Notation

- $\mathbb{R}$, real numbers
- $\mathbb{Z}$, integers
- $\mathbb{N}$, positive integers
- $\|x\| = \sqrt{\sum_{i\in[n]} x_i^2}$, the ℓ_2 or Euclidean norm of a vector $\vec{x} \in \mathbb{R}^n$.
- $\|x\|_\infty = \max_{i\in n}(x_i)$, the ℓ_∞ norm of a vector $\vec{x} \in \mathbb{R}^n$.
- $\mathcal{L}$ or Λ, lattice
- $\mathcal{L}(B)$or $\Lambda(B)$, lattice generated by basis B

Definitions of Lattices

1. what is lattice
2. bases of a lattice
3. what can we know from a basis
4. equivalent bases
5. Successive Minima
6. what does it tell?

definition

Definition 1 (Lattice) *$\mathcal{L} \subseteq \mathbb{R}^n$ is a lattice if $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. $\mathcal{L}$ is a rank k lattice, or k-dimensional, if $\dim(\mathcal{L}) = k$. $\mathcal{L}$ is said to be full-rank if $\dim(\mathcal{L}) = n$ (dimension of the ambient space).*

To be able to interpret this, one needs to define both what discrete and what additive subgroup means. Since our lattices are embedded in $\mathbb{R}^n$, the definitions given below rely on the additive structure and topology of $\mathbb{R}^n$.

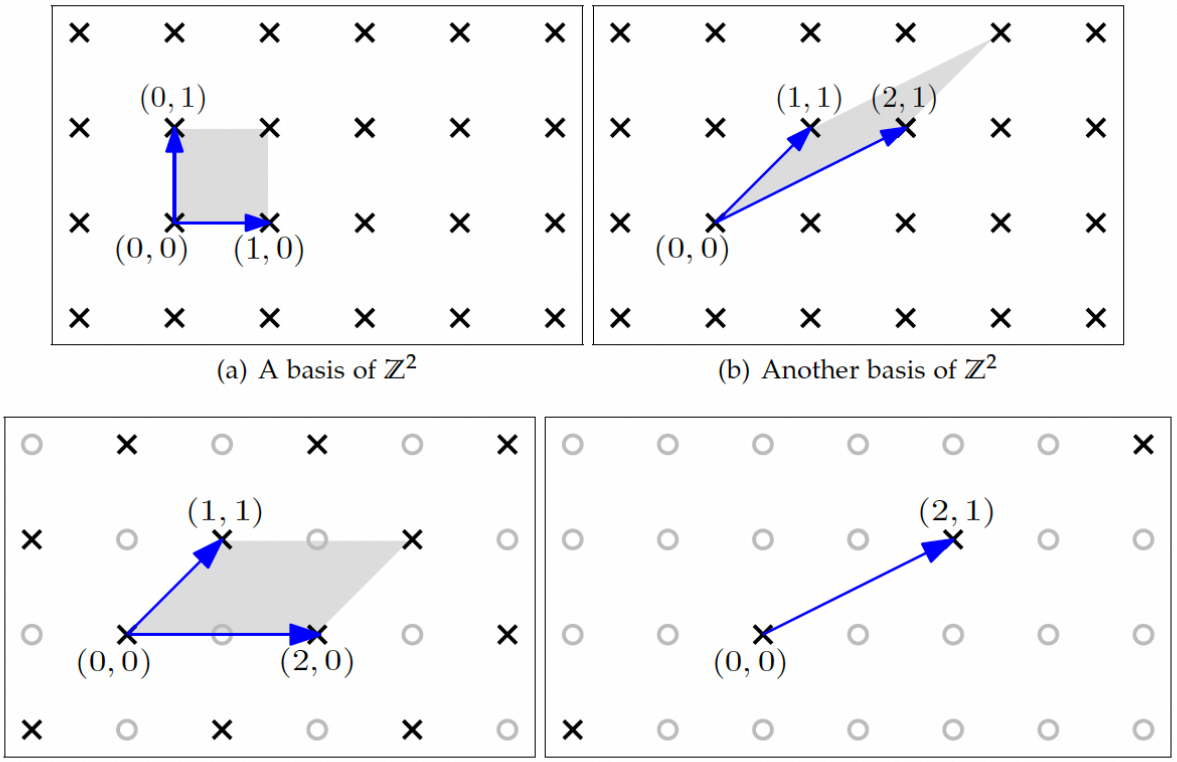
1. **Discrete:** $\mathcal{L}$ is discrete if the induced topology on $\mathcal{L}$ is discrete.
   That is, every subset of $\mathcal{L}$ is open.
2. **Additive subgroup:**
   (a) $\forall \mathbf{x}, \mathbf{y} \in \mathcal{L}, \mathbf{x} + \mathbf{y} \in \mathcal{L}$.
   (b) $\forall \mathbf{x} \in \mathcal{L}, -\mathbf{x} \in \mathcal{L}$.

