On the Maximum Distance Sublattice Problem and Closest Vector Problem

Mahesh Sreekumar Rajasree
Department of Computer Science & Engineering
IIT Delhi

Joint work with Rajendra Kumar (IITD) and Shashank K Mehta (IITK)
SYNASC 2024

Contents

Introduction

Lattice

Lattice

A *lattice* generated by a set of *linearly independent vectors* $B = \{b_1, \ldots, b_n\}$ is the set of all *integer linear combinations* of $\{b_1, \ldots, b_n\}$, i.e.,

Lattice

A *lattice* generated by a set of *linearly independent vectors* $B = \{b_1, \ldots, b_n\}$ is the set of all *integer linear combinations* of $\{b_1, \ldots, b_n\}$, i.e.,

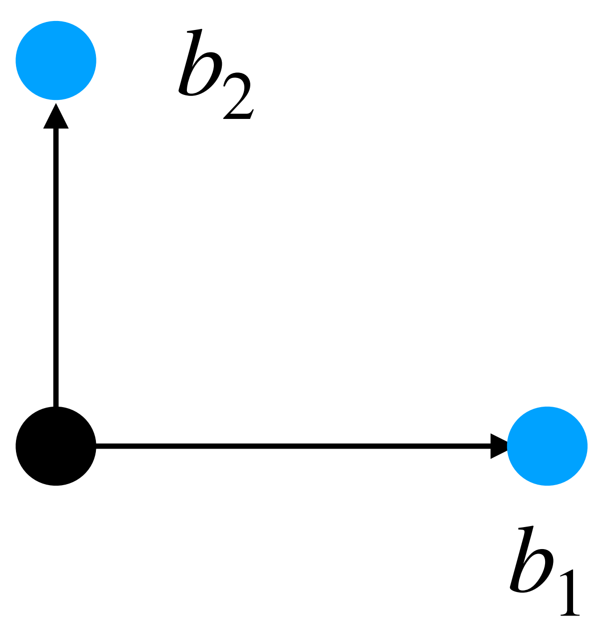
$$\mathscr{L}(b_1, \ldots, b_n) = \{ \sum_{i=1}^{n} z_i b_i \mid \forall (z_1, \ldots, z_n) \in \mathbb{Z}^n \}$$

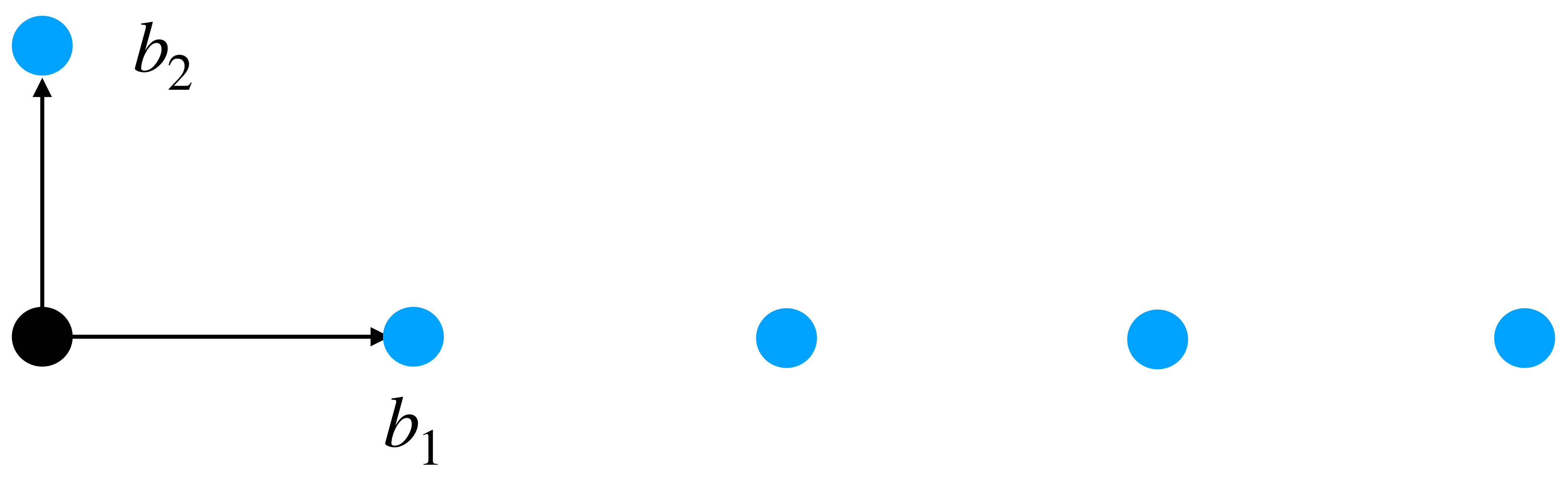
Lattice

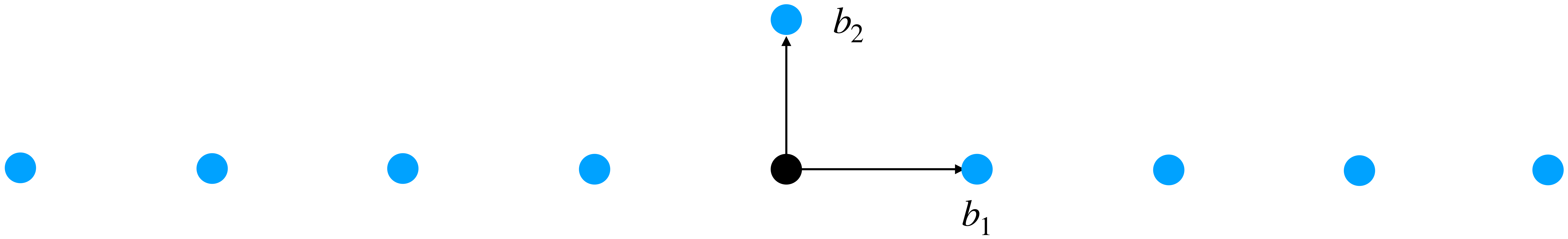
A *lattice* generated by a set of *linearly independent vectors* $B = \{b_1, \ldots, b_n\}$ is the set of all *integer linear combinations* of $\{b_1, \ldots, b_n\}$, i.e.,

$$\mathscr{L}(b_1, \ldots, b_n) = \{ \sum_{i=1}^{n} z_i b_i \mid \forall (z_1, \ldots, z_n) \in \mathbb{Z}^n \}$$

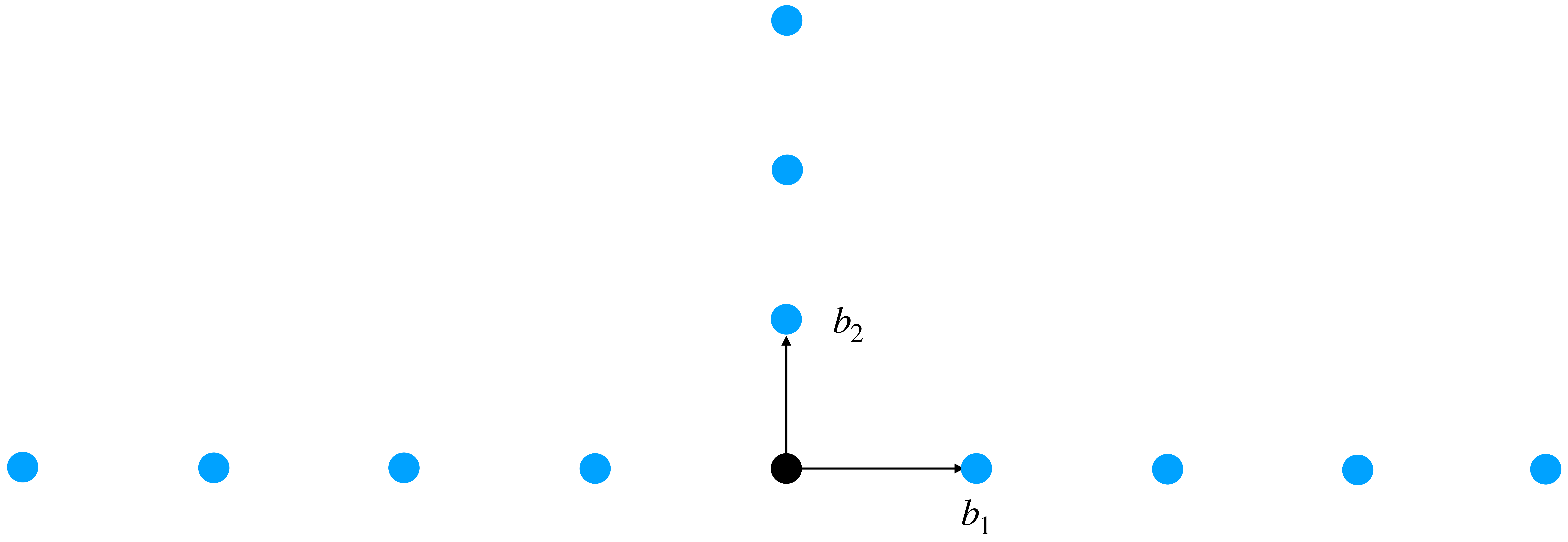
B is called a *basis* of $\mathscr{L}$.

