The Lattice Base Reduction Algorithm

This is a method which was developed in 1982 by Arjen Lenstra, Hendrik Lenstra and László Lovász to prove that factoring polynomials in $\mathbb{Z}[x]$ can be done in polynomial time.

The Lattice Base Reduction Algorithm

This is a method which was developed in 1982 by Arjen Lenstra, Hendrik Lenstra and László Lovász to prove that factoring polynomials in $\mathbb{Z}[x]$ can be done in polynomial time. It is sometimes called the LLL-algorithm or the L^3-algorithm.

Definitions and Notations.

The Lattice Base Reduction Algorithm

This is a method which was developed in 1982 by Arjen Lenstra, Hendrik Lenstra and László Lovász to prove that factoring polynomials in $\mathbb{Z}[x]$ can be done in polynomial time. It is sometimes called the LLL-algorithm or the L^3-algorithm.

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$.

The Lattice Base Reduction Algorithm

This is a method which was developed in 1982 by Arjen Lenstra, Hendrik Lenstra and László Lovász to prove that factoring polynomials in $\mathbb{Z}[x]$ can be done in polynomial time. It is sometimes called the LLL-algorithm or the L^3-algorithm.

Definitions and Notations. **Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For**

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \ldots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \ldots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \ldots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Further, we use A^T to denote the transpose of a matrix A, so the rows and columns of A are the same as the columns and rows of A^T, respectively.

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \dots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \dots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \dots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Further, we use A^T to denote the transpose of a matrix A, so the rows and columns of A are the same as the columns and rows of A^T, respectively. Let $\vec{b}_1, \dots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \dots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \dots, \vec{b}_n$.

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \ldots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Further, we use A^T to denote the transpose of a matrix A, so the rows and columns of A are the same as the columns and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1 \mathbb{Z} + \cdots + \vec{b}_n \mathbb{Z}.$$

Definitions and Notations. Let $\mathbb{Q}^n$ denote the set of vectors $\langle a_1, a_2, \ldots, a_n \rangle$ with $a_j \in \mathbb{Q}$. For

$$\vec{b} = \langle a_1, a_2, \ldots, a_n \rangle \in \mathbb{Q}^n \quad \text{and} \quad \vec{b}' = \langle a_1', a_2', \ldots, a_n' \rangle \in \mathbb{Q}^n,$$

define the usual dot product $\vec{b} \cdot \vec{b}'$ by

$$\vec{b} \cdot \vec{b}' = a_1 a_1' + a_2 a_2' + \cdots + a_n a_n',$$

and set

$$\|\vec{b}\| = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

Further, we use A^T to denote the transpose of a matrix A, so the rows and columns of A are the same as the columns and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = \big(\vec{b}_1, \ldots, \vec{b}_n\big)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1 \mathbb{Z} + \cdots + \vec{b}_n \mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment:

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

Given that $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathbb{R}^n$, it follows that UV is the identity matrix and $\det V = \pm 1$.

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

Given that $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathbb{R}^n$, it follows that UV is the identity matrix and $\det V = \pm 1$. The second equation above then implies

$$|\det(\vec{b}'_1, \ldots, \vec{b}'_n)| = |\det(\vec{b}_1, \ldots, \vec{b}_n)|.$$

