ and $v_2 = (6,21)^\mathsf{T}$. We have $\|v_1\|^2 = 26$, $\|v_2\|^2 = 477$, $\langle v_1, v_2\rangle = 111$. Therefore $t = -111/26 \approx -4.269$, $\lfloor t \rceil = -4$, so the new v_2 is $(6,21)^\mathsf{T} - 4(1,5)^\mathsf{T} = (2,1)^\mathsf{T}$.

Now $\|v_2\|^2 = 5$ so we swap v_1, v_2.

We have $\|v_1\|^2 = 5$, $\|v_2\|^2 = 26$, $\langle v_1, v_2\rangle = 7$. Therefore $t = -7/5 = -1.4$, $\lfloor t \rceil = -1$, so the new v_2 is $(1,5)^\mathsf{T} - (2,1)^\mathsf{T} = (-1,4)^\mathsf{T}$.

We have $\|v_1\|^2 = 5$, $\|v_2\|^2 = 17$, $\langle v_1, v_2\rangle = 2$, so $t = 2/5 = 0.4$. Since $\lfloor t \rceil = 0$ we stop and the output is

$$\left(\begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}-1\\4\end{bmatrix}\right).$$

In particular, the solution of the SVP in this lattice is $(2,1)^\mathsf{T}$.

step	v_1	v_2	$\|v_1\|^2$	$\|v_2\|^2$	$\langle v_1, v_2\rangle$	$\lfloor t \rceil$	Hadamard ratio $\mathcal{H}$
1	$\left[\begin{smallmatrix}1\\5\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}6\\21\end{smallmatrix}\right]$	26	477	111	-4	0.284
2	$\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1\\5\end{smallmatrix}\right]$	5	26	7	-1	0.888
3	$\left[\begin{smallmatrix}2\\1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}-1\\4\end{smallmatrix}\right]$	5	17	2	0	0.988

4.3.2 Higher dimensions: LLL reduction

A frustrating issue is that, even though the notion of Lagrange–Gauss reduced lattice can be extended to higher dimensions, algorithms for computing it are harder to come by, and it is not even clear that the result is particularly useful.

It turns out that a good solution is to loosen up the conditions of being reduced. One such relaxation is the notion of LLL-reduced, named after its proponents Arjen Lenstra, Hendrik Lenstra, and László Lovász.

It would be good to recall the setup of Gram–Schmidt orthogonalisation. Let $v_1, \dots, v_n$ be a basis for $\mathbf{R}^n$. For $i = 1, \dots, n$ let $V_i = \mathsf{Span}_{\mathbf{R}}\{v_1, \dots, v_i\}$.

The Gram–Schmidt process returns vectors $v_1^*, \dots, v_n^* \in \mathbf{R}^n$ and scalars $\mu_{ij} \in \mathbf{R}$ for $1 \leqslant j < i \leqslant n$, defined inductively by

$$v_i^* = \mathsf{proj}_{V_{i-1}^\perp}(v_i) = v_i - \mathsf{proj}_{V_{i-1}}(v_i) = v_i - \sum_{j=1}^{i-1} \mu_{ij} v_j^*$$

$$\mu_{ij} = \frac{\langle v_i, v_j^* \rangle}{\|v_j^*\|^2}$$

with $v_1^* = v_1$.

Note that, for all $i = 2, \dots, n$,

$$V_{i-1} = \mathsf{Span}_{\mathbf{R}}\{v_1, \dots, v_{i-1}\} = \mathsf{Span}_{\mathbf{R}}\{v_1^*, \dots, v_{i-1}^*\}$$

and $v_1^*, \dots, v_n^*$ is an orthogonal basis of $\mathbf{R}^n$.

Let's go back to the setup of a lattice $L \subset \mathbf{R}^n$. We say that a basis $v_1, \dots, v_n$ for L is *LLL-reduced* if

$$|\mu_{ij}| \leqslant \frac{1}{2} \qquad \text{for all } 1 \leqslant j < i \leqslant n$$

$$\|v_i^* + \mu_{i,i-1} v_{i-1}^*\|^2 \geqslant \frac{3}{4} \|v_{i-1}^*\|^2 \qquad \text{for all } 1 < i \leqslant n.$$

(Here 3/4 can be replaced by a parameter $\delta \in (1/4, 1)$.)

