

Solving CVP with the Voronoi cell

The Micciancio–Voulgaris algorithm, following Section 3.3 of Divesh Aggarwal's notes

Setting

The Voronoi cell

Relevant vectors

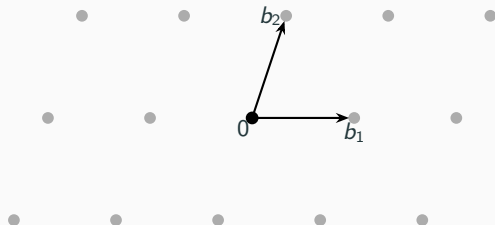
CVP given the relevant vectors

Computing the Voronoi cell

Setting

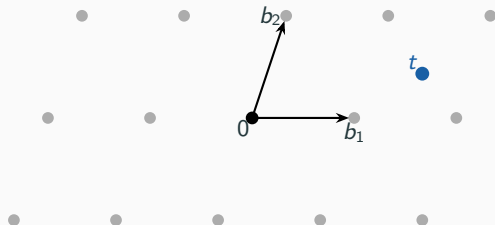
Closest Vector Problem

- A lattice $\mathcal{L} = \mathcal{L}(B)$, here $b_1 = (3, 0)$, $b_2 = (1, 3)$.



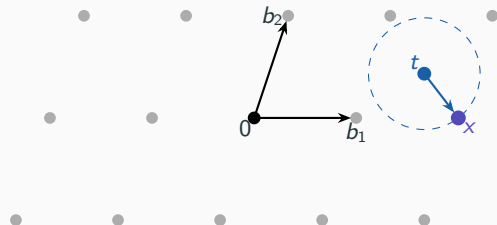
Closest Vector Problem

- A lattice $\mathcal{L} = \mathcal{L}(B)$, here $b_1 = (3, 0)$, $b_2 = (1, 3)$.
- A target $t \in \mathbb{R}^n$.



Closest Vector Problem

- A lattice $\mathcal{L} = \mathcal{L}(B)$, here $b_1 = (3, 0)$, $b_2 = (1, 3)$.
- A target $t \in \mathbb{R}^n$.
- Find $x \in \mathcal{L}$ minimising $\|t - x\|$.



What we are aiming for

- A *deterministic* algorithm running in time $2^{O(n)} \cdot \text{poly}(\text{input size})$.

What we are aiming for

- A *deterministic* algorithm running in time $2^{O(n)} \cdot \text{poly}(\text{input size})$.
- The notes derive $16^n \text{poly}(n)$; Micciancio–Voulgaris refine this to 4^n .

What we are aiming for

- A *deterministic* algorithm running in time $2^{O(n)} \cdot \text{poly}(\text{input size})$.
- The notes derive $16^n \text{poly}(n)$; Micciancio–Voulgaris refine this to 4^n .
- Assumptions, as in the notes: $\mathcal{L}$ is full rank, and $\mathcal{L} \subseteq \mathbb{Z}^n$.

1. **Geometry.** The Voronoi cell V is a polytope, described by at most 2^{n+1} *relevant vectors* $\mathcal{R}$.

The plan

1. **Geometry.** The Voronoi cell V is a polytope, described by at most 2^{n+1} *relevant vectors* $\mathcal{R}$.
2. **CVP given $\mathcal{R}$.** Walk the target into V by subtracting scaled relevant vectors.

The plan

1. **Geometry.** The Voronoi cell V is a polytope, described by at most 2^{n+1} *relevant vectors* $\mathcal{R}$.
2. **CVP given $\mathcal{R}$.** Walk the target into V by subtracting scaled relevant vectors.
3. **Computing $\mathcal{R}$.** Each relevant vector is a shortest vector of a coset of $2\mathcal{L}$: again CVP. Recurse on the rank.

The plan

1. **Geometry.** The Voronoi cell V is a polytope, described by at most 2^{n+1} *relevant vectors* $\mathcal{R}$.
2. **CVP given $\mathcal{R}$.** Walk the target into V by subtracting scaled relevant vectors.
3. **Computing $\mathcal{R}$.** Each relevant vector is a shortest vector of a coset of $2\mathcal{L}$: again CVP. Recurse on the rank.

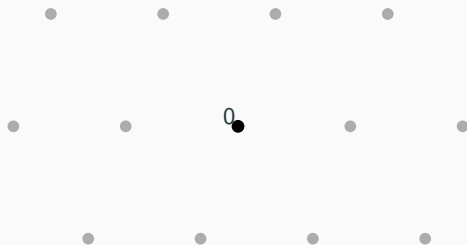
The idea in one line

CVP is *point location*: the cells tile space, and the answer is the centre of the cell containing t .

The Voronoi cell

Definition 3.3.1

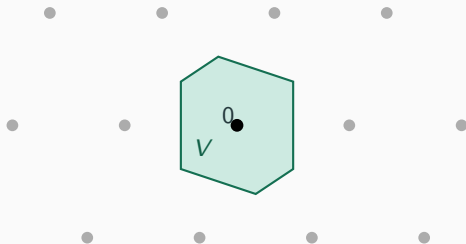
$$V = \{x : \|x\| \leq \|x - v\| \quad \forall v \in \mathcal{L} \setminus \{0\}\}$$



Definition 3.3.1

$$V = \{x : \|x\| \leq \|x - v\| \ \forall v \in \mathcal{L} \setminus \{0\}\}$$

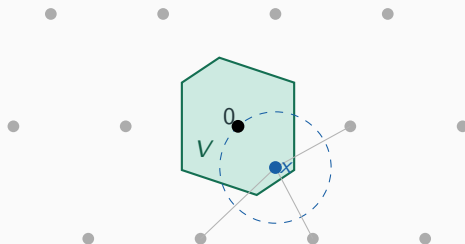
- Points whose closest lattice point is 0 (ties allowed).



Definition 3.3.1

$$V = \{x : \|x\| \leq \|x - v\| \ \forall v \in \mathcal{L} \setminus \{0\}\}$$

- Points whose closest lattice point is 0 (ties allowed).
- Equivalently: the ball around x through 0 has no lattice point inside.



Two facts we will use

- **The only lattice point in V is 0.**

Test the definition on v itself: $\|v\| \leq \|v - v\| = 0$.

Two facts we will use

- **The only lattice point in V is 0.**

Test the definition on v itself: $\|v\| \leq \|v - v\| = 0$.

- **V is symmetric:** $V = -V$.

$v \mapsto -v$ permutes $\mathcal{L} \setminus \{0\}$, so $\| -x \| \leq \| -x - v \|$ whenever $\|x\| \leq \|x + v\|$.

Definition 3.3.2: the half-space H_v

$$H_v = \{x : \|x\| \leq \|x - v\|\}$$



Definition 3.3.2: the half-space H_v

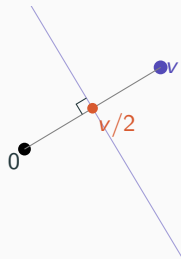
$$H_v = \{x : \|x\| \leq \|x - v\|\}$$

- Square and expand:

$$\|x - v\|^2 = \|x\|^2 - 2\langle x, v \rangle + \|v\|^2, \text{ so}$$

$$H_v = \{x : 2\langle x, v \rangle \leq \|v\|^2\}.$$

Boundary: the bisector of $[0, v]$.



Definition 3.3.2: the half-space H_v

$$H_v = \{x : \|x\| \leq \|x - v\|\}$$

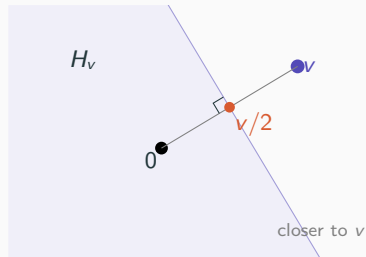
- Square and expand:

$$\|x - v\|^2 = \|x\|^2 - 2\langle x, v \rangle + \|v\|^2, \text{ so}$$

$$H_v = \{x : 2\langle x, v \rangle \leq \|v\|^2\}.$$

Boundary: the bisector of $[0, v]$.

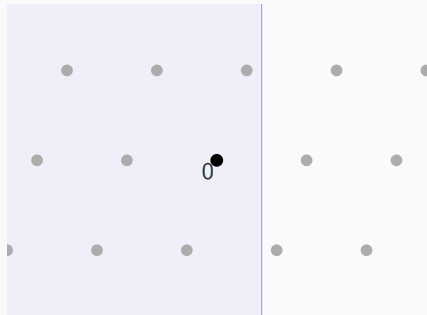
- A half-space: the side containing 0.



Remark 3.3.3: V is an intersection of half-spaces

$$V = \bigcap_{v \in \mathcal{L} \setminus \{0\}} H_v$$

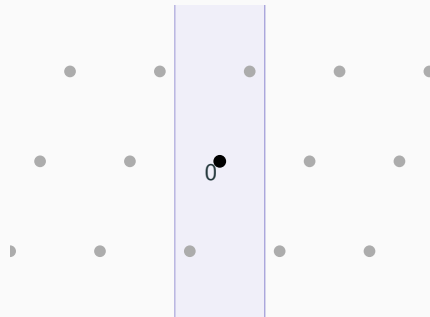
- Cut by H_{b_1} ,



Remark 3.3.3: V is an intersection of half-spaces

$$V = \bigcap_{v \in \mathcal{L} \setminus \{0\}} H_v$$

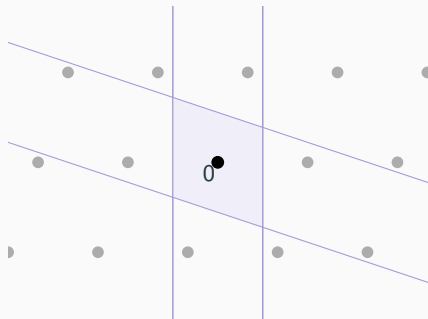
- Cut by H_{b_1} ,
- then by H_{-b_1} ,



Remark 3.3.3: V is an intersection of half-spaces

$$V = \bigcap_{v \in \mathcal{L} \setminus \{0\}} H_v$$

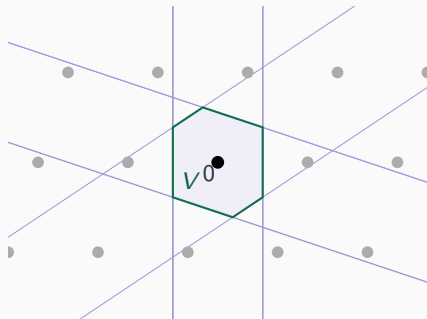
- Cut by H_{b_1} ,
- then by H_{-b_1} ,
- then by $H_{\pm b_2}$,



Remark 3.3.3: V is an intersection of half-spaces

$$V = \bigcap_{v \in \mathcal{L} \setminus \{0\}} H_v$$

- Cut by H_{b_1} ,
- then by H_{-b_1} ,
- then by $H_{\pm b_2}$,
- then by $H_{\pm(b_2-b_1)}$: the cell.



Remark 3.3.4: shape of V

- **Convex and closed:** an intersection of closed half-spaces.

Remark 3.3.4: shape of V

- **Convex and closed:** an intersection of closed half-spaces.
- **Symmetric** about 0.

Remark 3.3.4: shape of V

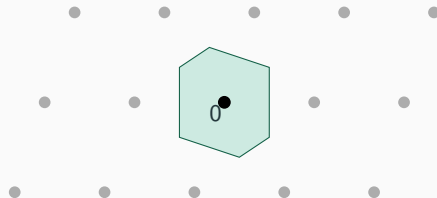
- **Convex and closed:** an intersection of closed half-spaces.
- **Symmetric** about 0.
- **Bounded:** the constraints from $\pm b_1, \dots, \pm b_n$ alone give $|\langle x, b_i \rangle| \leq \|b_i\|^2/2$, and the b_i span $\mathbb{R}^n$.

Remark 3.3.4: shape of V

- **Convex and closed:** an intersection of closed half-spaces.
- **Symmetric** about 0.
- **Bounded:** the constraints from $\pm b_1, \dots, \pm b_n$ alone give $|\langle x, b_i \rangle| \leq \|b_i\|^2/2$, and the b_i span $\mathbb{R}^n$.
- So V is a convex polytope. How many facets? That is the next section.

Remark 3.3.5: the cells tile $\mathbb{R}^n$

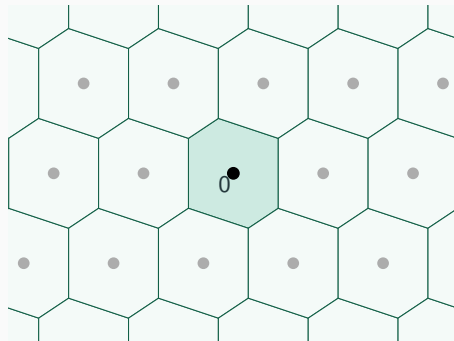
- V is the cell of 0.



Remark 3.3.5: the cells tile $\mathbb{R}^n$

- V is the cell of 0 .
- $u + V$ is the cell of u :

$$x \in u + V \iff \|x - u\| \leq \|x - w\| \quad \forall w \in \mathcal{L}.$$

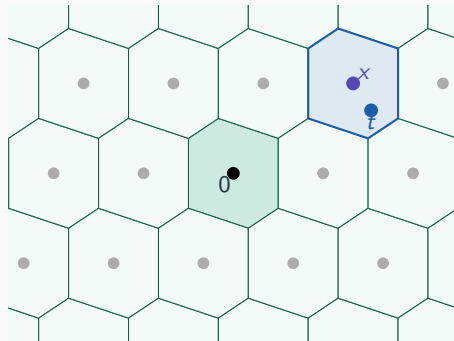


Remark 3.3.5: the cells tile $\mathbb{R}^n$

- V is the cell of 0 .
- $u + V$ is the cell of u :

$$x \in u + V \iff \|x - u\| \leq \|x - w\| \quad \forall w \in \mathcal{L}.$$

- Cells cover $\mathbb{R}^n$ and overlap only where there is a tie.



Reformulation (Remark 3.3.15)

x is a closest vector to $t \iff t \in x + V \iff t - x \in V.$

Reformulation (Remark 3.3.15)

x is a closest vector to $t \iff t \in x + V \iff t - x \in V.$

So the task is: **find the element of the coset $t - \mathcal{L}$ that lies in V** , and output $x = t - s$.

Reformulation (Remark 3.3.15)

x is a closest vector to $t \iff t \in x + V \iff t - x \in V.$

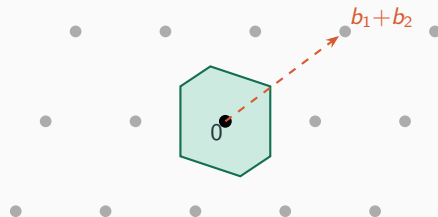
So the task is: **find the element of the coset $t - \mathcal{L}$ that lies in V** , and output $x = t - s$.

Everything that follows is about describing V by finitely many inequalities, and then walking s into it quickly.

Relevant vectors

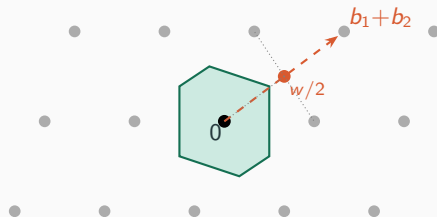
Most half-spaces are redundant

- Take $w = b_1 + b_2 = (4, 3)$.



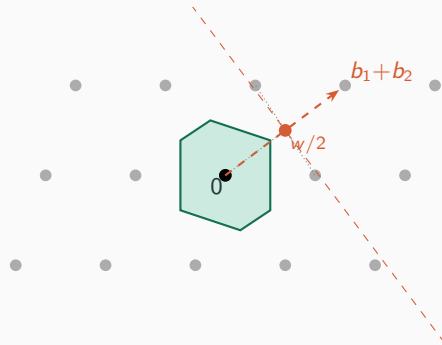
Most half-spaces are redundant

- Take $w = b_1 + b_2 = (4, 3)$.
- Its midpoint $w/2$ is closer to b_1 and b_2 (distance 1.80) than to 0 (distance 2.5).



Most half-spaces are redundant

- Take $w = b_1 + b_2 = (4, 3)$.
- Its midpoint $w/2$ is closer to b_1 and b_2 (distance 1.80) than to 0 (distance 2.5).
- So the bisector of w misses V : the constraint H_w is implied by others.



Definition 3.3.6: Voronoi relevant vectors

Definition

$v \neq 0$ is **relevant** if $\text{CVP}(v/2, \mathcal{L}) = \{0, v\}$: the set of *all* closest lattice points to $v/2$.

- 0 and v are always at distance $\|v\|/2$ from $v/2$: it lies on their bisector.

Definition 3.3.6: Voronoi relevant vectors

Definition

$v \neq 0$ is **relevant** if $\text{CVP}(v/2, \mathcal{L}) = \{0, v\}$: the set of *all* closest lattice points to $v/2$.

- 0 and v are always at distance $\|v\|/2$ from $v/2$: it lies on their bisector.
- So the condition says: *no other lattice point is that close to $v/2$.*

Definition 3.3.6: Voronoi relevant vectors

Definition

$v \neq 0$ is **relevant** if $\text{CVP}(v/2, \mathcal{L}) = \{0, v\}$: the set of *all* closest lattice points to $v/2$.

- 0 and v are always at distance $\|v\|/2$ from $v/2$: it lies on their bisector.
- So the condition says: *no other lattice point is that close to $v/2$.*
- Picture: the bisector of v meets V in a whole facet.

Only a third point can spoil relevance

- The reflection $u \mapsto v - u$ maps $\mathcal{L}$ to $\mathcal{L}$, fixes $v/2$, and preserves distance to $v/2$.

Only a third point can spoil relevance

- The reflection $u \mapsto v - u$ maps $\mathcal{L}$ to $\mathcal{L}$, fixes $v/2$, and preserves distance to $v/2$.
- So $\text{CVP}(v/2, \mathcal{L})$ is closed under it, and it swaps 0 and v : the sets $\{0\}$ and $\{v\}$ alone are impossible.

Only a third point can spoil relevance

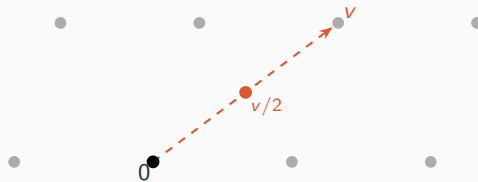
- The reflection $u \mapsto v - u$ maps $\mathcal{L}$ to $\mathcal{L}$, fixes $v/2$, and preserves distance to $v/2$.
- So $\text{CVP}(v/2, \mathcal{L})$ is closed under it, and it swaps 0 and v : the sets $\{0\}$ and $\{v\}$ alone are impossible.
- Relevance fails exactly when some *third* lattice point is at distance $\leq \|v\|/2$ from $v/2$.