and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

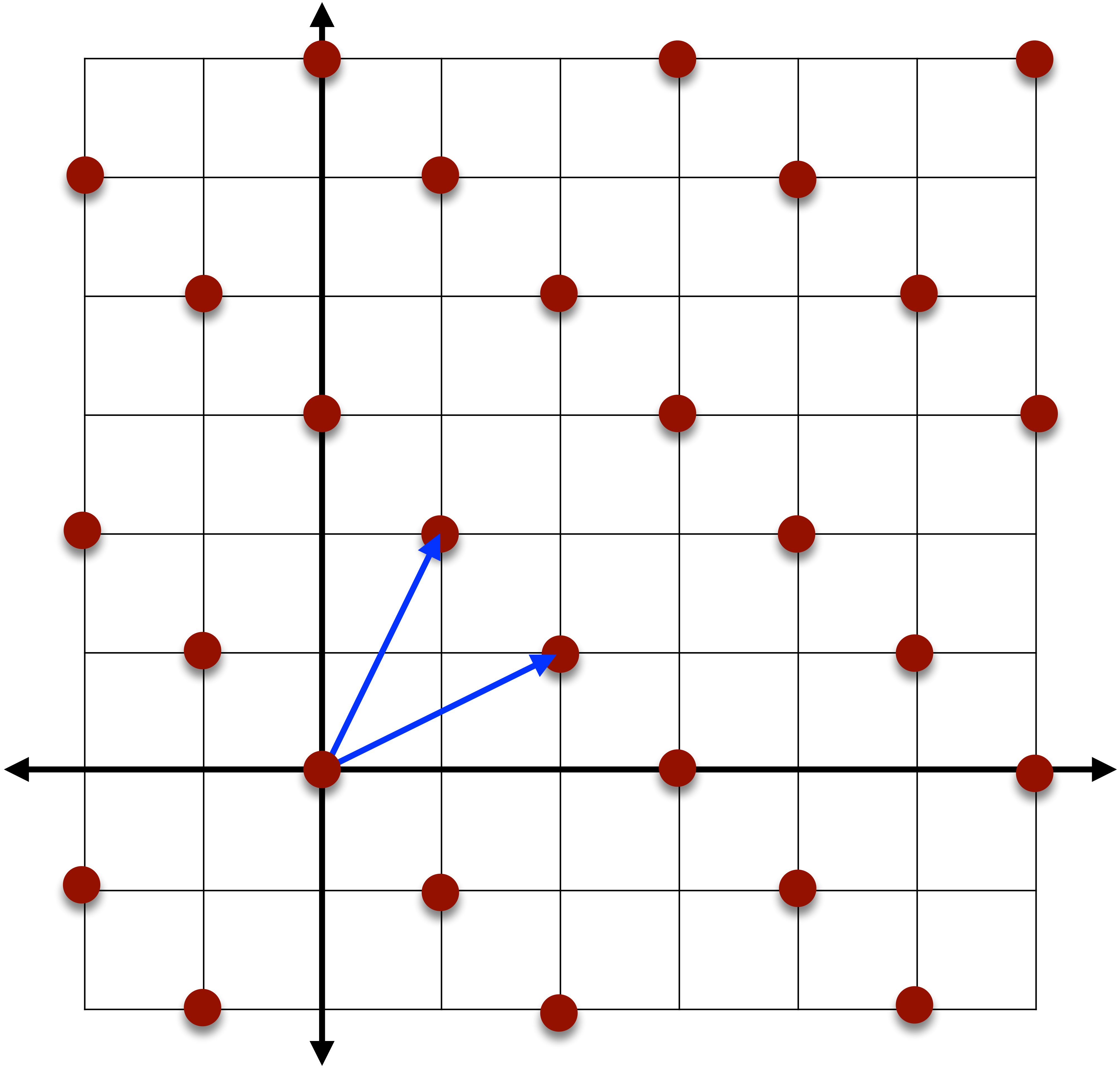
Given that $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathbb{R}^n$, it follows that UV is the identity matrix and $\det V = \pm 1$. The second equation above then implies