The advantage of an LLL-reduced basis is that its vectors are in some sense small:

Proposition 4.16. *If $\{v_1, \dots, v_n\}$ is an LLL-reduced basis of a lattice L, then*

$$\|v_j\|^2 \leqslant 2^{i-1} \|v_i^*\|^2 \qquad \textit{for all } 1 \leqslant j \leqslant i \leqslant n$$

$$\det L \leqslant \prod_i \|v_i\| \leqslant 2^{n(n-1)/4} \det L$$

$$\|v_1\| \leqslant 2^{(n-1)/4} (\det L)^{1/n}$$

$$\|v_1\|^2 \leqslant 2^{n-1} \|x\|^2 \qquad \textit{for all } x \in L \setminus \{0\}.$$

It is worth dwelling a little on this last inequality. If the constant (once L is fixed) multiplier 2^{n-1} were not there, we would have that v_1 is a shortest nonzero vector in L. Instead of trying to solve SVP directly (which we know is very expensive), an LLL-reduced basis gives up some control on the size of v_1, to the extent shown in the last inequality of the Proposition. What is gained however is that this can be computed in time polynomial in the dimension n, via the LLL reduction algorithm, which starts with an arbitrary basis of L and iteratively modifies it to achieve a reduced one.

Here is the idea of the LLL algorithm, starting with a $\mathbf{Z}$-basis $v_1, \dots, v_n$ of L:

(a) Compute the Gram–Schmidt orthogonalisation $v_1^*, \dots, v_n^*$ and the scalars μ_{ij} for $1 \leqslant j < i \leqslant n$.

(b) For each k from 2 to n:

i. Replace v_k with

$$v_k - \sum_{j=1}^{k-1} \lfloor \mu_{kj} \rceil v_j$$

and recalculate all the μ_{kj}.

ii. If $\|v_k^* + \mu_{k,k-1} v_{k-1}^*\|^2 \geqslant \frac{3}{4} \|v_{k-1}^*\|^2$ then move on to $k+1$; otherwise swap v_k and v_{k-1}, recalculate all the quantities depending on these indices and go back to step i.

Example 4.17. Consider the lattice with basis matrix

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 785398 & 197396 & 4184 \end{bmatrix}$$

The norms of the three basis vectors are roughly

$$785398.0, 197396.0, 4184.0$$

and the Hadamard ratio is ≈ 0.001.

The LLL algorithm returns the matrix

$$\begin{bmatrix} 1 & 42 & 29 \\ -4 & -162 & -121 \\ 1 & -241 & 265 \\ -2 & 220 & 386 \end{bmatrix}$$

whose columns are the vectors in the reduced basis, with norms roughly

$$4.7, 369.9, 484.5$$

and Hadamard ratio ≈ 0.988.

Remember that Proposition 4.16 only guarantees that the first basis vector is within a factor of $\sqrt{2^{3-1}} = 2$ of the shortest nonzero vector. In this example however, it can be checked that the first basis vector is actually a shortest vector.

Application to finding integer relations

Consider the real numbers $\zeta(2)$ and π^2; are there integers a and b such that

$$a\,\zeta(2) + b\,\pi^2 = 0?$$

We know that the answer is yes, since Euler proved that $\zeta(2) = \pi^2/6$; but this gives an example of an integer relation involving two real numbers.

More generally, given a vector $x = (x_1, \ldots, x_n)^\mathsf{T} \in \mathbf{R}^n$, we define an *integer relation for x* to be a nonzero vector $m = (m_1, \ldots, m_n)^\mathsf{T} \in \mathbf{Z}^n$ with integer entries such that

$$\langle m, x \rangle = m_1 x_1 + \cdots + m_n x_n = 0.$$

Of course, there is no guarantee that such a magical m exists. (Take, for instance, $x = (1, \sqrt{2})^\mathsf{T}$.) This leads us to state the

Integer Relation Problem. *Given $x \in \mathbf{R}^n$, either find a "small" integer relation m for x or prove that no such "small" integer relation exists.*

You may find the rather imprecise use of the adjective "small" distasteful. In that case, there is a more assertive version of the problem that fixes a bound 2^k and asks for $m \in \mathbf{Z}^n$ with $\|m\| \leqslant 2^{n+k}$ or a proof that there is no $m \in \mathbf{Z}^n$ with $\|m\| < 2^k$.

There is yet another version that is most attractive in practice, where we take the input vector $x \in \mathbf{Z}^n$ as well. The following example shows how this might come about.

