On the bases of $\mathbb{Z}^n$ lattice

Shashank K Mehta, Mahesh Sreekumar Rajasree
Department of Computer Science & Engineering
IIT Kanpur

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.,

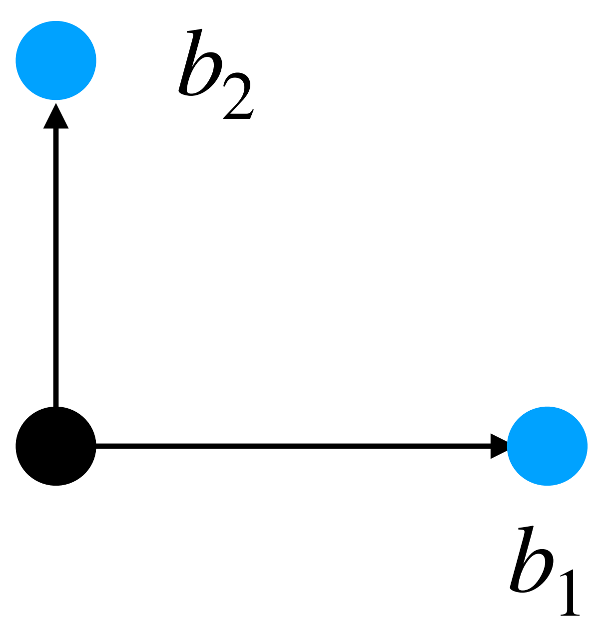
$$\mathscr{L}(b_1, \ldots, b_n) = \{ \sum_{i=1}^{n} z_i b_i \mid \forall (z_1, \ldots, z_n) \in \mathbb{Z}^n \}$$

Lattice

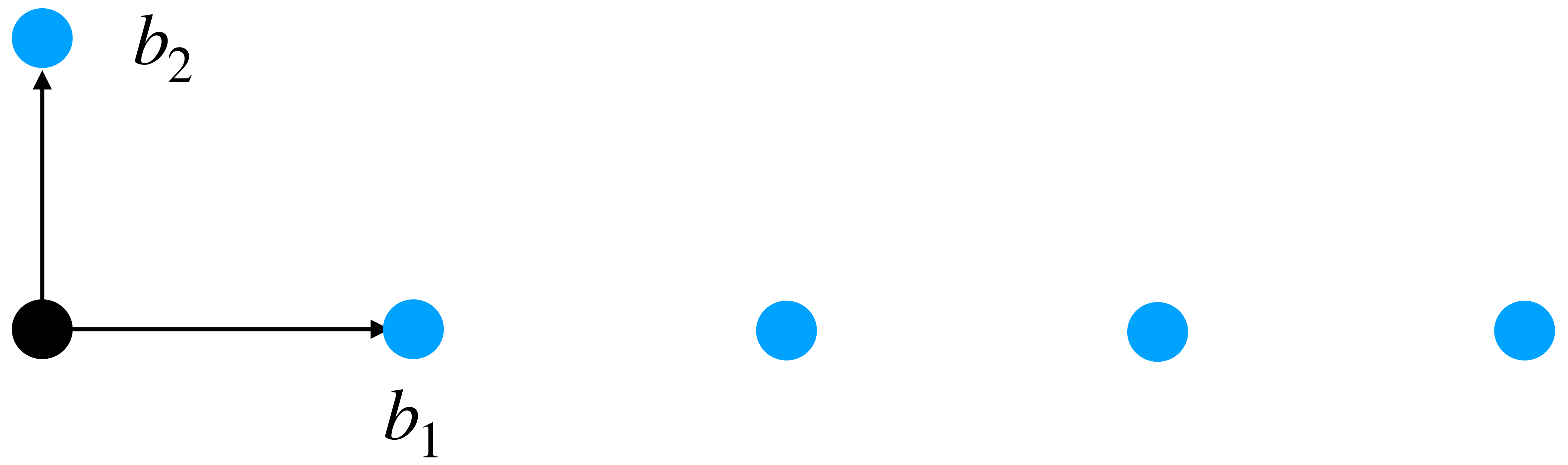
A *lattice* generated by a set of *linearly independent vectors* $B = \{b_1, \ldots, b_n\}$ is the set of all *integer linear combinations* of $\{b_1, \ldots, b_n\}$, i.e.,

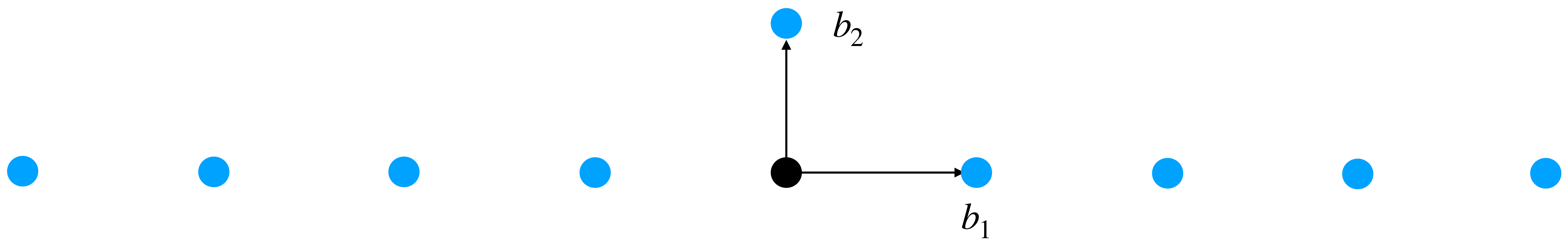
$$\mathscr{L}(b_1, \ldots, b_n) = \{ \sum_{i=1}^{n} z_i b_i \mid \forall (z_1, \ldots, z_n) \in \mathbb{Z}^n \}$$

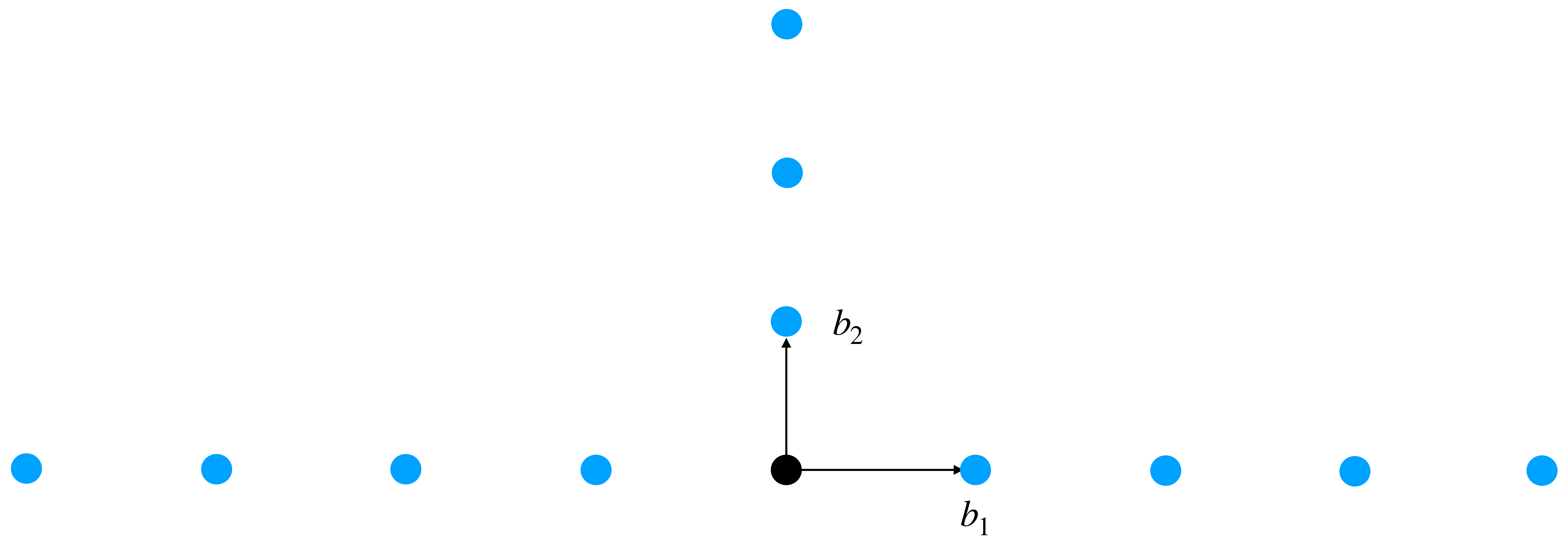
B is called a *basis* of $\mathscr{L}$.