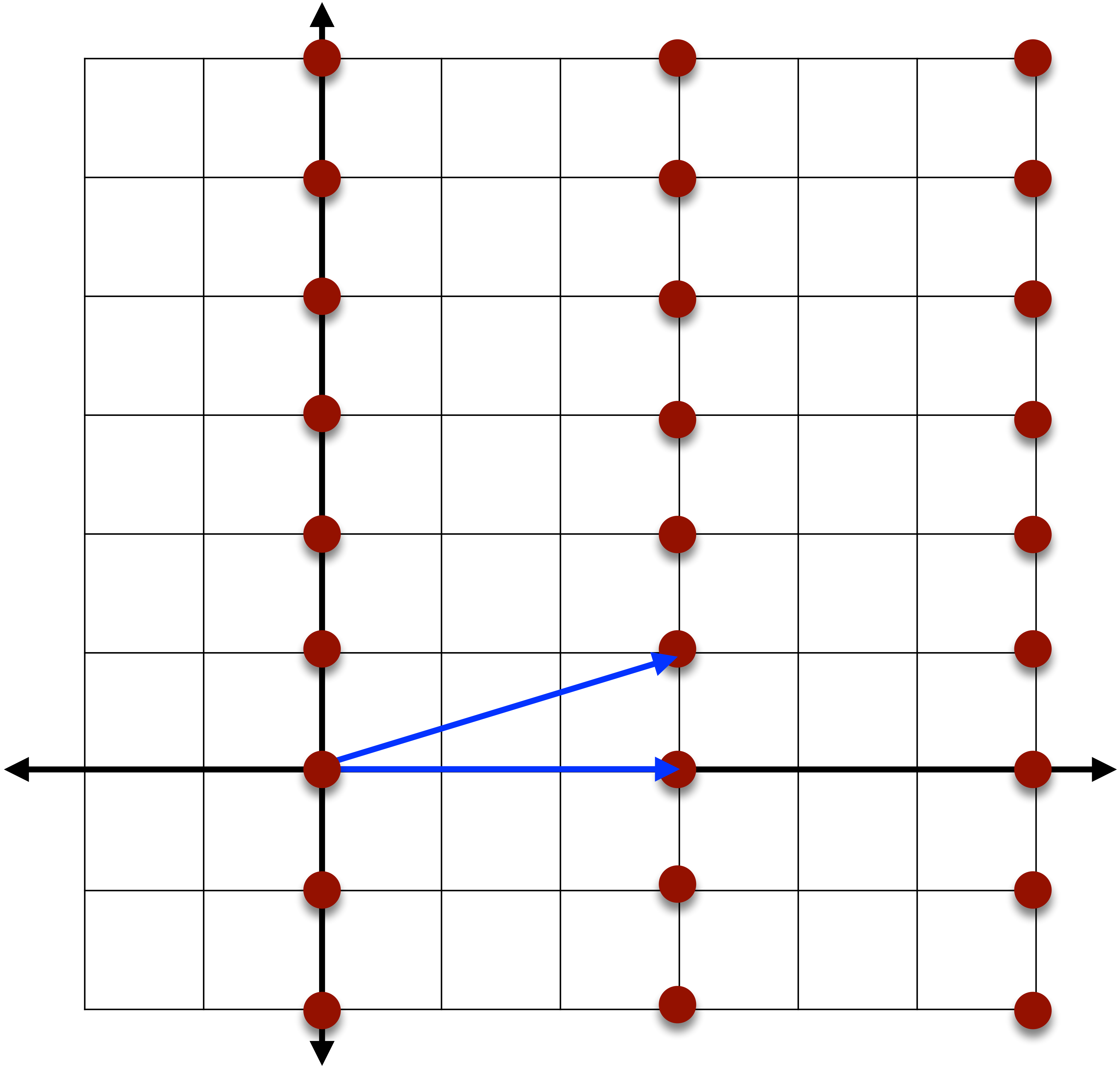
$$|\det(\vec{b}'_1, \ldots, \vec{b}'_n)| = |\det(\vec{b}_1, \ldots, \vec{b}_n)|.$$

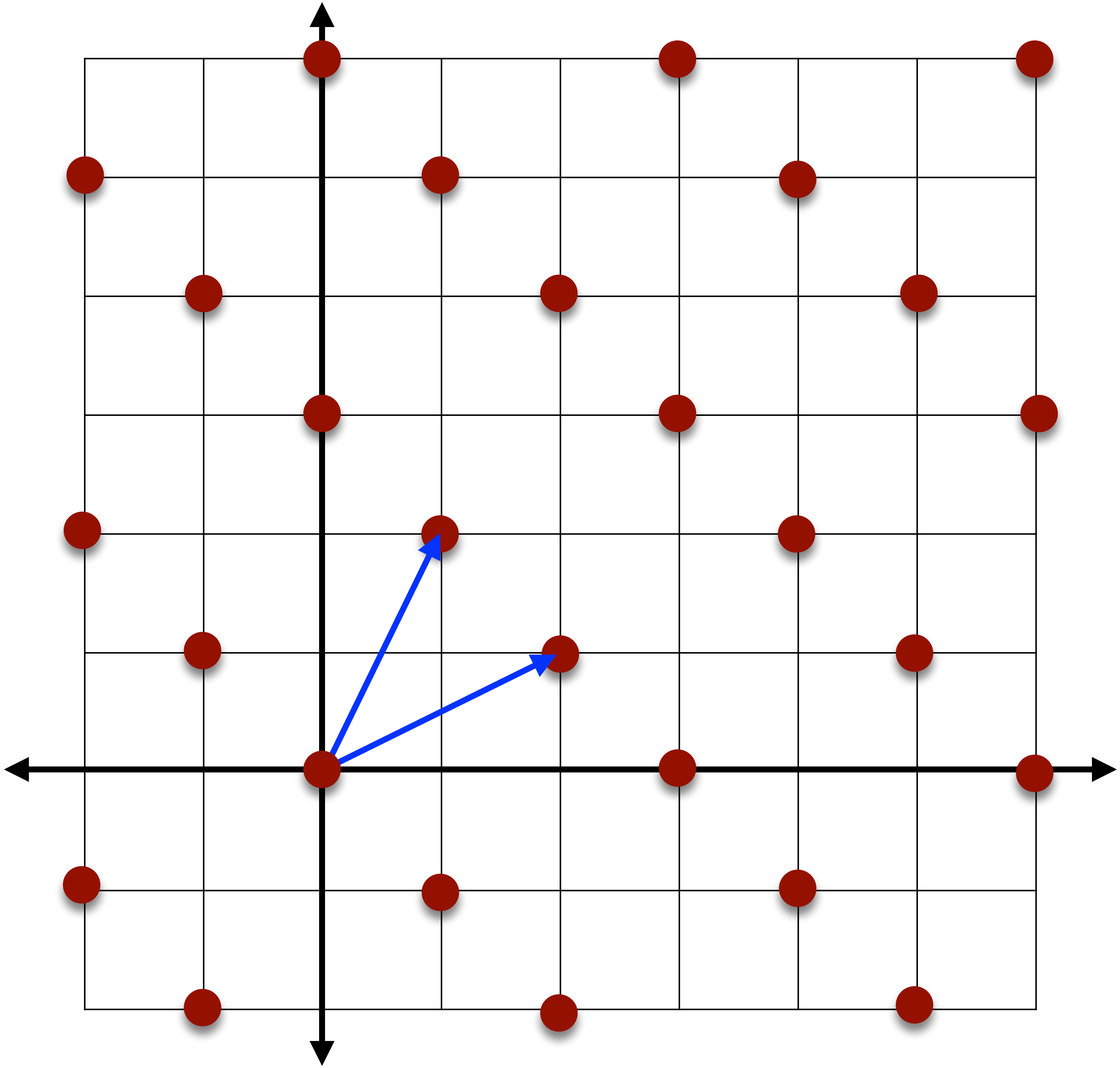
We set $\det \mathcal{L}$ to be this common value.