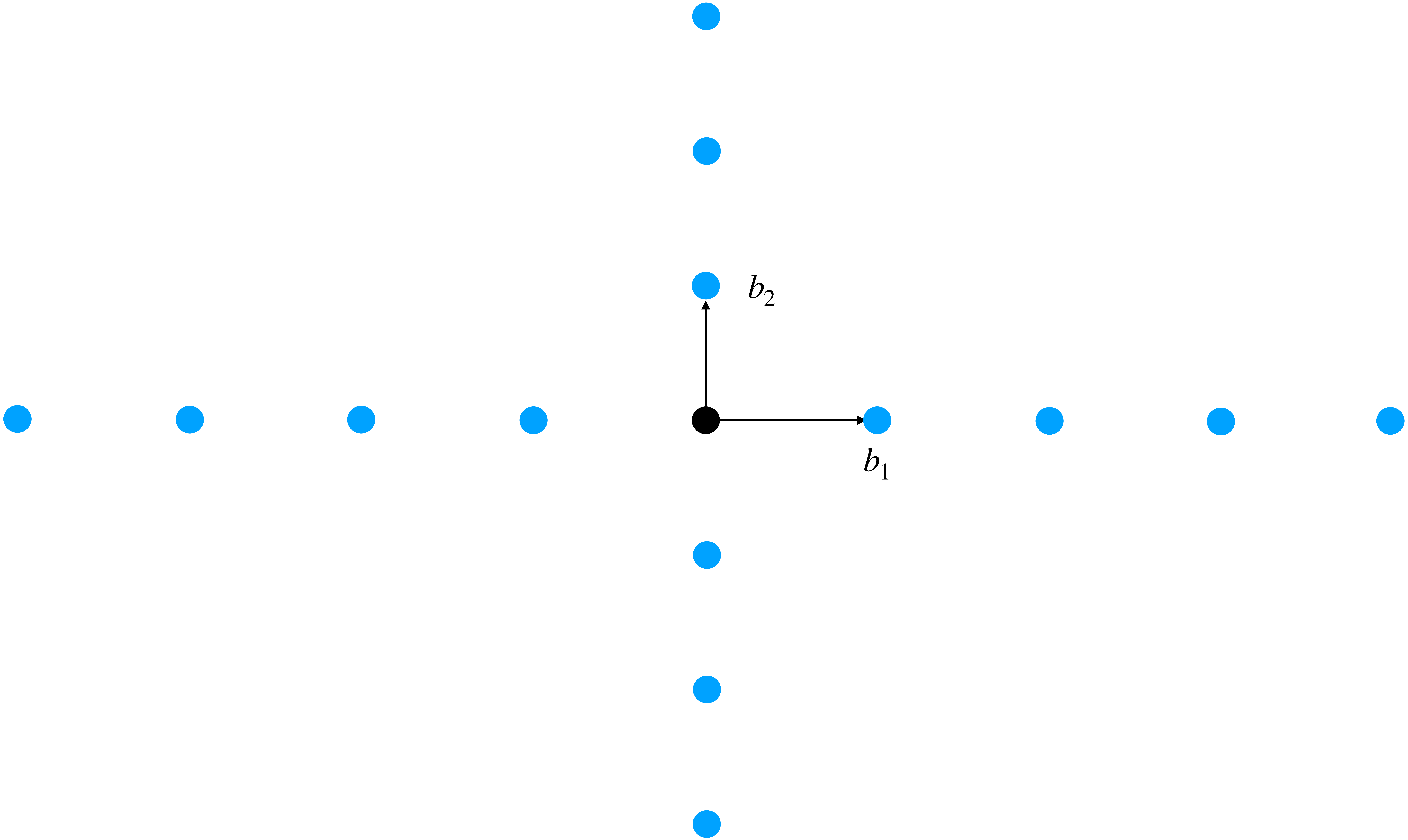

b_2
b_1

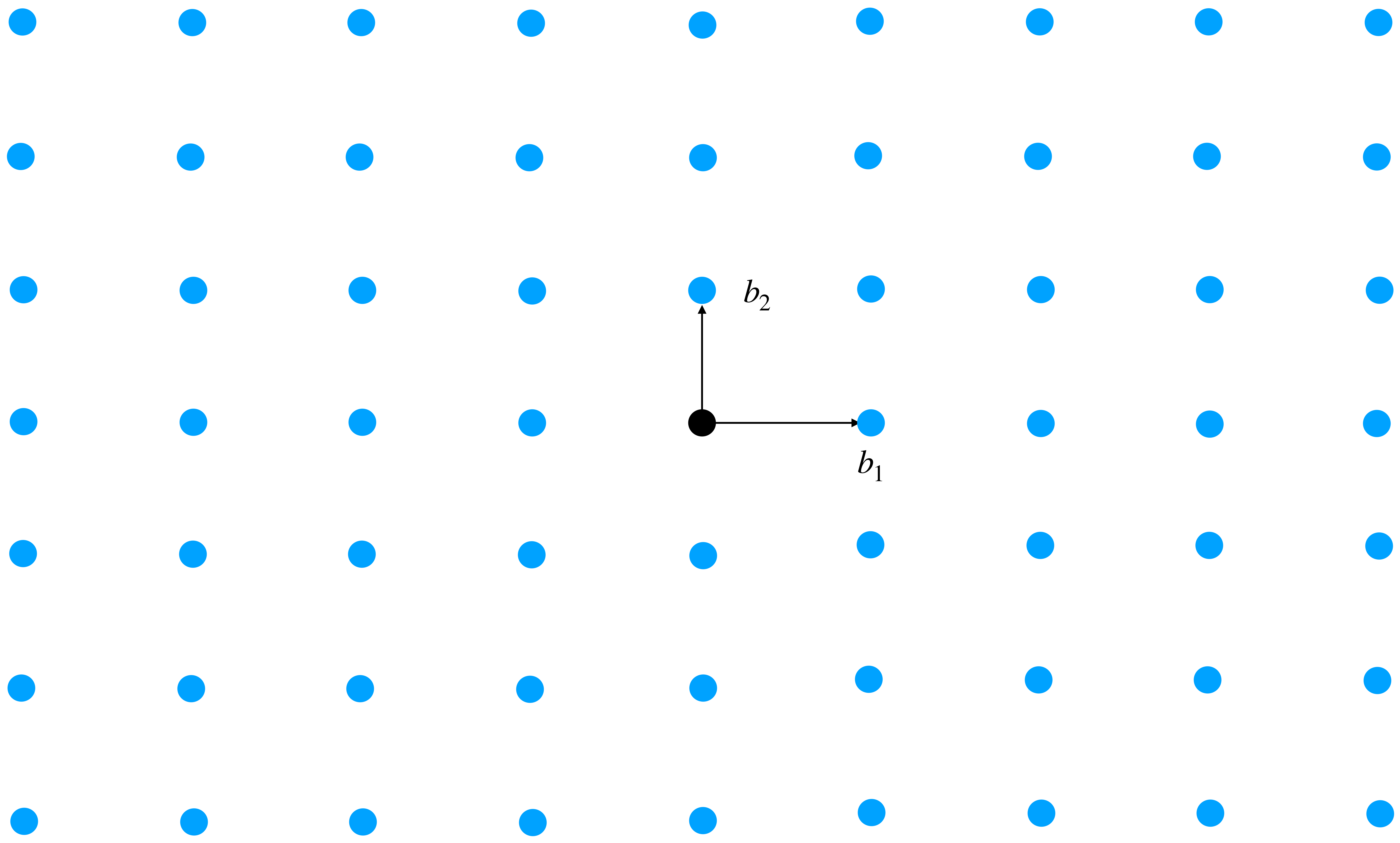

b_2
b_1



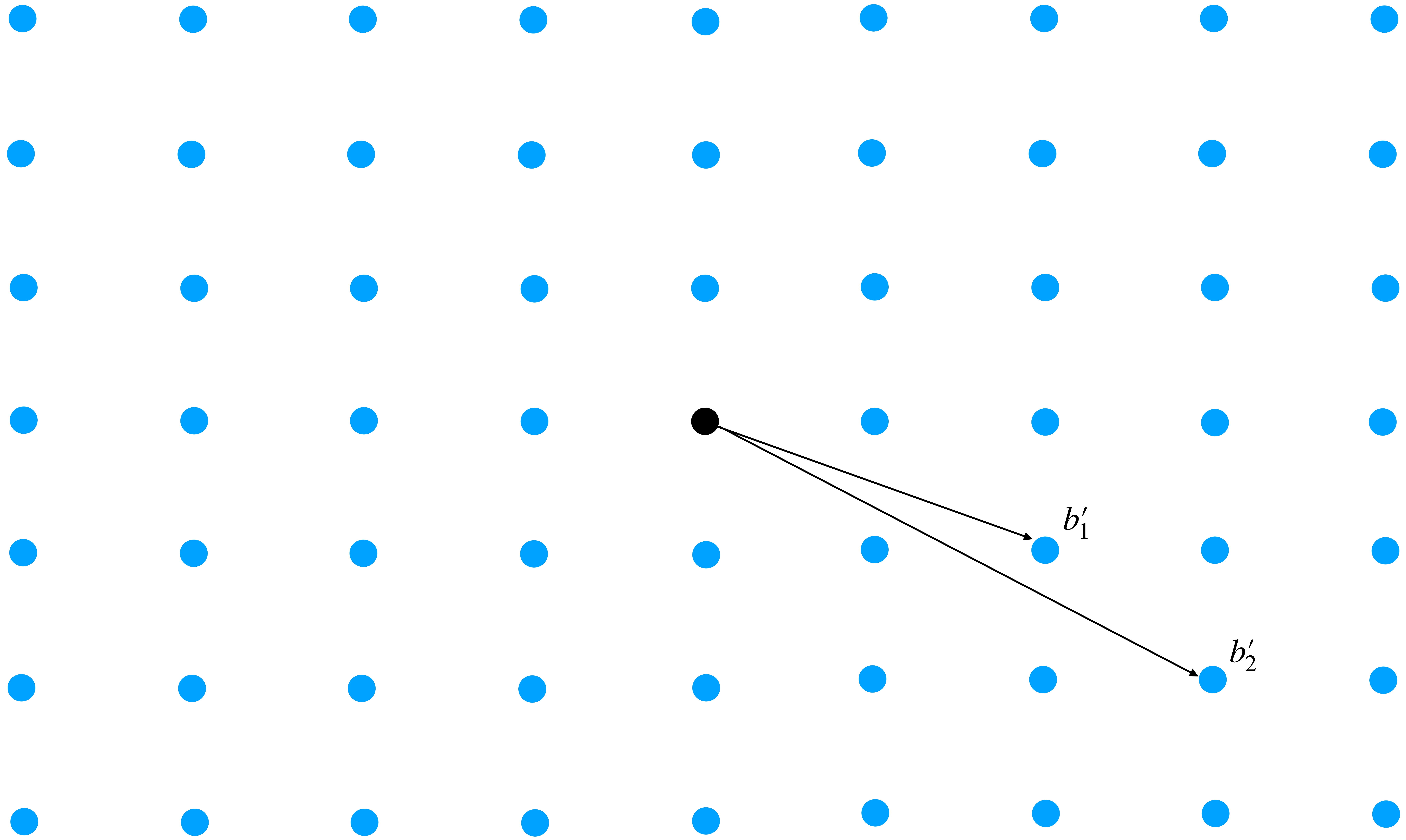
b_2
b_1


b_2
b_1


b_2
b_1



b_2
b_1


b_1'
b_2'

Bases of a lattice

Bases of a lattice

B and B' are bases of a lattice $\mathscr{L}$ $\iff$ $B' = BU$ where U is a unimodular matrix.

Bases of a lattice

B and B' are bases of a lattice $\mathscr{L} \iff B' = BU$ where U is a unimodular matrix.

A matrix U is unimodular if $U \in \mathbb{Z}^{n \times n}$ and $det(U) = \pm 1$.

Bases of a lattice

B and B' are bases of a lattice $\mathscr{L} \iff B' = BU$ where U is a unimodular matrix.

A matrix U is unimodular if $U \in \mathbb{Z}^{n \times n}$ and $det(U) = \pm 1$.

$B' = BU, B = B'V \implies B' = B'VU \implies I = VU$.

Bases of a lattice

B and B' are bases of a lattice $\mathscr{L} \iff B' = BU$ where U is a unimodular matrix.

A matrix U is unimodular if $U \in \mathbb{Z}^{n \times n}$ and $det(U) = \pm 1$.

$B' = BU, B = B'V \implies B' = B'VU \implies I = VU$.

Therefore, a lattice can have infinitely many bases!

Applications

Applications

- Factoring rational polynomials.

Applications

- Factoring rational polynomials.
- Integer linear programming.

Applications

- Factoring rational polynomials.
- Integer linear programming.
- Cryptanalysis of RSA, knapsack cryptosystems.