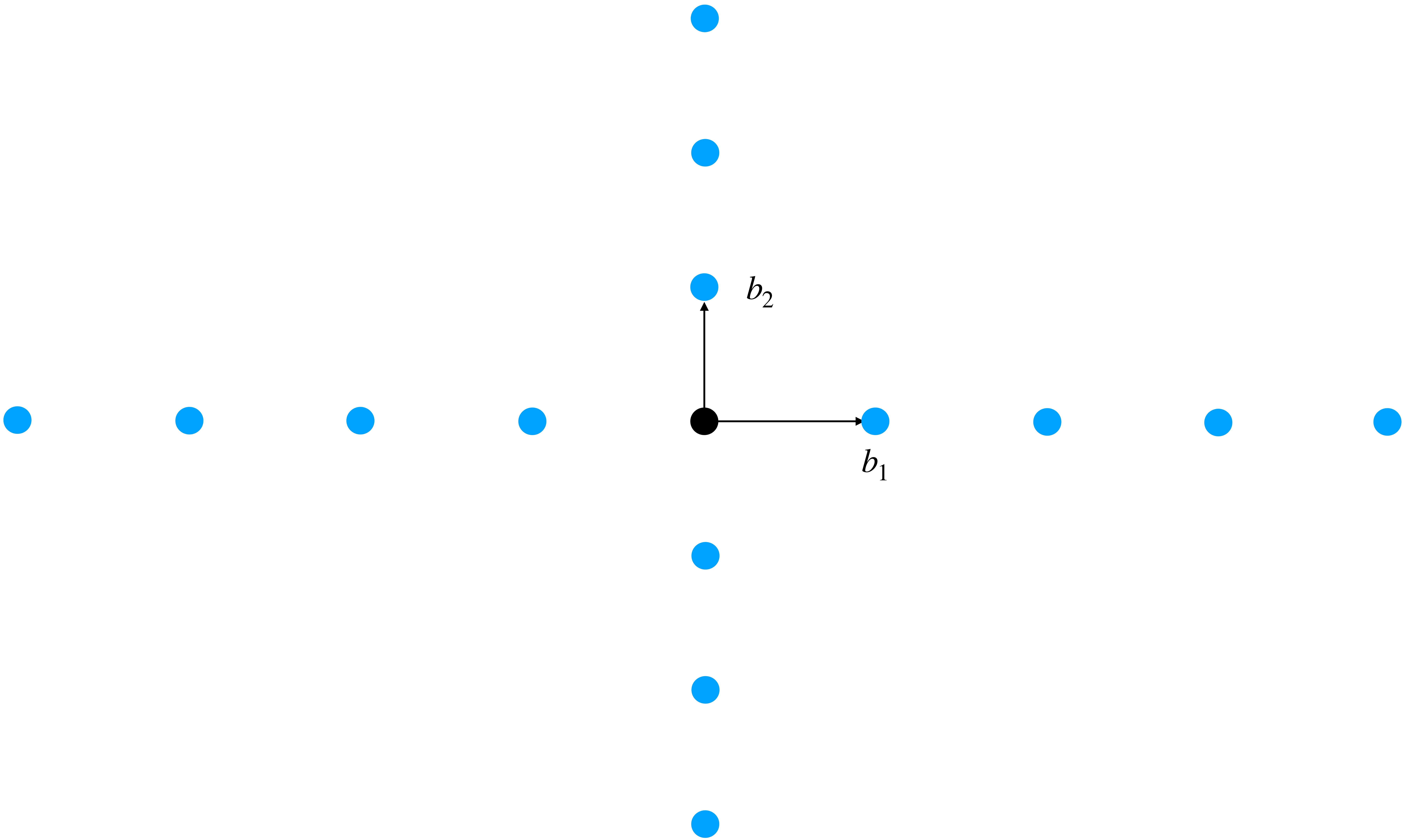
b_2
b_1

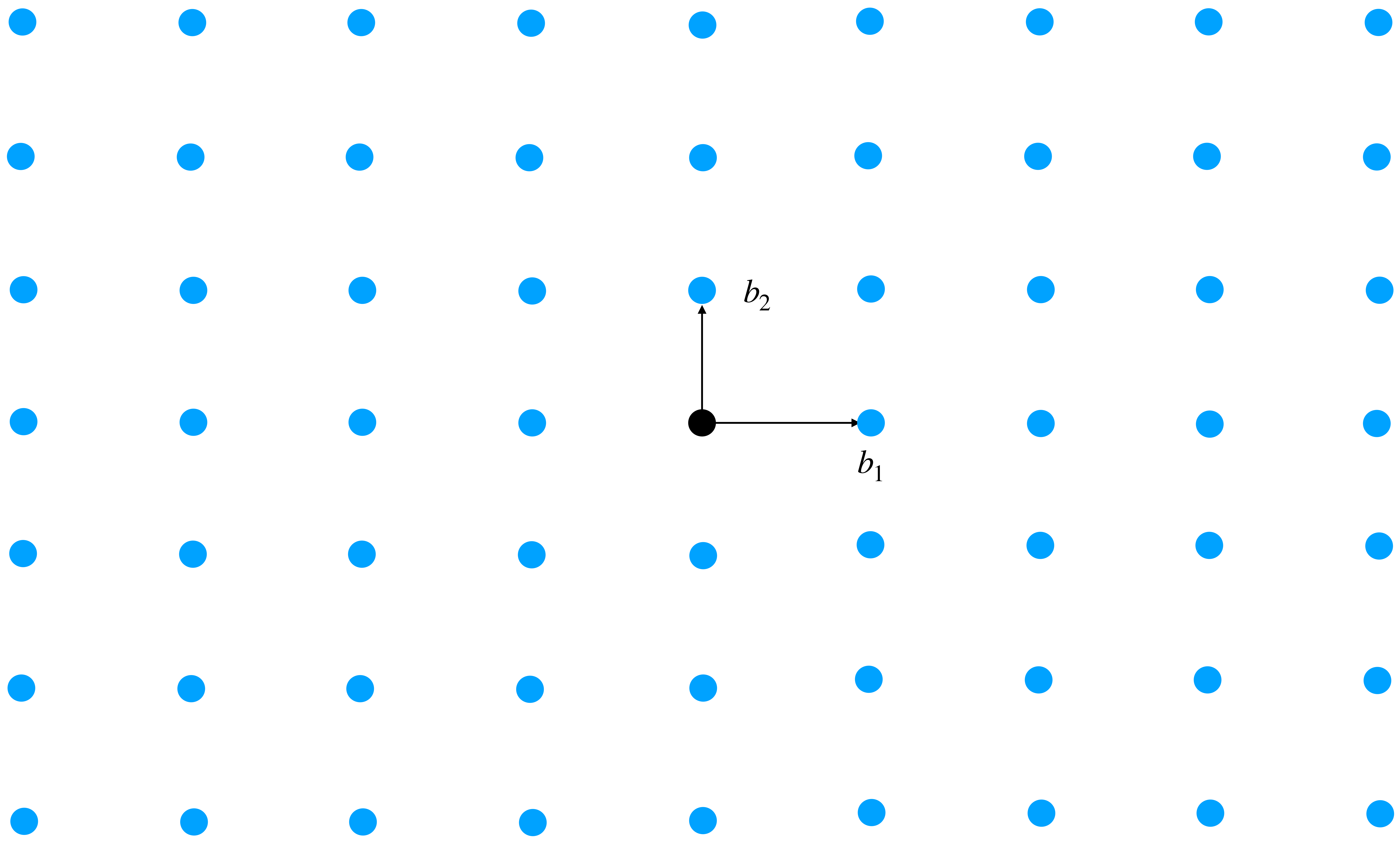

b_2
b_1


b_2
b_1

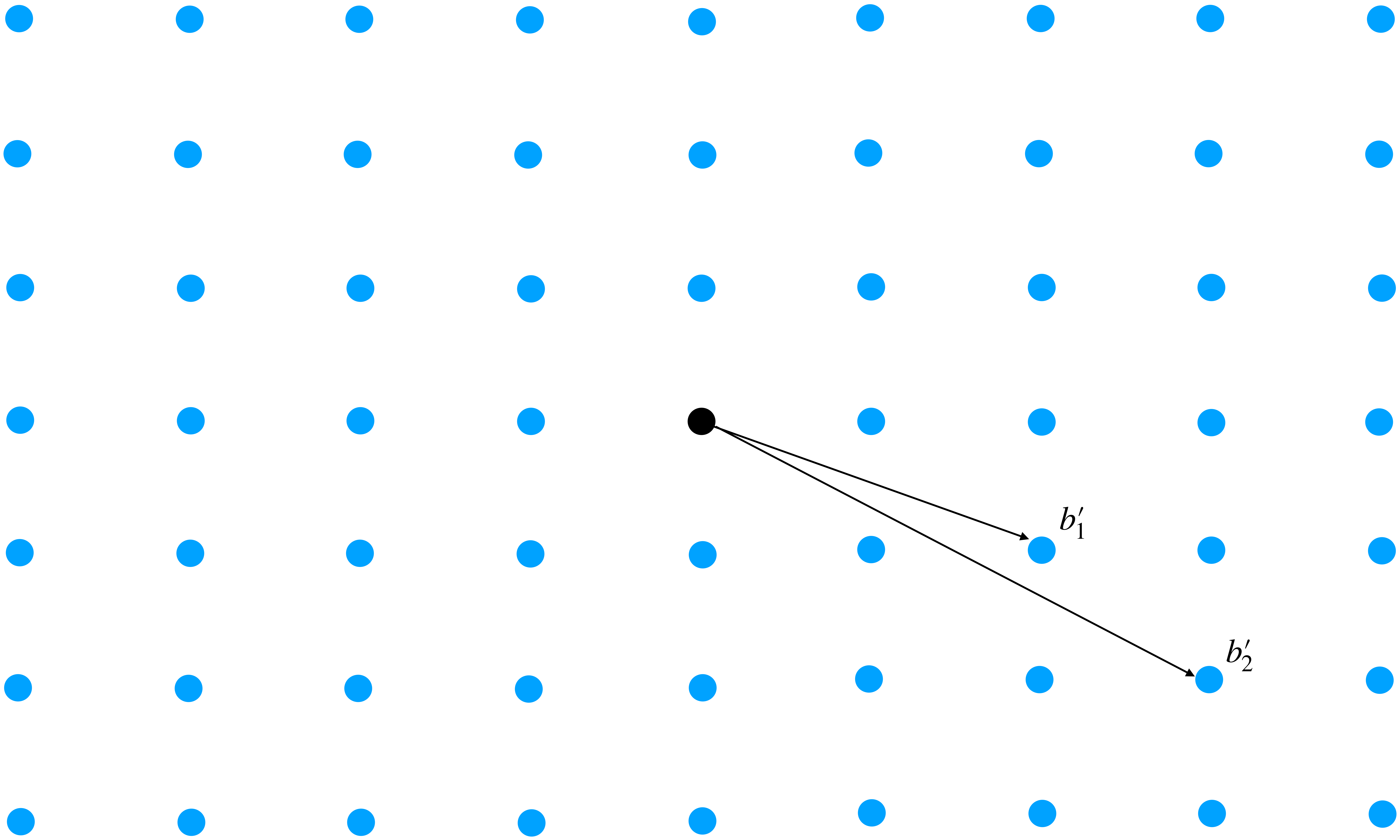


b_2
b_1


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

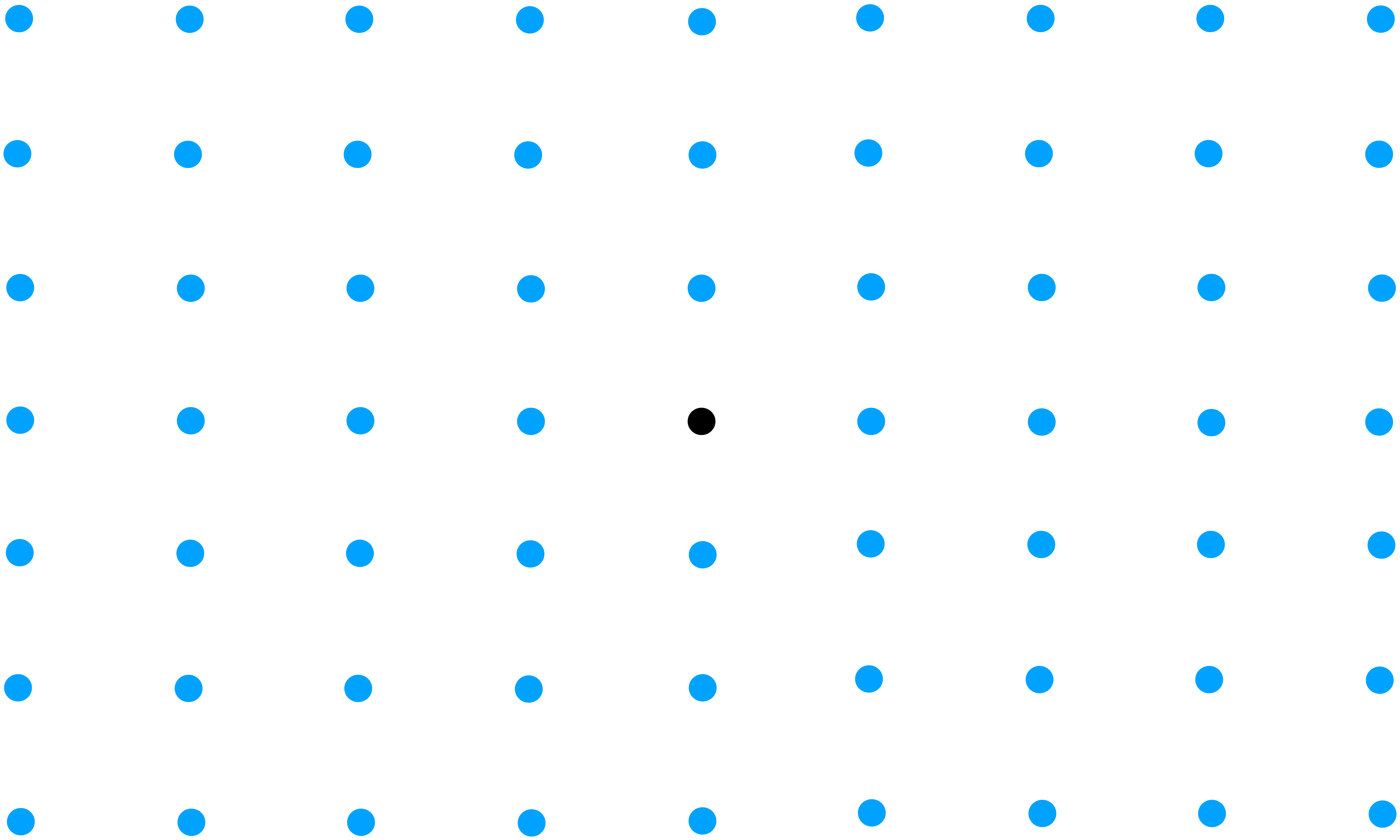
- Factoring rational polynomials.
- Integer linear programming.
- Cryptanalysis of RSA, knapsack cryptosystems.
- Building very strong cryptographic primitives (post-quantum).

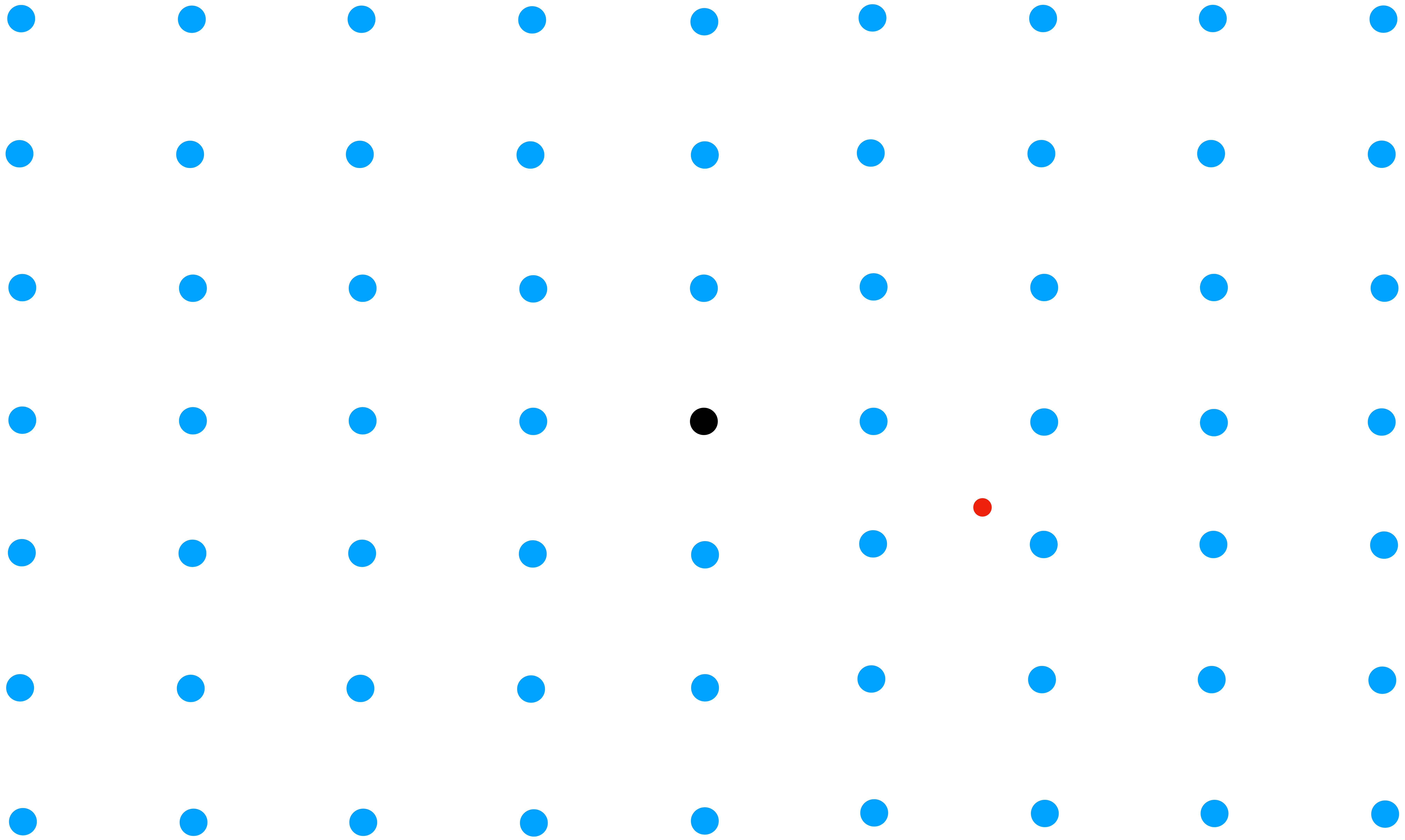
Closest Vector Problem (CVP)

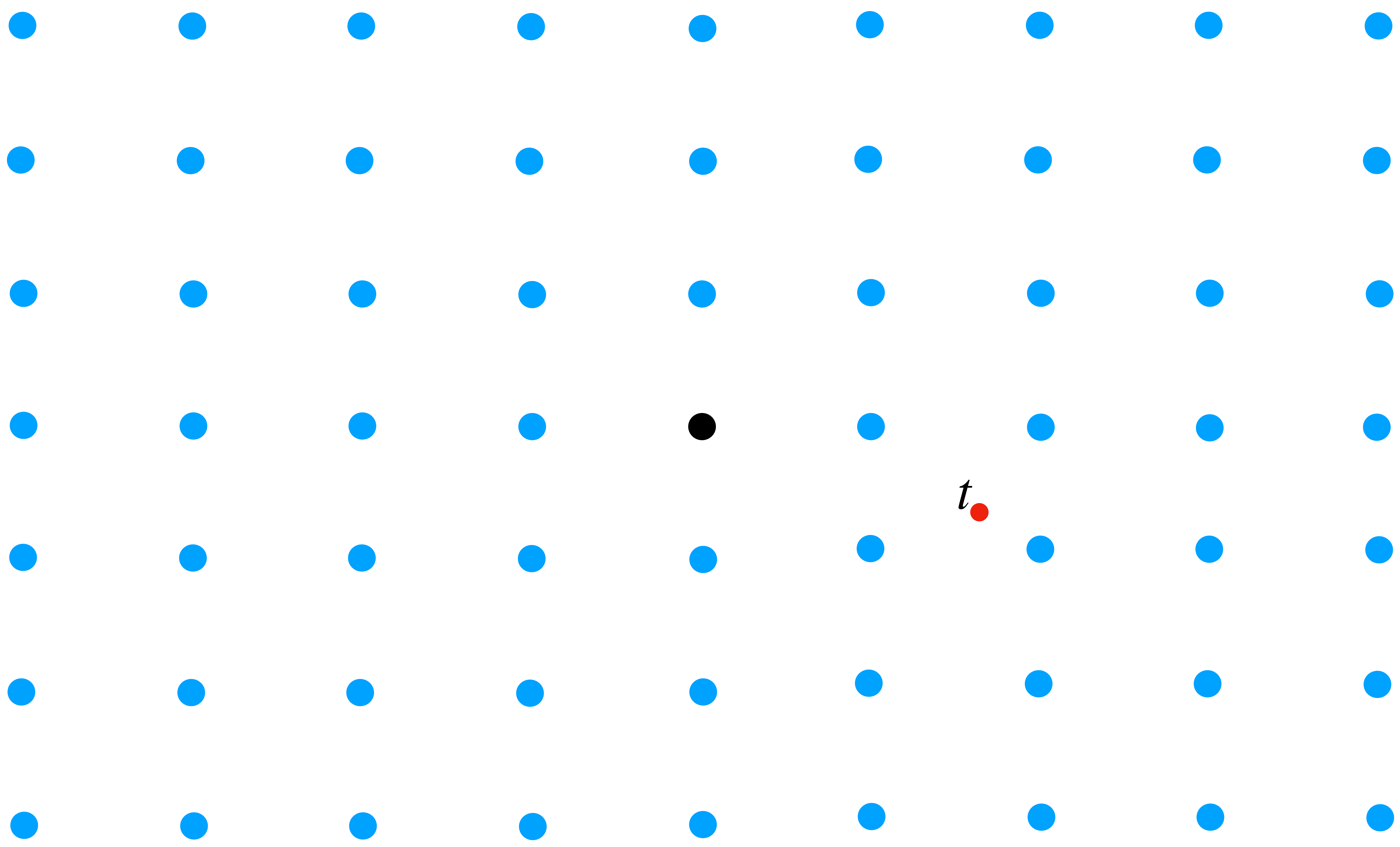
Closest Vector Problem (CVP)