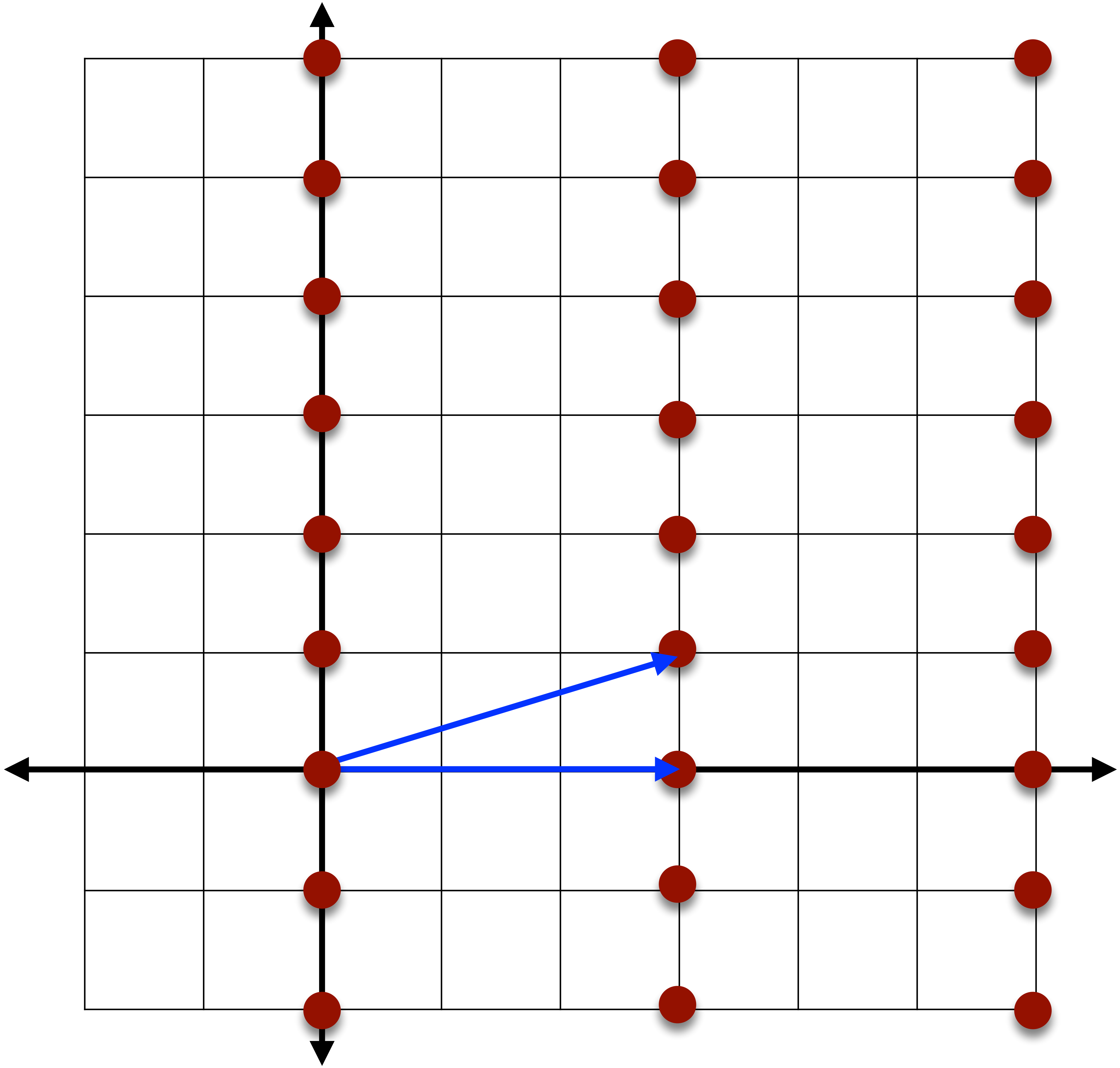
Example. In $\mathbb{R}^2$, the lattice formed from the basis $\langle 1, 0\rangle$ and $\langle 0, 1\rangle$ is the same as the lattice formed from the basis $\langle 1, 0\rangle$ and $\langle 1, 1\rangle$. This can be seen geometrically and algebraically.