Applications

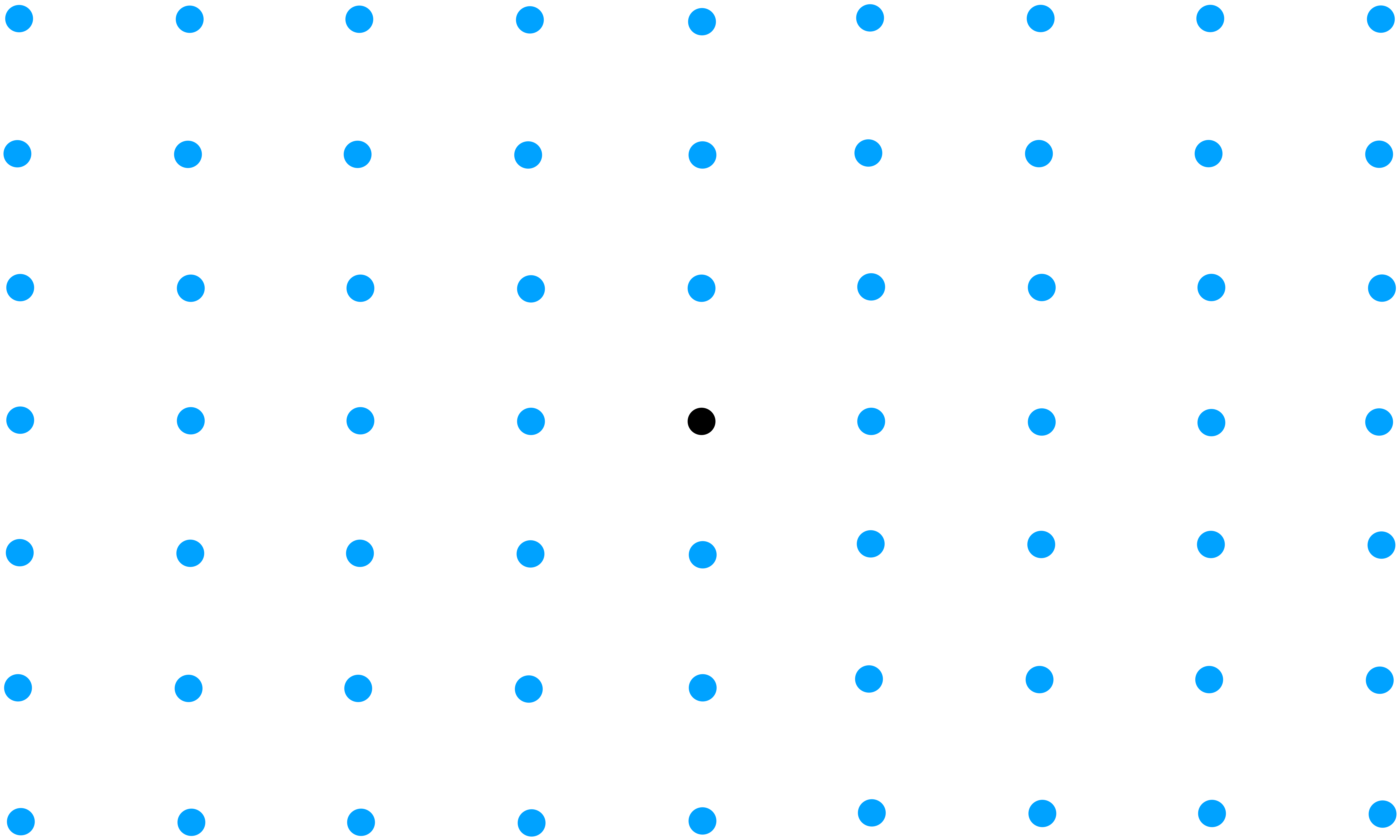
- Factoring rational polynomials.
- Integer linear programming.
- Cryptanalysis of RSA, knapsack cryptosystems.
- Building very strong cryptographic primitives (post-quantum).

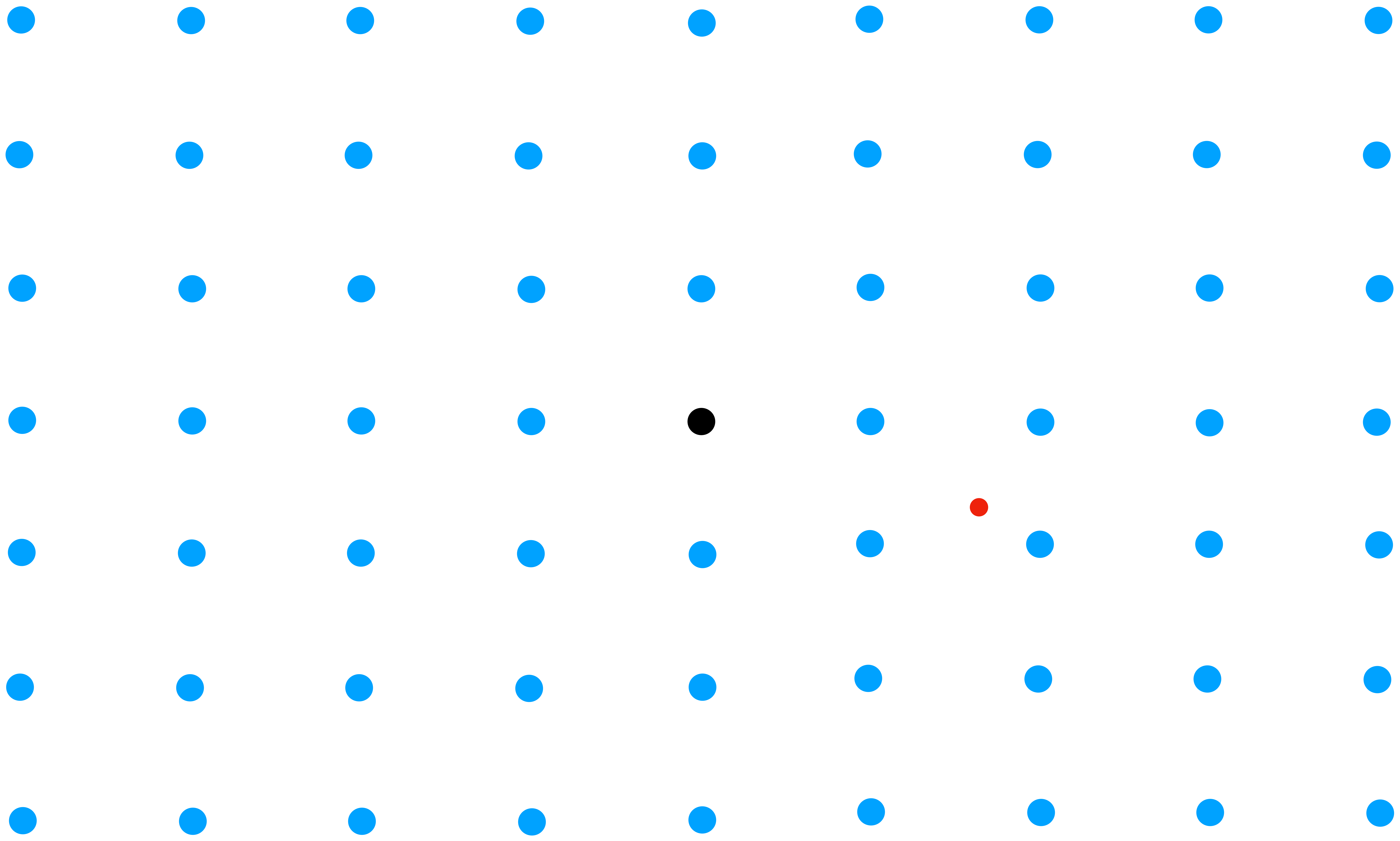
Closest Vector Problem (CVP)

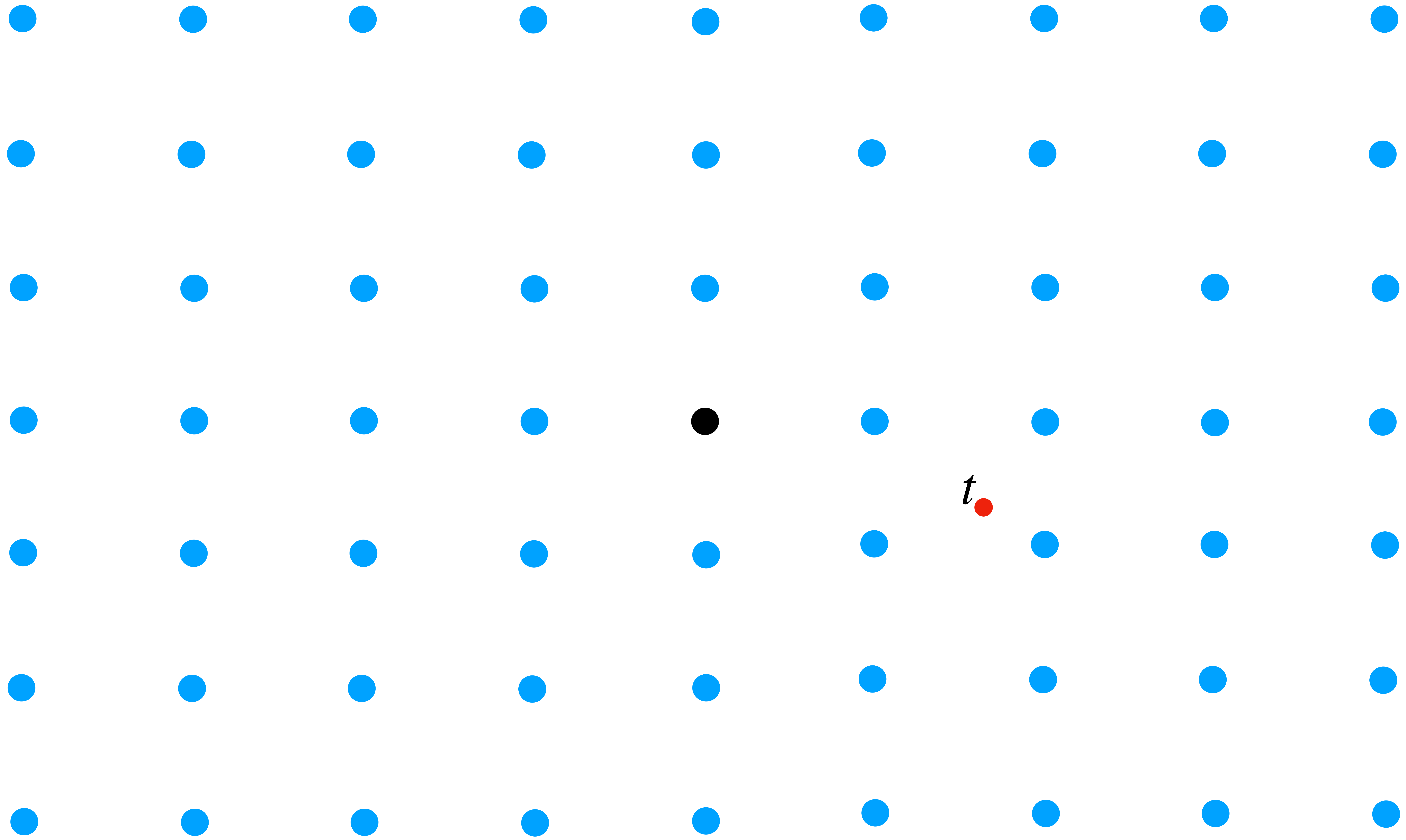
Closest Vector Problem (CVP)