Only a third point can spoil relevance

- The reflection $u \mapsto v - u$ maps $\mathcal{L}$ to $\mathcal{L}$, fixes $v/2$, and preserves distance to $v/2$.
- So $\text{CVP}(v/2, \mathcal{L})$ is closed under it, and it swaps 0 and v : the sets $\{0\}$ and $\{v\}$ alone are impossible.
- Relevance fails exactly when some *third* lattice point is at distance $\leq \|v\|/2$ from $v/2$.
- Special case: if $v \in 2\mathcal{L}$ then $v/2 \in \mathcal{L}$ and $\text{CVP}(v/2) = \{v/2\}$. **Vectors in $2\mathcal{L}$ are never relevant.**

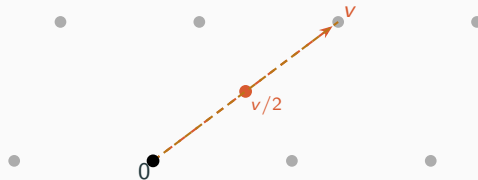
The reflection through $v/2$

- $\rho(u) = v - u$: in 2D, rotation by 180° about $v/2$. Here $v = b_1 + b_2$, $v/2 = (2, 1.5)$.



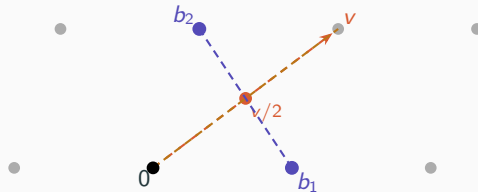
The reflection through $v/2$

- $\rho(u) = v - u$: in 2D, rotation by 180° about $v/2$. Here $v = b_1 + b_2$, $v/2 = (2, 1.5)$.
- ρ swaps 0 and v .



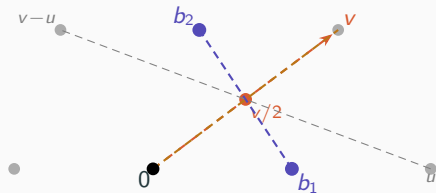
The reflection through $v/2$

- $\rho(u) = v - u$: in 2D, rotation by 180° about $v/2$. Here $v = b_1 + b_2$, $v/2 = (2, 1.5)$.
- ρ swaps 0 and v .
- It swaps b_1 and b_2 : $v - b_1 = b_2$.



The reflection through $v/2$

- $\rho(u) = v - u$: in 2D, rotation by 180° about $v/2$. Here $v = b_1 + b_2$, $v/2 = (2, 1.5)$.
- ρ swaps 0 and v .
- It swaps b_1 and b_2 : $v - b_1 = b_2$.
- In general it swaps u and $v - u$. Both are lattice points, since $u, v \in \mathcal{L}$.

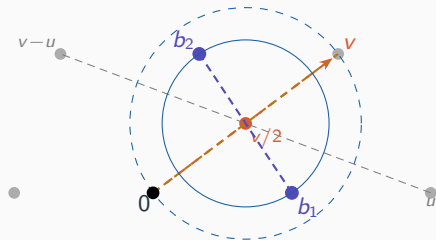


The reflection through $v/2$

- $\rho(u) = v - u$: in 2D, rotation by 180° about $v/2$. Here $v = b_1 + b_2$, $v/2 = (2, 1.5)$.
- ρ swaps 0 and v .
- It swaps b_1 and b_2 : $v - b_1 = b_2$.
- In general it swaps u and $v - u$. Both are lattice points, since $u, v \in \mathcal{L}$.
- It preserves distance to $v/2$:

$$\|(v - u) - \frac{v}{2}\| = \|u - \frac{v}{2}\|,$$

so circles centred at $v/2$ map to themselves.



Closest points to $v/2$ come in pairs

- **Step 1.** Take $u \in \text{CVP}(v/2, \mathcal{L})$. Then $\rho(u) = v - u$ is a lattice point at the *same* distance from $v/2$, so $\rho(u) \in \text{CVP}(v/2, \mathcal{L})$ too.
In words: ρ maps the set of closest points to itself.

Closest points to $v/2$ come in pairs

- **Step 1.** Take $u \in \text{CVP}(v/2, \mathcal{L})$. Then $\rho(u) = v - u$ is a lattice point at the *same* distance from $v/2$, so $\rho(u) \in \text{CVP}(v/2, \mathcal{L})$ too.
In words: ρ maps the set of closest points to itself.
- **Step 2.** $\rho(0) = v$ and $\rho(v) = 0$. With step 1:

$$0 \in \text{CVP}(v/2) \iff v \in \text{CVP}(v/2).$$

Closest points to $v/2$ come in pairs

- **Step 1.** Take $u \in \text{CVP}(v/2, \mathcal{L})$. Then $\rho(u) = v - u$ is a lattice point at the *same* distance from $v/2$, so $\rho(u) \in \text{CVP}(v/2, \mathcal{L})$ too.

In words: ρ maps the set of closest points to itself.

- **Step 2.** $\rho(0) = v$ and $\rho(v) = 0$. With step 1:

$$0 \in \text{CVP}(v/2) \iff v \in \text{CVP}(v/2).$$

- So 0 and v are *both* closest to $v/2$, or *neither* is. The answer can never be $\{0\}$ alone or $\{v\}$ alone.

Closest points to $v/2$ come in pairs

- **Step 1.** Take $u \in \text{CVP}(v/2, \mathcal{L})$. Then $\rho(u) = v - u$ is a lattice point at the *same* distance from $v/2$, so $\rho(u) \in \text{CVP}(v/2, \mathcal{L})$ too.
In words: ρ maps the set of closest points to itself.

- **Step 2.** $\rho(0) = v$ and $\rho(v) = 0$. With step 1:

$$0 \in \text{CVP}(v/2) \iff v \in \text{CVP}(v/2).$$

- So 0 and v are *both* closest to $v/2$, or *neither* is. The answer can never be $\{0\}$ alone or $\{v\}$ alone.
- More generally, the closest points to $v/2$ come in pairs $\{u, v - u\}$.

What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.

What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.
- So $\text{CVP}(v/2) = \{0, v\}$ fails only because of a **third** lattice point $u \notin \{0, v\}$ with $\|u - v/2\| \leq \|v\|/2$.

What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.
- So $\text{CVP}(v/2) = \{0, v\}$ fails only because of a **third** lattice point $u \notin \{0, v\}$ with $\|u - v/2\| \leq \|v\|/2$.
- Two ways:

What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.
- So $\text{CVP}(v/2) = \{0, v\}$ fails only because of a **third** lattice point $u \notin \{0, v\}$ with $\|u - v/2\| \leq \|v\|/2$.
- Two ways:
 - u strictly closer: then *neither* 0 nor v is in $\text{CVP}(v/2)$;

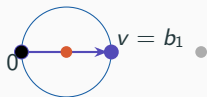
What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.
- So $\text{CVP}(v/2) = \{0, v\}$ fails only because of a **third** lattice point $u \notin \{0, v\}$ with $\|u - v/2\| \leq \|v\|/2$.
- Two ways:
 - u strictly closer: then *neither* 0 nor v is in $\text{CVP}(v/2)$;
 - u tied: then $\text{CVP}(v/2)$ is strictly larger than $\{0, v\}$.

What this means for Definition 3.3.6

- 0 and v are always at the same distance $\|v\|/2$ from $v/2$.
- So $\text{CVP}(v/2) = \{0, v\}$ fails only because of a **third** lattice point $u \notin \{0, v\}$ with $\|u - v/2\| \leq \|v\|/2$.
- Two ways:
 - u strictly closer: then *neither* 0 nor v is in $\text{CVP}(v/2)$;
 - u tied: then $\text{CVP}(v/2)$ is strictly larger than $\{0, v\}$.
- In both cases u brings its partner $v - u$ along.

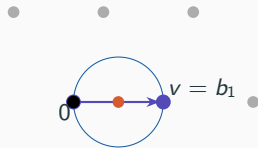
Examples



$v = b_1$: $\text{CVP}(v/2) = \{0, b_1\}$,
one pair, which is $\{0, v\}$ itself.

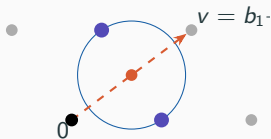
Relevant.

Examples



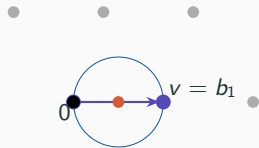
$v = b_1$: $\text{CVP}(v/2) = \{0, b_1\}$,
one pair, which is $\{0, v\}$ itself.

Relevant.



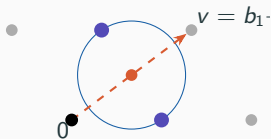
$v = b_1 + b_2$:
 $\text{CVP}(v/2) = \{b_1, b_2\}$, one pair.
 0 and v are both absent. **Not relevant.**

Examples

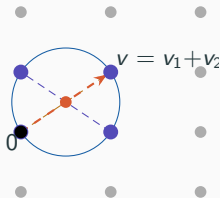


$v = b_1$: $\text{CVP}(v/2) = \{0, b_1\}$,
one pair, which is $\{0, v\}$ itself.

Relevant.



$v = b_1 + b_2$:
 $\text{CVP}(v/2) = \{b_1, b_2\}$, one pair.
 0 and v are both absent. **Not relevant.**



Square-like lattice, $v = v_1 + v_2$:
 $\text{CVP}(v/2) = \{0, v_1, v_2, v_1 + v_2\}$,
two pairs $\{0, v\}$ and $\{v_1, v_2\}$, all
tied. **Not relevant.**

The one exception: a fixed point

- ρ fixes exactly one point: $u = v/2$.

The one exception: a fixed point

- ρ fixes exactly one point: $u = v/2$.
- It is a lattice point exactly when $v \in 2\mathcal{L}$.

The one exception: a fixed point

- ρ fixes exactly one point: $u = v/2$.
- It is a lattice point exactly when $v \in 2\mathcal{L}$.
- Then $v/2$ is at distance 0 from itself, so $\text{CVP}(v/2) = \{v/2\}$: a set of size one, which is not a pair.

The one exception: a fixed point

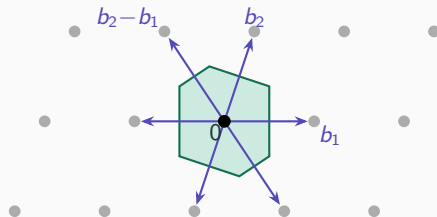
- ρ fixes exactly one point: $u = v/2$.
- It is a lattice point exactly when $v \in 2\mathcal{L}$.
- Then $v/2$ is at distance 0 from itself, so $\text{CVP}(v/2) = \{v/2\}$: a set of size one, which is not a pair.
- Example: $v = 2b_1 = (6, 0)$, $v/2 = b_1$, $\text{CVP}(v/2) = \{b_1\}$.

The one exception: a fixed point

- ρ fixes exactly one point: $u = v/2$.
- It is a lattice point exactly when $v \in 2\mathcal{L}$.
- Then $v/2$ is at distance 0 from itself, so $\text{CVP}(v/2) = \{v/2\}$: a set of size one, which is not a pair.
- Example: $v = 2b_1 = (6, 0)$, $v/2 = b_1$, $\text{CVP}(v/2) = \{b_1\}$.
- **Vectors in $2\mathcal{L}$ are never relevant.** This is used again in Lemma 3.3.9.

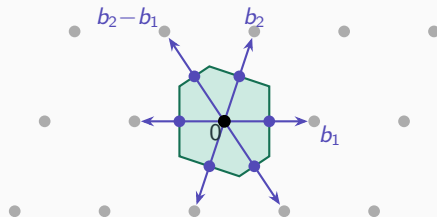
Where can the midpoint land?

- **Inside a facet of V :** only $0, v$ closest.
Relevant. Here $\pm b_1, \pm b_2, \pm(b_2 - b_1)$.



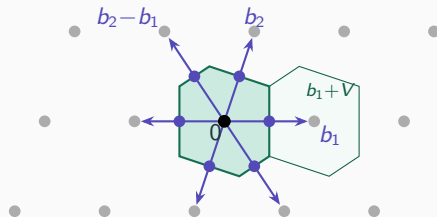
Where can the midpoint land?

- **Inside a facet of V :** only $0, v$ closest.
Relevant. Here $\pm b_1, \pm b_2, \pm(b_2 - b_1)$.
- Their midpoints $v/2$ are the facet centres.



Where can the midpoint land?

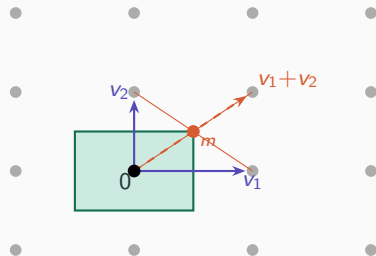
- **Inside a facet of V :** only $0, v$ closest.
Relevant. Here $\pm b_1, \pm b_2, \pm(b_2 - b_1)$.
- Their midpoints $v/2$ are the facet centres.
- Facet between the cells of 0 and b_1 :
the two cells are neighbours.



Example 3.3.7: the other two cases

Square-like lattice, $v_1 \perp v_2$:

- v_1, v_2 are relevant.



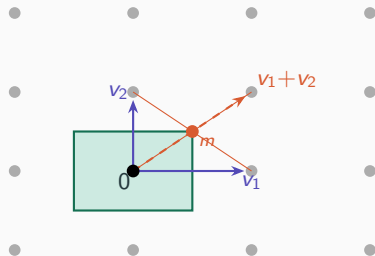
Example 3.3.7: the other two cases

Square-like lattice, $v_1 \perp v_2$:

- v_1, v_2 are relevant.
- $m = (v_1 + v_2)/2$ is a *corner* of V , equidistant from $0, v_1, v_2, v_1 + v_2$:

$$\text{CVP}(m) = \{0, v_1, v_2, v_1 + v_2\},$$

so $v_1 + v_2$ is not relevant (tie on a lower-dimensional face).



Example 3.3.7: the other two cases

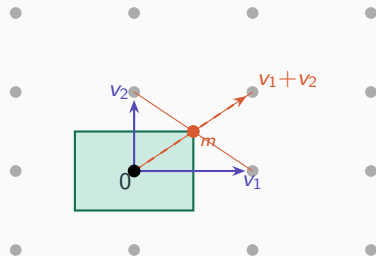
Square-like lattice, $v_1 \perp v_2$:

- v_1, v_2 are relevant.
- $m = (v_1 + v_2)/2$ is a *corner* of V , equidistant from $0, v_1, v_2, v_1 + v_2$:

$$\text{CVP}(m) = \{0, v_1, v_2, v_1 + v_2\},$$

so $v_1 + v_2$ is not relevant (tie on a lower-dimensional face).

- Earlier slide: $b_1 + b_2$, midpoint strictly outside V .



Lemma 3.3.8

Lemma 3.3.8

$V = \bigcap_{v \in \mathcal{R}} H_v$, where $\mathcal{R}$ is the set of relevant vectors.

- With Lemma 3.3.9 ($|\mathcal{R}| \leq 2^{n+1}$): V has a *finite* description.

Lemma 3.3.8

Lemma 3.3.8

$V = \bigcap_{v \in \mathcal{R}} H_v$, where $\mathcal{R}$ is the set of relevant vectors.

- With Lemma 3.3.9 ($|\mathcal{R}| \leq 2^{n+1}$): V has a *finite* description.
- Membership test: $x \in V \iff 2\langle x, v \rangle \leq \|v\|^2$ for all $v \in \mathcal{R}$. This is how Algorithm 7 tests “ $s \in V$ ”.

Lemma 3.3.8

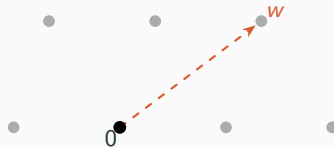
Lemma 3.3.8

$V = \bigcap_{v \in \mathcal{R}} H_v$, where $\mathcal{R}$ is the set of relevant vectors.

- With Lemma 3.3.9 ($|\mathcal{R}| \leq 2^{n+1}$): V has a *finite* description.
- Membership test: $x \in V \iff 2\langle x, v \rangle \leq \|v\|^2$ for all $v \in \mathcal{R}$. This is how Algorithm 7 tests “ $s \in V$ ”.
- To prove: every non-relevant H_w is implied by the relevant ones.

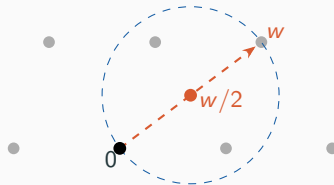
Proof, step 1: two shorter witnesses

- Let $w \neq 0$ be non-relevant.



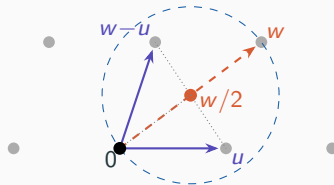
Proof, step 1: two shorter witnesses

- Let $w \neq 0$ be non-relevant.
- Then some $u \in \text{CVP}(w/2)$ has $u \notin \{0, w\}$, so $\|u - w/2\| \leq \|w\|/2$: u lies in the ball with diameter $[0, w]$.



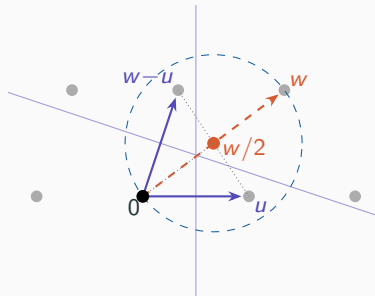
Proof, step 1: two shorter witnesses

- Let $w \neq 0$ be non-relevant.
- Then some $u \in \text{CVP}(w/2)$ has $u \notin \{0, w\}$, so $\|u - w/2\| \leq \|w\|/2$: u lies in the ball with diameter $[0, w]$.
- By the reflection, $w - u$ is there too, and also $\notin \{0, w\}$.



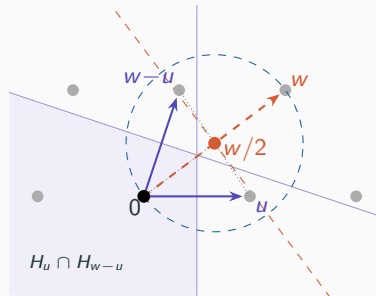
Proof, step 1: two shorter witnesses

- Let $w \neq 0$ be non-relevant.
- Then some $u \in \text{CVP}(w/2)$ has $u \notin \{0, w\}$, so $\|u - w/2\| \leq \|w\|/2$: u lies in the ball with diameter $[0, w]$.
- By the reflection, $w - u$ is there too, and also $\notin \{0, w\}$.



Proof, step 1: two shorter witnesses

- Let $w \neq 0$ be non-relevant.
- Then some $u \in \text{CVP}(w/2)$ has $u \notin \{0, w\}$, so $\|u - w/2\| \leq \|w\|/2$: u lies in the ball with diameter $[0, w]$.
- By the reflection, $w - u$ is there too, and also $\notin \{0, w\}$.



Proof, step 2: the key inequality

- From $\|u - w/2\|^2 \leq \|w/2\|^2$: $\|u\|^2 \leq \langle u, w \rangle$.