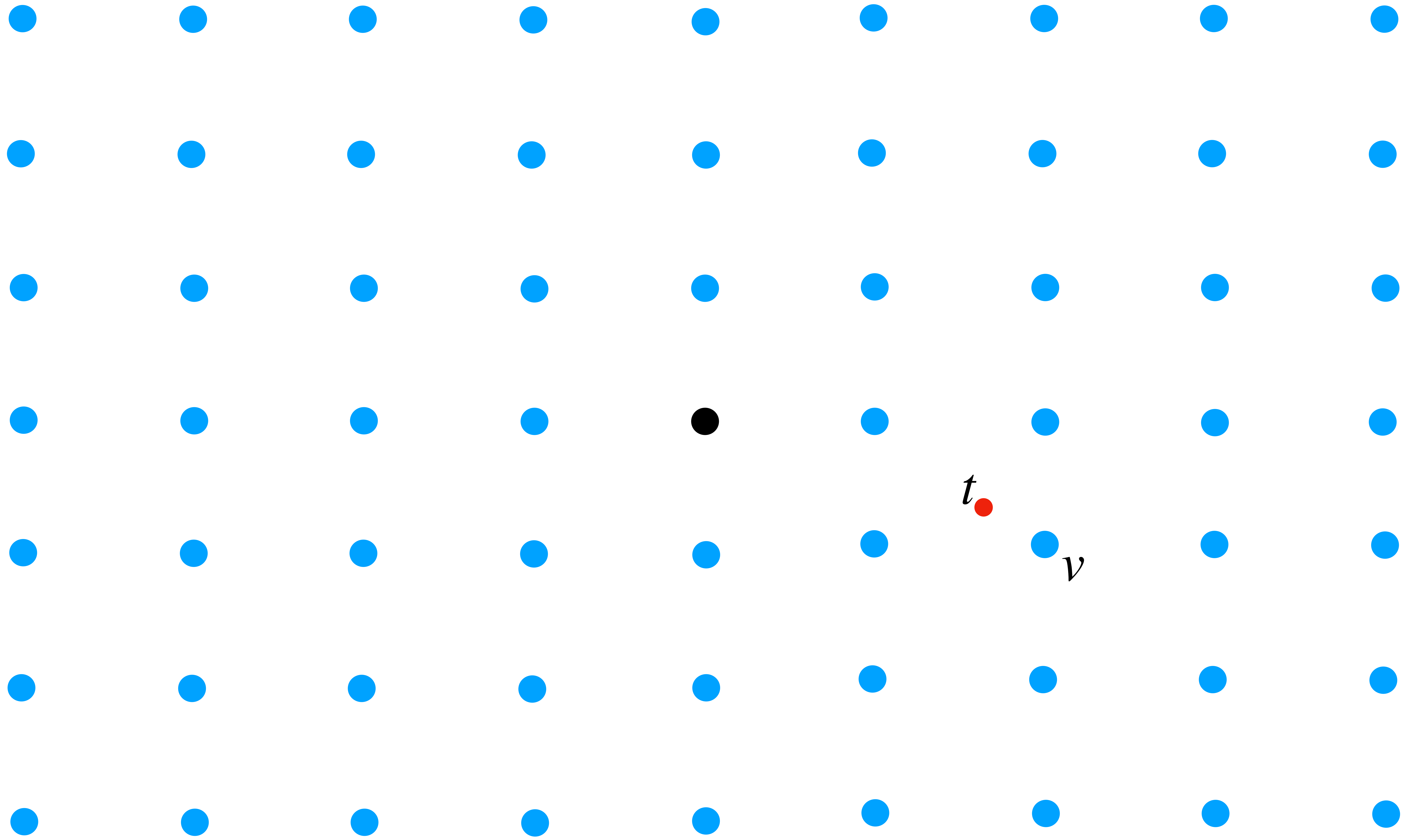
Given a basis $B = \{b_1, \ldots, b_n\}$ and a target $t \in \mathbb{R}^n$, find a vector $v \in \mathscr{L}(B)$ such that v is closest to t, i.e.,

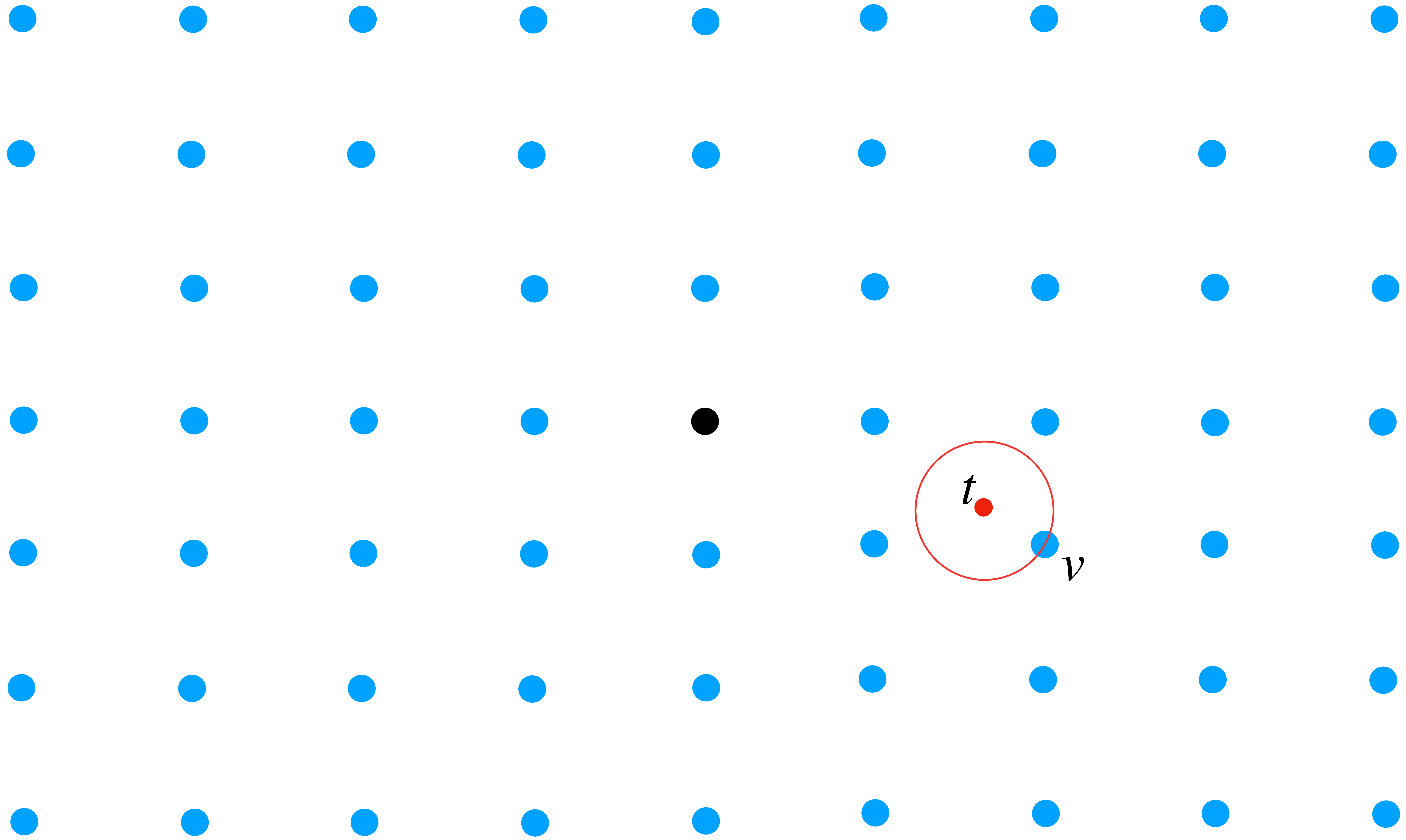
$$||v - t|| \leq ||u - t||, \forall u \in \mathscr{L}(B)$$



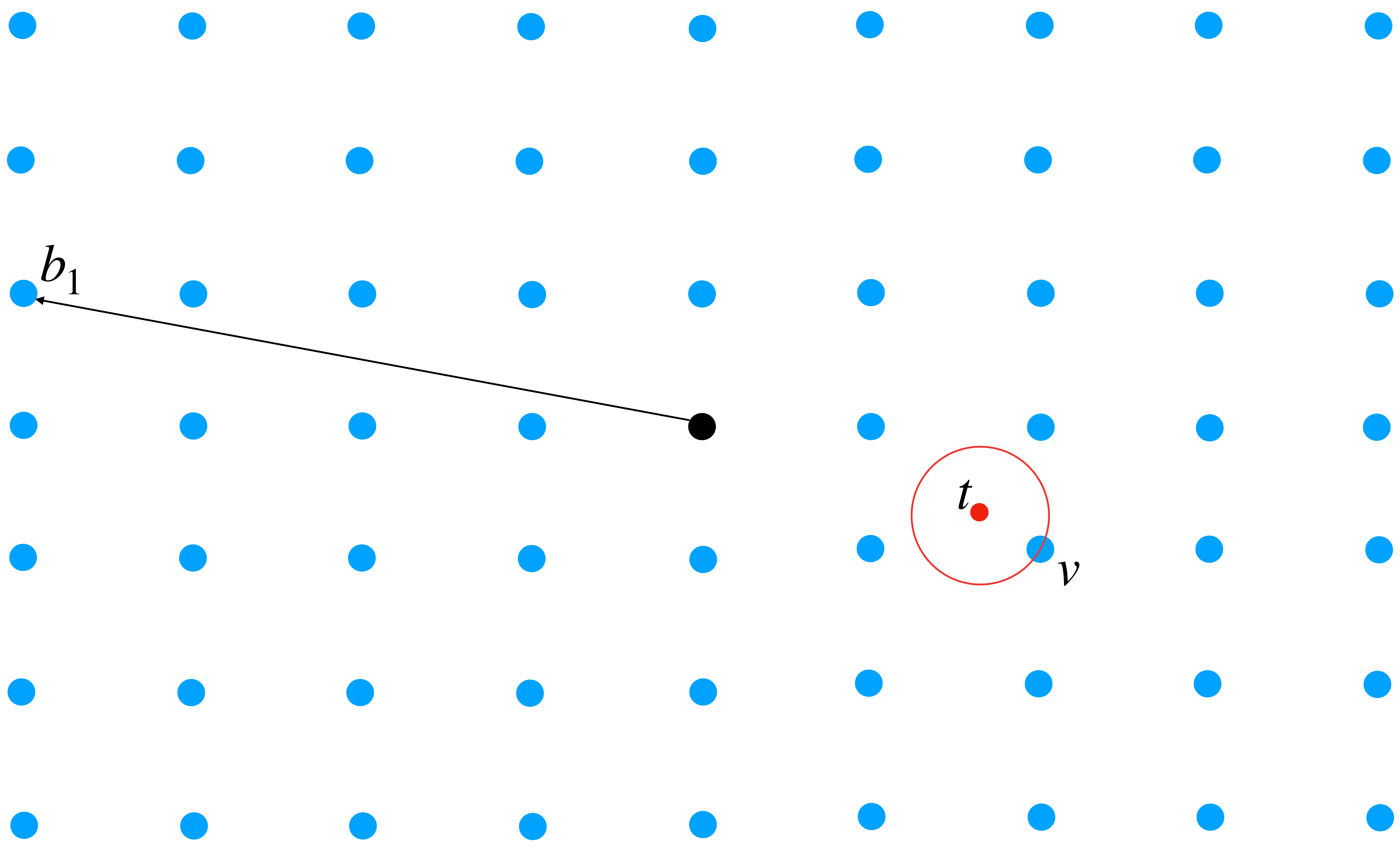



t

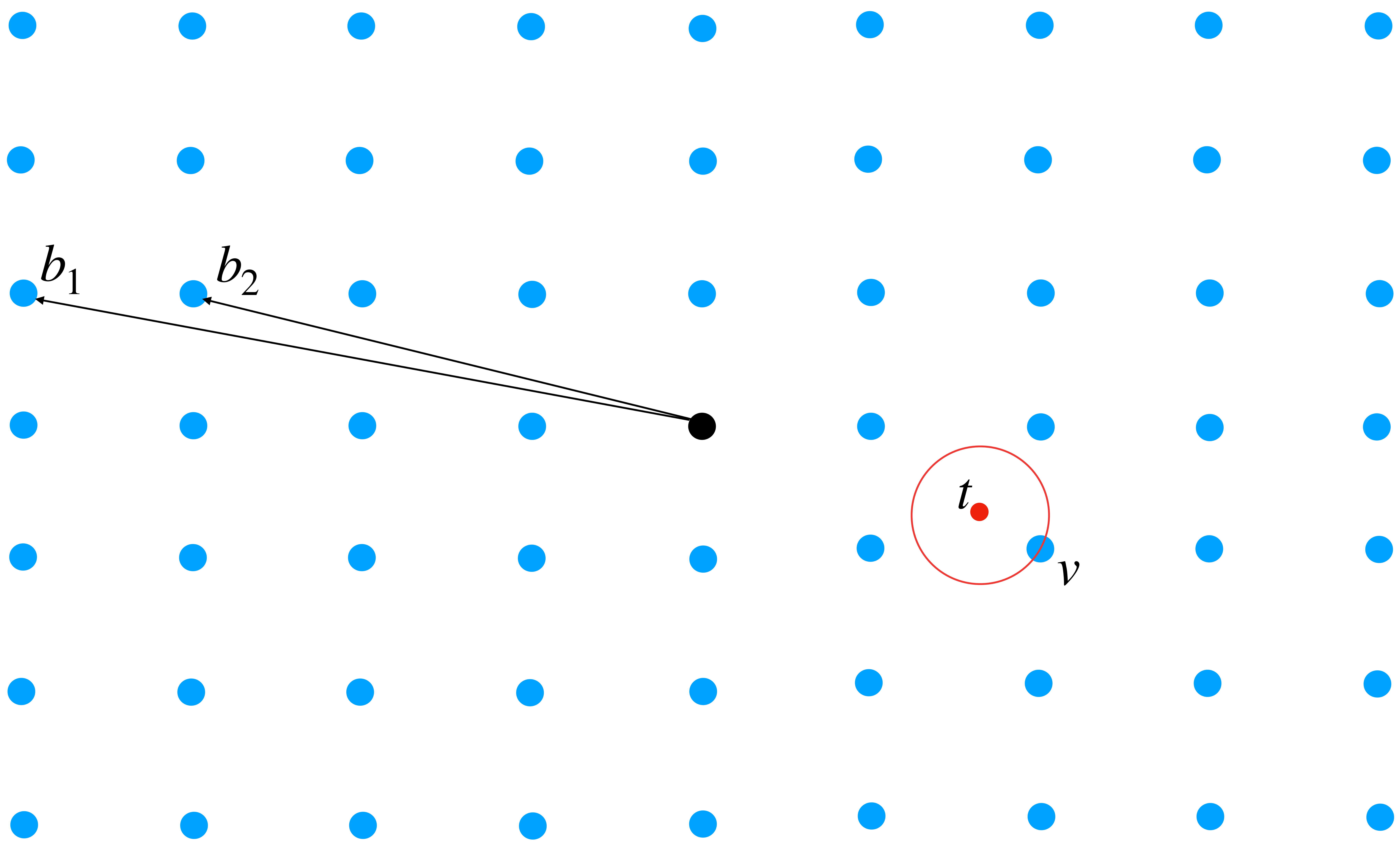

t
v



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	$2^{n+o(n)}$	$2^{n+o(n)}$

Other lattice problems

Other lattice problems

- Given a basis B, the **Shortest Vector Problem (SVP)** asks for a shortest non-zero vector $v \in \mathscr{L}(B)$, i.e., $||v|| \leq ||u||$ for all $u \in \mathscr{L}(B) \backslash \{0\}$.

Other lattice problems

- Given a basis B, the **Shortest Vector Problem (SVP)** asks for a shortest non-zero vector $v \in \mathscr{L}(B)$, i.e., $||v|| \leq ||u||$ for all $u \in \mathscr{L}(B) \backslash \{0\}$.