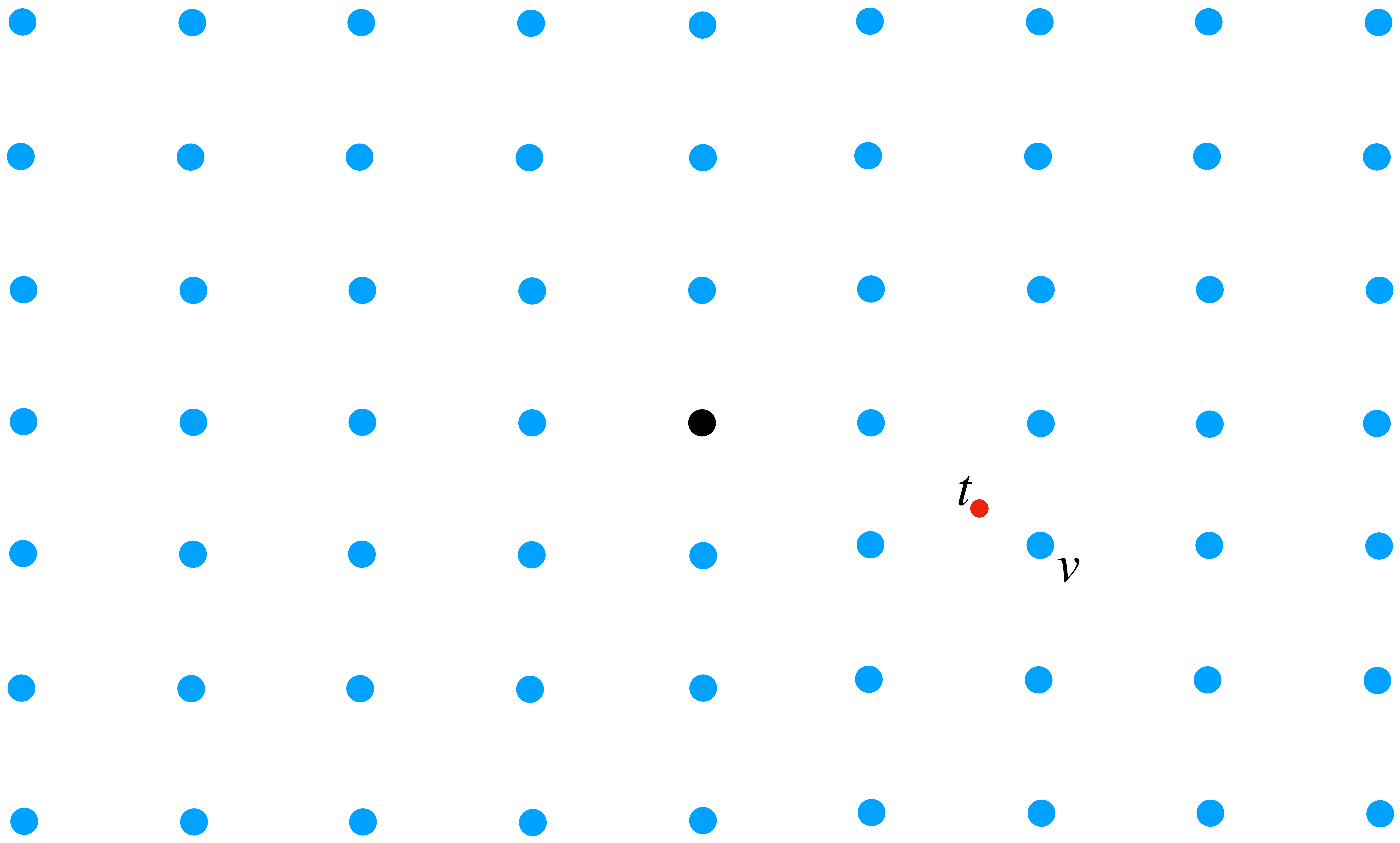
Given a basis $B = \{b_1, \ldots, b_n\}$ and a target $t \in \mathbb{R}^{n+1}$, find a vector $v \in \mathscr{L}(B)$ such that v is closest to t, i.e.,