Example 2. The lattice $\mathcal{L}_1$ with basis $\langle 2, 1\rangle$ and $\langle 1, 2\rangle$ and the lattice $\mathcal{L}_2$ with basis $\langle 3, 0\rangle$ and $\langle 3, 1\rangle$ are such that $\det \mathcal{L}_1 = \det \mathcal{L}_2$. But the lattices are quite different.









and rows of A^T, respectively. Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Q}^n$, and let $A = (\vec{b}_1, \ldots, \vec{b}_n)$ be the $n \times n$ matrix with column vectors $\vec{b}_1, \ldots, \vec{b}_n$. The lattice $\mathcal{L}$ generated by $\vec{b}_1, \ldots, \vec{b}_n$ is

$$\mathcal{L} = \mathcal{L}(A) = \vec{b}_1\mathbb{Z} + \cdots + \vec{b}_n\mathbb{Z}.$$

We typically want $\vec{b}_1, \ldots, \vec{b}_n$ to be linearly independent; in this case, $\vec{b}_1, \ldots, \vec{b}_n$ is called a basis for $\mathcal{L}$.

Comment: Different A can determine the same $\mathcal{L}$. But given $\mathcal{L}$, the value of $|\det A|$ is the same for all such A. To see this, observe that if $\vec{b}_1, \ldots, \vec{b}_n$ and $\vec{b}'_1, \ldots, \vec{b}'_n$ are two bases for $\mathcal{L}$, there are matrices U and V with integer entries such that

$$(\vec{b}_1, \ldots, \vec{b}_n)UV = (\vec{b}'_1, \ldots, \vec{b}'_n)V = (\vec{b}_1, \ldots, \vec{b}_n).$$

Given that $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathbb{R}^n$, it follows that UV is the identity matrix and $\det V = \pm 1$. The second equation above then implies

$$|\det(\vec{b}'_1, \ldots, \vec{b}'_n)| = |\det(\vec{b}_1, \ldots, \vec{b}_n)|.$$

We set $\det \mathcal{L}$ to be this common value.

The Gram-Schmidt orthogonalization process

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \le i \le n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \le j < i \le n.$$

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \le i \le n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \le j < i \le n.$$

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \le i \le n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \le j < i \le n.$$

Then for each $i \in \{1, \ldots, n\}$, the vectors $\vec{b}_1^*, \ldots, \vec{b}_i^*$ span the same subspace of $\mathbb{R}^n$ as $\vec{b}_1, \ldots, \vec{b}_i$. In other words,

$$\left\{a_1 \vec{b}_1^* + \cdots + a_i \vec{b}_i^* : a_j \in \mathbb{R} \text{ for } 1 \le j \le i\right\}$$
$$= \left\{a_1 \vec{b}_1 + \cdots + a_i \vec{b}_i : a_j \in \mathbb{R} \text{ for } 1 \le j \le i\right\}.$$

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \leq i \leq n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \leq j < i \leq n.$$

Then for each $i \in \{1, \ldots, n\}$, the vectors $\vec{b}_1^*, \ldots, \vec{b}_i^*$ span the same subspace of $\mathbb{R}^n$ as $\vec{b}_1, \ldots, \vec{b}_i$. In other words,

$$\begin{aligned}\{a_1\vec{b}_1^* + \cdots + a_i\vec{b}_i^* : a_j \in \mathbb{R} \text{ for } 1 \leq j \leq i\} \\ = \{a_1\vec{b}_1 + \cdots + a_i\vec{b}_i : a_j \in \mathbb{R} \text{ for } 1 \leq j \leq i\}.\end{aligned}$$

Furthermore, the vectors $\vec{b}_1^*, \ldots, \vec{b}_n^*$ are linearly independent (hence, non-zero) and pairwise orthogonal (i.e., for distinct i and j, we have $\vec{b}_i^* \cdot \vec{b}_j^* = 0$).