- The i-th **Successive minimum** $\lambda_i(\mathscr{L}(B))$ for a lattice $\mathscr{L}$ is the radius of smallest sphere centered at the origin containing at least i independent lattice vectors.

Other lattice problems

- Given a basis B, the **Shortest Vector Problem (SVP)** asks for a shortest non-zero vector $v \in \mathscr{L}(B)$, i.e., $||v|| \leq ||u||$ for all $u \in \mathscr{L}(B) \backslash \{0\}$.

- The i-th **Successive minimum** $\lambda_i(\mathscr{L}(B))$ for a lattice $\mathscr{L}$ is the radius of smallest sphere centered at the origin containing at least i independent lattice vectors.

$$\lambda_i(\mathscr{L}) = inf\{r \mid dim(\mathscr{L} \cap \mathscr{B}(0,r)) \geq i\}$$

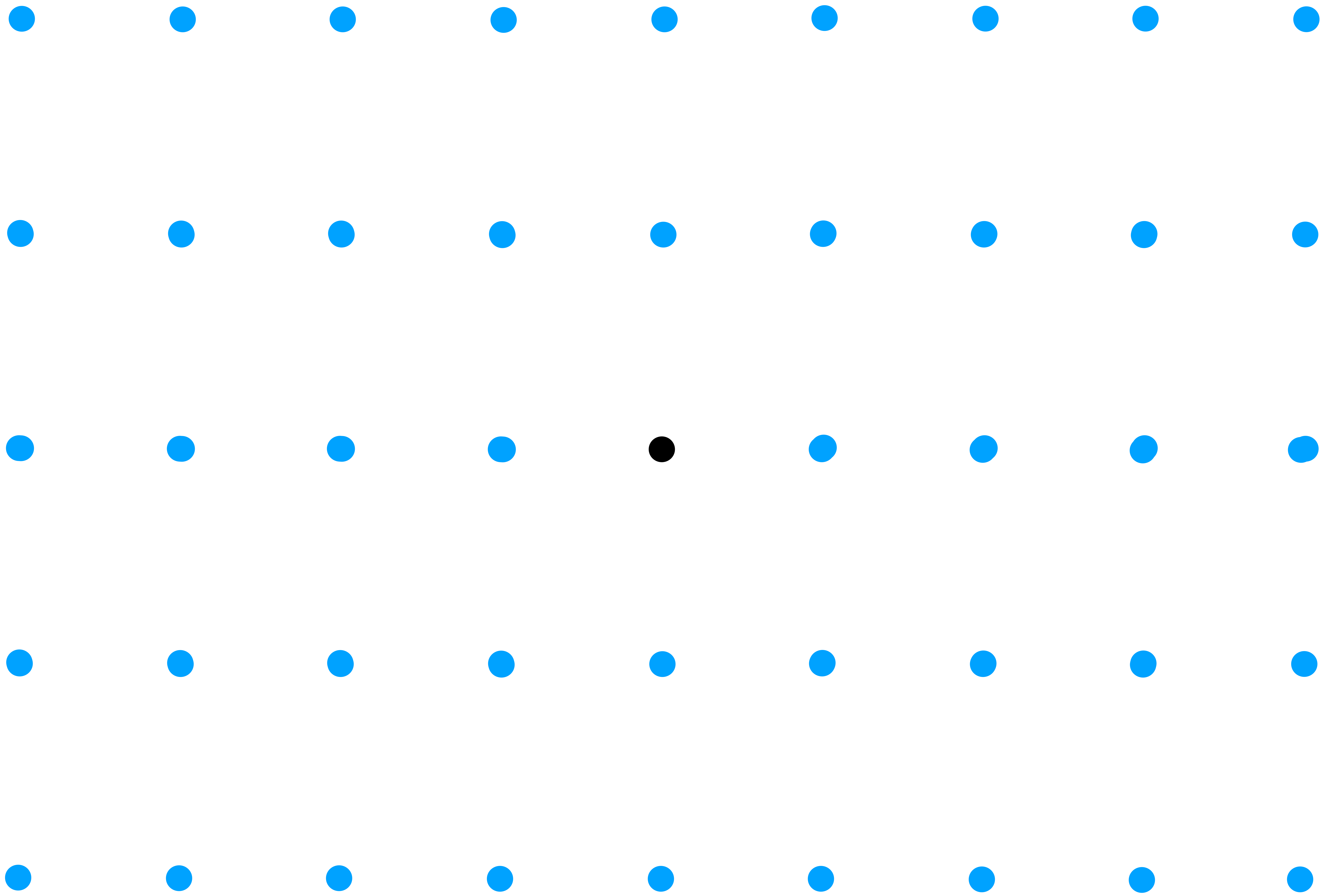
Other lattice problems

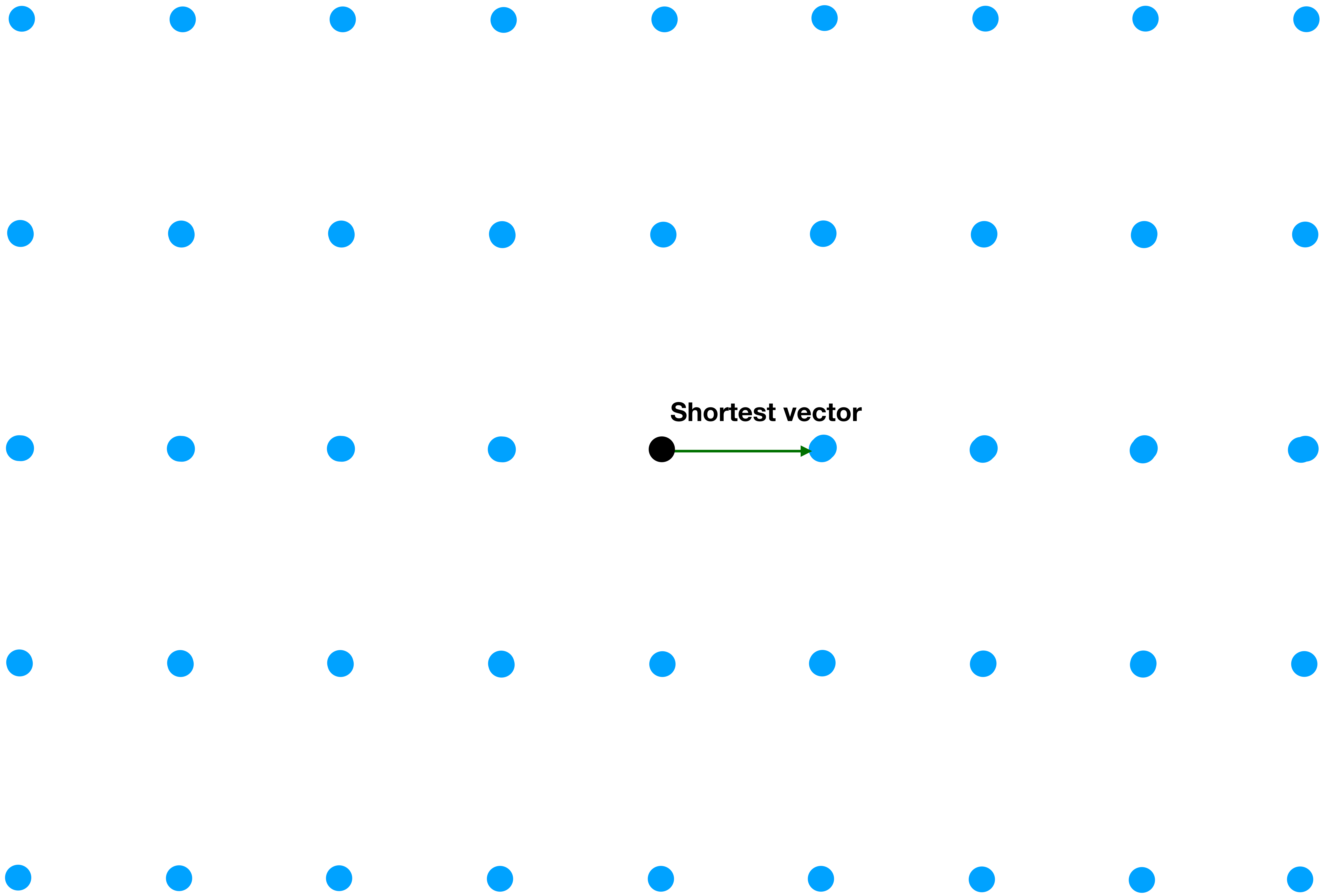
- Given a basis B, the **Shortest Vector Problem (SVP)** asks for a shortest non-zero vector $v \in \mathscr{L}(B)$, i.e., $||v|| \leq ||u||$ for all $u \in \mathscr{L}(B) \backslash \{0\}$.

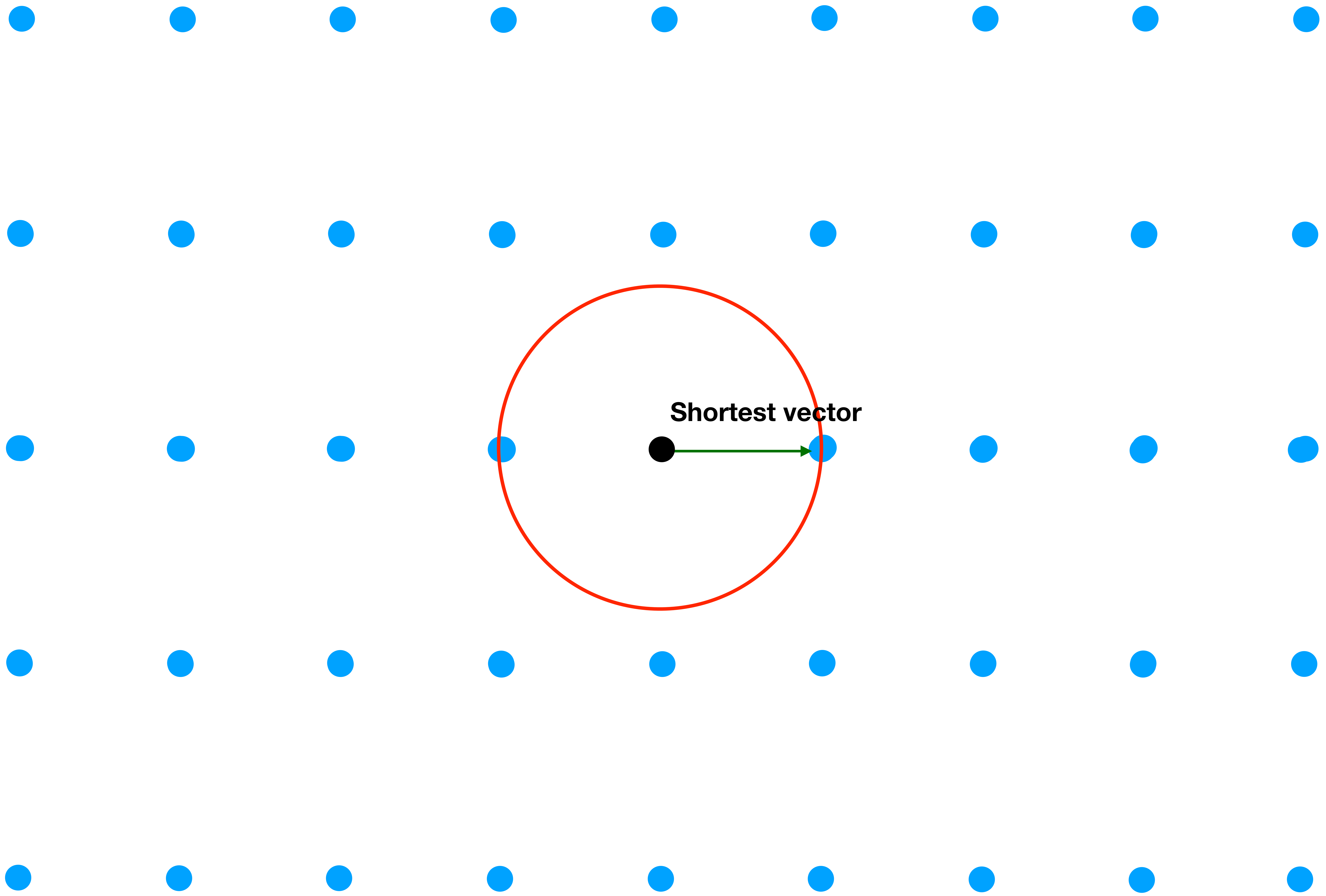
- The i-th **Successive minimum** $\lambda_i(\mathscr{L}(B))$ for a lattice $\mathscr{L}$ is the radius of smallest sphere centered at the origin containing at least i independent lattice vectors.

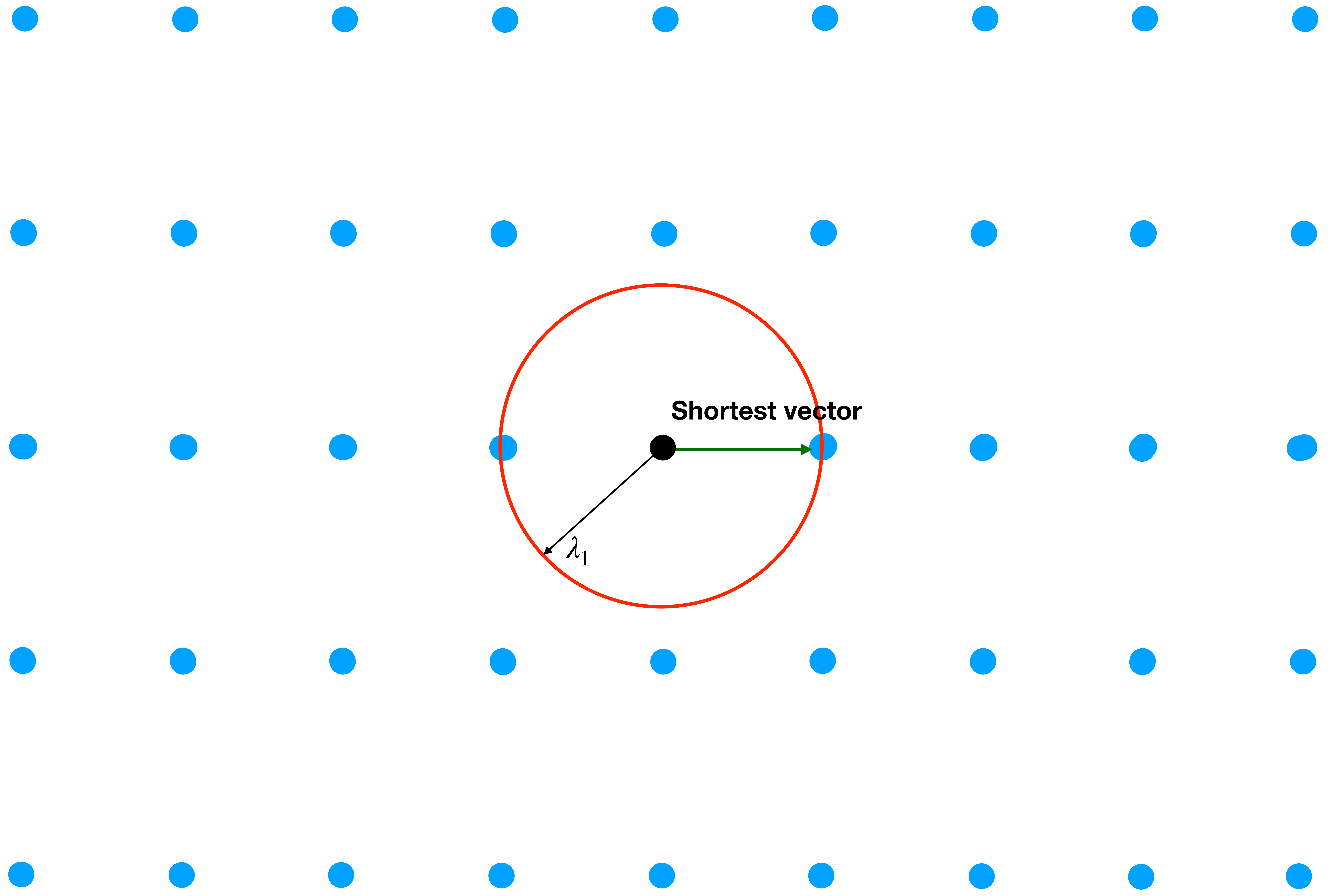
$$\lambda_i(\mathscr{L}) = inf\{r \mid dim(\mathscr{L} \cap \mathscr{B}(0,r)) \geq i\}$$