Example 4.18. Let

$$\begin{aligned} x_1 &= \arctan(1) = 0.7853981\ldots \\ x_2 &= \arctan(1/5) = 0.1973955\ldots \\ x_3 &= \arctan(1/239) = 0.0041840\ldots \end{aligned}$$

Can we find an integer relation m for $x = (x_1, x_2, x_3)^\mathsf{T}$:

$$m_1x_1 + m_2x_2 + m_3x_3 = 0?$$

We turn this into a question about integers by fixing a multiplier A, say $A = 10^6$, and considering

$$m_1\lfloor Ax_1 \rceil + m_2\lfloor Ax_2 \rceil + m_3\lfloor Ax_3 \rceil \approx 0,$$

that is

$$785398m_1 + 197396m_2 + 4184m_3 \approx 0.$$

There are several approaches to finding m_1, m_2, m_3 and we will be looking in more detail at one of them, the LLL algorithm. For now I will just say that this algorithm takes the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 785398 & 197396 & 4184 \end{bmatrix}$$

and returns the matrix

$$\begin{bmatrix} 1 & 42 & 29 \\ -4 & -162 & -121 \\ 1 & -241 & 265 \\ -2 & 220 & 386 \end{bmatrix}$$

The first column of this matrix will be telling us that

$$785398 \cdot 1 + 197396 \cdot (-4) + 4184 \cdot 1 = -2,$$

or, going back to our original real numbers, that

$$0.785398 \cdot 1 + 0.197396 \cdot (-4) + 0.004184 \cdot 1 = \frac{-2}{10^6} \approx 0.$$

In other words, $m = (1, -4, 1)^\mathsf{T}$ seems to be an integer relation.

Indeed, Machin found this formula in 1706:

$$\arctan(1) = 4\arctan(1/5) - \arctan(1/239).$$

It works remarkably well as a rapidly convergent approximation to $\pi = 4\arctan(1)$.

How does lattice reduction help with finding integer relations? (It may be good to follow along with Example 4.18.) Given $x_1, \dots, x_n \in \mathbf{R}$, let $x_1', \dots, x_n' \in \mathbf{R}$ be close approximations (such as, for instance, truncating after a certain number of digits). Let A be a multiplier. Consider the $\mathbf{Z}$-linear map $\mathbf{Z}^n \longrightarrow \mathbf{R}^{n+1}$ given by

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} \mapsto \begin{bmatrix} m_1 \\ \vdots \\ m_n \\ A\sum_i m_i x_i' \end{bmatrix}$$

Let L denote the image of this map; it is a lattice (of rank n) inside an n-dimensional subspace V of $\mathbf{R}^{n+1}$.

In other words, we consider the matrix representation of the $\mathbf{Z}$-linear map above

$$M = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ Ax_1' & Ax_2' & \dots & Ax_n' \end{bmatrix}$$

Letting $v_1, \dots, v_n$ denote the columns of this matrix, we have

$$L = \mathsf{Span}_{\mathbf{Z}}\{v_1, \dots, v_n\} \subset V = \mathsf{Span}_{\mathbf{R}}\{v_1, \dots, v_n\}$$

The crucial observation is that

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \\ \varepsilon \end{bmatrix} \in L \qquad \text{if and only if} \qquad m_1 x_1' + \dots + m_n x_n' = \frac{\varepsilon}{A}.$$

If ε is relatively small then (since $x_i' \approx x_i$)

$$m_1 x_1 + \dots + m_n x_n \approx 0.$$

So we are interested in finding elements of L that have small components. But, as we have seen above, the first vector in a reduced basis for L will be relatively small. So we apply LLL to the basis $v_1, \dots, v_n$ of L, obtain a reduced basis $w_1, \dots, w_n$, and take the relation determined by the first vector w_1.

Application to cryptanalysis

Consider the following question:

Subset Sum Problem. *Given a vector $v \in \mathbf{Z}^n_{\geqslant 1}$ and a positive integer T, find a vector $w \in \{0,1\}^n$ such that $\langle v, w\rangle = T$.*

(This is one of many variants referred to the Subset Sum Problem in the literature.)

Example 4.19. For $v = (2, 9, 4, 3, 14, 23)$ and $T = 21$, $w = (0, 0, 1, 1, 1, 0)$ works.

For $v = (2, 9, 4, 3, 14, 23)$ and $T = 29$, both $w = (1, 0, 1, 0, 0, 1)$ and $w = (1, 1, 1, 0, 1, 0)$ work.

The Subset Sum Problem is, in general, hard. However, special instances of it can be much easier.

A vector $v \in \mathbf{Z}^n_{\geqslant 1}$ is called *superincreasing* if

$$v_{j+1} \geqslant 2v_j \qquad \text{for all } 1 \leqslant j < n.$$

The following can be proved by an easy induction:

Lemma 4.20. *If v is a superincreasing vector, then*

$$v_j > v_{j-1} + \cdots + v_1 \qquad \textit{for all } 2 \leqslant j \leqslant n.$$

Let (v, T) be an instance of the Subset Sum Problem where v is a superincreasing vector. If a solution exists, then it is unique and can be found efficiently by the following greedy algorithm:

- If $T \geqslant v_n$, let $w_n = 1$ and replace T by $T - v_n$, otherwise let $w_n = 0$.
- Same with $v_{n-1}, \ldots, v_1$.