Proof, step 2: the key inequality

- From $\|u - w/2\|^2 \leq \|w/2\|^2$: $\|u\|^2 \leq \langle u, w \rangle$.
- Same for $w - u$: $\|w - u\|^2 \leq \langle w - u, w \rangle$.

Proof, step 2: the key inequality

- From $\|u - w/2\|^2 \leq \|w/2\|^2$: $\|u\|^2 \leq \langle u, w \rangle$.
- Same for $w - u$: $\|w - u\|^2 \leq \langle w - u, w \rangle$.
- Adding: $\|u\|^2 + \|w - u\|^2 \leq \|w\|^2$

Proof, step 2: the key inequality

- From $\|u - w/2\|^2 \leq \|w/2\|^2$: $\|u\|^2 \leq \langle u, w \rangle$.
- Same for $w - u$: $\|w - u\|^2 \leq \langle w - u, w \rangle$.
- Adding: $\|u\|^2 + \|w - u\|^2 \leq \|w\|^2$
- Since $u \neq 0$ and $w - u \neq 0$: $\|u\| < \|w\|$ and $\|w - u\| < \|w\|$.

Proof, step 2: the key inequality

- From $\|u - w/2\|^2 \leq \|w/2\|^2$: $\|u\|^2 \leq \langle u, w \rangle$.
- Same for $w - u$: $\|w - u\|^2 \leq \langle w - u, w \rangle$.
- Adding: $\|u\|^2 + \|w - u\|^2 \leq \|w\|^2$
- Since $u \neq 0$ and $w - u \neq 0$: $\|u\| < \|w\|$ and $\|w - u\| < \|w\|$.

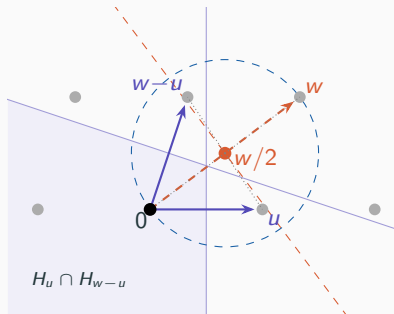
Geometric picture

$\|u\|^2 \leq \langle u, w \rangle$ says the angle at u in the triangle $0, u, w$ is at least 90° : Thales' ball again.

Proof, step 3: $H_u \cap H_{w-u} \subseteq H_w$

- Let $x \in H_u \cap H_{w-u}$:

$$2\langle x, u \rangle \leq \|u\|^2, \quad 2\langle x, w - u \rangle \leq \|w - u\|^2.$$



Proof, step 3: $H_u \cap H_{w-u} \subseteq H_w$

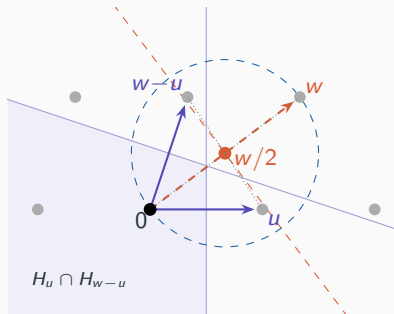
- Let $x \in H_u \cap H_{w-u}$:

$$2\langle x, u \rangle \leq \|u\|^2, \quad 2\langle x, w - u \rangle \leq \|w - u\|^2.$$

- Add them; the left sides give $2\langle x, w \rangle$:

$$2\langle x, w \rangle \leq \|u\|^2 + \|w - u\|^2 \leq \|w\|^2,$$

by step 2. So $x \in H_w$. $\square$



Proof, step 3: $H_u \cap H_{w-u} \subseteq H_w$

- Let $x \in H_u \cap H_{w-u}$:

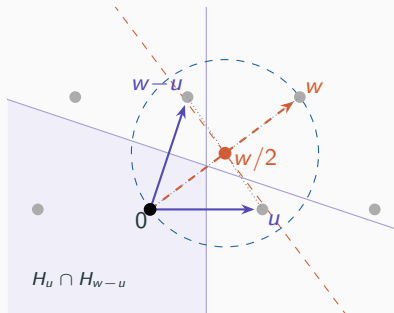
$$2\langle x, u \rangle \leq \|u\|^2, \quad 2\langle x, w - u \rangle \leq \|w - u\|^2.$$

- Add them; the left sides give $2\langle x, w \rangle$:

$$2\langle x, w \rangle \leq \|u\|^2 + \|w - u\|^2 \leq \|w\|^2,$$

by step 2. So $x \in H_w$. $\square$

- The shaded region lies entirely on 0's side of the red bisector.



Proof, step 4: why this finishes

Claim. If $x \in H_v$ for all $v \in \mathcal{R}$, then $x \in H_w$ for all $w \neq 0$.

- Induct on $\|w\|$. This is legitimate: a ball contains finitely many lattice vectors.

Proof, step 4: why this finishes

Claim. If $x \in H_v$ for all $v \in \mathcal{R}$, then $x \in H_w$ for all $w \neq 0$.

- Induct on $\|w\|$. This is legitimate: a ball contains finitely many lattice vectors.
- $w \in \mathcal{R}$: true by assumption.

Proof, step 4: why this finishes

Claim. If $x \in H_v$ for all $v \in \mathcal{R}$, then $x \in H_w$ for all $w \neq 0$.

- Induct on $\|w\|$. This is legitimate: a ball contains finitely many lattice vectors.
- $w \in \mathcal{R}$: true by assumption.
- $w \notin \mathcal{R}$: steps 1–2 give nonzero u , $w - u$, both shorter than w . By induction $x \in H_u \cap H_{w-u}$, and step 3 gives $x \in H_w$. $\square$

Proof, step 4: why this finishes

Claim. If $x \in H_v$ for all $v \in \mathcal{R}$, then $x \in H_w$ for all $w \neq 0$.

- Induct on $\|w\|$. This is legitimate: a ball contains finitely many lattice vectors.
- $w \in \mathcal{R}$: true by assumption.
- $w \notin \mathcal{R}$: steps 1–2 give nonzero u , $w - u$, both shorter than w . By induction $x \in H_u \cap H_{w-u}$, and step 3 gives $x \in H_w$. $\square$
- Also covers $w \in 2\mathcal{L}$: there $u = w - u = w/2$.

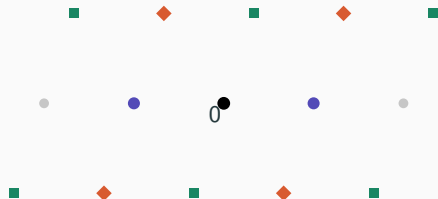
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.



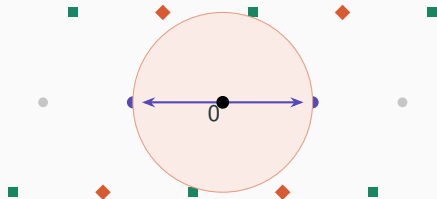
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.
- Here four classes; the grey one is $2\mathcal{L}$ itself.



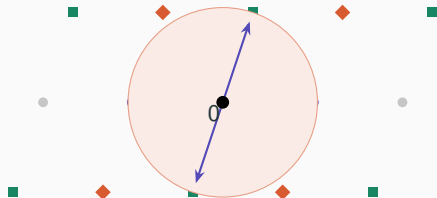
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.
- Here four classes; the grey one is $2\mathcal{L}$ itself.
- In each nonzero coset take the shortest vector v^* .



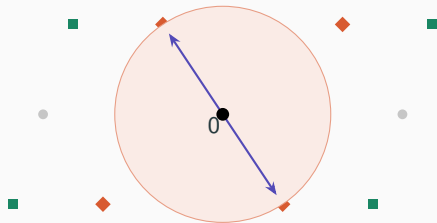
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.
- Here four classes; the grey one is $2\mathcal{L}$ itself.
- In each nonzero coset take the shortest vector v^* .



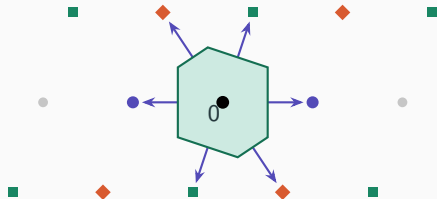
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.
- Here four classes; the grey one is $2\mathcal{L}$ itself.
- In each nonzero coset take the shortest vector v^* .



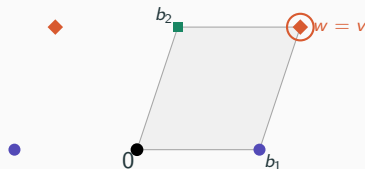
Lemma 3.3.9: at most 2^{n+1} relevant vectors

- Split $\mathcal{L}$ by parity of coefficients: the 2^n cosets of $2\mathcal{L}$.
- Here four classes; the grey one is $2\mathcal{L}$ itself.
- In each nonzero coset take the shortest vector v^* .
- Claim: only $\pm v^*$ can be relevant.
Here: exactly the six facets.



Proof of Lemma 3.3.9: setup

- $\mathcal{R}$ = the set of relevant vectors of $\mathcal{L}(B)$,
 $B = (b_1, \dots, b_n)$.



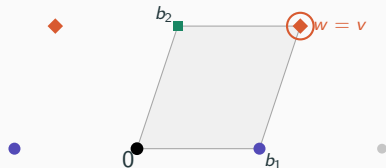
$\mathcal{P}(B)$ shaded. Its vertices $0, b_1, b_2, b_1 + b_2$ lie in the four cosets of $2\mathcal{L}$ (four shapes).

Proof of Lemma 3.3.9: setup

- $\mathcal{R}$ = the set of relevant vectors of $\mathcal{L}(B)$,
 $B = (b_1, \dots, b_n)$.
- The **vertices** of $\mathcal{P}(B)$: $v = \sum_i \alpha_i b_i$ with
 $\alpha \in \{0, 1\}^n$. There are 2^n of them.
- For each vertex v , let

$$v^* = \operatorname{argmin}\{\|x\| : x \in v + 2\mathcal{L}, x \neq 0\}$$

(any one, if there are ties).



$\mathcal{P}(B)$ shaded. Its vertices $0, b_1, b_2, b_1 + b_2$ lie in the four cosets of $2\mathcal{L}$ (four shapes).

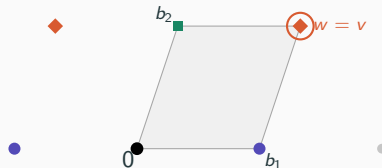
Proof of Lemma 3.3.9: setup

- $\mathcal{R}$ = the set of relevant vectors of $\mathcal{L}(B)$, $B = (b_1, \dots, b_n)$.
- The **vertices** of $\mathcal{P}(B)$: $v = \sum_i \alpha_i b_i$ with $\alpha \in \{0, 1\}^n$. There are 2^n of them.
- For each vertex v , let

$$v^* = \operatorname{argmin}\{\|x\| : x \in v + 2\mathcal{L}, x \neq 0\}$$

(any one, if there are ties).

- **Claim:** the vectors $\pm v^*$, over all vertices v , are the only possible relevant vectors.



$\mathcal{P}(B)$ shaded. Its vertices $0, b_1, b_2, b_1 + b_2$ lie in the four cosets of $2\mathcal{L}$ (four shapes).

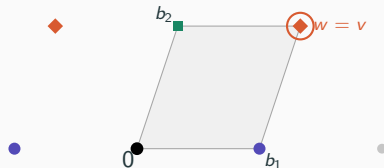
Proof of Lemma 3.3.9: setup

- $\mathcal{R}$ = the set of relevant vectors of $\mathcal{L}(B)$,
 $B = (b_1, \dots, b_n)$.
- The **vertices** of $\mathcal{P}(B)$: $v = \sum_i \alpha_i b_i$ with
 $\alpha \in \{0, 1\}^n$. There are 2^n of them.
- For each vertex v , let

$$v^* = \operatorname{argmin}\{\|x\| : x \in v + 2\mathcal{L}, x \neq 0\}$$

(any one, if there are ties).

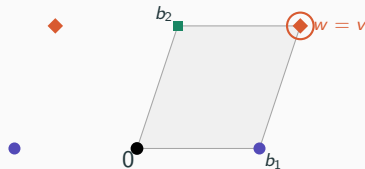
- **Claim:** the vectors $\pm v^*$, over all vertices v ,
are the only possible relevant vectors.
- Suppose not: some $w \in \mathcal{R}$ with
 $w \notin \{v^*, -v^*\}$. We derive a contradiction in
four steps.



$\mathcal{P}(B)$ shaded. Its vertices $0, b_1, b_2, b_1 + b_2$ lie in the
four cosets of $2\mathcal{L}$ (four shapes).

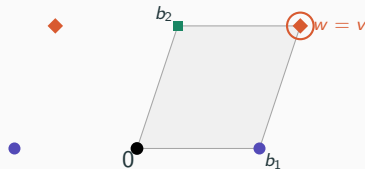
Step 1: the vertex v of w 's coset

- Write $w = \sum_i a_i b_i$ with $a_i \in \mathbb{Z}$.



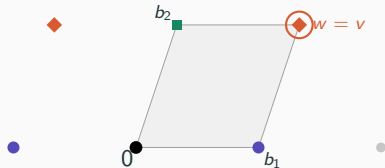
Step 1: the vertex v of w 's coset

- Write $w = \sum_i a_i b_i$ with $a_i \in \mathbb{Z}$.
- Not all a_i are even: otherwise $\frac{w}{2} \in \mathcal{L}$, so $\text{CVP}(\frac{w}{2}) = \{\frac{w}{2}\}$ and w is not relevant.



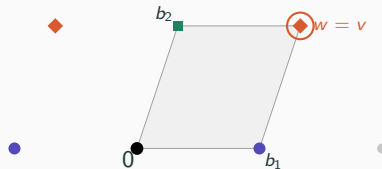
Step 1: the vertex v of w 's coset

- Write $w = \sum_i a_i b_i$ with $a_i \in \mathbb{Z}$.
- Not all a_i are even: otherwise $\frac{w}{2} \in \mathcal{L}$, so $\text{CVP}(\frac{w}{2}) = \{\frac{w}{2}\}$ and w is not relevant.
- Let $v = \sum_i (a_i \bmod 2) b_i$, a vertex of $\mathcal{P}(B)$, not 0. Then $\frac{v+w}{2} = \sum_i \frac{(a_i \bmod 2) + a_i}{2} b_i \in \mathcal{L}$: every coefficient is an integer.



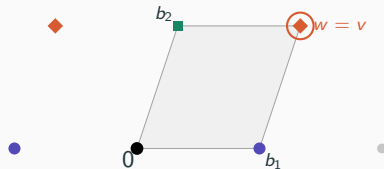
Step 1: the vertex v of w 's coset

- Write $w = \sum_i a_i b_i$ with $a_i \in \mathbb{Z}$.
- Not all a_i are even: otherwise $\frac{w}{2} \in \mathcal{L}$, so $\text{CVP}(\frac{w}{2}) = \{\frac{w}{2}\}$ and w is not relevant.
- Let $v = \sum_i (a_i \bmod 2) b_i$, a vertex of $\mathcal{P}(B)$, not 0. Then $\frac{v+w}{2} = \sum_i \frac{(a_i \bmod 2) + a_i}{2} b_i \in \mathcal{L}$: every coefficient is an integer.
- Equivalently, $w \in v + 2\mathcal{L}$: w lies in the coset of v .



Step 1: the vertex v of w 's coset

- Write $w = \sum_i a_i b_i$ with $a_i \in \mathbb{Z}$.
- Not all a_i are even: otherwise $\frac{w}{2} \in \mathcal{L}$, so $\text{CVP}(\frac{w}{2}) = \{\frac{w}{2}\}$ and w is not relevant.
- Let $v = \sum_i (a_i \bmod 2) b_i$, a vertex of $\mathcal{P}(B)$, not 0. Then $\frac{v+w}{2} = \sum_i \frac{(a_i \bmod 2) + a_i}{2} b_i \in \mathcal{L}$: every coefficient is an integer.
- Equivalently, $w \in v + 2\mathcal{L}$: w lies in the coset of v .
- Here $w = b_1 + b_2$ is itself a vertex, so $v = w$. (For $w = -b_1 - b_2$ we would also get $v = b_1 + b_2$.)

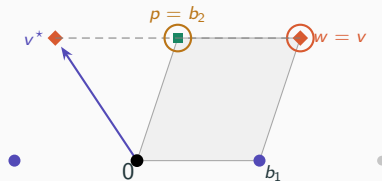


Step 2: a third lattice point p

- $v^* \in v + 2\mathcal{L}$, so, as in the notes,

$$\frac{v^* + w}{2} = \frac{v + 2\mathcal{L} + w}{2} = \frac{v + w}{2} + \mathcal{L} \subseteq \mathcal{L},$$

using step 1 for $\frac{v+w}{2} \in \mathcal{L}$.



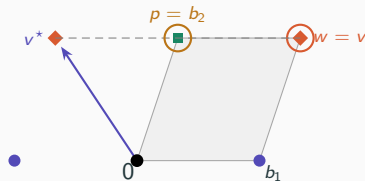
Step 2: a third lattice point p

- $v^* \in v + 2\mathcal{L}$, so, as in the notes,

$$\frac{v^* + w}{2} = \frac{v + 2\mathcal{L} + w}{2} = \frac{v + w}{2} + \mathcal{L} \subseteq \mathcal{L},$$

using step 1 for $\frac{v+w}{2} \in \mathcal{L}$.

- Call this lattice point $p = \frac{v^* + w}{2}$: the midpoint of v^* and w .



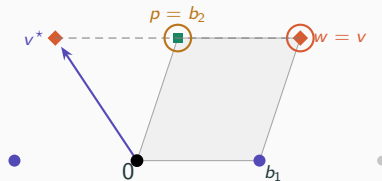
Step 2: a third lattice point p

- $v^* \in v + 2\mathcal{L}$, so, as in the notes,

$$\frac{v^* + w}{2} = \frac{v + 2\mathcal{L} + w}{2} = \frac{v + w}{2} + \mathcal{L} \subseteq \mathcal{L},$$

using step 1 for $\frac{v+w}{2} \in \mathcal{L}$.

- Call this lattice point $p = \frac{v^* + w}{2}$: the midpoint of v^* and w .
- $p \neq 0$, since $p = 0$ means $w = -v^*$. $p \neq w$, since $p = w$ means $w = v^*$. Both are excluded.



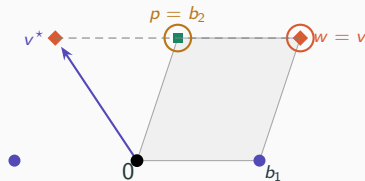
Step 2: a third lattice point p

- $v^* \in v + 2\mathcal{L}$, so, as in the notes,

$$\frac{v^* + w}{2} = \frac{v + 2\mathcal{L} + w}{2} = \frac{v + w}{2} + \mathcal{L} \subseteq \mathcal{L},$$

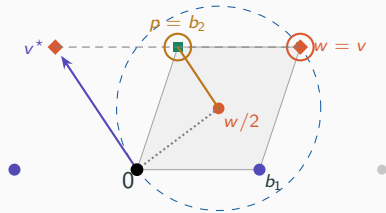
using step 1 for $\frac{v+w}{2} \in \mathcal{L}$.