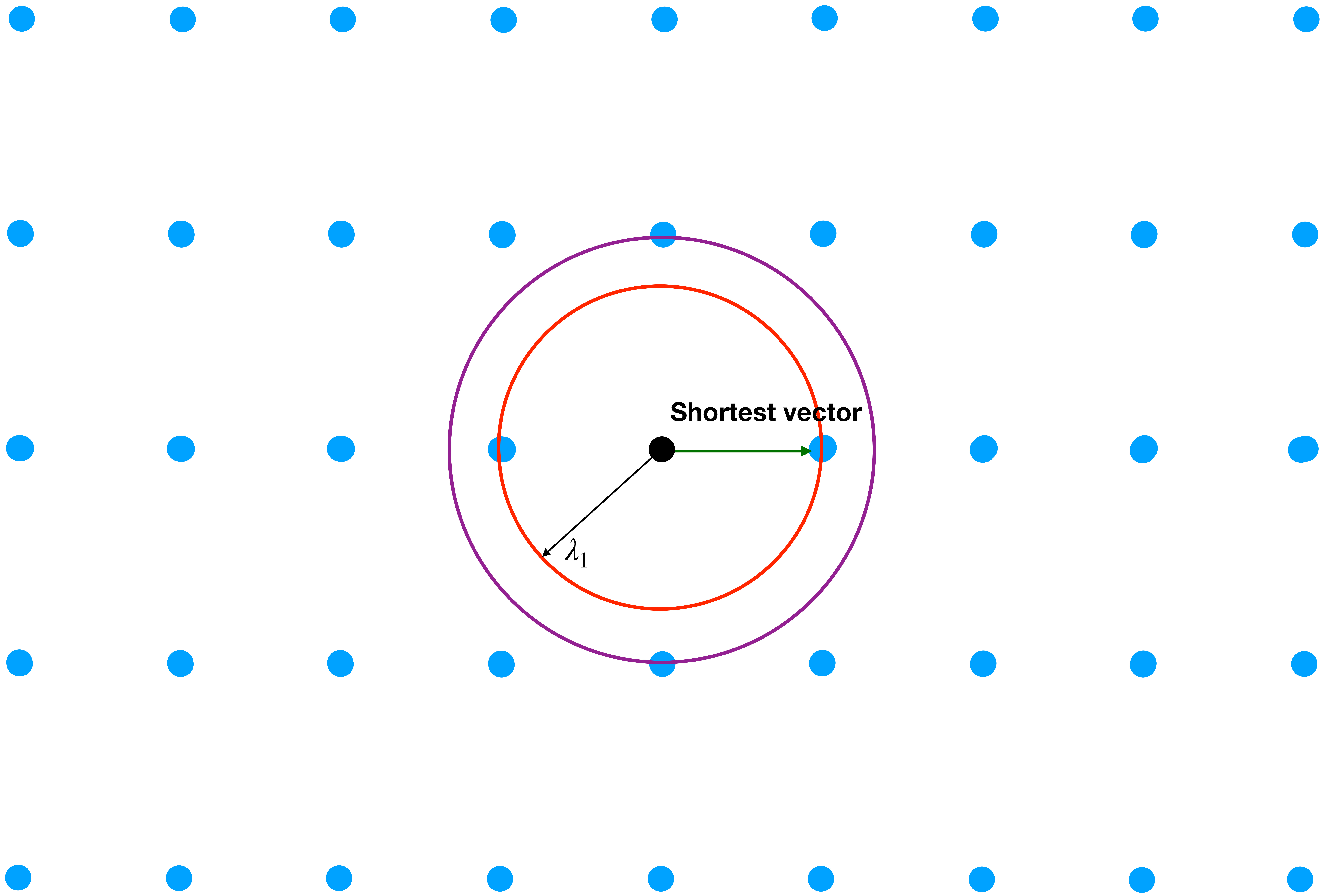
where $\mathscr{B}(x, y)$ is the sphere entered at x with radius y.

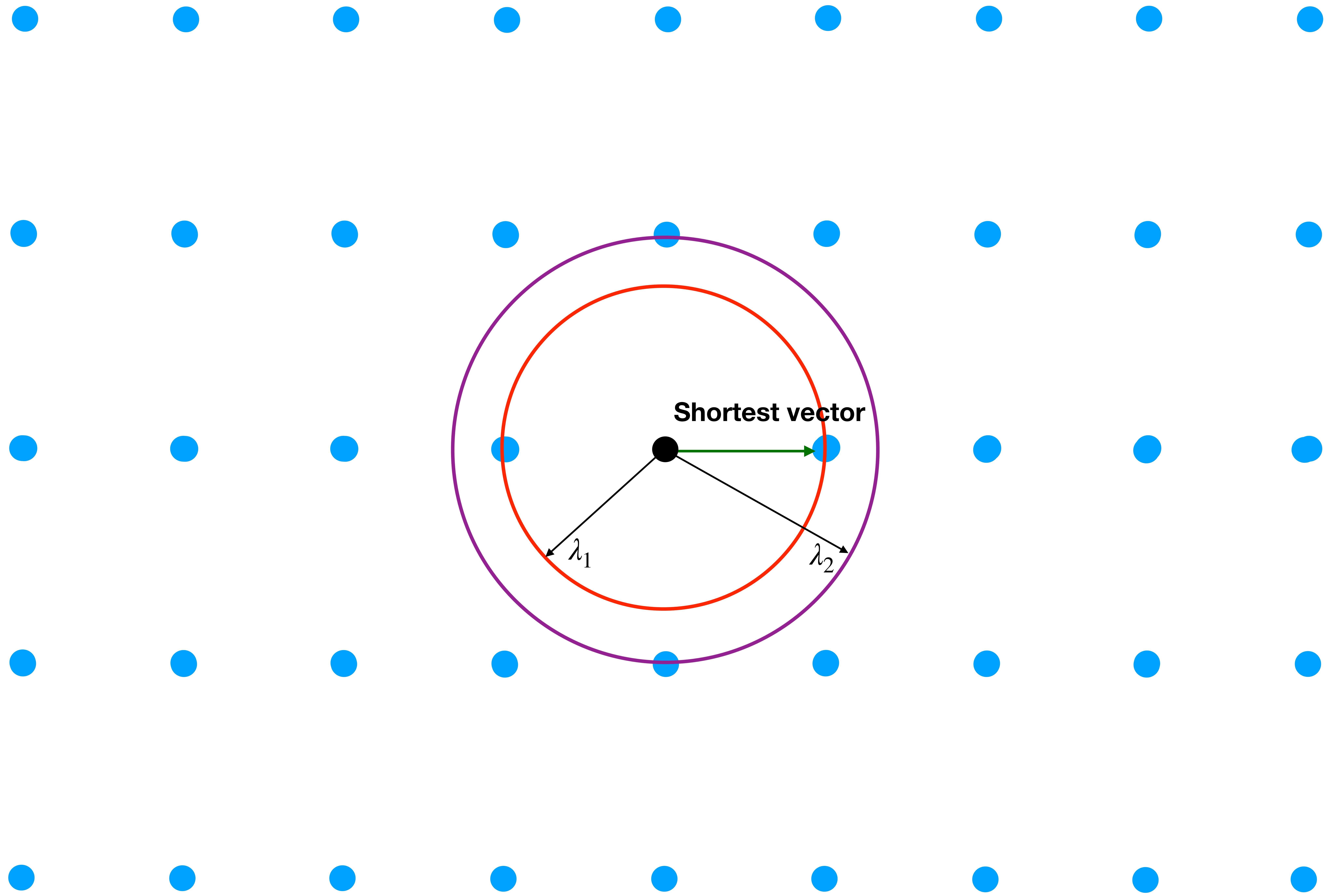



Shortest vector


Shortest vector


Shortest vector
λ_1


Shortest vector
λ_1


Shortest vector
λ1
λ2

Voronoi cell of a lattice

Voronoi cell of a lattice

The Voronoi cell of a lattice $\mathscr{L}$ is defined as

$$\mathscr{V}(\mathscr{L}) = \{x \in \mathbb{R}^n \mid \forall v \in \mathscr{L} \backslash \{0\}, ||x|| \leq ||x - v||\}$$

In other words, it is set of all points that are closer to the origin than all other non-zero lattice vectors.

Voronoi cell of a lattice

The Voronoi cell of a lattice $\mathscr{L}$ is defined as

$$\mathscr{V}(\mathscr{L}) = \{x \in \mathbb{R}^n \mid \forall v \in \mathscr{L} \backslash \{0\}, ||x|| \leq ||x - v||\}$$

In other words, it is set of all points that are closer to the origin than all other non-zero lattice vectors.

The half space of a non-zero lattice vector $v \in \mathscr{L}$ is defined as

$$H(v) = \{x \in \mathbb{R}^n \mid ||x|| \leq ||x - v||\}$$

Voronoi cell of a lattice

The Voronoi cell of a lattice $\mathscr{L}$ is defined as

$$\mathscr{V}(\mathscr{L}) = \{x \in \mathbb{R}^n \mid \forall v \in \mathscr{L} \backslash \{0\}, ||x|| \leq ||x - v||\}$$

In other words, it is set of all points that are closer to the origin than all other non-zero lattice vectors.

The half space of a non-zero lattice vector $v \in \mathscr{L}$ is defined as

$$H(v) = \{x \in \mathbb{R}^n \mid ||x|| \leq ||x - v||\}$$

Observe that $\mathscr{V}(\mathscr{L}) = \bigcap_{v \in \mathscr{L} \backslash \{0\}} H(v)$.

Voronoi cell of a lattice

The Voronoi cell of a lattice $\mathscr{L}$ is defined as

$$\mathscr{V}(\mathscr{L}) = \{x \in \mathbb{R}^n \mid \forall v \in \mathscr{L}\backslash\{0\}, ||x|| \leq ||x - v||\}$$

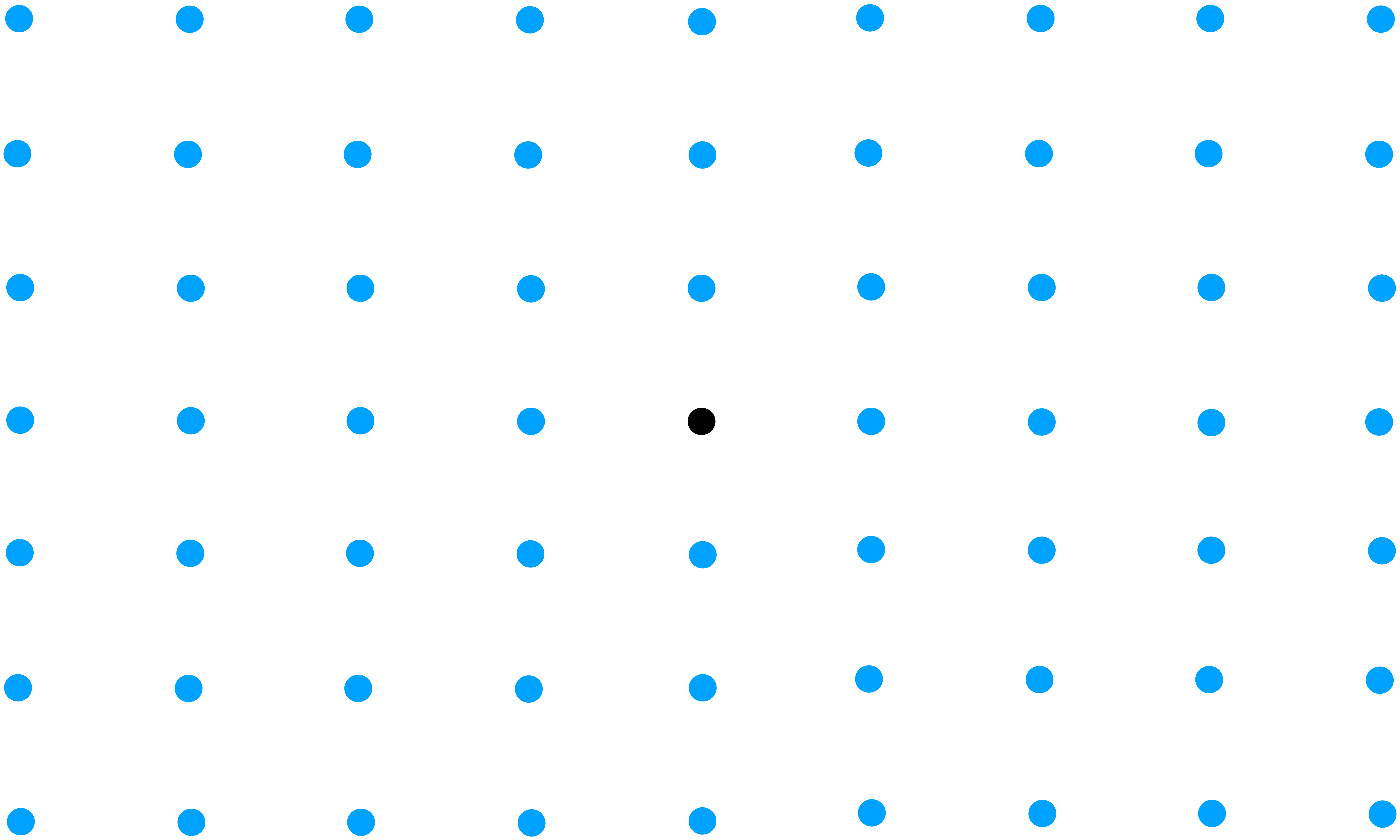
In other words, it is set of all points that are closer to the origin than all other non-zero lattice vectors.