Example 4.21. Let $v = (3, 11, 24, 50, 115)$ and $T = 142$.

We have $w_5 = 1$, new $T = 142 - 115 = 27$. We have $w_4 = 0$. We have $w_3 = 1$, new $T = 27 - 24 = 3$. We have $w_2 = 0$ and $w_1 = 1$.

So $w = (1, 0, 1, 0, 1)$.

This creates the opportunity for the type of asymmetry that can be exploited to make a public key cryptosystem. Merkle and Hellman did exactly this, as follows.

For the setup, Bob picks a superincreasing vector v and two large secret integers A and N such that

$$2v_n < N, \qquad \gcd(A, N) = 1.$$

He then uses A and N to scramble the vector v, producing a new vector u by

$$u_j \equiv Av_j \pmod{N}, \qquad 0 \leqslant u_j < N.$$

This new vector u, which is not likely to be superincreasing, is Bob's public key.

Alice takes her plaintext message $m \in \{0, 1\}^n$ and computes the ciphertext

$$c = \langle m, u \rangle = \sum_{j=1}^{n} m_j u_j.$$

Bob's decryption process has two steps. First, he computes $c' \equiv A^{-1}c \pmod{N}$, with $0 \leqslant c' < N$. Then he solves the Subset Sum Problem (v, c') and recovers the plaintext m.

Example 4.22. Suppose Bob picks the superincreasing vector $v = (3, 11, 24, 50, 115)$ from Example 4.21, with $A = 113$ and $N = 250$. The scrambled vector is $u \equiv 113v \pmod{250}$ is $u = (89, 243, 212, 150, 245)$.

Alice wants to send Bob the message $m = (1, 0, 1, 0, 1)$, so she encrypts it as

$$c = \langle m, u \rangle = 546.$$

Bob takes the inverse of 113 mod 250, getting 177, and computes $c' = 177 \cdot 546 \equiv 142 \pmod{250}$. It remains for him to solve the Subset Sum Problem with target $T = 142$ using the superincreasing vector v, which by Example 4.21 will give him $w = (1, 0, 1, 0, 1) = m$, the plaintext message.

We now put ourselves in the place of the eavesdropper Eve. Based on the information she has, her task is to solve the Subset Sum Problem (u, c). This is trickier because u is not a superincreasing vector. She can turn this into a question about lattices by building the $(n+1) \times (n+1)$ matrix

$$M = \begin{bmatrix} 2 & 0 & \dots & 0 & 1 \\ 0 & 2 & \dots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 2 & 1 \\ u_1 & u_2 & \dots & u_n & c \end{bmatrix}$$

and taking the lattice L with $\mathbf{Z}$-basis matrix M.

If $w = (w_1, \dots, w_n)$ is a solution of the Subset Sum Problem (u, c), then

$$v := \begin{bmatrix} 2w_1 - 1 \\ \vdots \\ 2w_n - 1 \\ 0 \end{bmatrix} = M \begin{bmatrix} w_1 \\ \vdots \\ w_n \\ -1 \end{bmatrix} \in L.$$

But the vector v has n entries that are ± 1 and one zero entry, so $\|v\| = \sqrt{n}$, which is pretty small compared to the norms of the columns of the basis matrix M. So maybe Eve should be looking for short vectors in L.

Example 4.23. We revisit Example 4.22. The relevant basis matrix is

$$M = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 89 & 243 & 212 & 150 & 245 & 546 \end{bmatrix}$$

The result of running LLL is the matrix

$$\begin{pmatrix} -1 & 1 & -1 & 1 & -2 & -6 \\ 1 & -1 & -1 & -1 & -2 & -4 \\ -1 & -1 & -1 & -1 & 4 & -6 \\ 1 & 1 & 1 & -1 & 0 & -6 \\ -1 & -1 & 1 & -1 & -2 & 0 \\ 0 & -1 & 2 & 2 & 0 & -3 \end{pmatrix}$$

so we pick the first column and we write it as a linear combination of the columns of the basis matrix M:

$$\begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 0 \end{bmatrix} = M \begin{bmatrix} -1 \\ 0 \\ -1 \\ 0 \\ -1 \\ 1 \end{bmatrix},$$

indicating the relation

$$-89 - 212 - 245 + 546 = 0,$$

which gives the solution $1 \cdot 89 + 0 \cdot 243 + 1 \cdot 212 + 0 \cdot 150 + 1 \cdot 245 = 546$ of the Subset Sum Problem.

Eve therefore has the plaintext message $(1, 0, 1, 0, 1)$.