- Call this lattice point $p = \frac{v^* + w}{2}$: the midpoint of v^* and w .
- $p \neq 0$, since $p = 0$ means $w = -v^*$. $p \neq w$, since $p = w$ means $w = v^*$. Both are excluded.
- Here $v^* = b_2 - b_1$ and $p = b_2$.



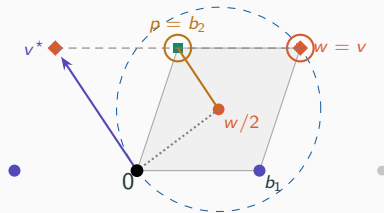
Step 3: p is as close to $w/2$ as 0 is

- $\|p - \frac{w}{2}\| = \|\frac{v^*}{2}\|$.



Step 3: p is as close to $w/2$ as 0 is

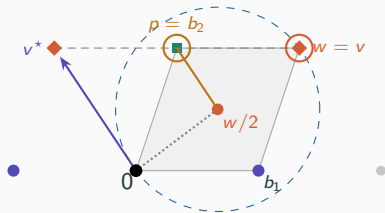
- $\|p - \frac{w}{2}\| = \|\frac{v^*}{2}\|$.
- Halving every vector of $v + 2\mathcal{L}$: $\frac{v^*}{2}$ is a shortest vector of the coset $\frac{v}{2} + \mathcal{L}$ (which does not contain 0).



Step 3: p is as close to $w/2$ as 0 is

- $\|p - \frac{w}{2}\| = \|\frac{v^*}{2}\|$.
- Halving every vector of $v + 2\mathcal{L}$: $\frac{v^*}{2}$ is a shortest vector of the coset $\frac{v}{2} + \mathcal{L}$ (which does not contain 0).
- $\frac{w}{2}$ lies in the same coset: $\frac{w}{2} + \frac{v}{2} \in \mathcal{L}$, so

$$\frac{w}{2} \in \mathcal{L} - \frac{v}{2} = (\mathcal{L} - v) + \frac{v}{2} = \frac{v}{2} + \mathcal{L}.$$



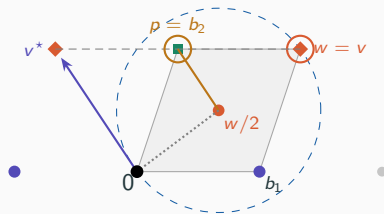
Step 3: p is as close to $w/2$ as 0 is

- $\|p - \frac{w}{2}\| = \|\frac{v^*}{2}\|$.
- Halving every vector of $v + 2\mathcal{L}$: $\frac{v^*}{2}$ is a shortest vector of the coset $\frac{v}{2} + \mathcal{L}$ (which does not contain 0).
- $\frac{w}{2}$ lies in the same coset: $\frac{w}{2} + \frac{v}{2} \in \mathcal{L}$, so

$$\frac{w}{2} \in \mathcal{L} - \frac{v}{2} = (\mathcal{L} - v) + \frac{v}{2} = \frac{v}{2} + \mathcal{L}.$$

- Hence $\|\frac{v^*}{2}\| \leq \|\frac{w}{2}\|$, that is,

$$\|p - \frac{w}{2}\| \leq \|0 - \frac{w}{2}\|.$$



Step 3: p is as close to $w/2$ as 0 is

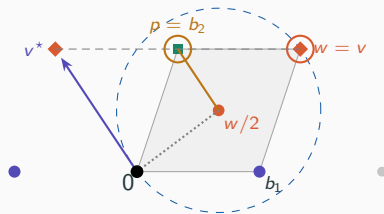
- $\|p - \frac{w}{2}\| = \|\frac{v^*}{2}\|$.
- Halving every vector of $v + 2\mathcal{L}$: $\frac{v^*}{2}$ is a shortest vector of the coset $\frac{v}{2} + \mathcal{L}$ (which does not contain 0).
- $\frac{w}{2}$ lies in the same coset: $\frac{w}{2} + \frac{v}{2} \in \mathcal{L}$, so

$$\frac{w}{2} \in \mathcal{L} - \frac{v}{2} = (\mathcal{L} - v) + \frac{v}{2} = \frac{v}{2} + \mathcal{L}.$$

- Hence $\|\frac{v^*}{2}\| \leq \|\frac{w}{2}\|$, that is,

$$\|p - \frac{w}{2}\| \leq \|0 - \frac{w}{2}\|.$$

- Picture: p lies inside the circle centred at $\frac{w}{2}$ through 0 and w .



Step 4: the contradiction

- w is relevant: $\text{CVP}(\frac{w}{2}) = \{0, w\}$. Both are at distance $\frac{\|w\|}{2}$, and every other lattice point is *strictly* farther from $\frac{w}{2}$.

Step 4: the contradiction

- w is relevant: $\text{CVP}(\frac{w}{2}) = \{0, w\}$. Both are at distance $\frac{\|w\|}{2}$, and every other lattice point is *strictly* farther from $\frac{w}{2}$.
- But $p \in \mathcal{L}$, $p \notin \{0, w\}$ (step 2), and $\|p - \frac{w}{2}\| \leq \frac{\|w\|}{2}$ (step 3). Contradiction.

Step 4: the contradiction

- w is relevant: $\text{CVP}(\frac{w}{2}) = \{0, w\}$. Both are at distance $\frac{\|w\|}{2}$, and every other lattice point is *strictly* farther from $\frac{w}{2}$.
- But $p \in \mathcal{L}$, $p \notin \{0, w\}$ (step 2), and $\|p - \frac{w}{2}\| \leq \frac{\|w\|}{2}$ (step 3). Contradiction.
- So the only relevant vectors in the coset $v + 2\mathcal{L}$ are among $v^*, -v^*$:

$$|\mathcal{R} \cap (v + 2\mathcal{L})| \leq 2.$$

Step 4: the contradiction

- w is relevant: $\text{CVP}(\frac{w}{2}) = \{0, w\}$. Both are at distance $\frac{\|w\|}{2}$, and every other lattice point is *strictly* farther from $\frac{w}{2}$.
- But $p \in \mathcal{L}$, $p \notin \{0, w\}$ (step 2), and $\|p - \frac{w}{2}\| \leq \frac{\|w\|}{2}$ (step 3). Contradiction.
- So the only relevant vectors in the coset $v + 2\mathcal{L}$ are among $v^*, -v^*$:

$$|\mathcal{R} \cap (v + 2\mathcal{L})| \leq 2.$$

- The notes say p is at distance “less than” that of 0. We only get “at most”, and that is enough: relevance excludes a third closest point as well as a strictly closer one.

- Every lattice vector lies in the coset $v + 2\mathcal{L}$ of exactly one of the 2^n vertices v . Each coset has at most 2 relevant vectors, so

$$|\mathcal{R}| \leq 2 \cdot 2^n = 2^{n+1}. \quad (\text{Lemma 3.3.9})$$

- Every lattice vector lies in the coset $v + 2\mathcal{L}$ of exactly one of the 2^n vertices v . Each coset has at most 2 relevant vectors, so

$$|\mathcal{R}| \leq 2 \cdot 2^n = 2^{n+1}. \quad (\text{Lemma 3.3.9})$$

- Sharper: the coset of the vertex $v = 0$ is $2\mathcal{L}$ itself, which contains no relevant vectors. So $|\mathcal{R}| \leq 2(2^n - 1)$.

- Every lattice vector lies in the coset $v + 2\mathcal{L}$ of exactly one of the 2^n vertices v . Each coset has at most 2 relevant vectors, so

$$|\mathcal{R}| \leq 2 \cdot 2^n = 2^{n+1}. \quad (\text{Lemma 3.3.9})$$

- Sharper: the coset of the vertex $v = 0$ is $2\mathcal{L}$ itself, which contains no relevant vectors. So $|\mathcal{R}| \leq 2(2^n - 1)$.
- If a coset has several shortest vectors, *none* of them is relevant: run the argument with each one as v^* . Square lattice: $|\mathcal{R}| = 4$, not 6.

- Every lattice vector lies in the coset $v + 2\mathcal{L}$ of exactly one of the 2^n vertices v . Each coset has at most 2 relevant vectors, so

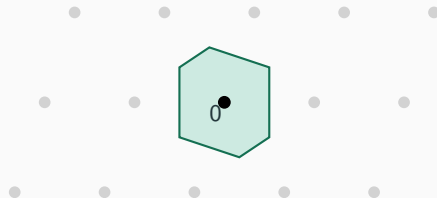
$$|\mathcal{R}| \leq 2 \cdot 2^n = 2^{n+1}. \quad (\text{Lemma 3.3.9})$$

- Sharper: the coset of the vertex $v = 0$ is $2\mathcal{L}$ itself, which contains no relevant vectors. So $|\mathcal{R}| \leq 2(2^n - 1)$.
- If a coset has several shortest vectors, *none* of them is relevant: run the argument with each one as v^* . Square lattice: $|\mathcal{R}| = 4$, not 6.
- Running lattice: the bound $2(2^2 - 1) = 6$ is attained.

CVP given the relevant vectors

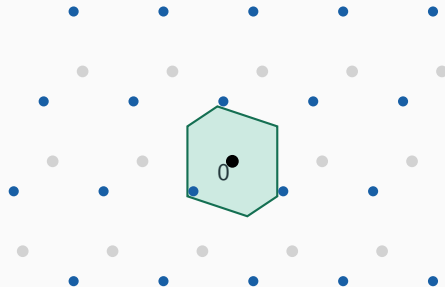
The task

- Goal: find $s \in (t - \mathcal{L}) \cap V$, then output $x = t - s$.



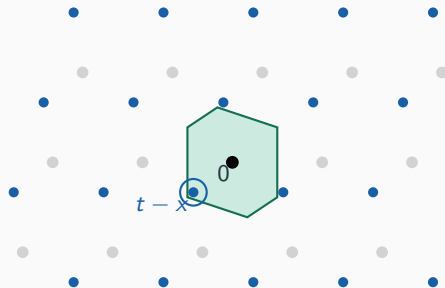
The task

- Goal: find $s \in (t - \mathcal{L}) \cap V$, then output $x = t - s$.
- Blue dots: the coset $t - \mathcal{L}$ for $t = (10.7, 8)$, a shifted copy of the lattice.



The task

- Goal: find $s \in (t - \mathcal{L}) \cap V$, then output $x = t - s$.
- Blue dots: the coset $t - \mathcal{L}$ for $t = (10.7, 8)$, a shifted copy of the lattice.
- Exactly one of them sits in V : here $t - (12, 9)$, so $x = (12, 9)$.



First attempt: greedy

- If $s \notin V$, Lemma 3.3.8 gives $v \in \mathcal{R}$ with $2\langle s, v \rangle > \|v\|^2$, i.e. $\|s - v\| < \|s\|$.

First attempt: greedy

- If $s \notin V$, Lemma 3.3.8 gives $v \in \mathcal{R}$ with $2\langle s, v \rangle > \|v\|^2$, i.e. $\|s - v\| < \|s\|$.
- So subtract v and repeat. It terminates: norms strictly drop, and a ball holds finitely many coset points.

First attempt: greedy

- If $s \notin V$, Lemma 3.3.8 gives $v \in \mathcal{R}$ with $2\langle s, v \rangle > \|v\|^2$, i.e. $\|s - v\| < \|s\|$.
- So subtract v and repeat. It terminates: norms strictly drop, and a ball holds finitely many coset points.
- But each step moves s by at most $\max_v \|v\|$. With ℓ -bit entries, $\|t\| \approx 2^\ell$ and we need $2^{\Theta(\ell)}$ steps, even for $n = 2$.

First attempt: greedy

- If $s \notin V$, Lemma 3.3.8 gives $v \in \mathcal{R}$ with $2\langle s, v \rangle > \|v\|^2$, i.e. $\|s - v\| < \|s\|$.
- So subtract v and repeat. It terminates: norms strictly drop, and a ball holds finitely many coset points.
- But each step moves s by at most $\max_v \|v\|$. With ℓ -bit entries, $\|t\| \approx 2^\ell$ and we need $2^{\Theta(\ell)}$ steps, even for $n = 2$.
- We want $2^{O(n)} \cdot \text{poly}(\ell)$: hardness should sit in the dimension, not in the numbers.

First attempt: greedy

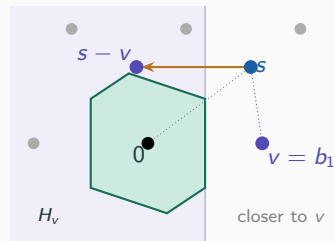
- If $s \notin V$, Lemma 3.3.8 gives $v \in \mathcal{R}$ with $2\langle s, v \rangle > \|v\|^2$, i.e. $\|s - v\| < \|s\|$.
- So subtract v and repeat. It terminates: norms strictly drop, and a ball holds finitely many coset points.
- But each step moves s by at most $\max_v \|v\|$. With ℓ -bit entries, $\|t\| \approx 2^\ell$ and we need $2^{\Theta(\ell)}$ steps, even for $n = 2$.
- We want $2^{O(n)} \cdot \text{poly}(\ell)$: hardness should sit in the dimension, not in the numbers.

One dimension

$\mathcal{L} = m\mathbb{Z}$: greedy is “subtract m repeatedly”. Long division subtracts $2^k m$ for decreasing k . Algorithm 7 is long division for lattices.

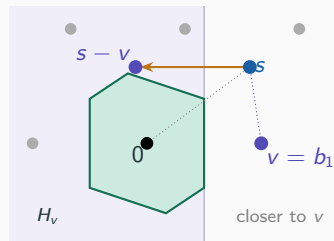
Why the greedy step shortens s

- By Lemma 3.3.8, $V = \bigcap_{v \in \mathcal{R}} H_v$. So if $s \notin V$, some $v \in \mathcal{R}$ has $s \notin H_v$.



Why the greedy step shortens s

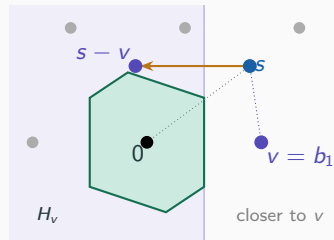
- By Lemma 3.3.8, $V = \bigcap_{v \in \mathcal{R}} H_v$. So if $s \notin V$, some $v \in \mathcal{R}$ has $s \notin H_v$.
- $H_v = \{x : 2\langle x, v \rangle \leq \|v\|^2\}$, so $s \notin H_v$ means $2\langle s, v \rangle > \|v\|^2$.



Why the greedy step shortens s

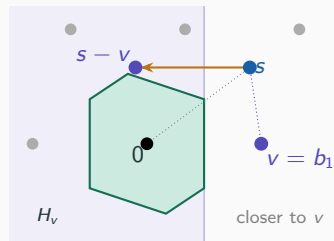
- By Lemma 3.3.8, $V = \bigcap_{v \in \mathcal{R}} H_v$. So if $s \notin V$, some $v \in \mathcal{R}$ has $s \notin H_v$.
- $H_v = \{x : 2\langle x, v \rangle \leq \|v\|^2\}$, so $s \notin H_v$ means $2\langle s, v \rangle > \|v\|^2$.
- Expand: $\|s - v\|^2 = \|s\|^2 - 2\langle s, v \rangle + \|v\|^2$.
Hence

$$\|s - v\|^2 < \|s\|^2 \iff 2\langle s, v \rangle > \|v\|^2.$$



The greedy step: picture and example

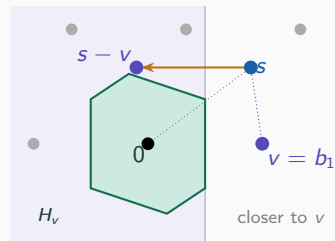
- $s \notin H_v$ says s is on v 's side of the bisector: strictly closer to v than to 0 . So $s - v$ is strictly closer to 0 than s was.



The greedy step: picture and example

- $s \notin H_v$ says s is on v 's side of the bisector: strictly closer to v than to 0 . So $s - v$ is strictly closer to 0 than s was.
- Here $s = (2.7, 2)$, $v = b_1$:
 $2\langle s, b_1 \rangle = 16.2 > 9 = \|b_1\|^2$, and

$$\|s - b_1\| \approx 2.02 < 3.36 \approx \|s\|.$$

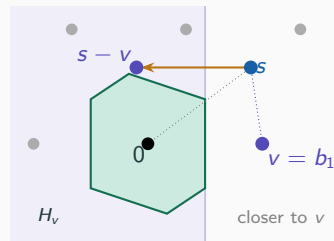


The greedy step: picture and example

- $s \notin H_v$ says s is on v 's side of the bisector: strictly closer to v than to 0 . So $s - v$ is strictly closer to 0 than s was.
- Here $s = (2.7, 2)$, $v = b_1$:
 $2\langle s, b_1 \rangle = 16.2 > 9 = \|b_1\|^2$, and

$$\|s - b_1\| \approx 2.02 < 3.36 \approx \|s\|.$$

- Since $v \in \mathcal{L}$, $s - v$ stays in the coset $t - \mathcal{L}$.

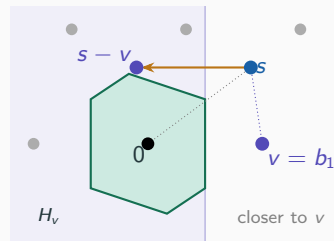


The greedy step: picture and example

- $s \notin H_v$ says s is on v 's side of the bisector: strictly closer to v than to 0 . So $s - v$ is strictly closer to 0 than s was.
- Here $s = (2.7, 2)$, $v = b_1$:
 $2\langle s, b_1 \rangle = 16.2 > 9 = \|b_1\|^2$, and

$$\|s - b_1\| \approx 2.02 < 3.36 \approx \|s\|.$$

- Since $v \in \mathcal{L}$, $s - v$ stays in the coset $t - \mathcal{L}$.



Why Lemma 3.3.8 is needed

The definition of V alone gives *some* lattice vector $v \neq 0$ with $\|s - v\| < \|s\|$, but with no finite list to search. Lemma 3.3.8 says one can be found among the at most 2^{n+1} vectors of $\mathcal{R}$.

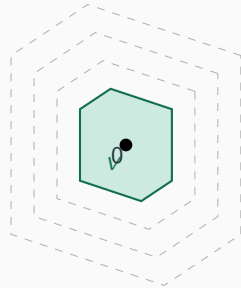
The gauge $\delta(s)$

- V , the unit cell.



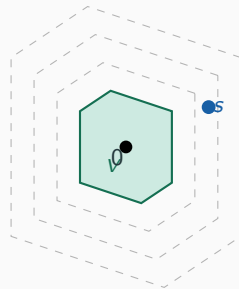
The gauge $\delta(s)$

- V , the unit cell.
- Its scaled copies δV .