Bases

A basis of $\mathcal{L}$ is an ordered set $\mathbb{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ such that

$$\mathcal{L} = \mathcal{L}(\mathbb{B}) = \mathbb{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}. \tag{1.1}$$

Note that by convention, $\mathbf{b}_i$ are column vectors and $\mathbb{B} \cdot \mathbf{k} = k_1\mathbf{b}_1 + \cdots + k_n\mathbf{b}_n$, where $\mathbf{k}$ is a column vector.



(a) A basis of $\mathbb{Z}^2$ (b) Another basis of $\mathbb{Z}^2$

(c) Not a basis of $\mathbb{Z}^2$ (d) Not a full-rank lattice

homework: explain why the subgroup generated by $(1+\sqrt{2})$ is not a lattice?

Fundamental Parallelepiped

DEFINITION 3 (FUNDAMENTAL PARALLELEPIPED) *For any lattice basis B we define*

$$\mathcal{P}(B) = \{Bx \mid x \in \mathbb{R}^n, \forall i : 0 \leq x_i < 1\}.$$

Examples of fundamental parallelepipeds are shown by the gray areas in Figure 2. Notice that $\mathcal{P}(B)$ depends on the basis B. It follows easily from the definitions above, that if we place one copy of $\mathcal{P}(B)$ at each lattice point in $\mathcal{L}(B)$ we obtain a tiling of the entire $\mathrm{span}(\mathcal{L}(B))$. See Figure 3.

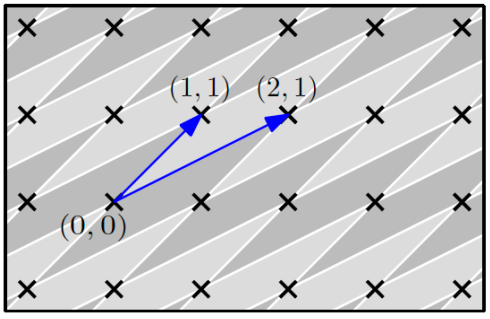


Figure 3: Tiling $\mathrm{span}(\mathcal{L}(B))$ with $\mathcal{P}(B)$

LEMMA 1 *Let Λ be a lattice of rank n, and let $b_1, b_2, \ldots, b_n \in \Lambda$ be n linearly independent lattice vectors. Then $b_1, b_2, \ldots, b_n$ form a basis of Λ if and only if $\mathcal{P}(b_1, b_2, \ldots, b_n) \cap \Lambda = \{0\}$.*

Equivalent bases

DEFINITION 4 (UNIMODULAR MATRIX) *A matrix* $U \in \mathbb{Z}^{n\times n}$ *is called* unimodular *if* $\det U = \pm 1$.

For example, the matrix

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

is unimodular. The following lemma appears in the homework. It tells us that the inverse of a unimodular matrix is also unimodular (so it follows that the set of unimodular matrices forms a group under matrix multiplication).