Define recursively

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*, \qquad \text{for } 1 \le i \le n,$$

where

$$\mu_{ij} = \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}, \qquad \text{for } 1 \le j < i \le n.$$

Then for each $i \in \{1, \ldots, n\}$, the vectors $\vec{b}_1^*, \ldots, \vec{b}_i^*$ span the same subspace of $\mathbb{R}^n$ as $\vec{b}_1, \ldots, \vec{b}_i$. In other words,

$$\begin{aligned} &\left\{a_1 \vec{b}_1^* + \cdots + a_i \vec{b}_i^* : a_j \in \mathbb{R} \text{ for } 1 \le j \le i\right\} \\ &\qquad = \left\{a_1 \vec{b}_1 + \cdots + a_i \vec{b}_i : a_j \in \mathbb{R} \text{ for } 1 \le j \le i\right\}. \end{aligned}$$

Furthermore, the vectors $\vec{b}_1^*, \ldots, \vec{b}_n^*$ are linearly independent (hence, non-zero) and pairwise orthogonal (i.e., for distinct i and j, we have $\vec{b}_i^* \cdot \vec{b}_j^* = 0$).

Hadamard's Inequality

The value of det $\mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$.

Hadamard's Inequality

The value of $\det \mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$.

Hadamard's Inequality

The value of $\det \mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$. Geometrically (in low dimensions),

$$\det \mathcal{L} \leq \; \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|.$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

The value of det $\mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$. Geometrically (in low dimensions),

$$\det \mathcal{L} \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|.$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*}$$

The value of $\det \mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$. Geometrically (in low dimensions),

$$\det \mathcal{L} \leq \ \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|.$$

This is Hadamard's inequality.

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

The value of $\det \mathcal{L}$ can be viewed as the volume of the polyhedron with edges parallel to and the same length as $\vec{b}_1, \ldots, \vec{b}_n$. This volume is independent of the basis that is used for $\mathcal{L}$. Geometrically (in low dimensions),

$$\det \mathcal{L} \leq \ \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|.$$

This is Hadamard's inequality.

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

Since $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathcal{L}$, we deduce that

$$(\det \mathcal{L})^2 = \det\left((\vec{b}_1^*, \ldots, \vec{b}_n^*)^T (\vec{b}_1^*, \ldots, \vec{b}_n^*)\right) = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

$$\boxed{\det \mathcal{L} \le \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|}$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

Since $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathcal{L}$, we deduce that

$$(\det \mathcal{L})^2 = \det\left((\vec{b}_1^*, \ldots, \vec{b}_n^*)^T (\vec{b}_1^*, \ldots, \vec{b}_n^*)\right) = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

$$\boxed{\det \mathcal{L} \le \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|}$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

Since $\vec{b}_1, \ldots, \vec{b}_n$ **is a basis for** $\mathcal{L}$**, we deduce that**

$$(\det \mathcal{L})^2 = \det\left((\vec{b}_1^*, \ldots, \vec{b}_n^*)^T (\vec{b}_1^*, \ldots, \vec{b}_n^*)\right) = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

Thus, $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$**. So it suffices to show** $\|\vec{b}_i^*\| \le \|\vec{b}_i\|$**.**

$$\boxed{\det \mathcal{L} \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|}$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

Since $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathcal{L}$, we deduce that

$$(\det \mathcal{L})^2 = \det\left((\vec{b}_1^*, \ldots, \vec{b}_n^*)^T (\vec{b}_1^*, \ldots, \vec{b}_n^*)\right) = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

Thus, $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$. So it suffices to show $\|\vec{b}_i^*\| \leq \|\vec{b}_i\|$. The orthogonality of the $\vec{b}_i^*$'s implies

$$\|\vec{b}_i\|^2 = \left\|\vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*\right\|^2 = \|\vec{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|\vec{b}_j^*\|^2.$$

$$\boxed{\det \mathcal{L} \le \|\vec{b}_1\|\,\|\vec{b}_2\|\cdots\|\vec{b}_n\|}$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*}$$