The gauge $\delta(s)$

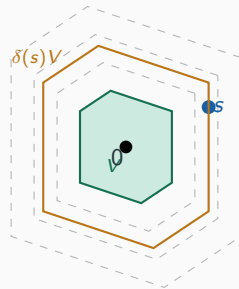
- V , the unit cell.
- Its scaled copies δV .
- How far must we inflate V to catch s ?
 $\delta(s) = \min\{\delta \geq 0 : s \in \delta V\}.$



The gauge $\delta(s)$

- V , the unit cell.
- Its scaled copies δV .
- How far must we inflate V to catch s ?
 $\delta(s) = \min\{\delta \geq 0 : s \in \delta V\}.$
- By Lemma 3.3.8,

$$\delta(s) = \max_{v \in \mathcal{R}} \frac{2\langle s, v \rangle}{\|v\|^2}, \quad s \in V \iff \delta(s) \leq 1.$$

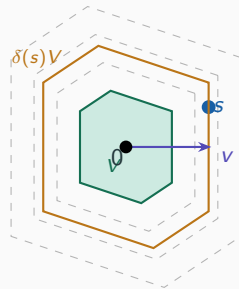


The gauge $\delta(s)$

- V , the unit cell.
- Its scaled copies δV .
- How far must we inflate V to catch s ?
 $\delta(s) = \min\{\delta \geq 0 : s \in \delta V\}.$
- By Lemma 3.3.8,

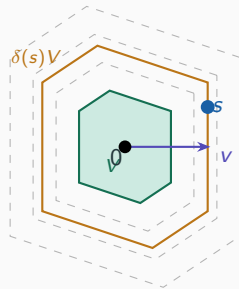
$$\delta(s) = \max_{v \in \mathcal{R}} \frac{2\langle s, v \rangle}{\|v\|^2}, \quad s \in V \iff \delta(s) \leq 1.$$

- The maximising v names the facet carrying s .



The gauge formula, step by step

- **Scaling.** For $\delta > 0$: $s \in \delta V \iff \frac{s}{\delta} \in V$.

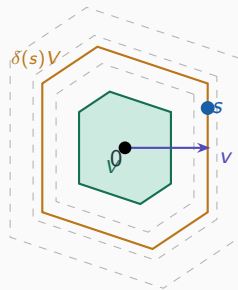


$s = (2.7, 1.3)$: $s/1.8 = (1.5, 0.72)$ is on the facet $x = 1.5$ of V ; for $\delta < 1.8$, s/δ violates H_{b_1} .

The gauge formula, step by step

- **Scaling.** For $\delta > 0$: $s \in \delta V \iff \frac{s}{\delta} \in V$.
- **Lemma 3.3.8:** $V = \bigcap_{v \in \mathcal{R}} H_v$. So for $\delta > 0$,

$$\begin{aligned} s \in \delta V &\iff 2\langle \frac{s}{\delta}, v \rangle \leq \|v\|^2 \quad \forall v \in \mathcal{R} \\ &\iff \frac{2\langle s, v \rangle}{\|v\|^2} \leq \delta \quad \forall v \in \mathcal{R}. \end{aligned}$$



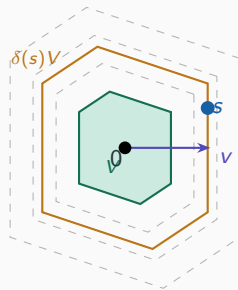
$s = (2.7, 1.3)$: $s/1.8 = (1.5, 0.72)$ is on the facet $x = 1.5$ of V ; for $\delta < 1.8$, s/δ violates H_{b_1} .

The gauge formula, step by step

- **Scaling.** For $\delta > 0$: $s \in \delta V \iff \frac{s}{\delta} \in V$.
- **Lemma 3.3.8:** $V = \bigcap_{v \in \mathcal{R}} H_v$. So for $\delta > 0$,

$$\begin{aligned} s \in \delta V &\iff 2\langle \frac{s}{\delta}, v \rangle \leq \|v\|^2 \quad \forall v \in \mathcal{R} \\ &\iff \frac{2\langle s, v \rangle}{\|v\|^2} \leq \delta \quad \forall v \in \mathcal{R}. \end{aligned}$$

- So $s \in \delta V \iff \delta \geq M(s) := \max_{v \in \mathcal{R}} \frac{2\langle s, v \rangle}{\|v\|^2}$.
The smallest such δ is $M(s)$, so $\delta(s) = M(s)$.
(It is ≥ 0 , as $\mathcal{R} = -\mathcal{R}$.)



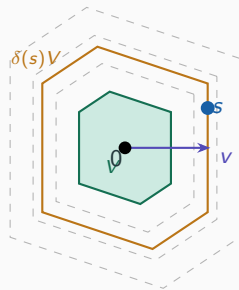
$s = (2.7, 1.3)$: $s/1.8 = (1.5, 0.72)$ is on the facet $x = 1.5$ of V ; for $\delta < 1.8$, s/δ violates H_{b_1} .

The gauge formula, step by step

- **Scaling.** For $\delta > 0$: $s \in \delta V \iff \frac{s}{\delta} \in V$.
- **Lemma 3.3.8:** $V = \bigcap_{v \in \mathcal{R}} H_v$. So for $\delta > 0$,

$$\begin{aligned} s \in \delta V &\iff 2\langle \frac{s}{\delta}, v \rangle \leq \|v\|^2 \quad \forall v \in \mathcal{R} \\ &\iff \frac{2\langle s, v \rangle}{\|v\|^2} \leq \delta \quad \forall v \in \mathcal{R}. \end{aligned}$$

- So $s \in \delta V \iff \delta \geq M(s) := \max_{v \in \mathcal{R}} \frac{2\langle s, v \rangle}{\|v\|^2}$.
The smallest such δ is $M(s)$, so $\delta(s) = M(s)$.
(It is ≥ 0 , as $\mathcal{R} = -\mathcal{R}$.)
- Taking $\delta = 1$: $s \in V \iff \delta(s) \leq 1$.



$s = (2.7, 1.3)$: $s/1.8 = (1.5, 0.72)$ is on the facet $x = 1.5$ of V ; for $\delta < 1.8$, s/δ violates H_{b_1} .

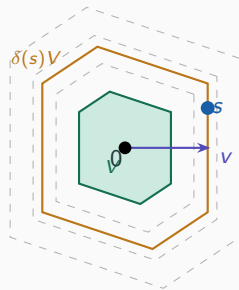
The gauge formula, step by step

- **Scaling.** For $\delta > 0$: $s \in \delta V \iff \frac{s}{\delta} \in V$.
- **Lemma 3.3.8:** $V = \bigcap_{v \in \mathcal{R}} H_v$. So for $\delta > 0$,

$$\begin{aligned} s \in \delta V &\iff 2\langle \frac{s}{\delta}, v \rangle \leq \|v\|^2 \quad \forall v \in \mathcal{R} \\ &\iff \frac{2\langle s, v \rangle}{\|v\|^2} \leq \delta \quad \forall v \in \mathcal{R}. \end{aligned}$$

- So $s \in \delta V \iff \delta \geq M(s) := \max_{v \in \mathcal{R}} \frac{2\langle s, v \rangle}{\|v\|^2}$.
The smallest such δ is $M(s)$, so $\delta(s) = M(s)$.
(It is ≥ 0 , as $\mathcal{R} = -\mathcal{R}$.)
- Taking $\delta = 1$: $s \in V \iff \delta(s) \leq 1$.

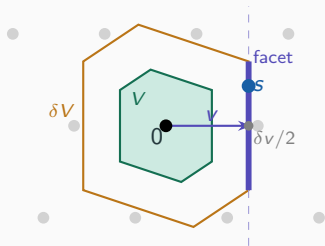
Role of Lemma 3.3.8: without it, the maximum would run over all of $\mathcal{L} \setminus \{0\}$, an infinite list; with it, over at most 2^{n+1} vectors.



$s = (2.7, 1.3)$: $s/1.8 = (1.5, 0.72)$ is on the facet $x = 1.5$ of V ; for $\delta < 1.8$, s/δ violates H_{b_1} .

Which facet carries s ?

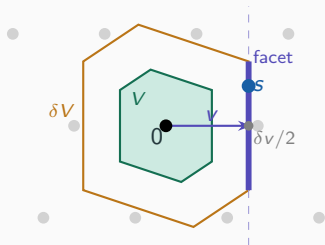
- Let $\delta = \delta(s)$, and let $v \in \mathcal{R}$ attain the maximum: $2\langle s, v \rangle = \delta \|v\|^2$.



Thick purple: the facet of δV perpendicular to $v = b_1$, on the line $x = 2.7$ through $\delta v/2$.

Which facet carries s ?

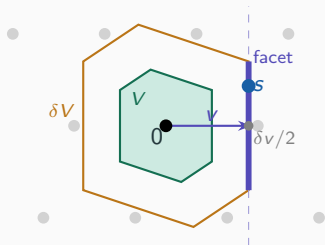
- Let $\delta = \delta(s)$, and let $v \in \mathcal{R}$ attain the maximum: $2\langle s, v \rangle = \delta \|v\|^2$.
- Every $u \in \mathcal{R}$ has $2\langle s, u \rangle \leq \delta \|u\|^2$, i.e. $s \in \delta H_u$.
So $s \in \delta V$.



Thick purple: the facet of δV perpendicular to $v = b_1$, on the line $x = 2.7$ through $\delta v/2$.

Which facet carries s ?

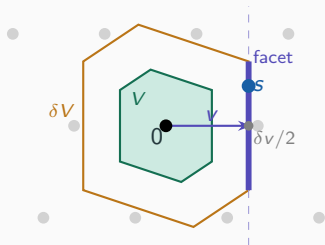
- Let $\delta = \delta(s)$, and let $v \in \mathcal{R}$ attain the maximum: $2\langle s, v \rangle = \delta \|v\|^2$.
- Every $u \in \mathcal{R}$ has $2\langle s, u \rangle \leq \delta \|u\|^2$, i.e. $s \in \delta H_u$. So $s \in \delta V$.
- The equality says s lies on $\partial(\delta H_v) = \{x : 2\langle x, v \rangle = \delta \|v\|^2\}$: the bisector of $[0, \delta v]$, through $\delta v/2$, orthogonal to v .



Thick purple: the facet of δV perpendicular to $v = b_1$, on the line $x = 2.7$ through $\delta v/2$.

Which facet carries s ?

- Let $\delta = \delta(s)$, and let $v \in \mathcal{R}$ attain the maximum: $2\langle s, v \rangle = \delta \|v\|^2$.
- Every $u \in \mathcal{R}$ has $2\langle s, u \rangle \leq \delta \|u\|^2$, i.e. $s \in \delta H_u$. So $s \in \delta V$.
- The equality says s lies on $\partial(\delta H_v) = \{x : 2\langle x, v \rangle = \delta \|v\|^2\}$: the bisector of $[0, \delta v]$, through $\delta v/2$, orthogonal to v .
- So $s \in \delta V \cap \partial(\delta H_v)$: the facet of δV centred at $\delta v/2$.



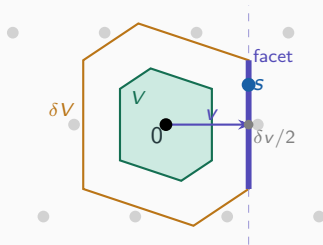
Thick purple: the facet of δV perpendicular to $v = b_1$, on the line $x = 2.7$ through $\delta v/2$.

Which facet carries s ? Example and remarks

- Here $s = (2.7, 1.3)$. The ratios $2\langle s, u \rangle / \|u\|^2$:

b_1	b_2	$b_1 - b_2$	$b_2 - b_1$	$-b_2$	$-b_1$
1.8	1.32	0.23	-0.23	-1.32	-1.8

Maximum at b_1 , so $\delta(s) = 1.8$ and s is on b_1 's facet.



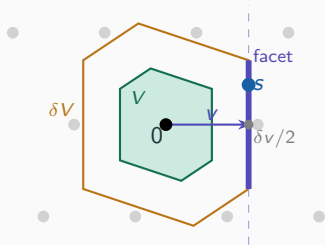
Which facet carries s ? Example and remarks

- Here $s = (2.7, 1.3)$. The ratios $2\langle s, u \rangle / \|u\|^2$:

b_1	b_2	$b_1 - b_2$	$b_2 - b_1$	$-b_2$	$-b_1$
1.8	1.32	0.23	-0.23	-1.32	-1.8

Maximum at b_1 , so $\delta(s) = 1.8$ and s is on b_1 's facet.

- If several v attain the maximum, s lies on all their facets: a lower-dimensional face (an edge or vertex in 2D). Any of them can be chosen.



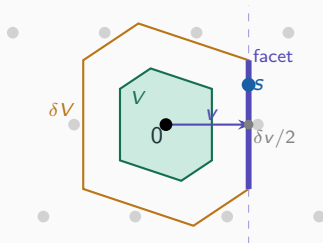
Which facet carries s ? Example and remarks

- Here $s = (2.7, 1.3)$. The ratios $2\langle s, u \rangle / \|u\|^2$:

b_1	b_2	$b_1 - b_2$	$b_2 - b_1$	$-b_2$	$-b_1$
1.8	1.32	0.23	-0.23	-1.32	-1.8

Maximum at b_1 , so $\delta(s) = 1.8$ and s is on b_1 's facet.

- If several v attain the maximum, s lies on all their facets: a lower-dimensional face (an edge or vertex in 2D). Any of them can be chosen.
- Why it matters:** line 5 of Algorithm 7 picks exactly this v , and Lemma 3.3.11 needs $s \in \partial(\delta H_v)$.



Algorithm 7

Input: B , target t , relevant vectors $\mathcal{R}$.

Output: $x \in \mathcal{L}$ minimising $\|t - x\|$.

```
1:  $s \leftarrow t$ 
2: while  $s \notin V$  do
3:    $\delta \leftarrow$  smallest  $\delta > 1$  with  $s \in \delta V$ 
4:   write  $\delta = \alpha 2^k$ ,  $1 < \alpha \leq 2$ ,  $k \geq 0$ 
5:    $v \leftarrow v \in \mathcal{R}$  with  $s \in \partial(\delta H_v)$ 
6:    $s \leftarrow s - 2^k v$ 
7: end while
8: return  $t - s$ 
```

Algorithm 7

Input: B , target t , relevant vectors $\mathcal{R}$.

Output: $x \in \mathcal{L}$ minimising $\|t - x\|$.

```
1:  $s \leftarrow t$ 
2: while  $s \notin V$  do
3:    $\delta \leftarrow$  smallest  $\delta > 1$  with  $s \in \delta V$ 
4:   write  $\delta = \alpha 2^k$ ,  $1 < \alpha \leq 2$ ,  $k \geq 0$ 
5:    $v \leftarrow v \in \mathcal{R}$  with  $s \in \partial(\delta H_v)$ 
6:    $s \leftarrow s - 2^k v$ 
7: end while
8: return  $t - s$ 
```

- $\delta = \delta(s)$, the gauge.

Algorithm 7

Input: B , target t , relevant vectors $\mathcal{R}$.

Output: $x \in \mathcal{L}$ minimising $\|t - x\|$.

```
1:  $s \leftarrow t$ 
2: while  $s \notin V$  do
3:    $\delta \leftarrow$  smallest  $\delta > 1$  with  $s \in \delta V$ 
4:   write  $\delta = \alpha 2^k$ ,  $1 < \alpha \leq 2$ ,  $k \geq 0$ 
5:    $v \leftarrow v \in \mathcal{R}$  with  $s \in \partial(\delta H_v)$ 
6:    $s \leftarrow s - 2^k v$ 
7: end while
8: return  $t - s$ 
```

- $\delta = \delta(s)$, the gauge.
- k says which shell s lies in:
 $2^k < \delta \leq 2^{k+1}$.

Algorithm 7

Input: B , target t , relevant vectors $\mathcal{R}$.

Output: $x \in \mathcal{L}$ minimising $\|t - x\|$.

```
1:  $s \leftarrow t$ 
2: while  $s \notin V$  do
3:    $\delta \leftarrow$  smallest  $\delta > 1$  with  $s \in \delta V$ 
4:   write  $\delta = \alpha 2^k$ ,  $1 < \alpha \leq 2$ ,  $k \geq 0$ 
5:    $v \leftarrow v \in \mathcal{R}$  with  $s \in \partial(\delta H_v)$ 
6:    $s \leftarrow s - 2^k v$ 
7: end while
8: return  $t - s$ 
```

- $\delta = \delta(s)$, the gauge.
- k says which shell s lies in:
 $2^k < \delta \leq 2^{k+1}$.
- v is the facet of δV carrying s : the
 argmax .

Algorithm 7

Input: B , target t , relevant vectors $\mathcal{R}$.

Output: $x \in \mathcal{L}$ minimising $\|t - x\|$.

```
1:  $s \leftarrow t$ 
2: while  $s \notin V$  do
3:    $\delta \leftarrow$  smallest  $\delta > 1$  with  $s \in \delta V$ 
4:   write  $\delta = \alpha 2^k$ ,  $1 < \alpha \leq 2$ ,  $k \geq 0$ 
5:    $v \leftarrow v \in \mathcal{R}$  with  $s \in \partial(\delta H_v)$ 
6:    $s \leftarrow s - 2^k v$ 
7: end while
8: return  $t - s$ 
```

- $\delta = \delta(s)$, the gauge.
- k says which shell s lies in:
 $2^k < \delta \leq 2^{k+1}$.
- v is the facet of δV carrying s : the
 argmax .
- Step size matched to the shell:
coarse far away, fine near 0.

Lines 3–4: choosing the scale

- The loop runs only while $s \notin V$, so $\delta > 1$ automatically.

Lines 3–4: choosing the scale

- The loop runs only while $s \notin V$, so $\delta > 1$ automatically.
- $k = \lceil \log_2 \delta \rceil - 1$ and $\alpha = \delta/2^k \in (1, 2]$. Equivalently

$$2^k < \delta(s) \leq 2^{k+1} \iff s \in 2^{k+1}V \setminus 2^kV.$$

Lines 3–4: choosing the scale

- The loop runs only while $s \notin V$, so $\delta > 1$ automatically.
- $k = \lceil \log_2 \delta \rceil - 1$ and $\alpha = \delta/2^k \in (1, 2]$. Equivalently

$$2^k < \delta(s) \leq 2^{k+1} \iff s \in 2^{k+1}V \setminus 2^kV.$$

- Nested shells $V \subset 2V \subset 4V \subset 8V \subset \dots$; k is the shell index.