LEMMA 2 *If* U *unimodular, then* U^{-1} *is also unimodular, and in particular* $U^{-1} \in \mathbb{Z}^{n\times n}$.

LEMMA 3 *Two bases* $B_1, B_2 \in \mathbb{R}^{m\times n}$ *are equivalent if and only if* $B_2 = B_1 U$ *for some unimodular matrix* U.

PROOF: First assume that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Then for each of the n columns b_i of B_2, $b_i \in \mathcal{L}(B_1)$. This implies that there exists an integer matrix $U \in \mathbb{Z}^{n\times n}$ for which $B_2 = B_1 U$. Similarly, there exists a $V \in \mathbb{Z}^{n\times n}$ such that $B_1 = B_2 V$. Hence $B_2 = B_1 U = B_2 V U$, and we get

$$B_2{}^T B_2 = (VU)^T B_2{}^T B_2 (VU).$$

Taking determinants, we obtain that $\det(B_2{}^T B_2) = (\det(VU))^2 \det(B_2{}^T B_2)$ and hence $\det(V)\det(U) = \pm 1$. Since V, U are both integer matrices, this means that $\det(U) = \pm 1$, as required.

For the other direction, assume that $B_2 = B_1 U$ for some unimodular matrix U. Therefore each column of B_2 is contained in $\mathcal{L}(B_1)$ and we get $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$. In addition, $B_1 = B_2 U^{-1}$, and since U^{-1} is unimodular (Lemma 2) we similarly get that $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$. We conclude that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ as required. $\square$

DEFINITION 5 (DETERMINANT) *Let* $\Lambda = \mathcal{L}(B)$ *be a lattice of rank* n. *We define the* determinant *of* Λ, *denoted* $\det(\Lambda)$, *as the* n*-dimensional volume of* $\mathcal{P}(B)$. *In symbols, this can be written as* $\det(\Lambda) := \sqrt{\det(B^T B)}$. *In the special case that* Λ *is a full rank lattice,* B *is a square matrix, and we have* $\det(\Lambda) = |\det(B)|$.

The determinant of a lattice is well-defined, in the sense that it is independent of our choice of basis B. Indeed, if B_1 and B_2 are two bases of Λ, then by Lemma 3, $B_2 = B_1 U$ for some unimodular matrix U. Hence,

$$\sqrt{\det(B_2{}^T B_2)} = \sqrt{\det(U^T B_1{}^T B_1 U)} = \sqrt{\det(B_1{}^T B_1)}.$$

The determinant of a lattice is inverse proportional to its density: the smaller the determinant, the denser the lattice is. In more precise terms, if one takes a large ball K (in the span of Λ) then the number of lattice points inside K approaches $\mathrm{vol}(K)/\det(\Lambda)$ as the size of K goes to infinity.

GSO

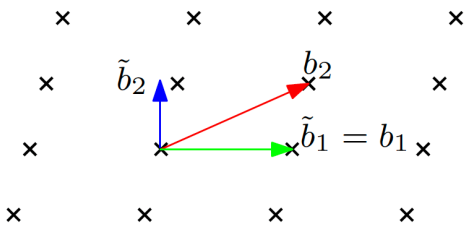


Figure 4: Gram-Schmidt orthogonalization

The Gram-Schmidt orthogonalization $\widetilde{\mathbb{B}}$ of a basis $\mathbb{B}$ of $\mathcal{L}$ is given by

$$\begin{aligned}
\mathbb{B} &= QR && (1.19)\\
&= Q\begin{pmatrix} \|\widetilde{\mathbf{b}_1}\| & & * \\ & \ddots & \\ 0 & & \|\widetilde{\mathbf{b}_n}\| \end{pmatrix} && (1.20)\\
&= \widetilde{\mathbb{B}}\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}, && (1.21)
\end{aligned}$$

where

$$\widetilde{\mathbb{B}} = Q\begin{pmatrix} \|\widetilde{\mathbf{b}_1}\| & & 0 \\ & \ddots & \\ 0 & & \|\widetilde{\mathbf{b}_n}\| \end{pmatrix},$$

and Q is an orthonormal basis reduced from $\widetilde{\mathbb{B}}$, and R is a representation of $\mathbb{B}$ with respect to this basis.