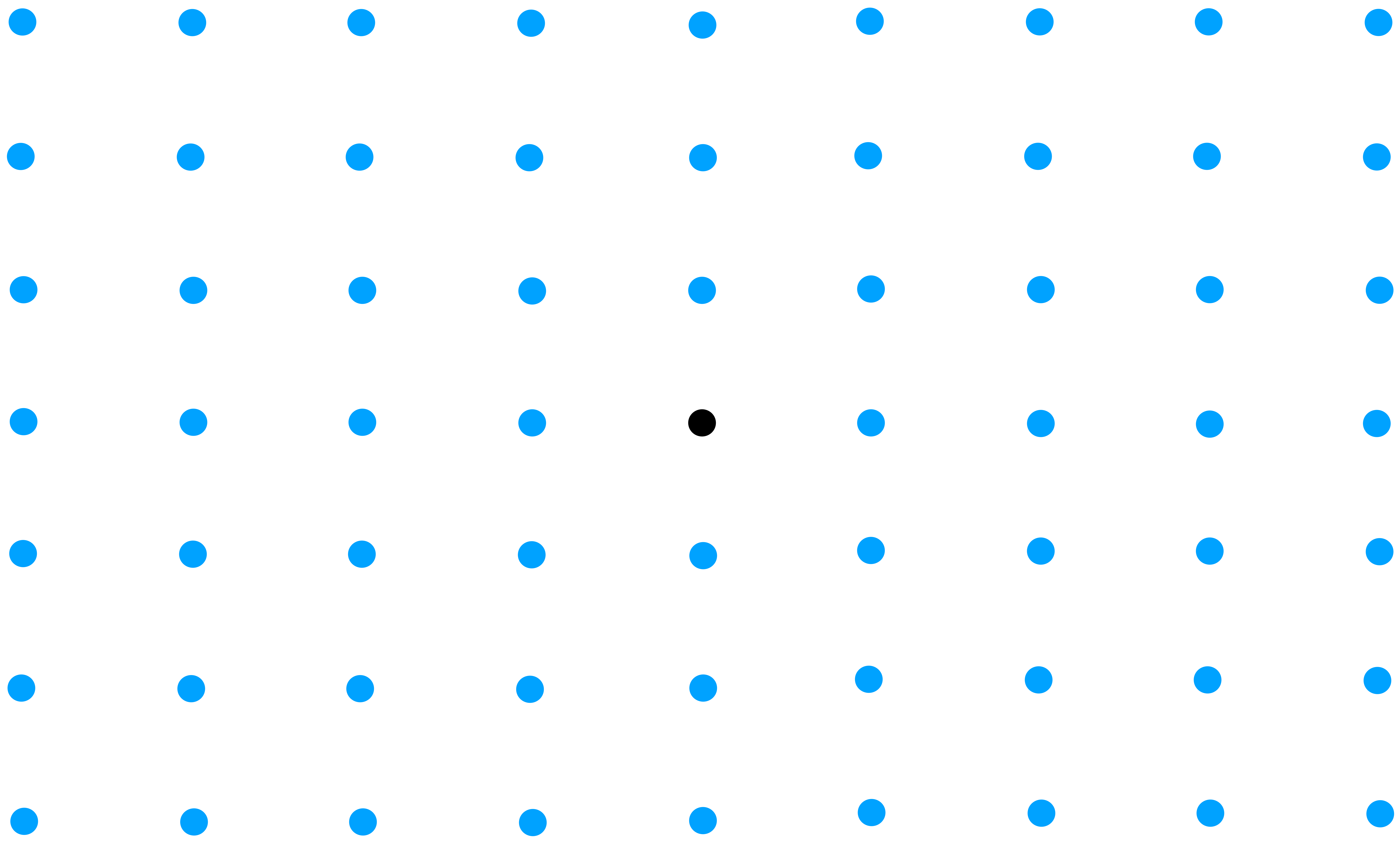
The half space of a non-zero lattice vector $v \in \mathscr{L}$ is defined as

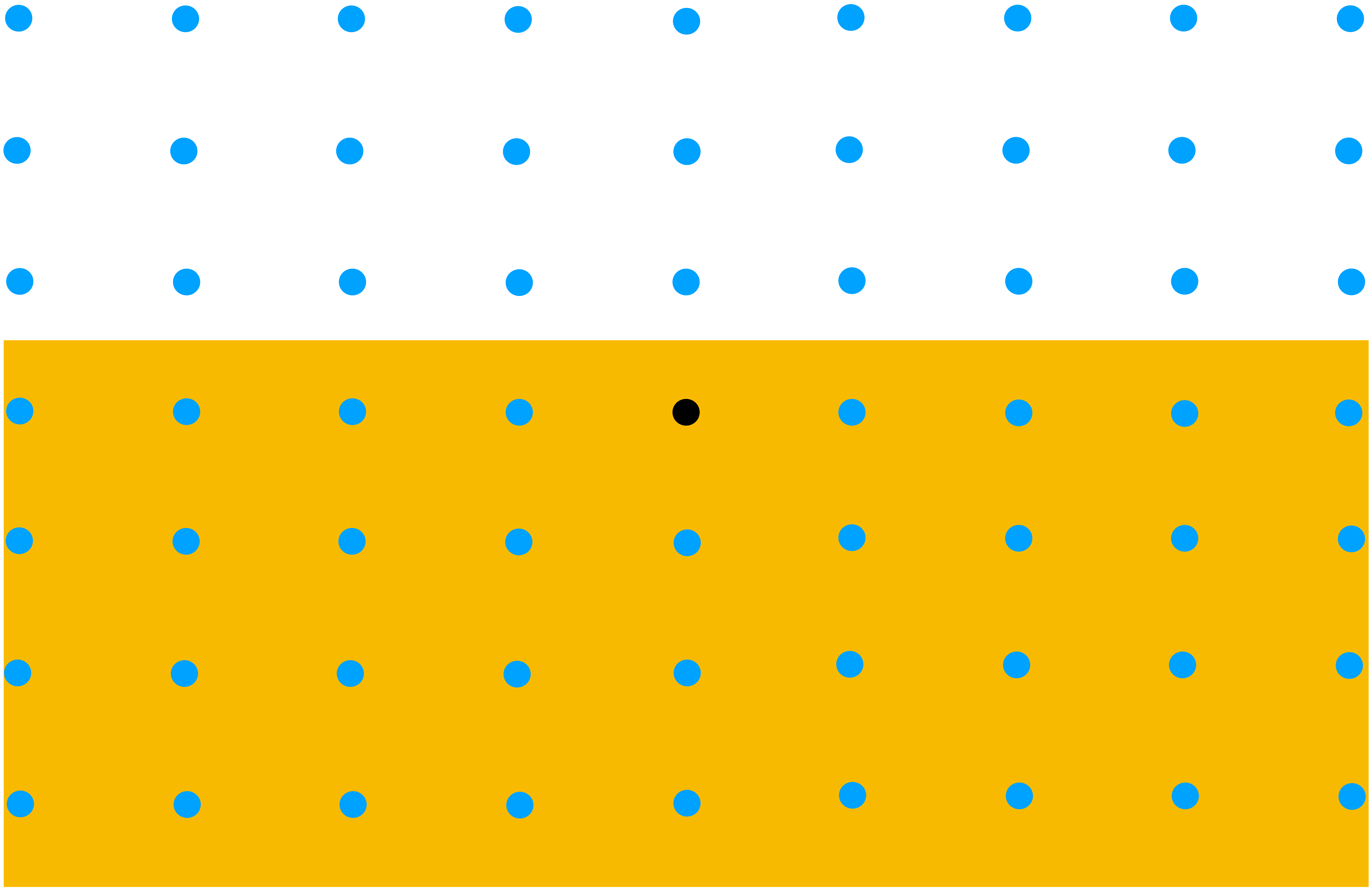
$$H(v) = \{x \in \mathbb{R}^n \mid ||x|| \leq ||x - v||\}$$

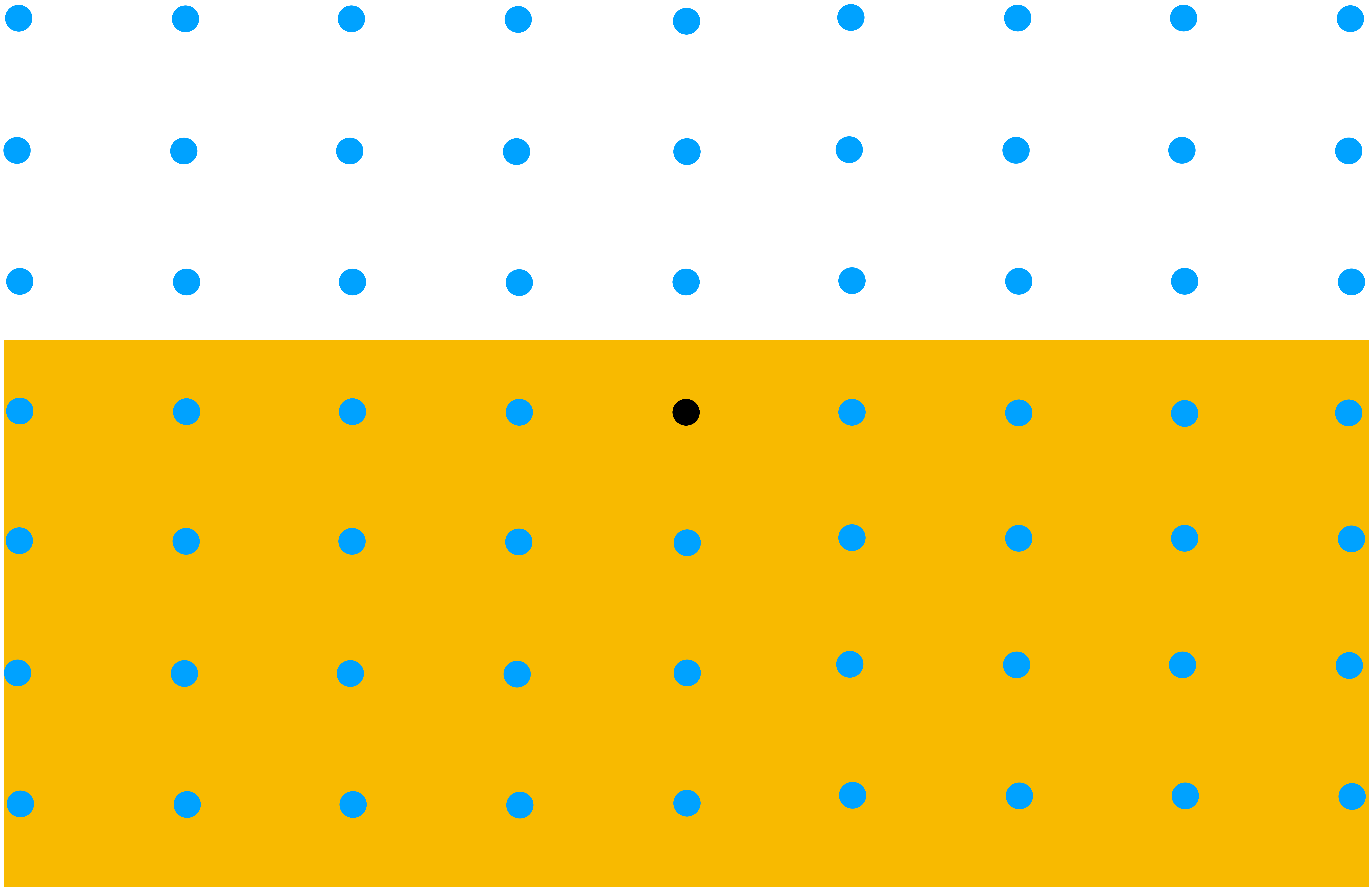
Observe that $\mathscr{V}(\mathscr{L}) = \bigcap_{v \in \mathscr{L}\backslash\{0\}} H(v)$.

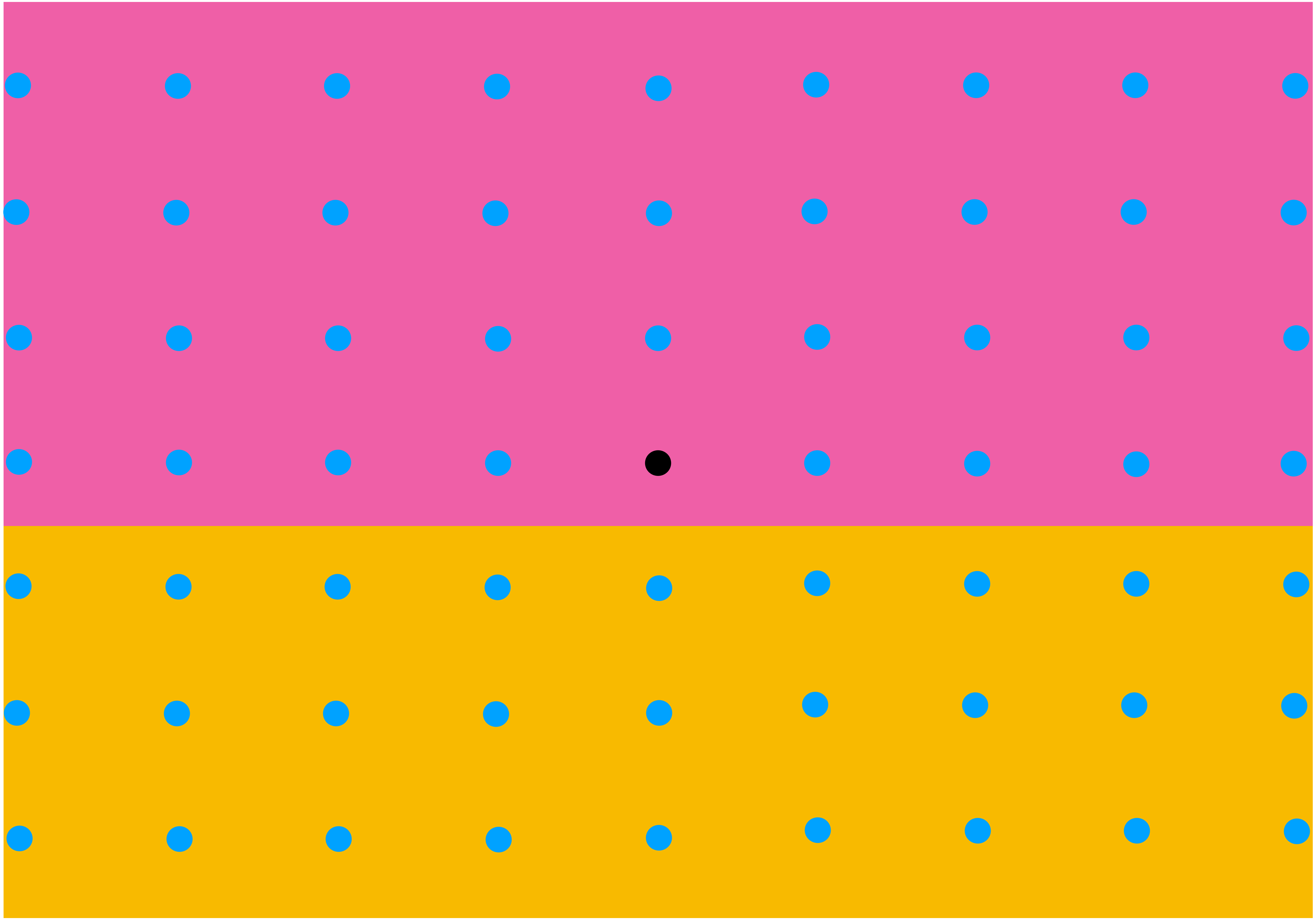
There is a minimal set of lattice vectors called Voronoi relevant vectors $V(L)$ such that $\mathscr{V}(\mathscr{L}) = \bigcap_{v \in V(\mathscr{L})} H(v)$.