Lines 3–4: choosing the scale

- The loop runs only while $s \notin V$, so $\delta > 1$ automatically.
- $k = \lceil \log_2 \delta \rceil - 1$ and $\alpha = \delta/2^k \in (1, 2]$. Equivalently

$$2^k < \delta(s) \leq 2^{k+1} \iff s \in 2^{k+1}V \setminus 2^kV.$$

- Nested shells $V \subset 2V \subset 4V \subset 8V \subset \dots$; k is the shell index.
- Example: $\delta = 7.13 \Rightarrow k = 2, \alpha = 1.78$. $\delta = 4 \Rightarrow k = 1, \alpha = 2$.

Lines 5–6: which facet, and which step

- **Line 5.** Take v attaining $\delta(s) = \max_v 2\langle s, v \rangle / \|v\|^2$. Then $2\langle s, v \rangle = \delta \|v\|^2$, i.e. s is on $\partial(\delta H_v)$. It exists because $\mathcal{R}$ is finite: Remark 3.3.10.

Lines 5–6: which facet, and which step

- **Line 5.** Take v attaining $\delta(s) = \max_v 2\langle s, v \rangle / \|v\|^2$. Then $2\langle s, v \rangle = \delta \|v\|^2$, i.e. s is on $\partial(\delta H_v)$. It exists because $\mathcal{R}$ is finite: Remark 3.3.10.
- **Line 6.** Scaling dictionary: the lattice $2^k \mathcal{L}$ has cell $2^k V$ and relevant vectors $2^k \mathcal{R}$.

Lines 5–6: which facet, and which step

- **Line 5.** Take v attaining $\delta(s) = \max_v 2\langle s, v \rangle / \|v\|^2$. Then $2\langle s, v \rangle = \delta \|v\|^2$, i.e. s is on $\partial(\delta H_v)$. It exists because $\mathcal{R}$ is finite: Remark 3.3.10.
- **Line 6.** Scaling dictionary: the lattice $2^k \mathcal{L}$ has cell $2^k V$ and relevant vectors $2^k \mathcal{R}$.
- With $\delta = \alpha 2^k$ and $v' = 2^k v$: $s \in \alpha \cdot (2^k V)$ and s is on the corresponding facet of it.

Lines 5–6: which facet, and which step

- **Line 5.** Take v attaining $\delta(s) = \max_v 2\langle s, v \rangle / \|v\|^2$. Then $2\langle s, v \rangle = \delta\|v\|^2$, i.e. s is on $\partial(\delta H_v)$. It exists because $\mathcal{R}$ is finite: Remark 3.3.10.
- **Line 6.** Scaling dictionary: the lattice $2^k \mathcal{L}$ has cell $2^k V$ and relevant vectors $2^k \mathcal{R}$.
- With $\delta = \alpha 2^k$ and $v' = 2^k v$: $s \in \alpha \cdot (2^k V)$ and s is on the corresponding facet of it.
- So every iteration is the case $1 < \delta \leq 2$ for the lattice $2^k \mathcal{L}$. That case is Lemma 3.3.11.

Lemma 3.3.11

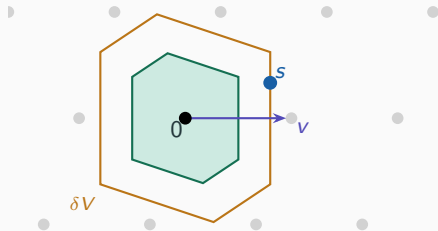
Lemma 3.3.11

$1 < \delta \leq 2$, $s \in \delta V$, $v \in \mathcal{R}$, $s \in \partial(\delta H_v)$.

Then

$$\|s - v\| < \|s\|, \quad s - v \in \delta V \subseteq 2V.$$

- Here $\delta = 1.6$, $s = (2.4, 1)$ on the facet of δV perpendicular to $v = b_1$.



Lemma 3.3.11

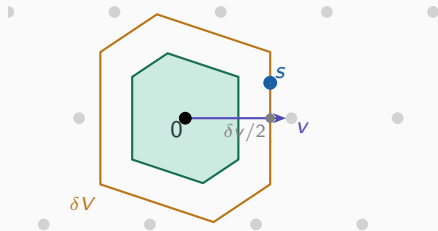
Lemma 3.3.11

$1 < \delta \leq 2$, $s \in \delta V$, $v \in \mathcal{R}$, $s \in \partial(\delta H_v)$.

Then

$$\|s - v\| < \|s\|, \quad s - v \in \delta V \subseteq 2V.$$

- Here $\delta = 1.6$, $s = (2.4, 1)$ on the facet of δV perpendicular to $v = b_1$.
- $s - \frac{\delta}{2}v \perp v$.



Lemma 3.3.11

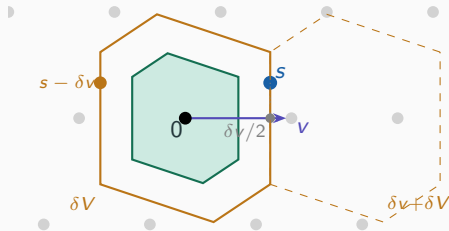
Lemma 3.3.11

$1 < \delta \leq 2$, $s \in \delta V$, $v \in \mathcal{R}$, $s \in \partial(\delta H_v)$.

Then

$$\|s - v\| < \|s\|, \quad s - v \in \delta V \subseteq 2V.$$

- Here $\delta = 1.6$, $s = (2.4, 1)$ on the facet of δV perpendicular to $v = b_1$.
- $s - \frac{\delta}{2}v \perp v$.
- $s - \delta v$ sits on the opposite facet.



Lemma 3.3.11

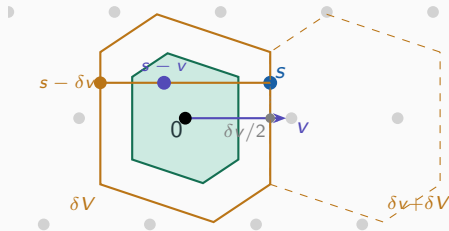
Lemma 3.3.11

$1 < \delta \leq 2$, $s \in \delta V$, $v \in \mathcal{R}$, $s \in \partial(\delta H_v)$.

Then

$$\|s - v\| < \|s\|, \quad s - v \in \delta V \subseteq 2V.$$

- Here $\delta = 1.6$, $s = (2.4, 1)$ on the facet of δV perpendicular to $v = b_1$.
- $s - \frac{\delta}{2}v \perp v$.
- $s - \delta v$ sits on the opposite facet.
- $s - v$ lies on the segment between them, so inside δV .



Proof, part 1: the step shortens s

- $s \in \partial(\delta H_v)$ means $2\langle s, v \rangle = \delta \|v\|^2$, i.e. $h := s - \frac{\delta}{2}v$ is orthogonal to v .

Proof, part 1: the step shortens s

- $s \in \partial(\delta H_v)$ means $2\langle s, v \rangle = \delta \|v\|^2$, i.e. $h := s - \frac{\delta}{2}v$ is orthogonal to v .
- Then $s = h + \frac{\delta}{2}v$ and $s - v = h - (1 - \frac{\delta}{2})v$, so by Pythagoras

$$\|s\|^2 = \|h\|^2 + \left(\frac{\delta}{2}\right)^2 \|v\|^2, \quad \|s - v\|^2 = \|h\|^2 + \left(1 - \frac{\delta}{2}\right)^2 \|v\|^2.$$

Proof, part 1: the step shortens s

- $s \in \partial(\delta H_v)$ means $2\langle s, v \rangle = \delta \|v\|^2$, i.e. $h := s - \frac{\delta}{2}v$ is orthogonal to v .
- Then $s = h + \frac{\delta}{2}v$ and $s - v = h - (1 - \frac{\delta}{2})v$, so by Pythagoras

$$\|s\|^2 = \|h\|^2 + \left(\frac{\delta}{2}\right)^2 \|v\|^2, \quad \|s - v\|^2 = \|h\|^2 + \left(1 - \frac{\delta}{2}\right)^2 \|v\|^2.$$

- Subtract: $\|s\|^2 - \|s - v\|^2 = (\delta - 1)\|v\|^2 > 0$ since $\delta > 1$.

Proof, part 2: the step stays inside δV

- Put $y = s/\delta \in V$. Being on the bisector of v gives $\|y\| = \|y - v\|$, so v is *also* a closest lattice point to y : $y \in v + V$.

Proof, part 2: the step stays inside δV

- Put $y = s/\delta \in V$. Being on the bisector of v gives $\|y\| = \|y - v\|$, so v is *also* a closest lattice point to y : $y \in v + V$.
- Hence $y - v \in V$, i.e. $s - \delta v \in \delta V$.

Proof, part 2: the step stays inside δV

- Put $y = s/\delta \in V$. Being on the bisector of v gives $\|y\| = \|y - v\|$, so v is *also* a closest lattice point to y : $y \in v + V$.
- Hence $y - v \in V$, i.e. $s - \delta v \in \delta V$.
- Convexity: $s - v = \left(1 - \frac{1}{\delta}\right) s + \frac{1}{\delta}(s - \delta v)$, a point of the segment $[s, s - \delta v]$, both ends in δV .

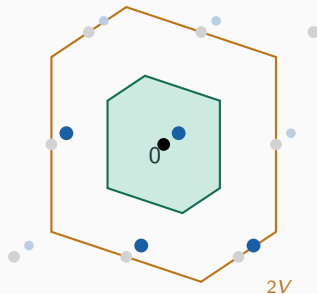
Proof, part 2: the step stays inside δV

- Put $y = s/\delta \in V$. Being on the bisector of v gives $\|y\| = \|y - v\|$, so v is *also* a closest lattice point to y : $y \in v + V$.
- Hence $y - v \in V$, i.e. $s - \delta v \in \delta V$.
- Convexity: $s - v = \left(1 - \frac{1}{\delta}\right) s + \frac{1}{\delta}(s - \delta v)$, a point of the segment $[s, s - \delta v]$, both ends in δV .
- Finally $\delta \leq 2$ gives $\delta V \subseteq 2V$. $\square$

Lemma 3.3.12: how many coset points sit in $2V$

Lemma 3.3.12

$|(s - \mathcal{L}) \cap 2V| \leq 4^n$ for every s .



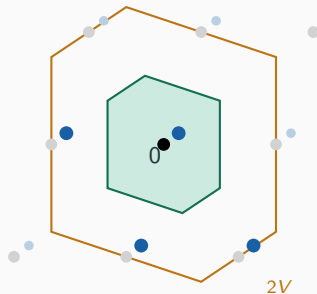
Here $s = (0.4, 0.3)$: four coset points in $2V$. The bound $4^n = 16$ is loose; the typical count is 2^n , since $\text{vol}(2V) = 2^n \det \mathcal{L}$.

Lemma 3.3.12: how many coset points sit in $2V$

Lemma 3.3.12

$|(s - \mathcal{L}) \cap 2V| \leq 4^n$ for every s .

- Suppose more than 4^n points. There are 4^n cosets of $4\mathcal{L}$, so two distinct points x, y have $\frac{x-y}{4} \in \mathcal{L}$.



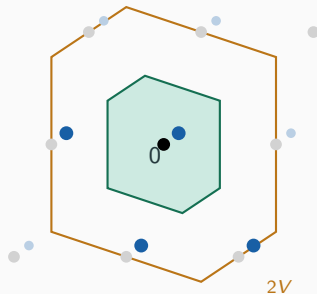
Here $s = (0.4, 0.3)$: four coset points in $2V$. The bound $4^n = 16$ is loose; the typical count is 2^n , since $\text{vol}(2V) = 2^n \det \mathcal{L}$.

Lemma 3.3.12: how many coset points sit in $2V$

Lemma 3.3.12

$|(s - \mathcal{L}) \cap 2V| \leq 4^n$ for every s .

- Suppose more than 4^n points. There are 4^n cosets of $4\mathcal{L}$, so two distinct points x, y have $\frac{x-y}{4} \in \mathcal{L}$.
- $x, y \in 2V \Rightarrow \frac{x}{2}, -\frac{y}{2} \in V$ (using $V = -V$), so their midpoint $\frac{x-y}{4} \in V$ by convexity.



Here $s = (0.4, 0.3)$: four coset points in $2V$. The bound $4^n = 16$ is loose; the typical count is 2^n , since $\text{vol}(2V) = 2^n \det \mathcal{L}$.

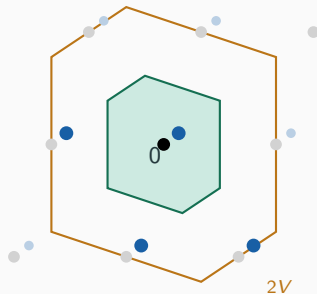
Lemma 3.3.12: how many coset points sit in $2V$

Lemma 3.3.12

$|(s - \mathcal{L}) \cap 2V| \leq 4^n$ for every s .

- Suppose more than 4^n points. There are 4^n cosets of $4\mathcal{L}$, so two distinct points x, y have $\frac{x-y}{4} \in \mathcal{L}$.
- $x, y \in 2V \Rightarrow \frac{x}{2}, -\frac{y}{2} \in V$ (using $V = -V$), so their midpoint $\frac{x-y}{4} \in V$ by convexity.
- But the only lattice point in V is 0, so $x = y$.

□



Here $s = (0.4, 0.3)$: four coset points in $2V$. The bound $4^n = 16$ is loose; the typical count is 2^n , since $\text{vol}(2V) = 2^n \det \mathcal{L}$.

Remark 3.3.13: why the loop ends

A **phase** is a run of iterations with the same k . Within one phase:

- all iterates lie in one coset of $2^k \mathcal{L}$ (we subtract multiples of $2^k v$);

Remark 3.3.13: why the loop ends

A **phase** is a run of iterations with the same k . Within one phase:

- all iterates lie in one coset of $2^k \mathcal{L}$ (we subtract multiples of $2^k v$);
- all lie in $2^{k+1} V$ (since $\delta \leq 2^{k+1}$);

Remark 3.3.13: why the loop ends

A **phase** is a run of iterations with the same k . Within one phase:

- all iterates lie in one coset of $2^k \mathcal{L}$ (we subtract multiples of $2^k v$);
- all lie in $2^{k+1} V$ (since $\delta \leq 2^{k+1}$);
- $\|s\|$ strictly decreases, so the iterates are distinct;

Remark 3.3.13: why the loop ends

A **phase** is a run of iterations with the same k . Within one phase:

- all iterates lie in one coset of $2^k \mathcal{L}$ (we subtract multiples of $2^k v$);
- all lie in $2^{k+1} V$ (since $\delta \leq 2^{k+1}$);
- $\|s\|$ strictly decreases, so the iterates are distinct;
- δ never increases, so k never increases.

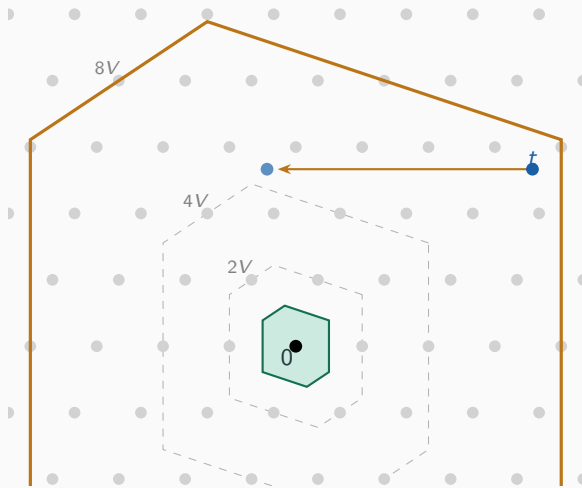
Remark 3.3.13: why the loop ends

A **phase** is a run of iterations with the same k . Within one phase:

- all iterates lie in one coset of $2^k \mathcal{L}$ (we subtract multiples of $2^k v$);
- all lie in $2^{k+1} V$ (since $\delta \leq 2^{k+1}$);
- $\|s\|$ strictly decreases, so the iterates are distinct;
- δ never increases, so k never increases.

By Lemma 3.3.12 (scaled), a phase has at most 4^n iterations; then k drops. In the last phase, $k = 0$, the loop exits with $s \in V$.

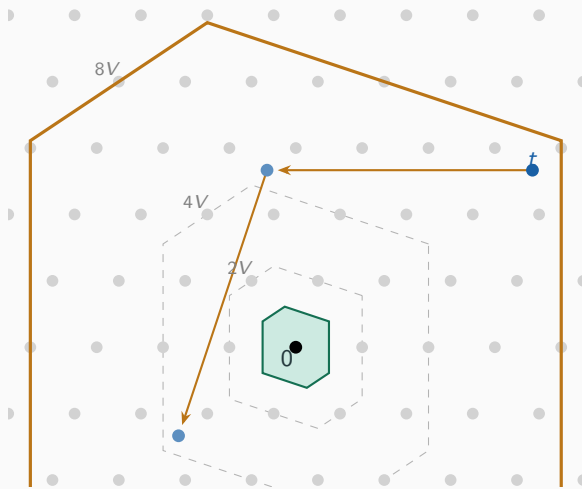
Worked example: $t = (10.7, 8.0)$



Step 1. $\delta = 7.13$, so $k = 2$: $s \in 8V \setminus 4V$.
Facet $v = b_1$. Subtract $4b_1 = (12, 0)$.

Thick outline: the shell $2^{k+1}V$ of the current phase.

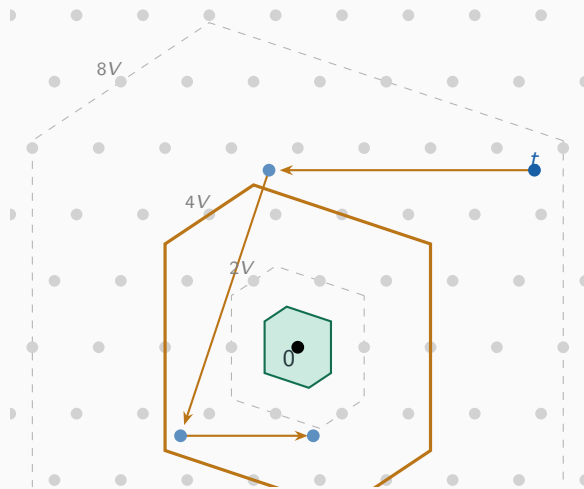
Worked example: $t = (10.7, 8.0)$



Step 2. $s = (-1.3, 8)$, $\delta = 4.54$, still $k = 2$. Facet b_2 ; subtract $4b_2 = (4, 12)$. The step overshoots the origin, yet $\|s\|$ drops from 8.10 to 6.64.

Thick outline: the shell $2^{k+1}V$ of the current phase.