$$||v - t|| \leq ||u - t||, \forall u \in \mathscr{L}(B)$$

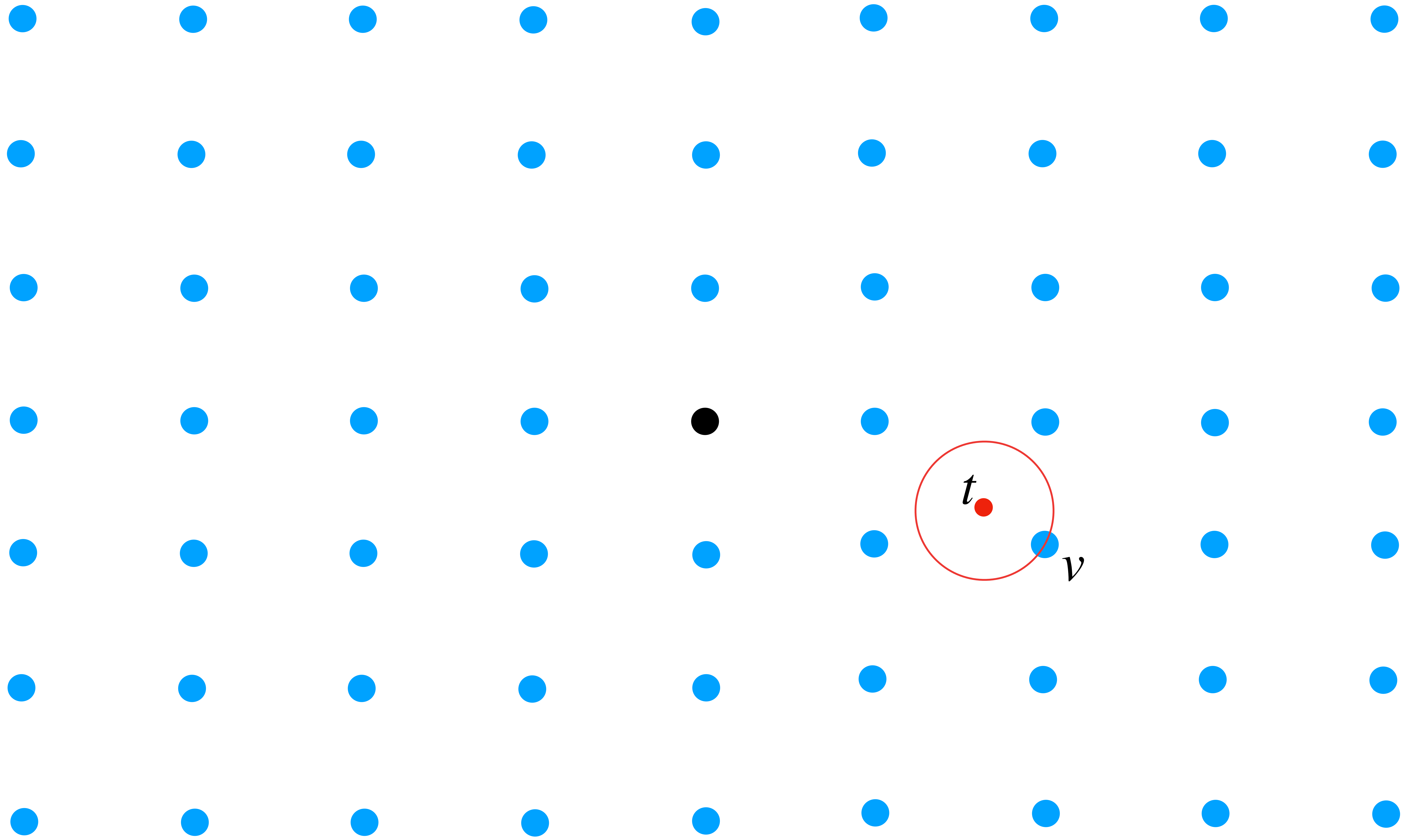


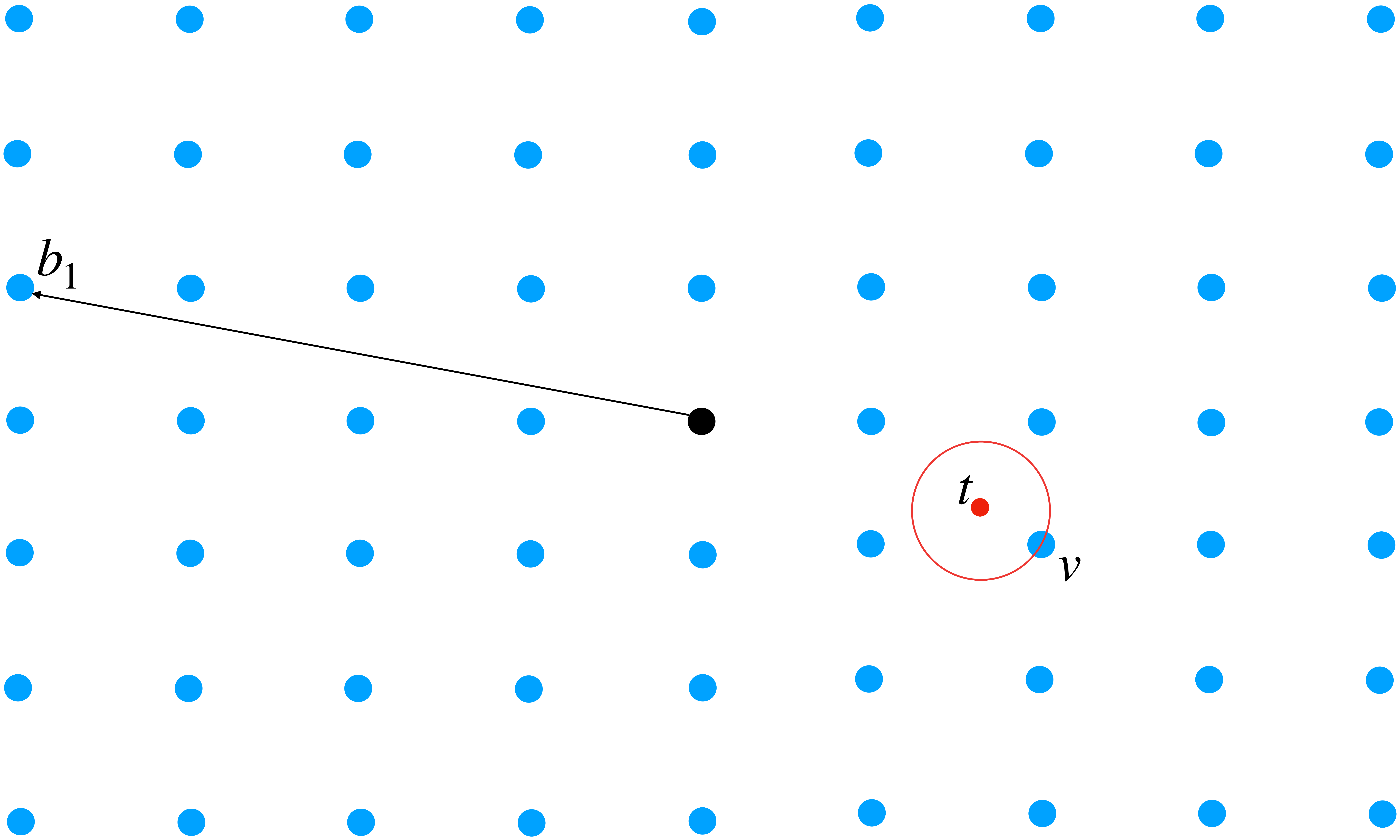



t

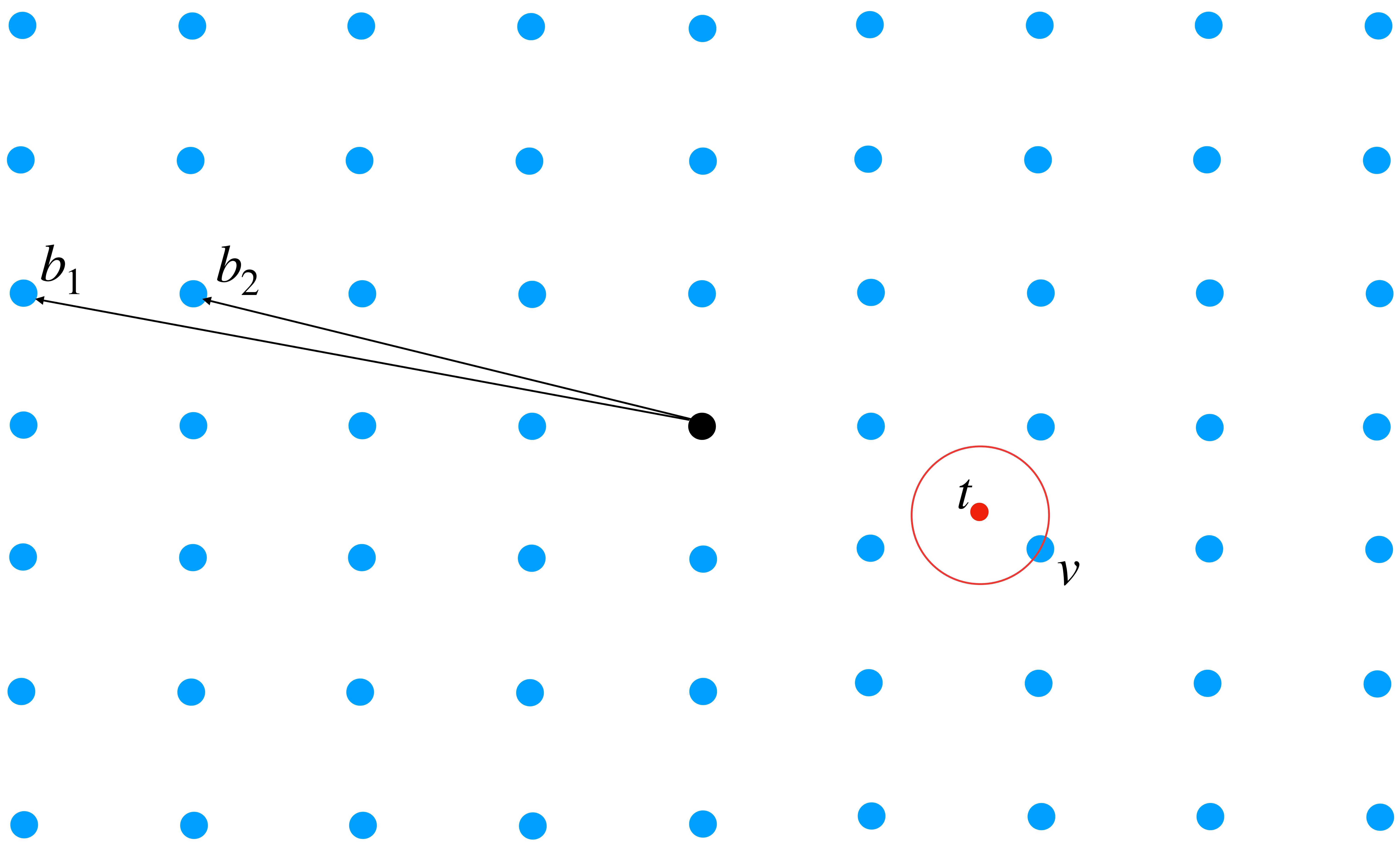


t
v


t
v



b_1
t
v



b_1
b_2
t
v

Facts about CVP

Facts about CVP

- CVP is NP-Complete under all norms.

Facts about CVP

- CVP is NP-Complete under all norms.
- Al-most all other lattice problems reduces to CVP in polynomial time.

Facts about CVP

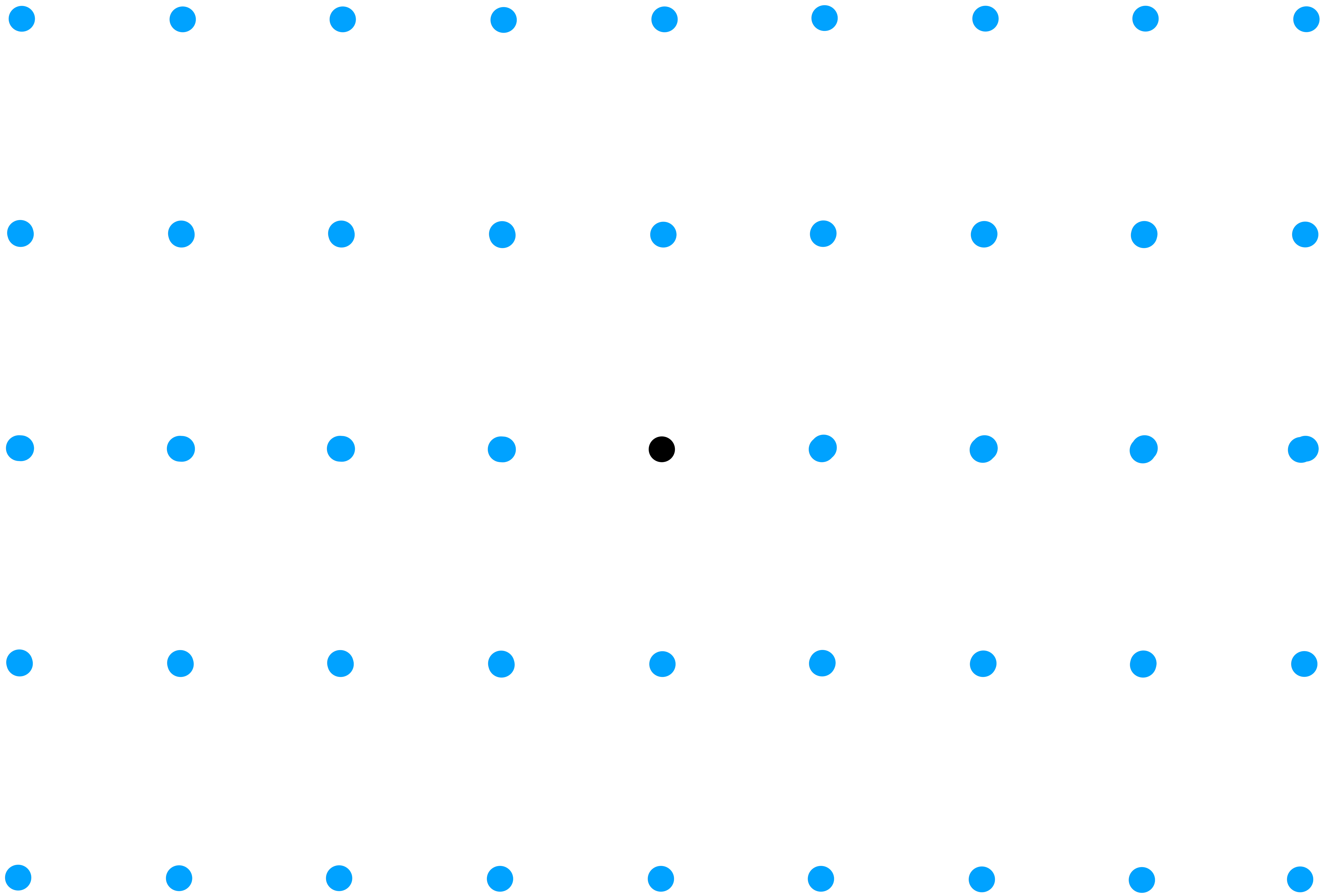
- CVP is NP-Complete under all norms.
- Al-most all other lattice problems reduces to CVP in polynomial time.

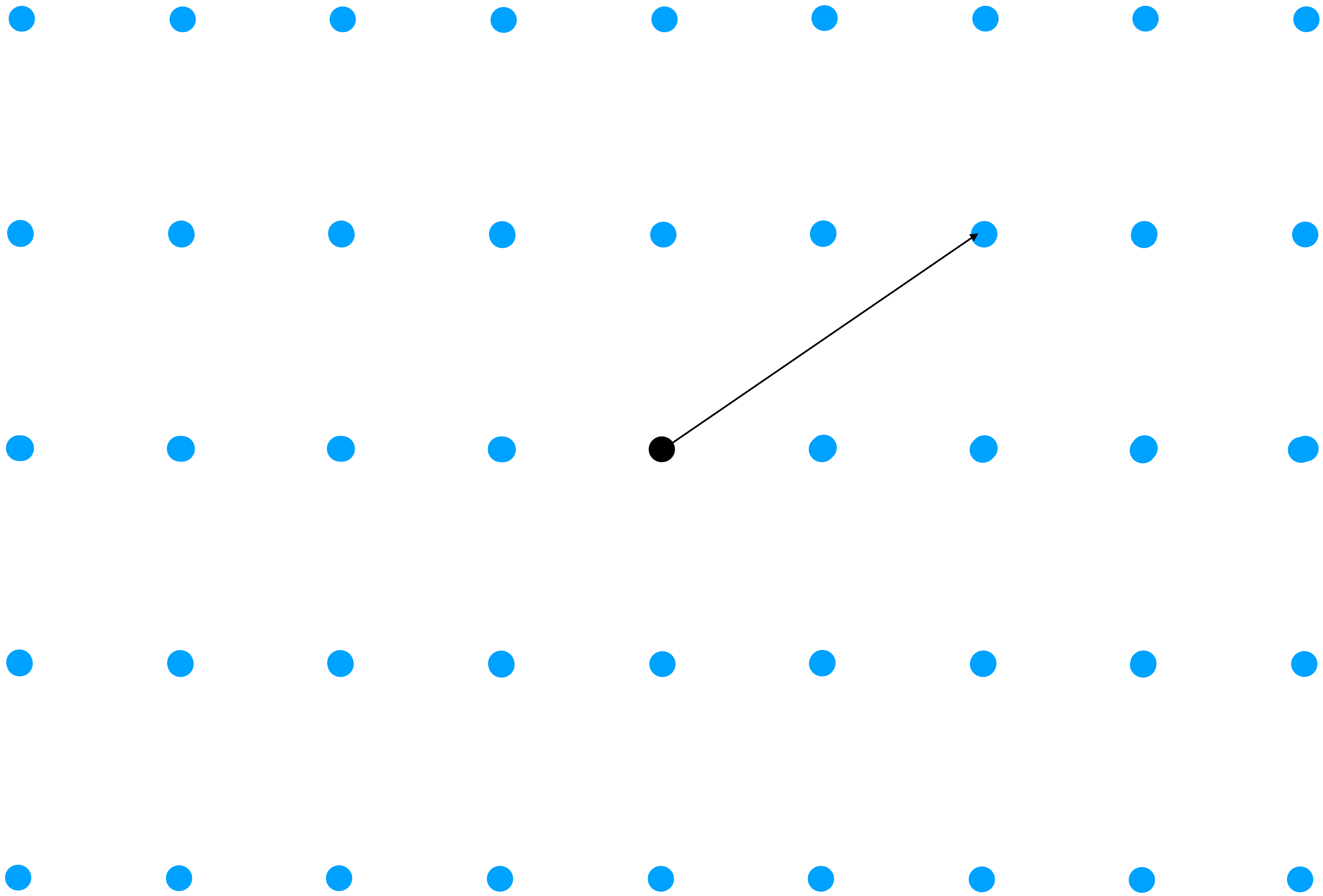
Algorithm	Time	Space
Enumeration	$n^{O(n)}$	$poly(n)$
Sieving	$2^{O(n)}$	$2^{O(n)}$
Voronoi	$\tilde{O}(2^{2n})$	$\tilde{O}(2^n)$
Gaussian	$2^{n+o(n)}$	$2^{n+o(n)}$