Successive minima

Successive minima of linearly independent vectors are defined as follows:

- $\lambda_1(\mathcal{L}) := \min_{0\neq\mathbf{v}\in\mathcal{L}} \|\mathbf{v}\| = \min_{\mathbf{x}\neq\mathbf{y}\in\mathcal{L}} \|\mathbf{x}-\mathbf{y}\|$
- $\lambda_i(\mathcal{L}) := \min\{r : \mathcal{L} \text{ contains } i \text{ linearly independent vectors of length} \leq r\}$.

Then $\lambda_1(\mathcal{L}) \leq \lambda_2(\mathcal{L}) \leq \cdots \leq \lambda_n(\mathcal{L})$. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be corresponding lattice elements. Note that $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ need not be a basis of $\mathcal{L}$.

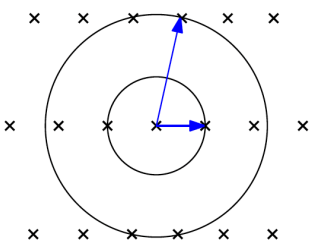


Figure 5: $\lambda_1(\Lambda) = 1, \lambda_2(\Lambda) = 2.3$

THEOREM 5 *Let B be a rank-n lattice basis, and let $\tilde{B}$ be its Gram-Schmidt orthogonalization. Then*

$$\lambda_1(\mathcal{L}(B)) \geq \min_{i=1,\ldots,n} \|\tilde{b}_i\| > 0.$$

Upper Bounding λ_1: Minkowski's Theorem

Theorem 1.1.6 (Minkowski Theorem 1)**.** Any convex centrally symmetric body S of volume $> 2^n \det(\mathcal{L})$ contains a nonzero lattice point.

Corollary 1.1.7.

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}. \tag{1.34}$$

Theorem 1.1.9 (Minkowski Theorem 2)**.** $(\prod_{i=1}^{n} \lambda_i(\mathcal{L}))^{\frac{1}{n}} \leq \sqrt{n}(\det \mathcal{L})^{\frac{1}{n}}$.

worst-case computational problems

Easy computational problems

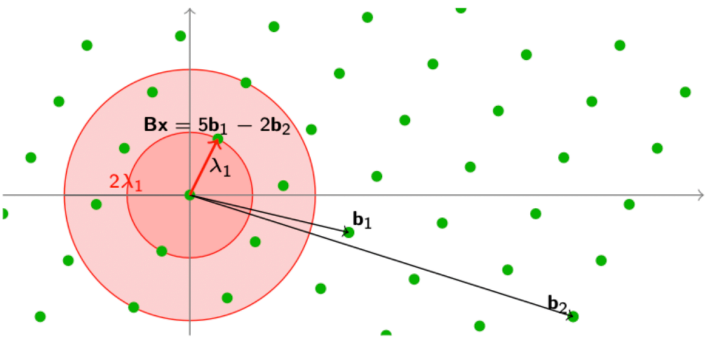
- **Membership**: Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ and a vector $v \in \mathbb{Z}^m$, decide if $v \in \mathcal{L}(B)$.
  The equation $Bx = v$ can be seen as a system of m linear equations in n variables. We can therefore solve it efficiently by Gaussian elimination. If a solution exists and it happens to be in $\mathbb{Z}^n$ (as opposed to $\mathbb{Q}^n$), output YES; otherwise output NO.
- **Equivalence**: Given $B_1, B_2 \in \mathbb{Z}^{m\times n}$, decide if $\mathcal{L}(B_1) = \mathcal{L}(B_2)$.
  To solve this, we check two things: that each column of B_1 is contained in $\mathcal{L}(B_2)$ and that each column of B_2 is contained in $\mathcal{L}(B_1)$. If $\mathcal{L}(B_1) = \mathcal{L}(B_2)$, these two checks are satisfied. Conversely, if these checks are satisfied, then $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$ and $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$ and hence $\mathcal{L}(B_1) = \mathcal{L}(B_2)$.