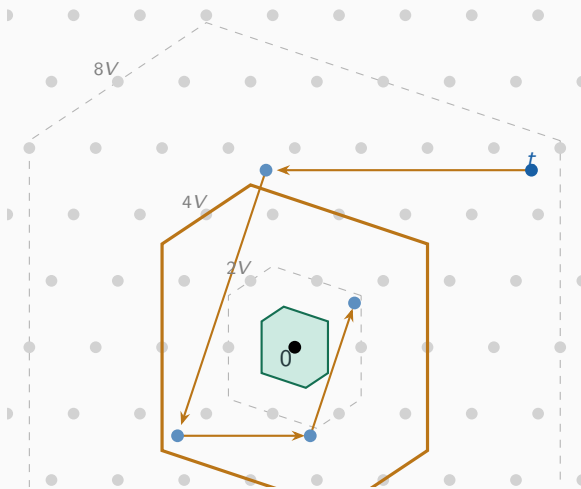
Worked example: $t = (10.7, 8.0)$



Step 3. $s = (-5.3, -4)$, $\delta = 3.53$: now $k = 1$. Facet $-b_1$; add $(6, 0)$.

Thick outline: the shell $2^{k+1}V$ of the current phase.

Worked example: $t = (10.7, 8.0)$

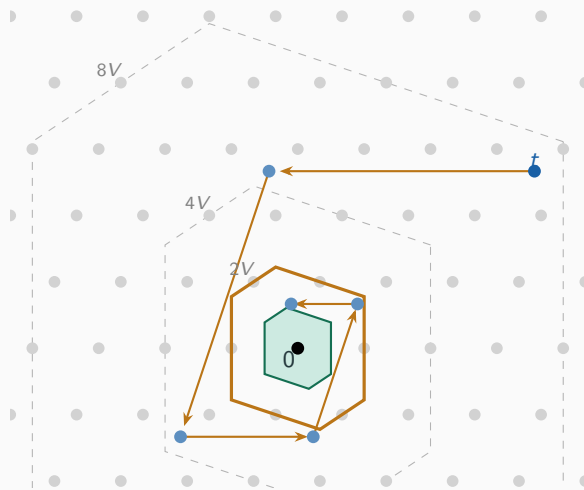


Step 4. $s = (0.7, -4)$, $\delta = 2.26$, $k = 1$.

Facet $-b_2$; add $(2, 6)$.

Thick outline: the shell $2^{k+1}V$ of the current phase.

Worked example: $t = (10.7, 8.0)$

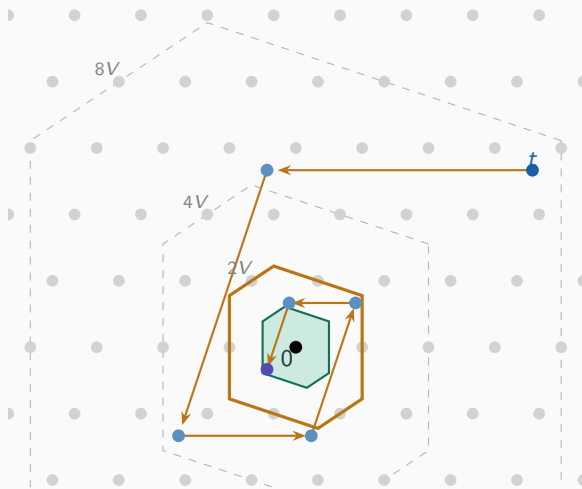


Step 5. $s = (2.7, 2)$, $\delta = 1.8$: $k = 0$.

Facet b_1 ; subtract $(3, 0)$.

Thick outline: the shell $2^{k+1}V$ of the current phase.

Worked example: $t = (10.7, 8.0)$

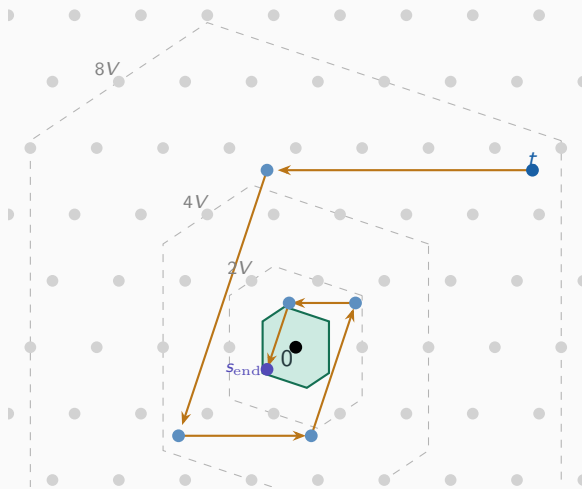


Step 6. $s = (-0.3, 2)$, $\delta = 1.14$, $k = 0$.

Facet b_2 ; subtract $(1, 3)$.

Thick outline: the shell $2^{k+1}V$ of the current phase.

Worked example: $t = (10.7, 8.0)$



Stop. $s = (-1.3, -1)$ has $\delta = 0.87 \leq 1$, so $s \in V$.

Output $x = t - s = (12, 9) = 3b_1 + 3b_2$, at distance 1.640. Brute force agrees; the runner-up is at 1.972.

Thick outline: the shell $2^{k+1}V$ of the current phase.

The same run in numbers

step	s	$\ s\ $	$\delta(s)$	k	facet v	subtract
1	(10.7, 8.0)	13.360	7.133	2	b_1	(12, 0)
2	(-1.3, 8.0)	8.105	4.540	2	b_2	(4, 12)
3	(-5.3, -4.0)	6.640	3.533	1	$-b_1$	(-6, 0)
4	(0.7, -4.0)	4.061	2.260	1	$-b_2$	(-2, -6)
5	(2.7, 2.0)	3.360	1.800	0	b_1	(3, 0)
6	(-0.3, 2.0)	2.022	1.140	0	b_2	(1, 3)
end	(-1.3, -1.0)	1.640	0.867			

The same run in numbers

step	s	$\ s\ $	$\delta(s)$	k	facet v	subtract
1	(10.7, 8.0)	13.360	7.133	2	b_1	(12, 0)
2	(-1.3, 8.0)	8.105	4.540	2	b_2	(4, 12)
3	(-5.3, -4.0)	6.640	3.533	1	$-b_1$	(-6, 0)
4	(0.7, -4.0)	4.061	2.260	1	$-b_2$	(-2, -6)
5	(2.7, 2.0)	3.360	1.800	0	b_1	(3, 0)
6	(-0.3, 2.0)	2.022	1.140	0	b_2	(1, 3)
end	(-1.3, -1.0)	1.640	0.867			

δ is non-increasing, $\|s\|$ strictly decreasing, and each row obeys $\|s\|^2 - \|s'\|^2 = (\alpha - 1)\|2^k v\|^2$.

Remark 3.3.14: running time

- Number of phases: $\delta(t) \leq \frac{2\|t\|}{\lambda_1(\mathcal{L})} \leq 2\|t\|$ because $\mathcal{L} \subseteq \mathbb{Z}^n$. So $k_0 = O(\log \|t\|)$ phases.

Remark 3.3.14: running time

- Number of phases: $\delta(t) \leq \frac{2\|t\|}{\lambda_1(\mathcal{L})} \leq 2\|t\|$ because $\mathcal{L} \subseteq \mathbb{Z}^n$. So $k_0 = O(\log \|t\|)$ phases.
- Iterations per phase: at most 4^n (Remark 3.3.13).

Remark 3.3.14: running time

- Number of phases: $\delta(t) \leq \frac{2\|t\|}{\lambda_1(\mathcal{L})} \leq 2\|t\|$ because $\mathcal{L} \subseteq \mathbb{Z}^n$. So $k_0 = O(\log \|t\|)$ phases.
- Iterations per phase: at most 4^n (Remark 3.3.13).
- Work per iteration: one pass over $\mathcal{R}$, that is $O(|\mathcal{R}| n) = 2^n \text{poly}(n)$.

Remark 3.3.14: running time

- Number of phases: $\delta(t) \leq \frac{2\|t\|}{\lambda_1(\mathcal{L})} \leq 2\|t\|$ because $\mathcal{L} \subseteq \mathbb{Z}^n$. So $k_0 = O(\log \|t\|)$ phases.
- Iterations per phase: at most 4^n (Remark 3.3.13).
- Work per iteration: one pass over $\mathcal{R}$, that is $O(|\mathcal{R}| n) = 2^n \text{poly}(n)$.
- Notes: “CVP in 4^n time, given $\mathcal{R}$ ”. The count above gives 8^n ; the gap and its fix are in the appendix. The conclusion $4^n \text{poly}(n) \log \|t\|$ is correct.

Remark 3.3.15: correctness

- On exit, $s \in V$, and $s \in t - \mathcal{L}$ because only lattice vectors were subtracted.

Remark 3.3.15: correctness

- On exit, $s \in V$, and $s \in t - \mathcal{L}$ because only lattice vectors were subtracted.
- So $x = t - s \in \mathcal{L}$, and for every $v \in \mathcal{L}$,

$$\|t - x\| = \|s\| \leq \|s - v\| = \|t - (x + v)\|.$$

Remark 3.3.15: correctness

- On exit, $s \in V$, and $s \in t - \mathcal{L}$ because only lattice vectors were subtracted.
- So $x = t - s \in \mathcal{L}$, and for every $v \in \mathcal{L}$,

$$\|t - x\| = \|s\| \leq \|s - v\| = \|t - (x + v)\|.$$

- As $x + v$ runs over $\mathcal{L}$, this says x is a closest vector. $\square$

Computing the Voronoi cell

- Algorithm 7 needs $\mathcal{R}$, and $\mathcal{R}$ consists of shortest vectors of cosets of $2\mathcal{L}$: that is CVP again.

Chicken and egg

- Algorithm 7 needs $\mathcal{R}$, and $\mathcal{R}$ consists of shortest vectors of cosets of $2\mathcal{L}$: that is CVP again.
- Way out: recurse on the rank. Write $T_{\text{Vor}}(n)$ for computing $\mathcal{R}$, and $T_{\text{CVP}}(n, N)$ for N CVP instances on one rank- n lattice.

Chicken and egg

- Algorithm 7 needs $\mathcal{R}$, and $\mathcal{R}$ consists of shortest vectors of cosets of $2\mathcal{L}$: that is CVP again.
- Way out: recurse on the rank. Write $T_{\text{Vor}}(n)$ for computing $\mathcal{R}$, and $T_{\text{CVP}}(n, N)$ for N CVP instances on one rank- n lattice.

$$(A) \quad T_{\text{Vor}}(n) \leq T_{\text{CVP}}(n, 2^n)$$

$$(B) \quad T_{\text{CVP}}(n, 2^n) \leq T_{\text{CVP}}(n-1, 2^{2n+1})$$

$$(C) \quad T_{\text{CVP}}(n-1, 2^{2n+1}) \leq T_{\text{Vor}}(n-1) + 2^{2n+1} \cdot 4^n \text{poly}(n)$$

(A) Relevant vectors from 2^n CVP instances

- Coset representatives: the vertices $v = \sum_i \alpha_i b_i$, $\alpha \in \{0, 1\}^n \setminus \{0\}$, of $\mathcal{P}(B)$.

(A) Relevant vectors from 2^n CVP instances

- Coset representatives: the vertices $v = \sum_i \alpha_i b_i$, $\alpha \in \{0, 1\}^n \setminus \{0\}$, of $\mathcal{P}(B)$.
- For each, solve $y = \text{CVP}(2\mathcal{L}, v)$ and set $v^* = v - y$.

(A) Relevant vectors from 2^n CVP instances

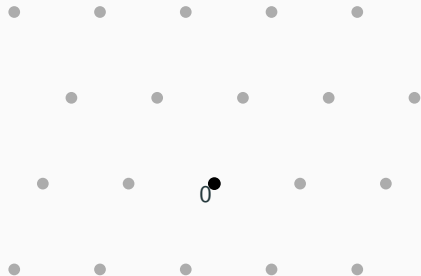
- Coset representatives: the vertices $v = \sum_i \alpha_i b_i$, $\alpha \in \{0, 1\}^n \setminus \{0\}$, of $\mathcal{P}(B)$.
- For each, solve $y = \text{CVP}(2\mathcal{L}, v)$ and set $v^* = v - y$.
- As y runs over $2\mathcal{L}$, $v - y$ runs over the coset $v + 2\mathcal{L}$. So v^* is a shortest vector of that coset, and it is nonzero.

(A) Relevant vectors from 2^n CVP instances

- Coset representatives: the vertices $v = \sum_i \alpha_i b_i$, $\alpha \in \{0, 1\}^n \setminus \{0\}$, of $\mathcal{P}(B)$.
- For each, solve $y = \text{CVP}(2\mathcal{L}, v)$ and set $v^* = v - y$.
- As y runs over $2\mathcal{L}$, $v - y$ runs over the coset $v + 2\mathcal{L}$. So v^* is a shortest vector of that coset, and it is nonzero.
- Output $\{\pm v^*\}$: at most $2(2^n - 1)$ vectors, containing $\mathcal{R}$ by Lemma 3.3.9.

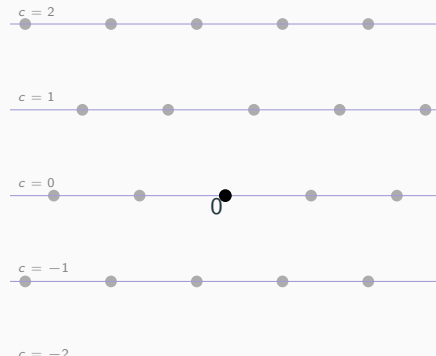
(B) Rank reduction: slicing into layers

- Write $\mathcal{L}_{n-1} = \mathcal{L}(b_1, \dots, b_{n-1})$ after LLL reduction.



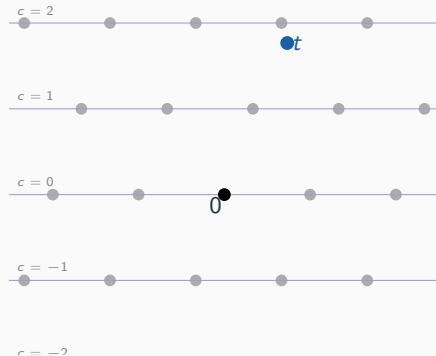
(B) Rank reduction: slicing into layers

- Write $\mathcal{L}_{n-1} = \mathcal{L}(b_1, \dots, b_{n-1})$ after LLL reduction.
- $\mathcal{L} = \bigsqcup_c (c b_n + \mathcal{L}_{n-1})$: parallel layers, spaced $\|\tilde{b}_n\|$ apart.



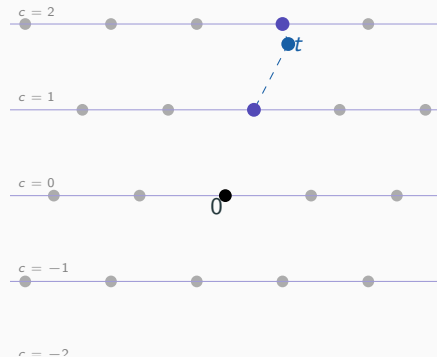
(B) Rank reduction: slicing into layers

- Write $\mathcal{L}_{n-1} = \mathcal{L}(b_1, \dots, b_{n-1})$ after LLL reduction.
- $\mathcal{L} = \bigsqcup_c (c b_n + \mathcal{L}_{n-1})$: parallel layers, spaced $\|\tilde{b}_n\|$ apart.
- Target t .



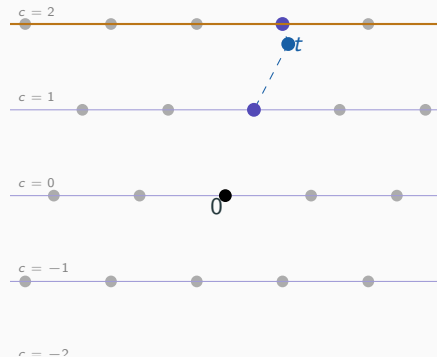
(B) Rank reduction: slicing into layers

- Write $\mathcal{L}_{n-1} = \mathcal{L}(b_1, \dots, b_{n-1})$ after LLL reduction.
- $\mathcal{L} = \bigsqcup_c (c b_n + \mathcal{L}_{n-1})$: parallel layers, spaced $\|\tilde{b}_n\|$ apart.
- Target t .
- In each nearby layer, solve a rank- $(n-1)$ CVP for the best point.



(B) Rank reduction: slicing into layers

- Write $\mathcal{L}_{n-1} = \mathcal{L}(b_1, \dots, b_{n-1})$ after LLL reduction.
- $\mathcal{L} = \bigsqcup_c (c b_n + \mathcal{L}_{n-1})$: parallel layers, spaced $\|\tilde{b}_n\|$ apart.
- Target t .
- In each nearby layer, solve a rank- $(n-1)$ CVP for the best point.
- Keep the best over the layers.



(B) How many layers?

- Only layers at distance $\leq \text{dist}(t, \mathcal{L})$ from t can contain the answer.

(B) How many layers?

- Only layers at distance $\leq \text{dist}(t, \mathcal{L})$ from t can contain the answer.
- The notes take 2^{n+1} choices of the last coefficient, so

$$T_{\text{CVP}}(n, 2^n) \leq T_{\text{CVP}}(n-1, 2^{n+1} \cdot 2^n) = T_{\text{CVP}}(n-1, 2^{2n+1}).$$

(B) How many layers?

- Only layers at distance $\leq \text{dist}(t, \mathcal{L})$ from t can contain the answer.
- The notes take 2^{n+1} choices of the last coefficient, so

$$T_{\text{CVP}}(n, 2^n) \leq T_{\text{CVP}}(n-1, 2^{n+1} \cdot 2^n) = T_{\text{CVP}}(n-1, 2^{2n+1}).$$

- Any bound of the form $2^{O(n)}$ is enough here. (What the notes cite gives a different constant; see the appendix.)

(C) Preprocess once, query many times

- All those instances live on the *same* lattice $\mathcal{L}_{n-1}$ (up to the factor 2).

(C) Preprocess once, query many times

- All those instances live on the *same* lattice $\mathcal{L}_{n-1}$ (up to the factor 2).
- Compute its Voronoi cell once, then answer each instance by Algorithm 7:

$$T_{\text{CVP}}(n-1, 2^{2n+1}) \leq T_{\text{Vor}}(n-1) + 2^{2n+1} \cdot 4^n \text{poly}(n).$$

(C) Preprocess once, query many times

- All those instances live on the *same* lattice $\mathcal{L}_{n-1}$ (up to the factor 2).
- Compute its Voronoi cell once, then answer each instance by Algorithm 7:

$$T_{\text{CVP}}(n-1, 2^{2n+1}) \leq T_{\text{Vor}}(n-1) + 2^{2n+1} \cdot 4^n \text{poly}(n).$$

- The two costs add, they do not multiply. This is exactly CVP *with preprocessing*.