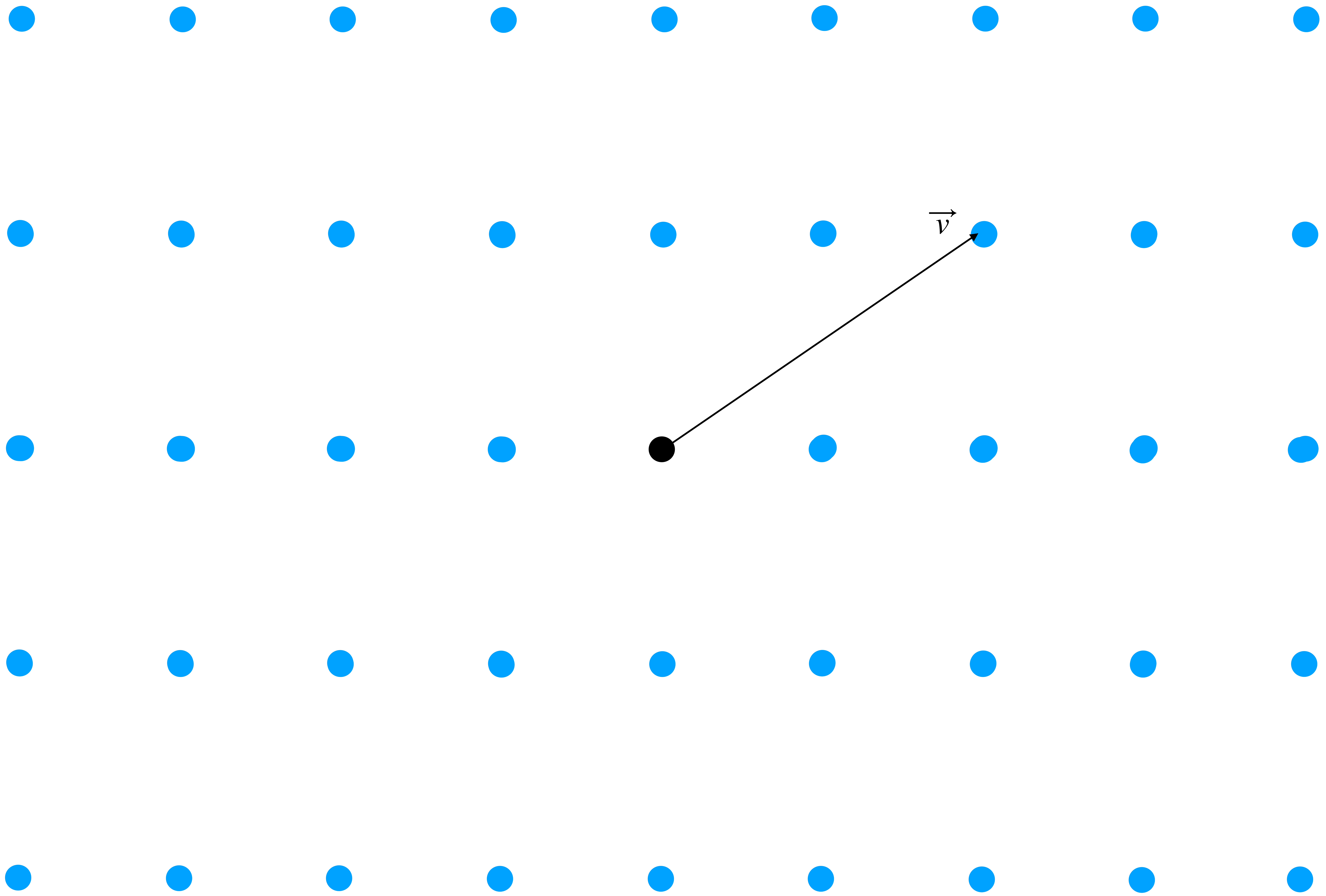
Maximum Distance Sublattice Problem (MDSP)

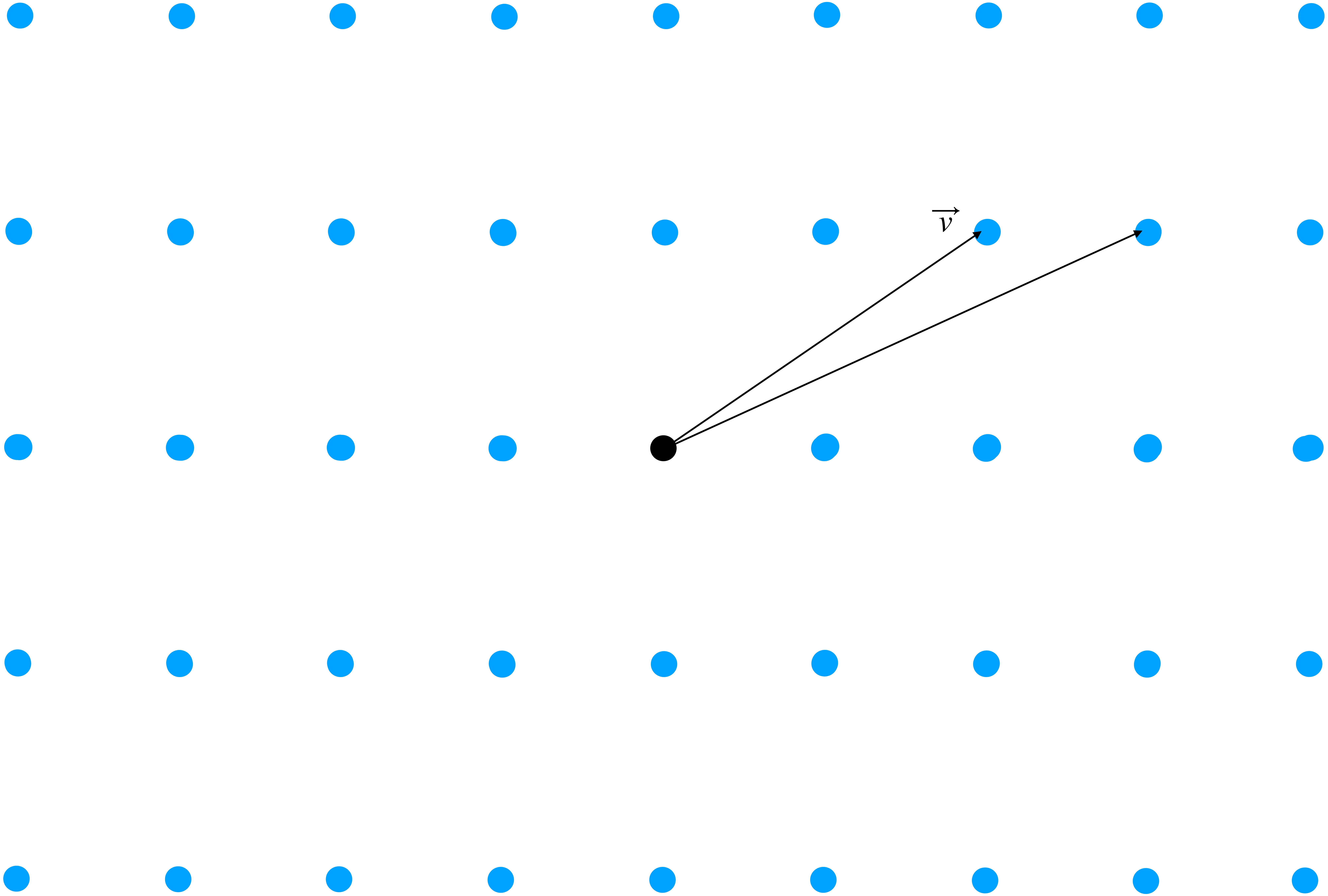
Maximum Distance Sublattice Problem (MDSP)

- Given a basis $[\overrightarrow{v} \mid B] = \{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ for an $n+1$ dimensional lattice $\mathscr{L}$, find $B' = \{\overrightarrow{b'_1}, \ldots, \overrightarrow{b'_n}\}$ such that $\{\overrightarrow{v}, \overrightarrow{b'_1}, \ldots, \overrightarrow{b'_n}\}$ is also a basis for $\mathscr{L}$ and the distance $dist(\overrightarrow{v}, span(B'))$ is maximum.
- Here, we call $\overrightarrow{v}$ the fixed vector.