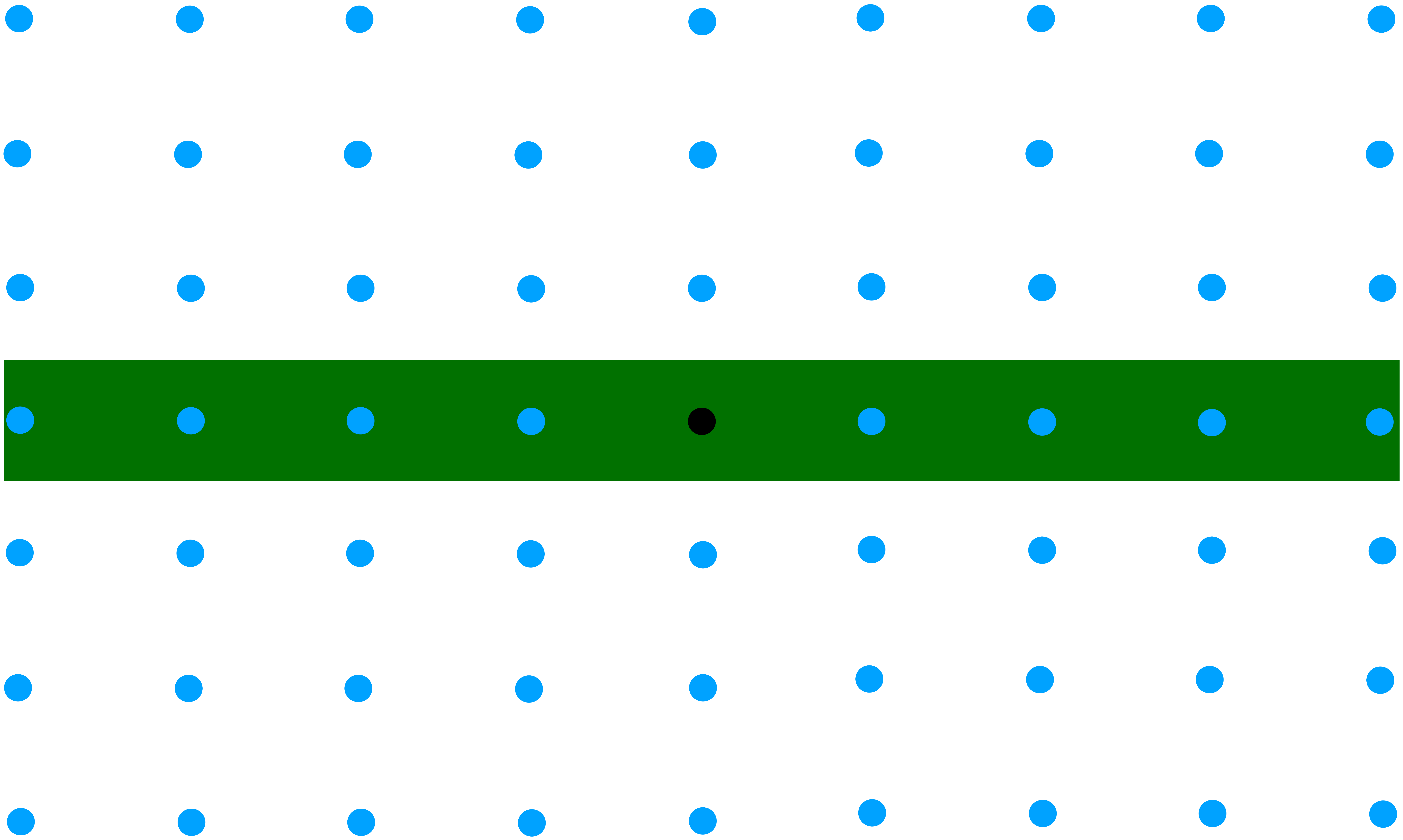


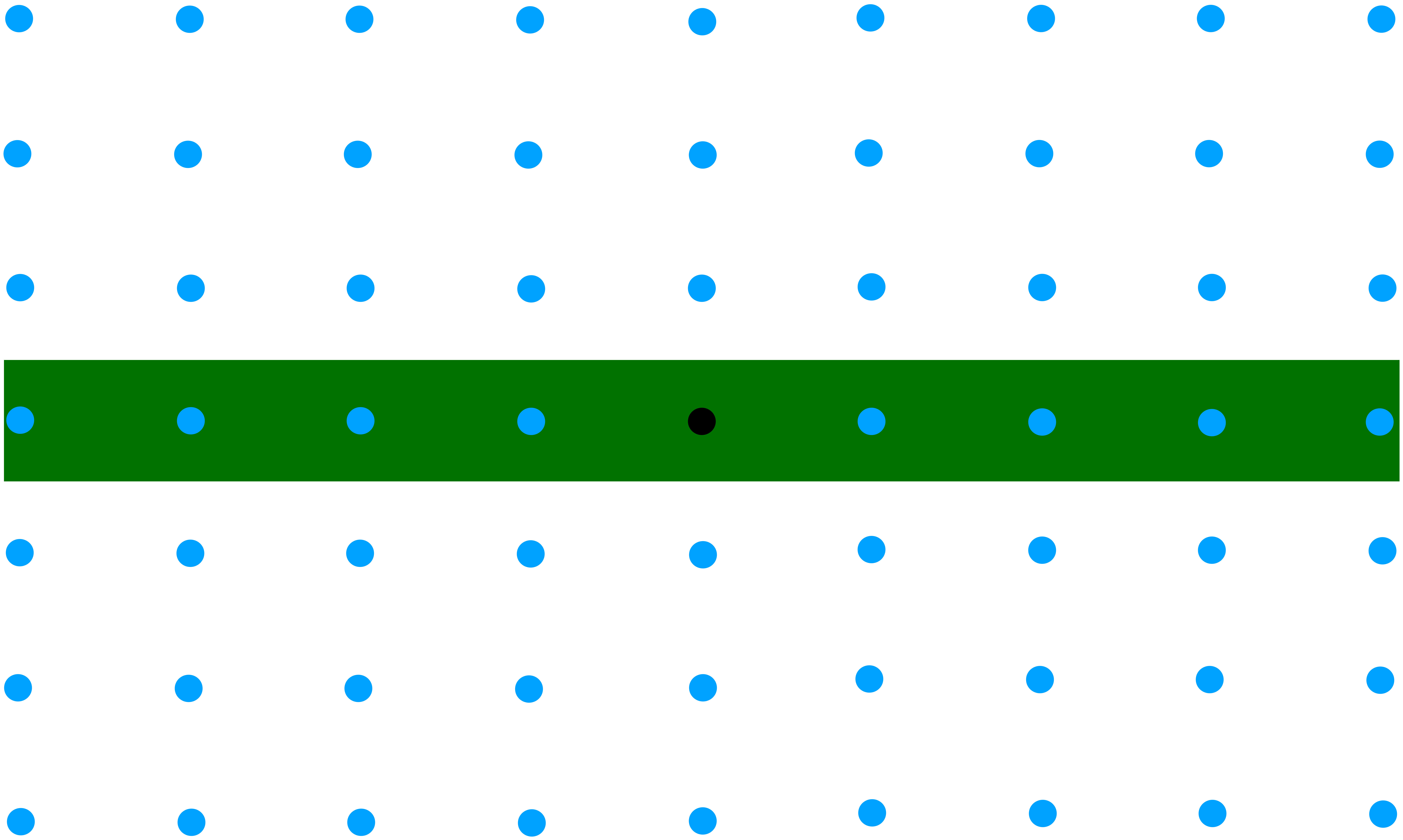


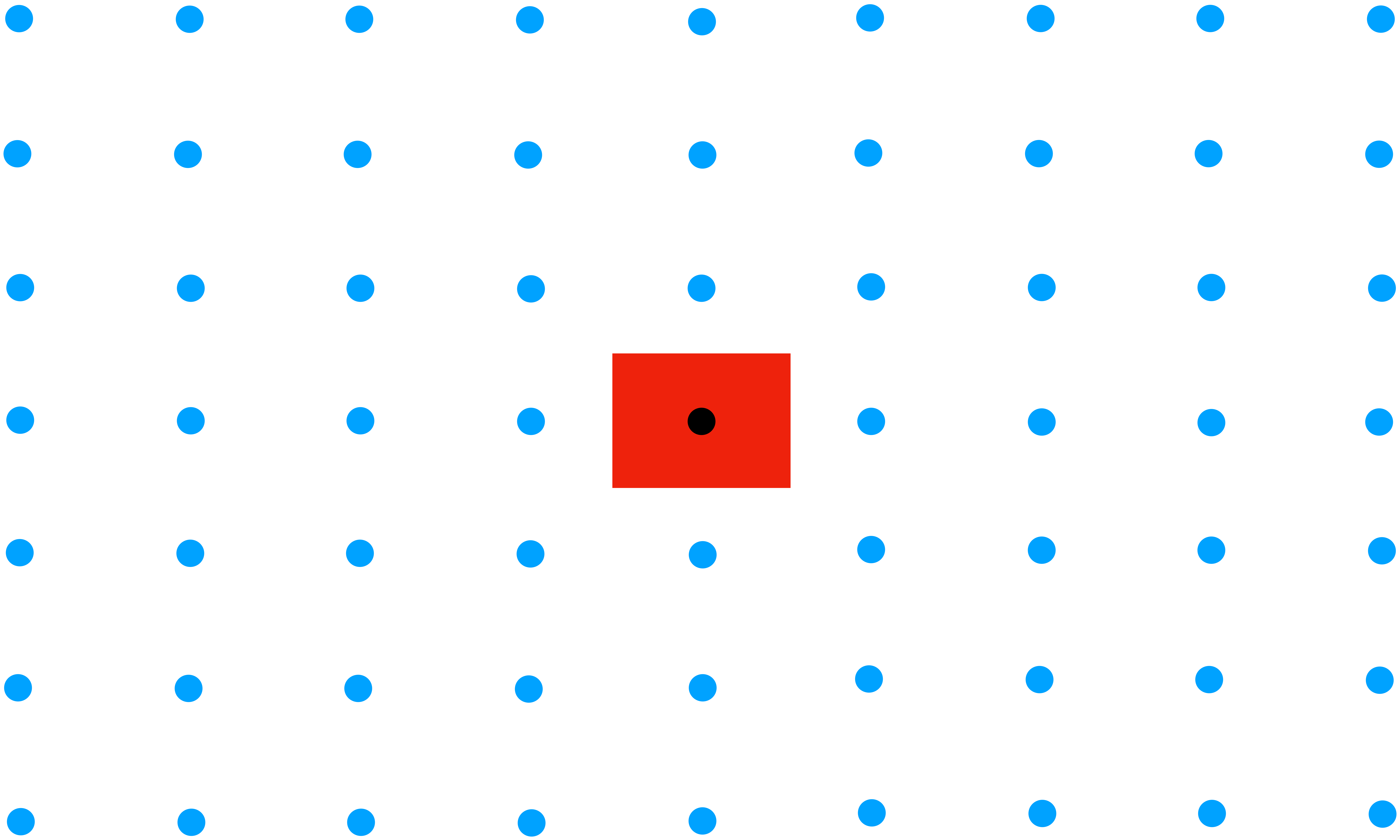


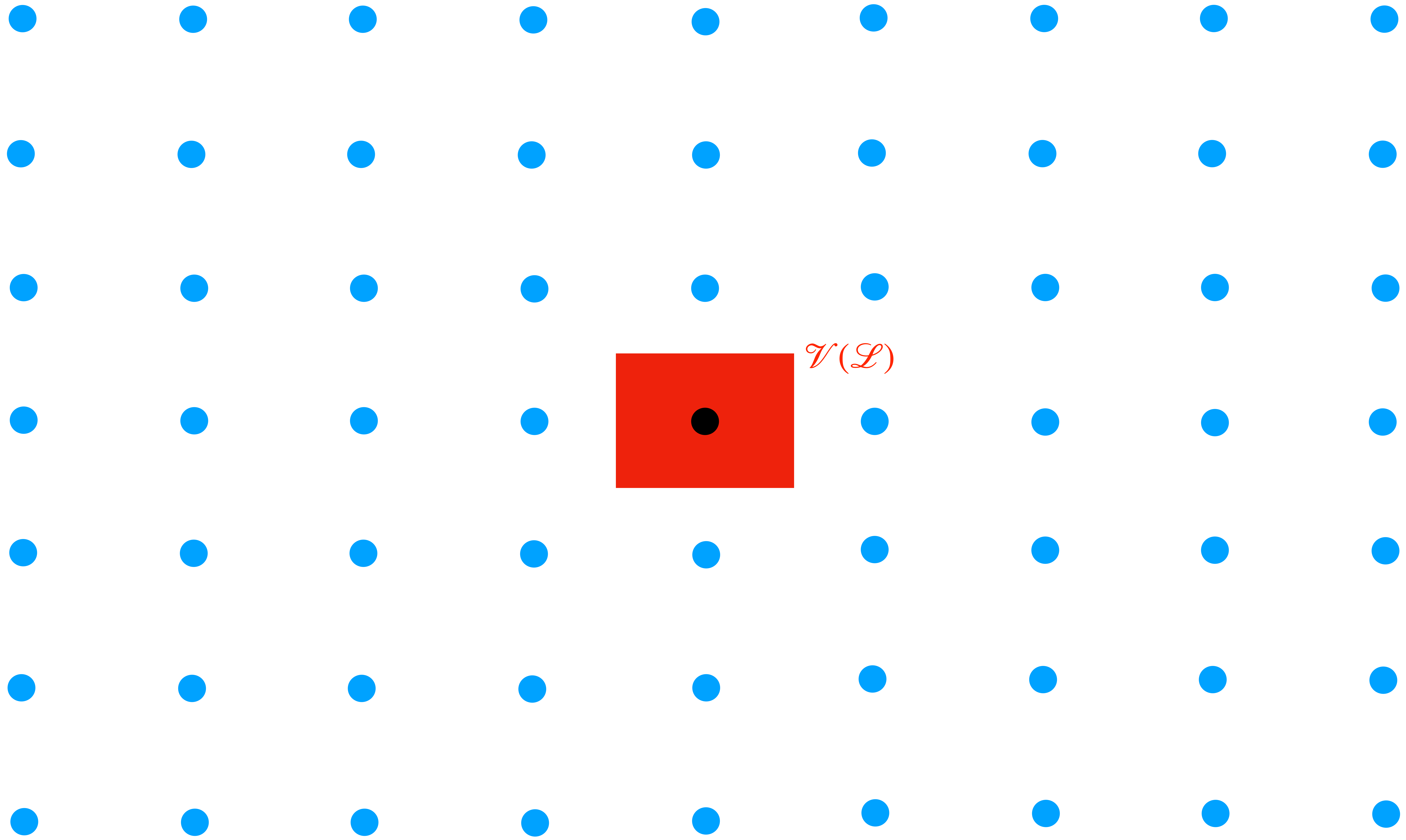


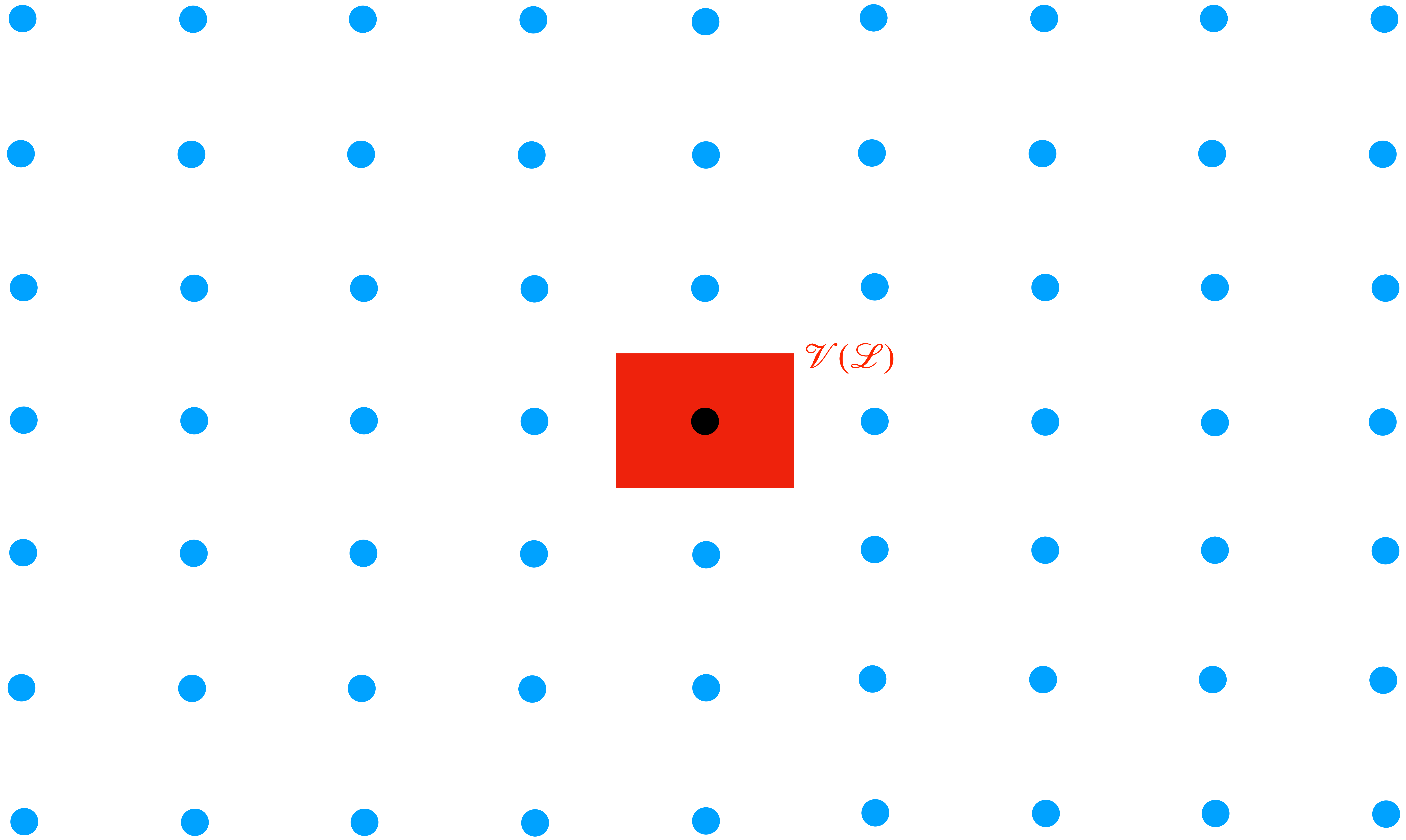









$\mathscr{V}(\mathscr{L})$


$\mathscr{V}(\mathscr{L})$

Extension Lemma

Preliminaries

Preliminaries

- $\mathbb{Z}^n$ is the lattice spanned by $\{e_1, e_2, \ldots, e_n\}$.

