

A geometric procedure for Presburger arithmetic

Alessio Mansutti

joint work with Dmitry Chistikov and Christoph Haase



Presburger arithmetic (PA)

The first-order theory of $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$

“Every integer is either even or odd”

$$\forall x \exists y : x = 2y \vee x = 2y + 1$$

Why Presburger arithmetic?

Wide range of applications in verification, program synthesis, compiler optimisation, games...



M. Presburger

Presburger arithmetic (PA)

The first-order theory of $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$

“Every integer is either even or odd”

$$\forall x \exists y : x = 2y \vee x = 2y + 1$$

Why Presburger arithmetic?

Wide range of applications in verification, program synthesis, compiler optimisation, games...



M. Presburger

Several applications require to reason on the **set of solutions** of a formula.

Example [Verdoolaege et al., Algorithmica 48, 2007]:

“How many times is a loop executed?” $\rightsquigarrow f(\mathbf{y}) = \#\{\mathbf{x} \in \mathbb{Z}^d \mid A \cdot \mathbf{x} \geq B \cdot \mathbf{y} + \mathbf{c}\}$

Presburger arithmetic (PA)

The first-order theory of $\langle \mathbb{Z}, 0, 1, +, \leq \rangle$

“Every integer is either even or odd”

$$\forall x \exists y : x = 2y \vee x = 2y + 1$$

Why Presburger arithmetic?

Wide range of applications in verification, program synthesis, compiler optimisation, games...



M. Presburger

Theorem (Ginsburg and Spanier, '66)

Sets definable in Presburger arithmetic coincide with the family of **semilinear sets**.

Semilinear sets

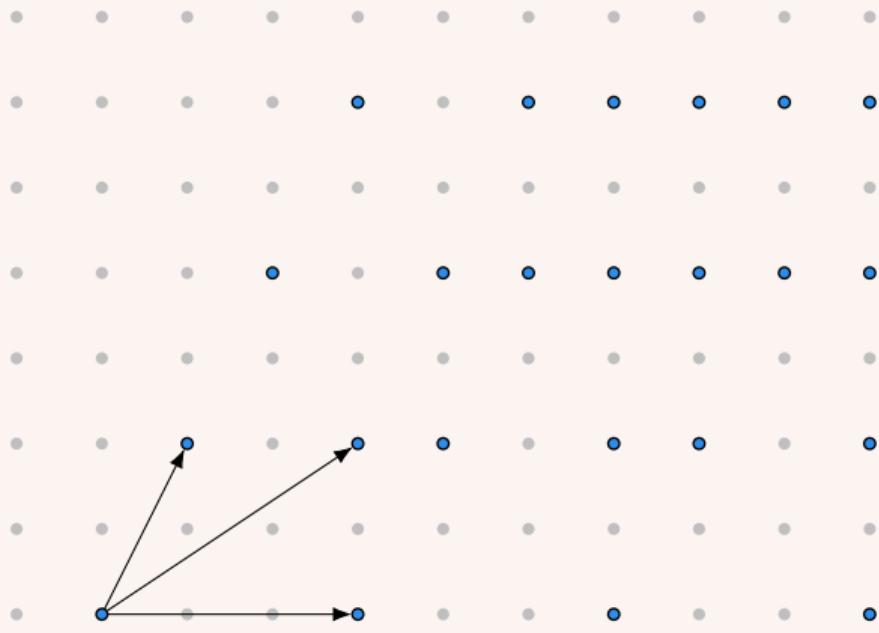
Arithmetic progression



$b + i \cdot p$, where $i \in \mathbb{N}$

b base point, p period

Semilinear sets

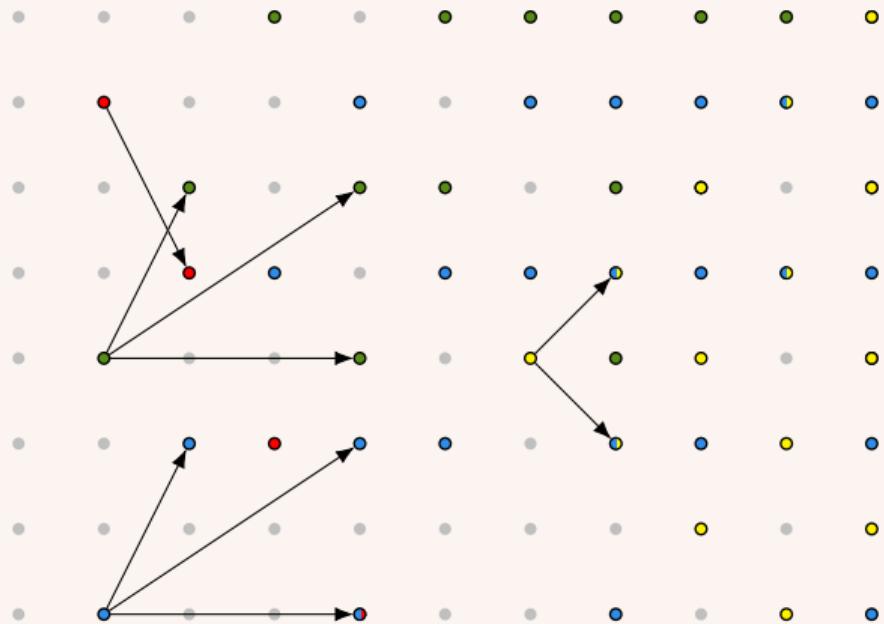


Linear set

(arithmetic progression
in multiple dimensions)