Proof (in any dimensions). Column operations imply

$$\det\left(\vec{b}_1, \ldots, \vec{b}_n\right) = \det\left(\vec{b}_1^*, \ldots, \vec{b}_n^*\right).$$

Since $\vec{b}_1, \ldots, \vec{b}_n$ is a basis for $\mathcal{L}$, we deduce that

$$(\det \mathcal{L})^2 = \det\left((\vec{b}_1^*, \ldots, \vec{b}_n^*)^T(\vec{b}_1^*, \ldots, \vec{b}_n^*)\right) = \left(\prod_{i=1}^{n} \|\vec{b}_i^*\|\right)^2.$$

Thus, $\det \mathcal{L} = \prod_{i=1}^{n} \|\vec{b}_i^*\|$. So it suffices to show $\|\vec{b}_i^*\| \le \|\vec{b}_i\|$. The orthogonality of the $\vec{b}_i^*$'s implies

$$\|\vec{b}_i\|^2 = \left\|\vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij}\vec{b}_j^*\right\|^2 = \|\vec{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2\|\vec{b}_j^*\|^2.$$

The inequality $\|\vec{b}_i^*\| \le \|\vec{b}_i\|$ follows. $\blacksquare$

$$\det \mathcal{L} \leq \|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\|$$

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\| \leq c_n \det \mathcal{L}.$$

$$\det \mathcal{L} \le \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|$$

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\| \le c_n \det \mathcal{L}.$$

It is known that $c_n \le n^n$.

$$\det \mathcal{L} \leq \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|$$

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\| \leq c_n \det \mathcal{L}.$$

It is known that $c_n \leq n^n$. Minkowski has shown that there exist n linearly independent vectors $\vec{b}'_1, \ldots, \vec{b}'_n$ in $\mathcal{L}$ such that

$$\|\vec{b}'_1\|\,\|\vec{b}'_2\| \cdots \|\vec{b}'_n\| \leq n^{n/2} \det \mathcal{L},$$

but $\vec{b}'_1, \ldots, \vec{b}'_n$ is not necessarily a basis for $\mathcal{L}$.

$$\det \mathcal{L} \leq \|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\|$$

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\|\,\|\vec{b}_2\| \cdots \|\vec{b}_n\| \leq c_n \det \mathcal{L}.$$

It is known that $c_n \leq n^n$. Minkowski has shown that there exist n linearly independent vectors $\vec{b}'_1, \ldots, \vec{b}'_n$ in $\mathcal{L}$ such that

$$\|\vec{b}'_1\|\,\|\vec{b}'_2\| \cdots \|\vec{b}'_n\| \leq n^{n/2} \det \mathcal{L},$$

but $\vec{b}'_1, \ldots, \vec{b}'_n$ is not necessarily a basis for $\mathcal{L}$. Further, we note that the problem of finding a basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$ for which $\|\vec{b}_1\| \cdots \|\vec{b}_n\|$ is minimal is known to be NP-hard.

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\| \leq c_n \det \mathcal{L}.$$

It is known that $c_n \leq n^n$. Minkowski has shown that there exist n linearly independent vectors $\vec{b}'_1, \ldots, \vec{b}'_n$ in $\mathcal{L}$ such that

$$\|\vec{b}'_1\| \, \|\vec{b}'_2\| \cdots \|\vec{b}'_n\| \leq n^{n/2} \det \mathcal{L},$$

but $\vec{b}'_1, \ldots, \vec{b}'_n$ is not necessarily a basis for $\mathcal{L}$. Further, we note that the problem of finding a basis $\vec{b}_1, \ldots, \vec{b}_n$ of $\mathcal{L}$ for which $\|\vec{b}_1\| \cdots \|\vec{b}_n\|$ is minimal is known to be NP-hard.

Hermite's result implies there is a constant c'_n, depending only on n, such that $\|\vec{b}\| \leq c'_n \sqrt[n]{\det \mathcal{L}}$.

Comments: Hermite proved there is a constant c_n (depending only on n) such that for some basis $\vec{b}_1, \dots, \vec{b}_n$ of $\mathcal{L}$, we have

$$\|\vec{b}_1\| \, \|\vec{b}_2\| \cdots \|\vec{b}_n\| \le c_n \det \mathcal{L}.$$

It is known that $c_n \le n^n$. Minkowski has shown that there exist n linearly independent vectors $\vec{b}'_1, \dots, \vec{b}'_n$ in $\mathcal{L}$ such that

$$\|\vec{b}'_1\| \, \|\vec{b}'_2\| \cdots \|\vec{b}'_n\| \le n^{n/2} \det \mathcal{L},$$

but $\vec{b}'_1, \dots, \vec{b}'_n$ is not necessarily a basis for $\mathcal{L}$. Further, we note that the problem of finding a basis $\vec{b}_1, \dots, \vec{b}_n$ of $\mathcal{L}$ for which $\|\vec{b}_1\| \cdots \|\vec{b}_n\|$ is minimal is known to be NP-hard.