- Chaining (A), (B), (C):

$$T_{\text{Vor}}(n) \leq T_{\text{Vor}}(n-1) + 2 \cdot 16^n \text{poly}(n).$$

- Chaining (A), (B), (C):

$$T_{\text{Vor}}(n) \leq T_{\text{Vor}}(n-1) + 2 \cdot 16^n \text{poly}(n).$$

- The geometric sum is dominated by its last term:

$$T_{\text{Vor}}(n) = O(16^n \text{poly}(n)), \quad T_{\text{CVP}}(n, 1) = O(16^n \text{poly}(n)).$$

- Chaining (A), (B), (C):

$$T_{\text{Vor}}(n) \leq T_{\text{Vor}}(n-1) + 2 \cdot 16^n \text{poly}(n).$$

- The geometric sum is dominated by its last term:

$$T_{\text{Vor}}(n) = O(16^n \text{poly}(n)), \quad T_{\text{CVP}}(n, 1) = O(16^n \text{poly}(n)).$$

- The notes remark that a better analysis gives 4^n . That is Micciancio–Voulgaris; it is not derived in the notes.

1. V = points whose closest lattice point is 0; the cells tile space, so CVP is point location.

Summary

1. V = points whose closest lattice point is 0; the cells tile space, so CVP is point location.
2. $V = \bigcap_{v \in \mathcal{R}} H_v$ with $|\mathcal{R}| \leq 2^{n+1}$: one relevant pair per nonzero coset of $2\mathcal{L}$.

Summary

1. V = points whose closest lattice point is 0; the cells tile space, so CVP is point location.
2. $V = \bigcap_{v \in \mathcal{R}} H_v$ with $|\mathcal{R}| \leq 2^{n+1}$: one relevant pair per nonzero coset of $2\mathcal{L}$.
3. Walk: measure $\delta(s)$, pick the shell 2^k , subtract $2^k v$ for the facet v . Each step shortens s and stays in δV .

Summary

1. V = points whose closest lattice point is 0; the cells tile space, so CVP is point location.
2. $V = \bigcap_{v \in \mathcal{R}} H_v$ with $|\mathcal{R}| \leq 2^{n+1}$: one relevant pair per nonzero coset of $2\mathcal{L}$.
3. Walk: measure $\delta(s)$, pick the shell 2^k , subtract $2^k v$ for the facet v . Each step shortens s and stays in δV .
4. Count: within a phase the iterates are distinct points of one coset inside $2^{k+1}V$, so at most 4^n of them; $O(\log \|t\|)$ phases.

Summary

1. V = points whose closest lattice point is 0; the cells tile space, so CVP is point location.
2. $V = \bigcap_{v \in \mathcal{R}} H_v$ with $|\mathcal{R}| \leq 2^{n+1}$: one relevant pair per nonzero coset of $2\mathcal{L}$.
3. Walk: measure $\delta(s)$, pick the shell 2^k , subtract $2^k v$ for the facet v . Each step shortens s and stays in δV .
4. Count: within a phase the iterates are distinct points of one coset inside $2^{k+1}V$, so at most 4^n of them; $O(\log \|t\|)$ phases.
5. Bootstrap: relevant vectors come from CVP on $2\mathcal{L}$, solved by slicing into layers of rank $n - 1$.

Appendix: corrections and extras

Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.

Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.
- **Lemma 3.3.8, eq. (3.3.1).** Neither inequality in the notes' chain is strict on its own; the strictness of $\|w - u\| < \|w\|$ comes from $u \neq 0$, not from $u \neq w$. ($u \neq w$ gives the other bound $\|u\| < \|w\|$.)

Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.
- **Lemma 3.3.8, eq. (3.3.1).** Neither inequality in the notes' chain is strict on its own; the strictness of $\|w - u\| < \|w\|$ comes from $u \neq 0$, not from $u \neq w$. ($u \neq w$ gives the other bound $\|u\| < \|w\|$.)
- **Lemma 3.3.8, end.** "We can keep repeating this, but not infinitely" should be an induction on $\|w\|$.

Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.
- **Lemma 3.3.8, eq. (3.3.1).** Neither inequality in the notes' chain is strict on its own; the strictness of $\|w - u\| < \|w\|$ comes from $u \neq 0$, not from $u \neq w$. ($u \neq w$ gives the other bound $\|u\| < \|w\|$.)
- **Lemma 3.3.8, end.** "We can keep repeating this, but not infinitely" should be an induction on $\|w\|$.
- **Lemma 3.3.9.** "At the boundary of $\mathcal{P}(B)$ " should read "at the vertices". The distance of $\frac{v^* + w}{2}$ from $\frac{w}{2}$ is "at most", not "less than", that of 0 (which still suffices). The proof gives the sharper $|\mathcal{R}| \leq 2(2^n - 1)$.

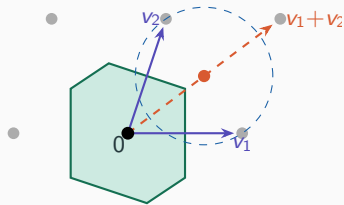
Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.
- **Lemma 3.3.8, eq. (3.3.1).** Neither inequality in the notes' chain is strict on its own; the strictness of $\|w - u\| < \|w\|$ comes from $u \neq 0$, not from $u \neq w$. ($u \neq w$ gives the other bound $\|u\| < \|w\|$.)
- **Lemma 3.3.8, end.** "We can keep repeating this, but not infinitely" should be an induction on $\|w\|$.
- **Lemma 3.3.9.** "At the boundary of $\mathcal{P}(B)$ " should read "at the vertices". The distance of $\frac{v^* + w}{2}$ from $\frac{w}{2}$ is "at most", not "less than", that of 0 (which still suffices). The proof gives the sharper $|\mathcal{R}| \leq 2(2^n - 1)$.
- **Algorithm 7.** The input should be $B \in \mathbb{R}^{n \times n}$, not $\mathbb{R}^{n \times m}$.

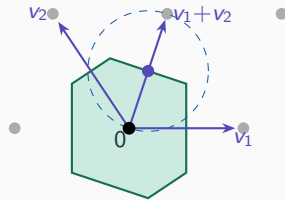
Corrections to the notes (1)

- **Example 3.3.7.** The four-way tie needs $v_1 \perp v_2$. In general $\|m - v_1\|^2 - \|m\|^2 = -\langle v_1, v_2 \rangle$ with $m = (v_1 + v_2)/2$: for an obtuse pair $v_1 + v_2$ can be relevant. Next slide.
- **Lemma 3.3.8, eq. (3.3.1).** Neither inequality in the notes' chain is strict on its own; the strictness of $\|w - u\| < \|w\|$ comes from $u \neq 0$, not from $u \neq w$. ($u \neq w$ gives the other bound $\|u\| < \|w\|$.)
- **Lemma 3.3.8, end.** "We can keep repeating this, but not infinitely" should be an induction on $\|w\|$.
- **Lemma 3.3.9.** "At the boundary of $\mathcal{P}(B)$ " should read "at the vertices". The distance of $\frac{v^* + w}{2}$ from $\frac{w}{2}$ is "at most", not "less than", that of 0 (which still suffices). The proof gives the sharper $|\mathcal{R}| \leq 2(2^n - 1)$.
- **Algorithm 7.** The input should be $B \in \mathbb{R}^{n \times n}$, not $\mathbb{R}^{n \times m}$.
- **Remark 3.3.13.** "Infinite vectors in $(s - 2^k \mathcal{L}) \cap 2^{k+1} V$ " should read "more than 4^n ".

Correction: Example 3.3.7 depends on the angle

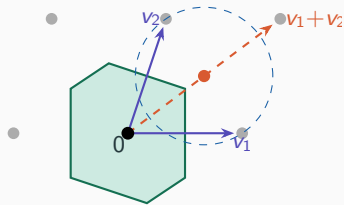


$v_1 = b_1$, $v_2 = b_2$, acute: $v_1 + v_2$ is not relevant.

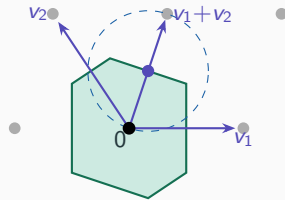


The *same* lattice with $v_1 = b_1$, $v_2 = b_2 - b_1$, obtuse: now $v_1 + v_2 = b_2$ is relevant.

Correction: Example 3.3.7 depends on the angle



$v_1 = b_1$, $v_2 = b_2$, acute: $v_1 + v_2$ is not relevant.



The *same* lattice with $v_1 = b_1$, $v_2 = b_2 - b_1$, obtuse: now $v_1 + v_2 = b_2$ **is** relevant.

So “a sum of two relevant vectors is not relevant” is false; the notes’ claim holds when $\langle v_1, v_2 \rangle \geq 0$.

Correction: Remark 3.3.14 counts iterations, not time

- Each iteration costs a pass over $\mathcal{R}$: $2^n \text{poly}(n)$. With 4^n iterations per phase the notes' argument gives 8^n , and the recursion would then give 32^n , not 16^n .

Correction: Remark 3.3.14 counts iterations, not time

- Each iteration costs a pass over $\mathcal{R}$: $2^n \text{poly}(n)$. With 4^n iterations per phase the notes' argument gives 8^n , and the recursion would then give 32^n , not 16^n .
- **Equal-norm lemma.** If $a, b \in V$ and $a - b \in \mathcal{L}$, then $\|a\| = \|b\|$.
Proof: $\|a\| \leq \|a - (a - b)\| = \|b\|$ and $\|b\| \leq \|b + (a - b)\| = \|a\|$.

Correction: Remark 3.3.14 counts iterations, not time

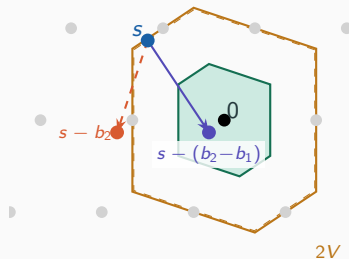
- Each iteration costs a pass over $\mathcal{R}$: $2^n \text{poly}(n)$. With 4^n iterations per phase the notes' argument gives 8^n , and the recursion would then give 32^n , not 16^n .
- **Equal-norm lemma.** If $a, b \in V$ and $a - b \in \mathcal{L}$, then $\|a\| = \|b\|$.
Proof: $\|a\| \leq \|a - (a - b)\| = \|b\|$ and $\|b\| \leq \|b + (a - b)\| = \|a\|$.
- **Consequence.** Two iterates $x \neq y$ of one phase cannot satisfy $x - y \in 2^{k+1}\mathcal{L}$: applying the lemma to $x/2, y/2 \in 2^k V$ would force $\|x\| = \|y\|$, contradicting strict descent.

Correction: Remark 3.3.14 counts iterations, not time

- Each iteration costs a pass over $\mathcal{R}$: $2^n \text{poly}(n)$. With 4^n iterations per phase the notes' argument gives 8^n , and the recursion would then give 32^n , not 16^n .
- **Equal-norm lemma.** If $a, b \in V$ and $a - b \in \mathcal{L}$, then $\|a\| = \|b\|$.
Proof: $\|a\| \leq \|a - (a - b)\| = \|b\|$ and $\|b\| \leq \|b + (a - b)\| = \|a\|$.
- **Consequence.** Two iterates $x \neq y$ of one phase cannot satisfy $x - y \in 2^{k+1}\mathcal{L}$: applying the lemma to $x/2, y/2 \in 2^k V$ would force $\|x\| = \|y\|$, contradicting strict descent.
- So a phase has at most $[2^k \mathcal{L} : 2^{k+1} \mathcal{L}] = 2^n$ iterations, and the total is $O(4^n n \log \|t\|)$, as the notes claim.

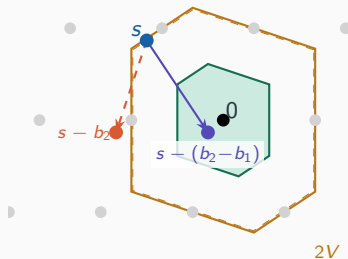
Why line 5 must take the argmax

- $s = (-2.5, 2.6)$: $\delta(s) \approx 1.97$, argmax
 $v = b_2 - b_1$.



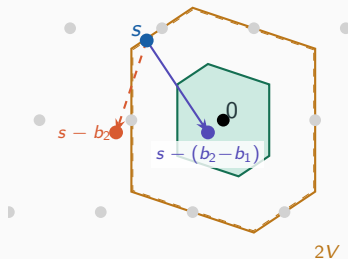
Why line 5 must take the argmax

- $s = (-2.5, 2.6)$: $\delta(s) \approx 1.97$, $\operatorname{argmax} v = b_2 - b_1$.
- b_2 is violated too:
 $2\langle s, b_2 \rangle / \|b_2\|^2 = 1.06 > 1$, and
 $\|s - b_2\| \approx 3.52 < 3.61 \approx \|s\|$.



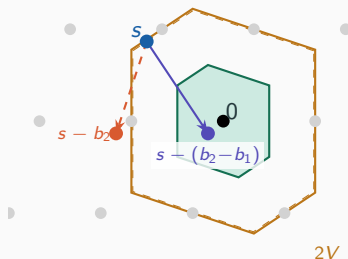
Why line 5 must take the argmax

- $s = (-2.5, 2.6)$: $\delta(s) \approx 1.97$, $\operatorname{argmax} v = b_2 - b_1$.
- b_2 is violated too:
 $2\langle s, b_2 \rangle / \|b_2\|^2 = 1.06 > 1$, and
 $\|s - b_2\| \approx 3.52 < 3.61 \approx \|s\|$.
- But $\delta(s - b_2) = 7/3 > 2$: that step leaves $2V$, and the counting argument breaks.

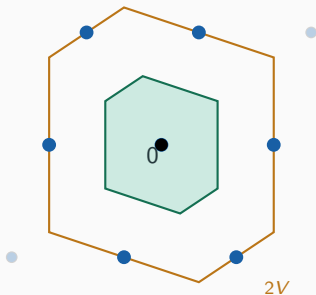


Why line 5 must take the argmax

- $s = (-2.5, 2.6)$: $\delta(s) \approx 1.97$, $\operatorname{argmax} v = b_2 - b_1$.
- b_2 is violated too:
 $2\langle s, b_2 \rangle / \|b_2\|^2 = 1.06 > 1$, and
 $\|s - b_2\| \approx 3.52 < 3.61 \approx \|s\|$.
- But $\delta(s - b_2) = 7/3 > 2$: that step leaves $2V$, and the counting argument breaks.
- Reason: s is not on $\partial(\delta H_{b_2})$, so part 2 of Lemma 3.3.11 does not apply.



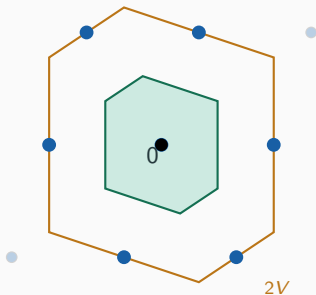
Two remarks on the counting



$s = 0$: seven points of $s - \mathcal{L}$ in $2V$, namely 0 and the six relevant vectors on the boundary.

- $\text{vol}(2V) = 2^n \det \mathcal{L}$, so a generic coset has about 2^n points in $2V$; the bound 4^n of Lemma 3.3.12 is loose but correct.

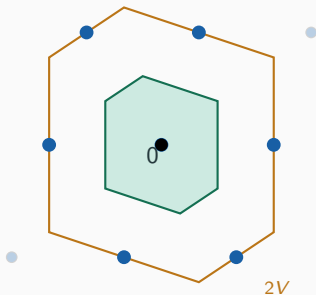
Two remarks on the counting



$s = 0$: seven points of $s - \mathcal{L}$ in $2V$, namely 0 and the six relevant vectors on the boundary.

- $\text{vol}(2V) = 2^n \det \mathcal{L}$, so a generic coset has about 2^n points in $2V$; the bound 4^n of Lemma 3.3.12 is loose but correct.
- The Micciancio slides state $|(\bar{t} - \Lambda) \cap 2\mathcal{V}| \leq 2^n$. Taken literally that is false for closed $\mathcal{V}$: the picture on the left gives $7 > 4$, and $\mathcal{L} = \mathbb{Z}$, $t = 0$ gives $\{-1, 0, 1\}$.

Two remarks on the counting



$s = 0$: seven points of $s - \mathcal{L}$ in $2V$, namely 0 and the six relevant vectors on the boundary.

- $\text{vol}(2V) = 2^n \det \mathcal{L}$, so a generic coset has about 2^n points in $2V$; the bound 4^n of Lemma 3.3.12 is loose but correct.
- The Micciancio slides state $|(\bar{t} - \Lambda) \cap 2\mathcal{V}| \leq 2^n$. Taken literally that is false for closed $\mathcal{V}$: the picture on the left gives $7 > 4$, and $\mathcal{L} = \mathbb{Z}$, $t = 0$ gives $\{-1, 0, 1\}$.
- What is true is the bound on the *iterates*, via the equal-norm lemma.

Loose ends in the computation of $\mathcal{R}$

- **The candidate list may be too big.** If a coset has several shortest vectors, $\pm v^*$ is not relevant. Harmless: $V = \bigcap_{v \in \mathcal{R}'} H_v$ for any $\mathcal{R} \subseteq \mathcal{R}' \subseteq \mathcal{L} \setminus \{0\}$, and Algorithm 7 only uses $\mathcal{R}$ through $\max_v 2\langle s, v \rangle / \|v\|^2$.

Loose ends in the computation of $\mathcal{R}$

- **The candidate list may be too big.** If a coset has several shortest vectors, $\pm v^*$ is not relevant. Harmless: $V = \bigcap_{v \in \mathcal{R}'} H_v$ for any $\mathcal{R} \subseteq \mathcal{R}' \subseteq \mathcal{L} \setminus \{0\}$, and Algorithm 7 only uses $\mathcal{R}$ through $\max_v 2\langle s, v \rangle / \|v\|^2$.
- **The layer count.** The notes say 2^{n+1} and point to Algorithm 6, whose Theorem 3.2.1 gives about $2^{n/2}$ layers for an LLL basis. Micciancio–Voulgaris use dual LLL and get 2^n . Any $2^{O(n)}$ bound suffices.

Loose ends in the computation of $\mathcal{R}$

- **The candidate list may be too big.** If a coset has several shortest vectors, $\pm v^*$ is not relevant. Harmless: $V = \bigcap_{v \in \mathcal{R}'} H_v$ for any $\mathcal{R} \subseteq \mathcal{R}' \subseteq \mathcal{L} \setminus \{0\}$, and Algorithm 7 only uses $\mathcal{R}$ through $\max_v 2\langle s, v \rangle / \|v\|^2$.
- **The layer count.** The notes say 2^{n+1} and point to Algorithm 6, whose Theorem 3.2.1 gives about $2^{n/2}$ layers for an LLL basis. Micciancio–Voulgaris use dual LLL and get 2^n . Any $2^{O(n)}$ bound suffices.
- **Rank- $(n-1)$ instances** live in $\text{span}(\mathcal{L}_{n-1})$: project the target there first, the orthogonal part is a common constant.

- D. Aggarwal, *Lattices*, lecture notes, Section 3.3.
- D. Micciancio and P. Voulgaris, STOC 2010 / SIAM J. Comput. 42(3), 2013.
- D. Micciancio, slides, Barriers II Workshop, Princeton, 2010.

All figures are computed from the lattice $b_1 = (3, 0)$, $b_2 = (1, 3)$; the worked example was checked against brute-force enumeration.