Preliminaries

- $\mathbb{Z}^n$ is the lattice spanned by $\{e_1, e_2, \ldots, e_n\}$.

- A vector v in a lattice $\mathscr{L}$ is primitive if $\forall k > 1, v/k \notin \mathscr{L}$.

Preliminaries

- $\mathbb{Z}^n$ is the lattice spanned by $\{e_1, e_2, \ldots, e_n\}$.
- A vector v in a lattice $\mathscr{L}$ is primitive if $\forall k > 1, v/k \notin \mathscr{L}$.
- B is a basis of $\mathbb{Z}^n \iff B$ is unimodular.
  ($BC = I \implies det(B)det(C) = 1$. But, both
  $B, C \in \mathbb{Z}^{n \times n} \implies det(B) = \pm 1$).

Main Theorem

Main Theorem

Let $v \in \mathbb{Z}^n$ be a primitive vector such that $||v||^2 > 1$. Then, there exists a unimodular matrix $B = \{b_1, b_2, \ldots, b_n\}$ such that $b_n = v$ and $||v||^2 > ||b_i||^2, \forall i \in [n-1]$.

Proof of Main Theorem

Proof of Main Theorem

- Case 1: $n = 2$

Proof of Main Theorem

- Case 1: n = 2
  - $v = [a, b]$. Consider $b_1 = [-d, c]$ such that $c \,.\, a + b \,.\, d = 1$.

Proof of Main Theorem

- Case 1: n = 2
  - $v = [a, b]$. Consider $b_1 = [-d, c]$ such that $c \,.\, a + b \,.\, d = 1$.
  - $B = [b_1, v]$ is unimodular.

Proof of Main Theorem

- Case 1: n = 2
  - $v = [a, b]$. Consider $b_1 = [-d, c]$ such that $c \,.\, a + b \,.\, d = 1$.
  - $B = [b_1, v]$ is unimodular.
  - We can find c, d such that $|c| < |b|, |d| < |a|$.

Proof of Main Theorem

Proof of Main Theorem

- Case 2: v has at least one component as 0.

Proof of Main Theorem

- Case 2: v has at least one component as 0.
  - WLOG, let $v_n = 0$

Proof of Main Theorem

- Case 2: v has at least one component as 0.
  - WLOG, let $v_n = 0$
  - Consider $b'_n = [v_1, v_2, \ldots, v_{n-1}]$

Proof of Main Theorem

- Case 2: v has at least one component as 0.
  - WLOG, let $v_n = 0$
  - Consider $b'_n = [v_1, v_2, \ldots, v_{n-1}]$
  - From induction hypothesis, there exists $B' = [b'_2, \ldots, b'_n]$ such that $||b'_i||^2 < ||b'_n||^2 = ||v||^2, 2 \leq i \leq n-1.$

Proof of Main Theorem

- Case 2: v has at least one component as 0.
  - WLOG, let $v_n = 0$
  - Consider $b'_n = [v_1, v_2, \ldots, v_{n-1}]$
  - From induction hypothesis, there exists $B' = [b'_2, \ldots, b'_n]$ such that $||b'_i||^2 < ||b'_n||^2 = ||v||^2, 2 \leq i \leq n-1.$
  - $B = \begin{bmatrix} 0 & B' \\ 1 & 0 \end{bmatrix}$

Proof of Main Theorem

Proof of Main Theorem

- Case 3: v has at least one component as 1.

Proof of Main Theorem

- Case 3: v has at least one component as 1.
  - WLOG, let $v_n = 1$

Proof of Main Theorem

- Case 3: v has at least one component as 1.
  - WLOG, let $v_n = 1$
  - $B = [e_1, \dots, e_{n-1}, v]$

Proof of Main Theorem

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.

  - $v = [v_n, v_{n-1}, \ldots, v_1]$ and $d_i = gcd(v_1, v_2, \ldots, v_i)$

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
  - $v = [v_n, v_{n-1}, \ldots, v_1]$ and $d_i = gcd(v_1, v_2, \ldots, v_i)$
  - Let $r_i, s_i \in \mathbb{Z}$ such that $r_i v_i + s_i d_{i-1} = d_i$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
  - $v = [v_n, v_{n-1}, \ldots, v_1]$ and $d_i = gcd(v_1, v_2, \ldots, v_i)$
  - Let $r_i, s_i \in \mathbb{Z}$ such that $r_i v_i + s_i d_{i-1} = d_i$.
  - Let $T_2 = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \ldots & r_2 & s_2 \\ 0 & 0 & \ldots & -d_1/d_2 & v_2/d_2 \end{bmatrix}$ where $d_1 = v_1$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
  - $v = [v_n, v_{n-1}, \ldots, v_1]$ and $d_i = gcd(v_1, v_2, \ldots, v_i)$
  - Let $r_i, s_i \in \mathbb{Z}$ such that $r_i v_i + s_i d_{i-1} = d_i$.
  - Let $T_2 = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \ldots & r_2 & s_2 \\ 0 & 0 & \ldots & -d_1/d_2 & v_2/d_2 \end{bmatrix}$ where $d_1 = v_1$.
  - $T_2 v = [v_n, v_{n-1}, \ldots, d_2, 0]^T$

Proof of Main Theorem

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
  - Similarly, we can construct T_i using v_i, s_i, d_i, d_{i-1} such that $T_n T_{n-1} \dots T_2 v = e_1$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
  - Similarly, we can construct T_i using v_i, s_i, d_i, d_{i-1} such that $T_n T_{n-1} \dots T_2 v = e_1$.
  - $v = T_2^{-1} \dots, T_{n-1}^{-1} T_n^{-1} e_1$

Proof of Main Theorem

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.

Proof of Main Theorem

- Case 4: $v_i \notin \{-1,0,1\}$.
- $$B = T_2^{-1}\ldots, T_{n-1}^{-1}T_n^{-1} = \begin{bmatrix} v_n & -s_n & 0 & \ldots & 0 & 0 \\ v_{n-1} & \frac{v_{n-1}r_n}{d_{n-1}} & -s_{n-1} & \ldots & 0 & 0 \\ v_{n-2} & \frac{v_{n-2}r_n}{d_{n-1}} & \frac{v_{n-2}r_{n-1}}{d_{n-2}} & \ldots & 0 & 0 \\ \vdots & & & & & \\ v_2 & \frac{v_2r_n}{d_{n-1}} & \frac{v_2r_{n-1}}{d_{n-2}} & \ldots & \frac{v_2r_3}{d_2} & -s_2 \\ v_1 & \frac{v_1r_n}{d_{n-1}} & \frac{v_1r_{n-1}}{d_{n-2}} & \ldots & \frac{v_1r_3}{d_2} & r_2 \end{bmatrix}$$

Successive Minima from Voronoi Relevant Vectors

Main theorem

Main theorem

Let $S = \{s_1, \ldots, s_n\}$ be a set of linearly independent lattice vector in a lattice $\mathscr{L}$ such that $||s_i|| = \lambda_i(\mathscr{L})$, then S is a subset of the set of Voronoi relevant vectors $V(\mathscr{L})$ of $\mathscr{L}$.

Main theorem

Let $S = \{s_1, \ldots, s_n\}$ be a set of linearly independent lattice vector in a lattice $\mathscr{L}$ such that $||s_i|| = \lambda_i(\mathscr{L})$, then S is a subset of the set of Voronoi relevant vectors $V(\mathscr{L})$ of $\mathscr{L}$.

Given a basis $B = \{b_1, \ldots, b_n\}$, the **Successive Minima Problem (SMP)** ask for n linearly independent vectors $\{s_1, \ldots, s_n\} \subseteq \mathscr{L}(B)$ such that $||s_i|| = \lambda_i(\mathscr{L}(B))$.

Corollaries

Corollaries

1) For any lattice $\mathscr{L}$

$$\lambda_n(\mathscr{L}) \leq ||V(\mathscr{L})|| \leq \frac{n^{3/2}}{2}\lambda_n(\mathscr{L})$$

Corollaries

1) For any lattice $\mathscr{L}$

$$\lambda_n(\mathscr{L}) \leq ||V(\mathscr{L})|| \leq \frac{n^{3/2}}{2}\lambda_n(\mathscr{L})$$

2) We can modify the algorithm given by Micciancio and Voulgaris to find a solution to SMP without using CVP oracles.

Conclusion

Conclusion

- We looked into the definition of lattice, lattice problems and Voronoi cell and vectors.

Conclusion

- We looked into the definition of lattice, lattice problems and Voronoi cell and vectors.
- We showed how to construct a basis for $\mathbb{Z}^n$ from a primitive vector v such that the rest of the basis vectors are strictly shorter than v.

Conclusion

- We looked into the definition of lattice, lattice problems and Voronoi cell and vectors.
- We showed how to construct a basis for $\mathbb{Z}^n$ from a primitive vector v such that the rest of the basis vectors are strictly shorter than v.
- Discussed that a solution to SMP is contained in the set of Voronoi relevant vectors.

Conclusion

- We looked into the definition of lattice, lattice problems and Voronoi cell and vectors.
- We showed how to construct a basis for $\mathbb{Z}^n$ from a primitive vector v such that the rest of the basis vectors are strictly shorter than v.
- Discussed that a solution to SMP is contained in the set of Voronoi relevant vectors.
- Is it possible to extend $v_1, v_2, \ldots, v_k$ to a basis $[v_1, \ldots, v_k, b_{k+1}, \ldots, b_n]$ of $\mathbb{Z}^n$ such that every b_i's are strictly shorter than the longest v_j.

Thank You !

Proof for an SMP solution is a subset of $V(\mathscr{L})$

Proof for an SMP solution is a subset of $V(\mathscr{L})$

- v is a Voronoi relevant vector of $\mathscr{L} \iff \pm v$ are the only shortest vectors in $v + 2\mathscr{L}$

Proof for an SMP solution is a subset of $V(\mathscr{L})$

- v is a Voronoi relevant vector of $\mathscr{L} \iff \pm v$ are the only shortest vectors in $v + 2\mathscr{L}$

- This implies that if v is not Voronoi relevant, then $\exists w \in \mathscr{L} \backslash \{0, v\}$ such that $||v/2 - w|| \leq ||v/2||$

Proof for an SMP solution is a subset of $V(\mathscr{L})$

- v is a Voronoi relevant vector of $\mathscr{L} \iff \pm v$ are the only shortest vectors in $v + 2\mathscr{L}$

- This implies that if v is not Voronoi relevant, then $\exists w \in \mathscr{L} \backslash \{0, v\}$ such that $||v/2 - w|| \leq ||v/2||$

- Let us first show that all shortest vector belongs to $V(\mathscr{L})$. Assume the contrary.

Proof for an SMP solution is a subset of $V(\mathscr{L})$

- v is a Voronoi relevant vector of $\mathscr{L} \iff \pm v$ are the only shortest vectors in $v + 2\mathscr{L}$

- This implies that if v is not Voronoi relevant, then $\exists w \in \mathscr{L} \backslash \{0, v\}$ such that $||v/2 - w|| \leq ||v/2||$

- Let us first show that all shortest vector belongs to $V(\mathscr{L})$. Assume the contrary.

  - $||s/2 - w|| < ||s/2|| \implies ||s - 2w|| < ||s||$

Proof for an SMP solution is a subset of $V(\mathscr{L})$

- v is a Voronoi relevant vector of $\mathscr{L} \iff \pm v$ are the only shortest vectors in $v + 2\mathscr{L}$
- This implies that if v is not Voronoi relevant, then $\exists w \in \mathscr{L} \setminus \{0, v\}$ such that $||v/2 - w|| \leq ||v/2||$
- Let us first show that all shortest vector belongs to $V(\mathscr{L})$. Assume the contrary.
  - $||s/2 - w|| < ||s/2|| \implies ||s - 2w|| < ||s||$
  - $||s/2 - w|| = ||s/2|| \implies cos(\theta) = ||w||/||s||$. Since, $||w|| \geq ||s|| \implies cos(\theta) \geq 1$. But, this implies $w = s$.

- Assume that $s_1, \ldots, s_{i-1} \in V(\mathscr{L})$ and $s_i \notin V(\mathscr{L})$ for some i.

- Assume that $s_1, \ldots, s_{i-1} \in V(\mathscr{L})$ and $s_i \notin V(\mathscr{L})$ for some i.

  - $||s_i - 2w|| < ||s_i||$: We can show that $s_i - 2w \in Span(s_1, \ldots, s_{i-1})$.
    $||w|| = ||w - s_i/2 + s_i/2|| < ||s_i|| \implies w \in Span(s_1, \ldots, s_{i-1})$.
    But, this implies that $s_i \in Span(s_1, \ldots, s_{i-1})$.

- Assume that $s_1, \ldots, s_{i-1} \in V(\mathscr{L})$ and $s_i \notin V(\mathscr{L})$ for some i.

  - $||s_i - 2w|| < ||s_i||$: We can show that $s_i - 2w \in Span(s_1, \ldots, s_{i-1})$.
    $||w|| = ||w - s_i/2 + s_i/2|| < ||s_i|| \implies w \in Span(s_1, \ldots, s_{i-1})$.
    But, this implies that $s_i \in Span(s_1, \ldots, s_{i-1})$.

  - $||s_i - 2w|| = ||s_i||$:
    $||w||^2 = < s_i, w > \implies cos(\theta) = ||w||/||s_i||$. $\theta \neq 0$, therefore
    $||s_i|| > ||w||$ and $w \in Span(s_1, \ldots, s_{i-1})$. Also,
    $||s_i - w||^2 = ||s_i||^2 - ||w||^2 < ||s_i||^2$. Therefore,
    $s_i - w \in Span(s_1, \ldots, s_{i-1}) \implies s_i \in Span(s_1, \ldots, s_{i-1})$.

Thanks again!