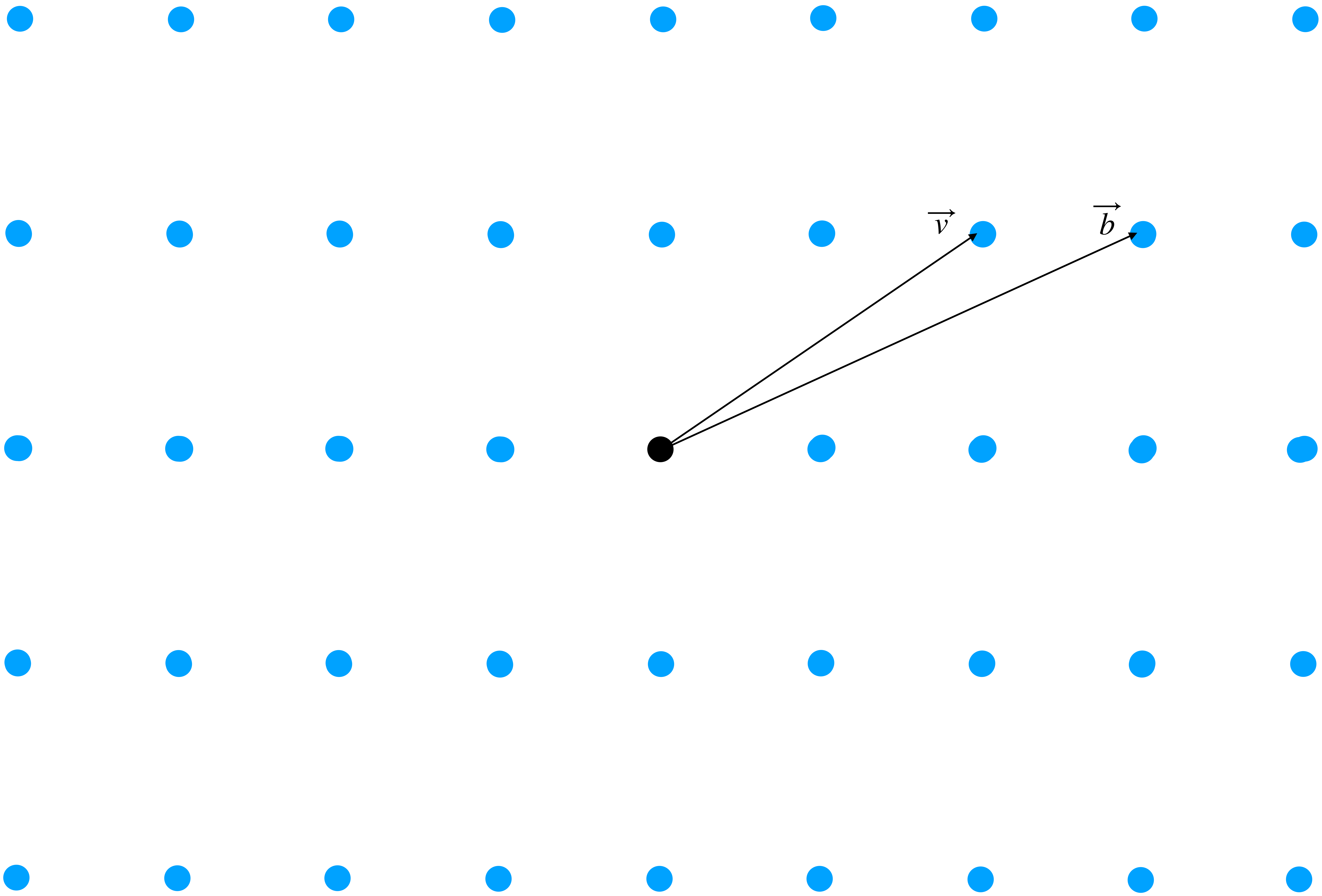




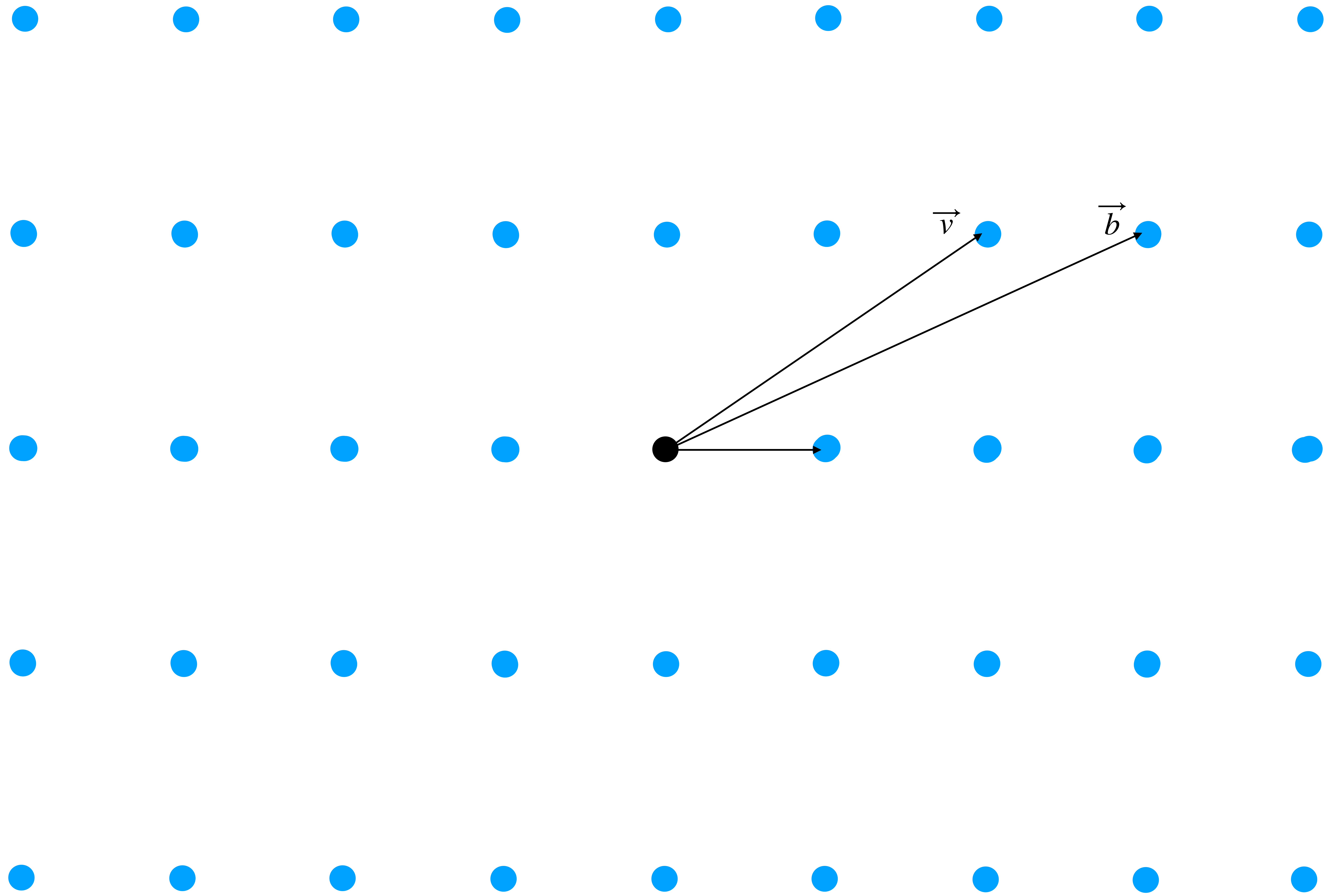

$\vec{v}$

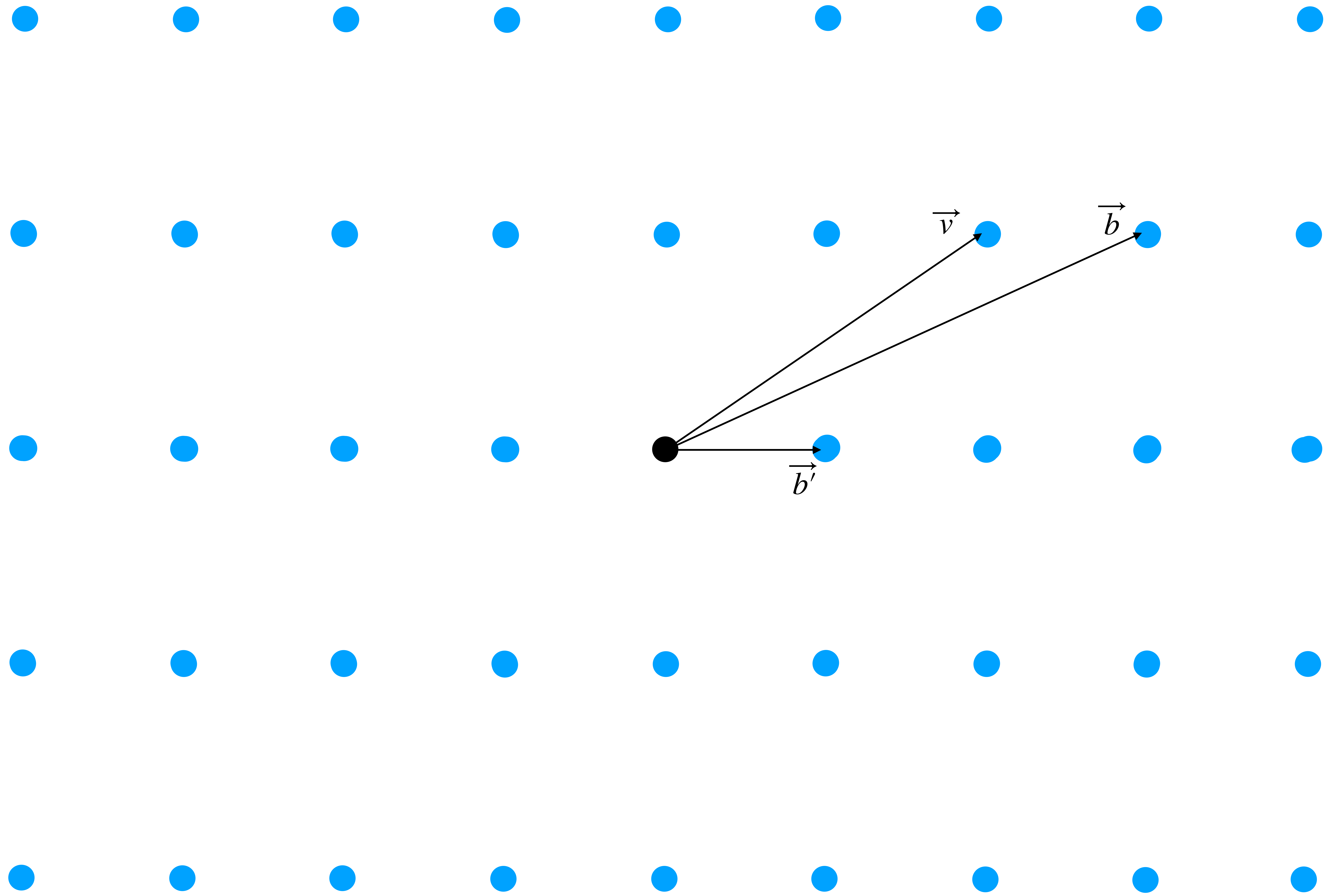


$\vec{v}$

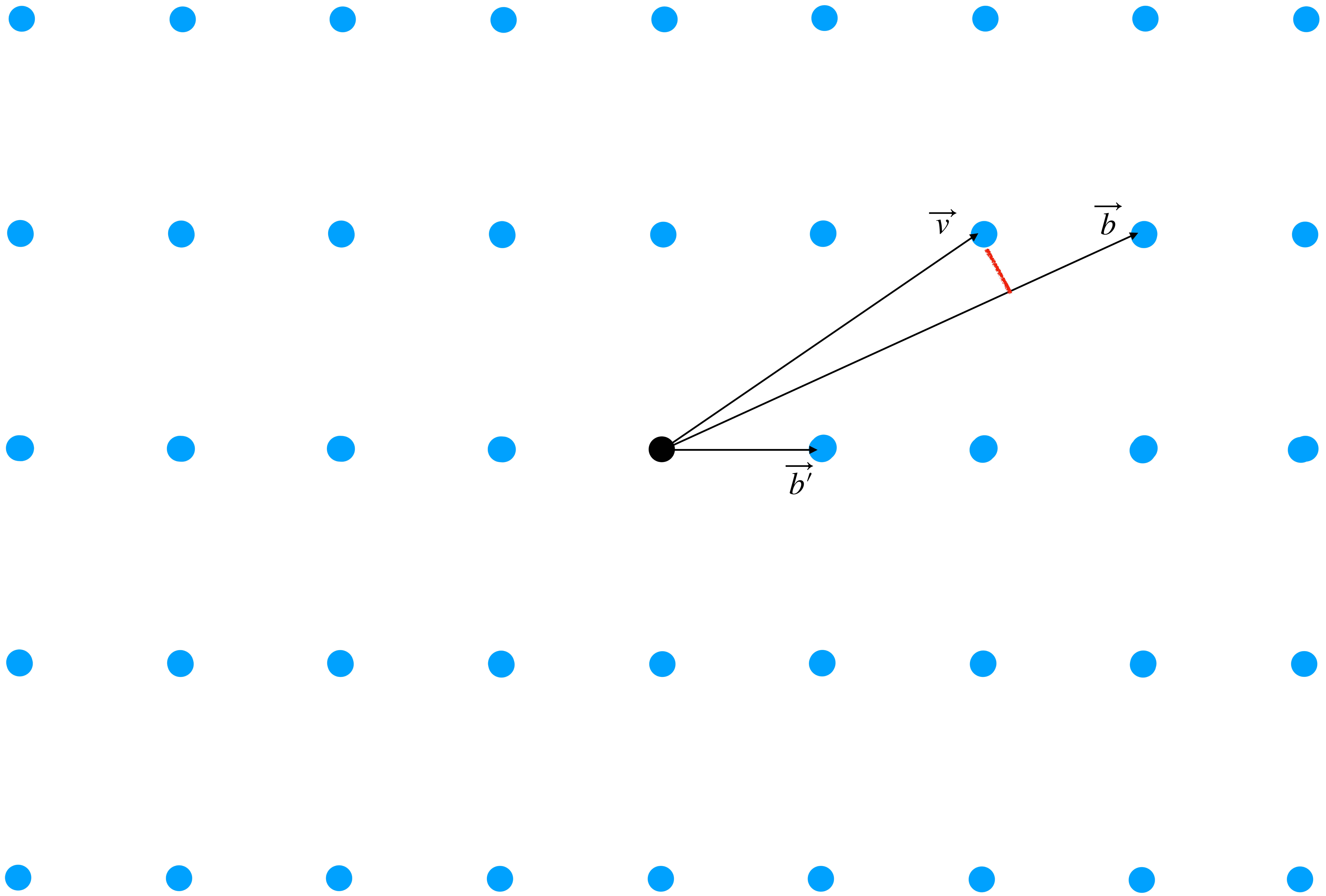


$\vec{v}$
$\vec{b}$

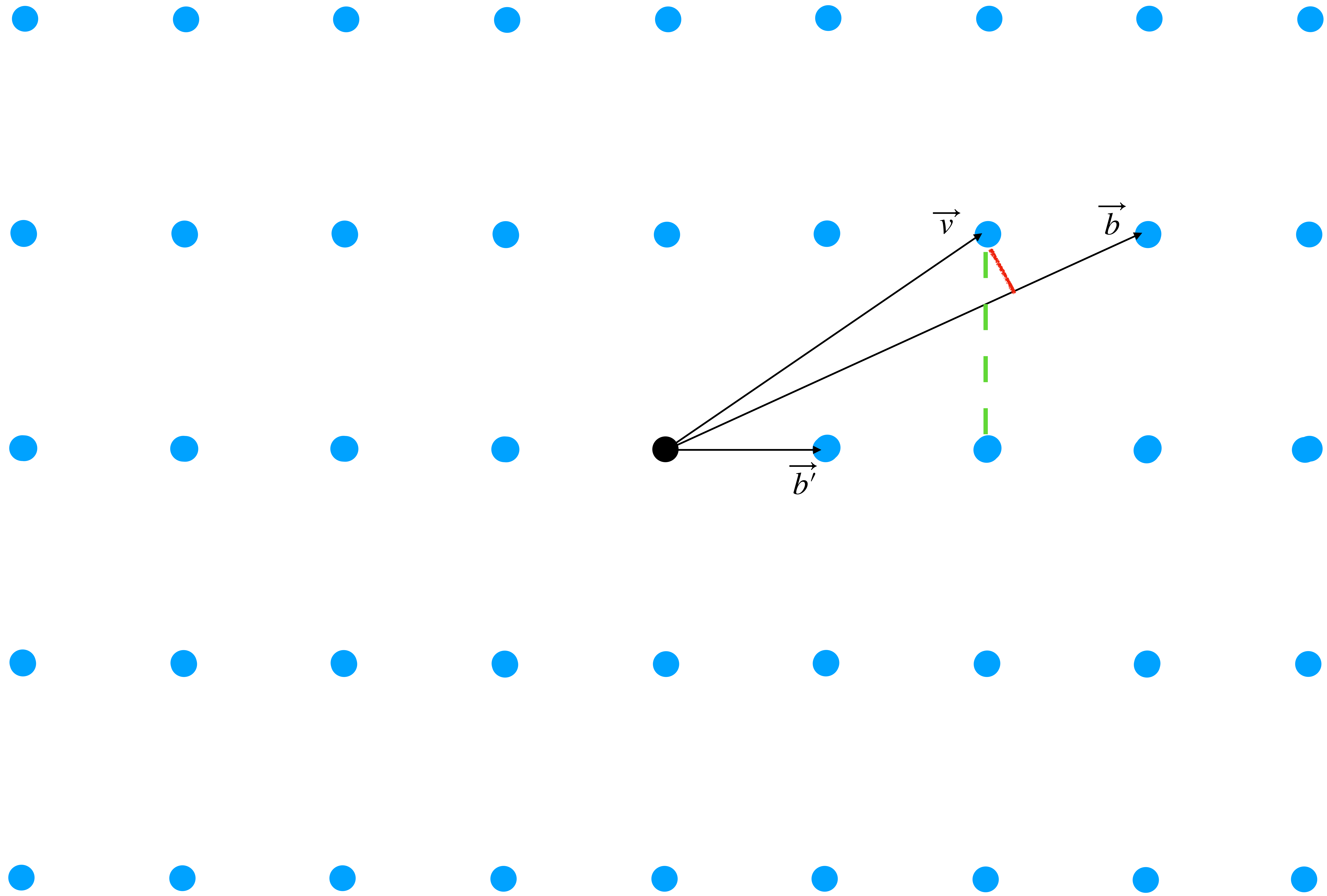

$\vec{v}$
$\vec{b}$



$\vec{v}$
$\vec{b}$
$\vec{b'}$



$\vec{v}$
$\vec{b}$
$\vec{b'}$


$\vec{v}$
$\vec{b}$
$\vec{b'}$

Equivalence Theorem using Dual Lattice

Preliminaries

Preliminaries

A dual lattice of a lattice $\mathscr{L}$ is a lattice $\mathscr{L}'$ such that

Preliminaries

A dual lattice of a lattice $\mathscr{L}$ is a lattice $\mathscr{L}'$ such that

$$\mathscr{L}' = \{y \mid \ < x, y > \in \mathbb{Z}, \forall x \in \mathscr{L}\}$$

Preliminaries

A dual lattice of a lattice $\mathscr{L}$ is a lattice $\mathscr{L}'$ such that

$$\mathscr{L}' = \{y \mid\ < x, y > \in \mathbb{Z}, \forall x \in \mathscr{L}\}$$

Preliminaries

A dual lattice of a lattice $\mathscr{L}$ is a lattice $\mathscr{L}'$ such that

$$\mathscr{L}' = \{y \mid \ < x, y > \in \mathbb{Z}, \forall x \in \mathscr{L}\}$$

If B is a basis for $\mathscr{L}$, then B^{-T} (dual of B) is a basis for $\mathscr{L}'$.

Theorem

Theorem

There exist polynomial time rank and dimension preserving many-one (Karp) reductions between CVP and MDSP.

Given an MDSP input $[\vec{v}, \vec{b}_1, \ldots, \vec{b}_n]$, the CVP instance is the basis $[\vec{d}_1, \ldots, \vec{d}_n]$ and target is $\vec{u}$ where $[\vec{u}, \vec{d}_1, \ldots, \vec{d}_n]$ is the dual of $[\vec{v}, \vec{b}_1, \ldots, \vec{b}_n]$.

Equivalence Theorem without using Dual Lattice

Observation

Observation

- Given an MDSP input $[\overrightarrow{v}, \overrightarrow{b}_1, \ldots, \overrightarrow{b}_n]$, there is a solution of the form $[\overrightarrow{v}, \overrightarrow{b}_1 + x_1\overrightarrow{v}, \ldots, \overrightarrow{b}_n + x_n\overrightarrow{v}]$ where x_i's are integers.

Observation

- Given an MDSP input $[\overrightarrow{v}, \overrightarrow{b}_1, \ldots, \overrightarrow{b}_n]$, there is a solution of the form $[\overrightarrow{v}, \overrightarrow{b}_1 + x_1\overrightarrow{v}, \ldots, \overrightarrow{b}_n + x_n\overrightarrow{v}]$ where x_i's are integers.

- We are interested in the distance of $\overrightarrow{v}$ from the plane/subspace $P_{x_1,\ldots,x_n}$ where $P_{x_1,\ldots,x_n}$ is the spanned by $[\overrightarrow{b}_1 + x_1\overrightarrow{v}, \ldots, \overrightarrow{b}_n + x_n\overrightarrow{v}]$.

Observation

- Given an MDSP input $[\overrightarrow{v}, \overrightarrow{b}_1, \ldots, \overrightarrow{b}_n]$, there is a solution of the form $[\overrightarrow{v}, \overrightarrow{b}_1 + x_1\overrightarrow{v}, \ldots, \overrightarrow{b}_n + x_n\overrightarrow{v}]$ where x_i's are integers.

- We are interested in the distance of $\overrightarrow{v}$ from the plane/subspace $P_{x_1,\ldots,x_n}$ where $P_{x_1,\ldots,x_n}$ is the spanned by $[\overrightarrow{b}_1 + x_1\overrightarrow{v}, \ldots, \overrightarrow{b}_n + x_n\overrightarrow{v}]$.