Hermite's result implies there is a constant c'_n, depending only on n, such that $\|\vec{b}\| \le c'_n \sqrt[n]{\det \mathcal{L}}$. A lattice $\mathcal{L}$ can contain a vector that is much shorter than this, but it is known that the best constant c'_n for all lattices $\mathcal{L}$ satisfies

$$\sqrt{n/(2e\pi)} \le c'_n \le \sqrt{n/(e\pi)}.$$

Hermite's result implies there is a constant c'_n, depending only on n, such that $\|\vec{b}\| \leq c'_n \sqrt[n]{\det \mathcal{L}}$. A lattice $\mathcal{L}$ can contain a vector that is much shorter than this, but it is known that the best constant c'_n for all lattices $\mathcal{L}$ satisfies

$$\sqrt{n/(2e\pi)} \leq c'_n \leq \sqrt{n/(e\pi)}.$$

No one knows a polynomial time algorithm for finding $\vec{b} \in \mathcal{L}$ with $\|\vec{b}\|$ minimal, but it is not known to be NP-complete.

Hermite's result implies there is a constant c_n', depending only on n, such that $\|\vec{b}\| \leq c_n' \sqrt[n]{\det \mathcal{L}}$. A lattice $\mathcal{L}$ can contain a vector that is much shorter than this, but it is known that the best constant c_n' for all lattices $\mathcal{L}$ satisfies

$$\sqrt{n/(2e\pi)} \leq c_n' \leq \sqrt{n/(e\pi)}.$$

No one knows a polynomial time algorithm for finding $\vec{b} \in \mathcal{L}$ with $\|\vec{b}\|$ minimal, but it is not known to be NP-complete. Lagarias has, however, proved that the problem of finding a vector $\vec{b} \in \mathcal{L}$ which minimizes the maximal absolute value of a component is NP-hard.

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}\| \geq \min\{\|\vec{b}_1^*\|, \|\vec{b}_2^*\|, \ldots, \|\vec{b}_n^*\|\}$$

$$\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*$$

$$\boxed{\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^*}$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \quad \Longrightarrow \quad \|\vec{b}\| \geq \min\{\|\vec{b}_1^*\|, \|\vec{b}_2^*\|, \ldots, \|\vec{b}_n^*\|\}$$

$$\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^* \qquad\qquad \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}$$

$$\vec{b} = u_1 \vec{b}_1 + \cdots + u_k \vec{b}_k, \qquad \text{where each } u_j \in \mathbb{Z} \text{ and } u_k \neq 0$$

$$\vec{b} = v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*, \qquad \text{where each } v_j \in \mathbb{Q} \text{ and } v_k = u_k$$

$$\|\vec{b}\|^2 = \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right) \cdot \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right)$$

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \quad \Longrightarrow \quad \|\vec{b}\| \geq \min\{\|\vec{b}_1^*\|, \|\vec{b}_2^*\|, \ldots, \|\vec{b}_n^*\|\}$$

$$\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \vec{b}_j^* \qquad\qquad \mu_{i,j} = \frac{\vec{b}_i \cdot \vec{b}_j^*}{\vec{b}_j^* \cdot \vec{b}_j^*}$$

$$\vec{b} = u_1 \vec{b}_1 + \cdots + u_k \vec{b}_k, \qquad \text{where each } u_j \in \mathbb{Z} \text{ and } u_k \neq 0$$

$$\vec{b} = v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*, \qquad \text{where each } v_j \in \mathbb{Q} \text{ and } v_k = u_k$$

$$\begin{aligned} \|\vec{b}\|^2 &= \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right) \cdot \left(v_1 \vec{b}_1^* + \cdots + v_k \vec{b}_k^*\right) \\ &= v_1^2 \|\vec{b}_1^*\|^2 + \cdots + v_k^2 \|\vec{b}_k^*\|^2 \geq \|\vec{b}_k^*\|^2 \end{aligned}$$

$$(*) \qquad \vec{b} \in \mathcal{L},\ k \text{ as above} \quad \Longrightarrow \quad \|\vec{b}\|^2 \geq \|\vec{b}_k^*\|^2$$