SVP

- **Search** SVP_γ: Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ find $v \in \mathcal{L}(B)$ such that $v \neq 0$ and $\|v\| \leq \gamma \cdot \lambda_1(\mathcal{L}(B))$.
- **Optimization** SVP_γ: Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ find d such that $d \leq \lambda_1(\mathcal{L}(B)) \leq \gamma \cdot d$.
- **Promise** SVP_γ: An instance of the problem is given by a pair (B, r) where $B \in \mathbb{Z}^{m\times n}$ is a lattice basis and $r \in \mathbb{Q}$. In YES instances, $\lambda_1(\mathcal{L}(B)) \leq r$. In NO instances, $\lambda_1(\mathcal{L}(B)) > \gamma \cdot r$.

Definition (SVP_γ)

Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma\lambda_1$

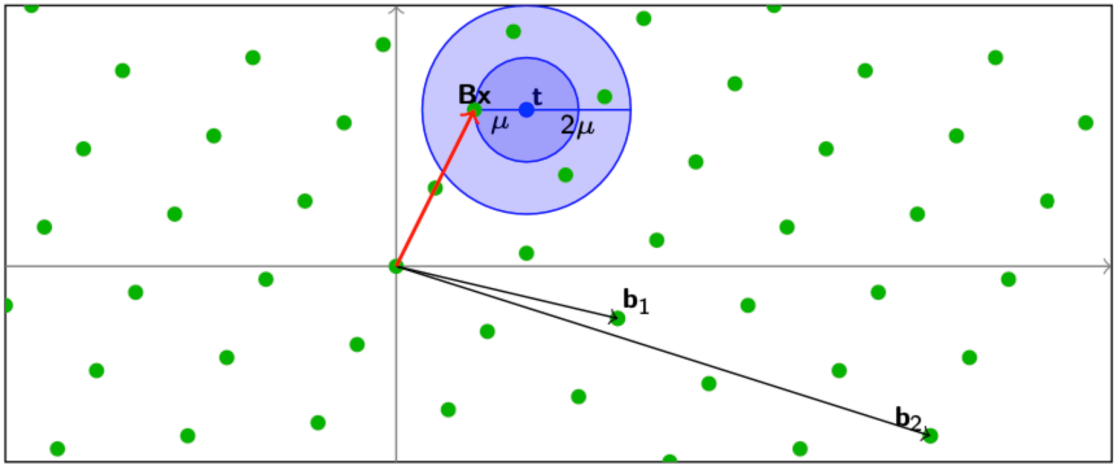


CVP

- **Search** CVP_γ: Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ and a vector $t \in \mathbb{Z}^m$, find $v \in \mathcal{L}(B)$ such that $\|v - t\| \le \gamma \cdot \mathrm{dist}(t, \mathcal{L}(B))$.
- **Optimization** CVP_γ: Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ and a vector $t \in \mathbb{Z}^m$, find d such that $d \le \mathrm{dist}(t, \mathcal{L}(B)) \le \gamma \cdot d$.
- **Promise** CVP_γ: An instance of the problem is given by a triple (B, t, r) where $B \in \mathbb{Z}^{m\times n}$ is a lattice basis, $t \in \mathbb{Z}^m$, and $r \in \mathbb{Q}$. In YES instances, $\mathrm{dist}(t, \mathcal{L}(B)) \le r$. In NO instances, $\mathrm{dist}(t, \mathcal{L}(B)) > \gamma \cdot r$.