- Lemma: Let $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ be an orthonormal basis. Then the distance of point $\overrightarrow{v}$ from $P_{x_1,\ldots,x_n}$ is $1/\sqrt{1 + \sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.

Reduction

Reduction

- Therorem: Let $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ be an orthogonal basis in which all but $\overrightarrow{v}$ are unit vectors. Then the distance of point $\overrightarrow{v}$ from $P_{x_1, \ldots, x_n}$ is $\|\overrightarrow{v}\| / \sqrt{1 + \|\overrightarrow{v}\|^2 \sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.

Reduction

- Therorem: Let $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ be an orthogonal basis in which all but $\overrightarrow{v}$ are unit vectors. Then the distance of point $\overrightarrow{v}$ from $P_{x_1,\ldots,x_n}$ is $\|\overrightarrow{v}\| / \sqrt{1 + \|\overrightarrow{v}\|^2 \sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.

- The MDSP input $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ needs not be orthogonal. Let $\overrightarrow{b}'_i = \overrightarrow{b}_i - \gamma_i \overrightarrow{v}$ be the orthogonal component of $\overrightarrow{b}_i$ perpendicular to $\overrightarrow{v}$. Let $B' = [\overrightarrow{b}'_1, \ldots, \overrightarrow{b}'_n]$ and B'' be the Gram Schmidt Orthonormalization of B', i.e., $B'' = B'L$.

Reduction

- Therorem: Let $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ be an orthogonal basis in which all but $\overrightarrow{v}$ are unit vectors. Then the distance of point $\overrightarrow{v}$ from $P_{x_1,\ldots,x_n}$ is $\|\overrightarrow{v}\| / \sqrt{1 + \|\overrightarrow{v}\|^2 \sum_{i=1}^{n} x_i^2}$ for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$.

- The MDSP input $\{\overrightarrow{v}, \overrightarrow{b_1}, \ldots, \overrightarrow{b_n}\}$ needs not be orthogonal. Let $\overrightarrow{b}'_i = \overrightarrow{b}_i - \gamma_i \overrightarrow{v}$ be the orthogonal component of $\overrightarrow{b}_i$ perpendicular to $\overrightarrow{v}$. Let $B' = [\overrightarrow{b}'_1, \ldots, \overrightarrow{b}'_n]$ and B'' be the Gram Schmidt Orthonormalization of B', i.e., $B'' = B'L$.

- The CVP instance is the basis L^T and target vector is $\overrightarrow{u} = -L^T\overrightarrow{\gamma}$.

Conclusion

Conclusion

- We looked into the definition of lattice, CVP, MDSP and Dual lattice.

Conclusion

- We looked into the definition of lattice, CVP, MDSP and Dual lattice.
- We saw equivalence between CVP and MDSP using dual lattice.

Conclusion

- We looked into the definition of lattice, CVP, MDSP and Dual lattice.
- We saw equivalence between CVP and MDSP using dual lattice.
- We saw equivalence between CVP and MDSP without using dual lattice.

Conclusion

- We looked into the definition of lattice, CVP, MDSP and Dual lattice.
- We saw equivalence between CVP and MDSP using dual lattice.
- We saw equivalence between CVP and MDSP without using dual lattice.
- What is the relation between the dual lattice and the lattice in the second reduction.

Thank You !