Definition (CVP_γ)

Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \le \gamma\mu$ from the target



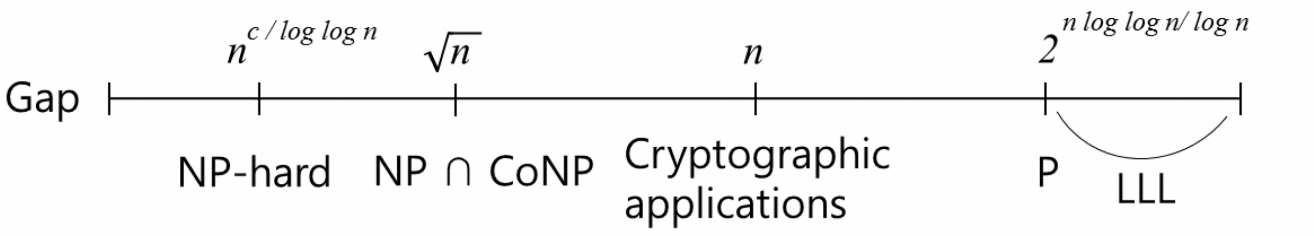
LLL

DEFINITION 1 *Given n linearly independent vectors $b_1, \ldots, b_n \in \mathbb{R}^n$, the* ***Gram-Schmidt orthogonalization*** *of $b_1, \ldots, b_n$ is defined by $\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j}\tilde{b}_j$, where $\mu_{i,j} = \frac{\langle b_i, \tilde{b}_j\rangle}{\langle \tilde{b}_j, \tilde{b}_j\rangle}$.*

DEFINITION 2 *A basis $B = \{b_1, \ldots, b_n\} \in \mathbb{R}^n$ is a* ***δ-LLL Reduced Basis*** *if the following holds:*

1. $\forall 1 \le i \le n, j < i. |\mu_{i,j}| \le \frac{1}{2}$,
2. $\forall 1 \le i < n.\ \delta\|\tilde{b}_i\|^2 \le \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2$.

CLAIM 1 *Let $b_1, \ldots, b_n \in \mathbb{R}^n$ be a δ-LLL-reduced basis. Then $\|b_1\| \le (\frac{2}{\sqrt{4\delta - 1}})^{n-1}\lambda_1(\mathcal{L})$.*



- $GapSVP_\gamma$: Given a basis $\mathbb{B}$ of $\mathcal{L}$ and a real d, decide between $\lambda_1(\mathcal{L}) \leq d$ and $\lambda_1(\mathcal{L}) > \gamma d$.

average-case problems

1. q-ary lattice
2. SIS problems

q-ary lattice

- Cryptography typically uses (random) lattices $\wedge$ such that $\wedge \subseteq \mathbb{Z}^d$ is an integer lattice and $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer q.
- Cryptographic functions based on q-ary lattices involve only arithmetic modulo q.

Definition (q-ary lattice)

Λ is a q-ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

Definition 2 (Parity check lattice) *Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix with coefficients in $\mathbb{Z}_q$. Define*

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{x} = 0 \ mod\ q\} \quad (= \ker(\mathbf{A} : \mathbb{Z}_q \to \mathbb{Z}_q^n)).$$

Technically, explicting the "mod q" is not required in the above definition, but is included as a helpful reminder to the reader: $\mathbb{Z}_q$ is $\mathbb{Z}$-module, so the product $\mathbf{A}\mathbf{x}$ is well defined, and belong to $\mathbb{Z}_q^n$.

Definition 3 (Row-generated lattice) *Let $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$. Define*

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \mid y = \mathbf{A}\mathbf{s} \ mod\ q, \ for\ some\ \mathbf{s} \in \mathbb{Z}^n\} = \mathbf{A}\mathbb{Z}^n + q\mathbb{Z}^m.$$

Lemma 5 *Let q be prime, and let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix.*

- $\lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})) \leq q^{n/m}$
- $\lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})) > \frac{(q/2)^{n/m}-1}{2}$ *except with probability at most 2^{-n} over the choice of a uniform random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.*

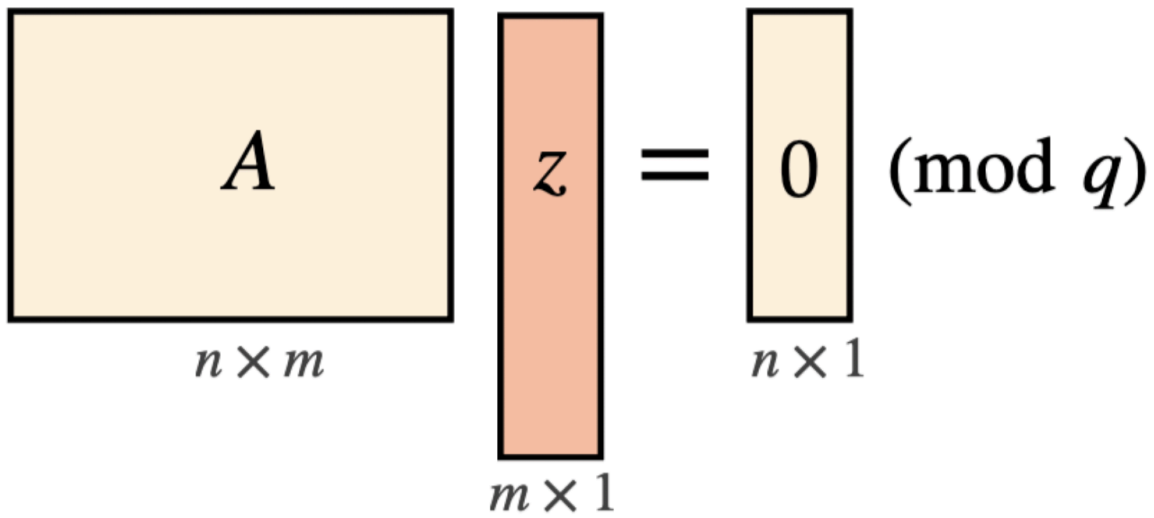
The first inequality is an application of Minkowski theorem, using

$$(2 \cdot \lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})))^m \leq 2^m \cdot \det(\Lambda_q^\perp(\mathbf{A})) \leq 2^m \cdot q^{n/m}.$$

SIS problem

Definition 4.1.1 (Short Integer Solution ($\mathrm{SIS}_{n,q,\beta,m}$)). Given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $\|\mathbf{z}\| \leq \beta$ such that

$$f_{\mathbf{A}}(\mathbf{z}) := \mathbf{A}\mathbf{z} = \sum_i \mathbf{a}_i \cdot z_i = \mathbf{0} \in \mathbb{Z}_q^n. \tag{4.1.1}$$



Definition (SVP in SIS lattice)

Given $A \in_R \mathbb{Z}_q^{n\times m}$, find a nonzero $z \in [-B, B]^m$ in the SIS lattice $L_A^{\perp} = L(C)$ where $C = \begin{bmatrix} qI_n & -\bar{A} \\ 0 & I_{m-n} \end{bmatrix}$.

Remark 7 An instance $\mathbf{A}$ of the SIS problem is equivalent to finding a short non-zero vector in the lattice $\Lambda_q^{\perp}(\mathbf{A})$

Depending on the parameters, the hardness of the SIS-problem can range from 'vacuously hard' to having a polynomial time algorithm giving a solution.

- If $\beta \ll q^{n/m}$, the problem is vacuously hard: Lemma 5 showed that, most likely, such solutions do not exists.
- If $\beta \gg \gamma_2^m \cdot q^{n/m}$, this is an instance of approx-SVP with exponential approximation factor γ_2^m, which can be solved by LLL.
- Somewhere in between these bounds is where cryptography takes place, typically for $\beta = q^{n/m} \cdot \mathrm{poly}(n)$.