$L(b, P)$, where b base
and $P = \{p_1, \dots, p_n\}$ periods

Semilinear sets

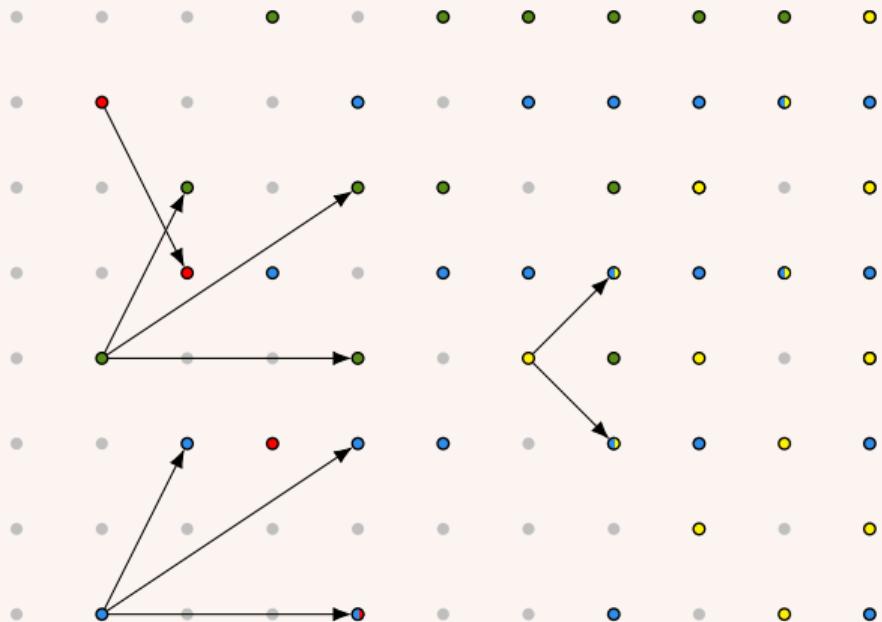


Semilinear set

(finite union of
linear sets)

$\bigcup_{i \in I} L(b_i, P_i),$
where I finite set of indices

Semilinear sets

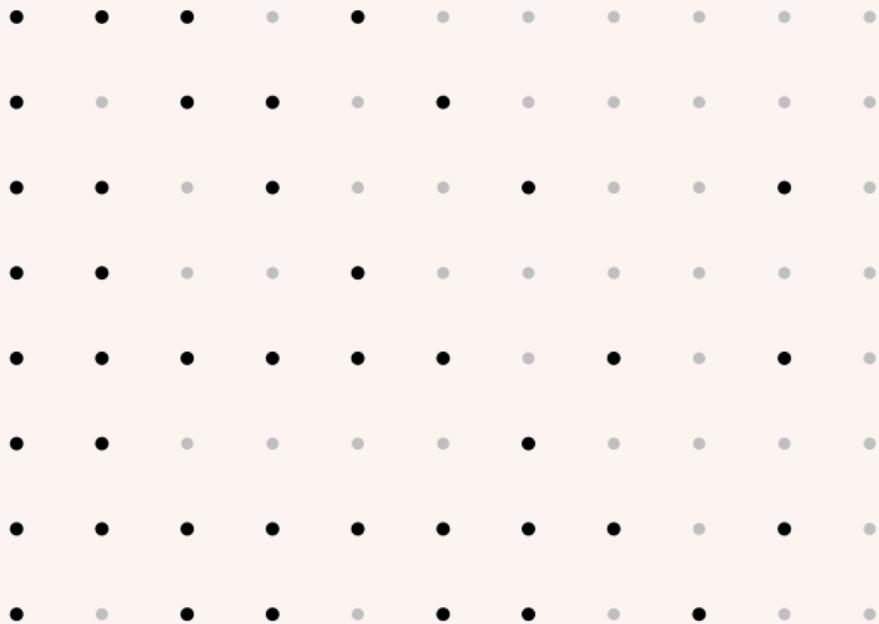


Ginsburg & Spanier, '66

The set of solutions of a system of linear inequalities over \mathbb{Z} is semilinear. Semilinear sets are closed under

- union
- projection
- complementation

Semilinear sets



Ginsburg & Spanier, '66

The set of solutions of a system of linear inequalities over \mathbb{Z} is semilinear. Semilinear sets are closed under

- union
- projection
- complementation

Main problem: How to compute the complement of a semilinear set **optimally?**

A geometric procedure for Presburger arithmetic

In this talk: We discuss an optimal algorithm to complement semilinear sets.

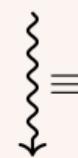
A geometric procedure for Presburger arithmetic

In this talk: We discuss an optimal algorithm to complement semilinear sets.

Quantifier elimination

[Presburger, '29]

$$\exists x : \varphi(x, \mathbf{y})$$

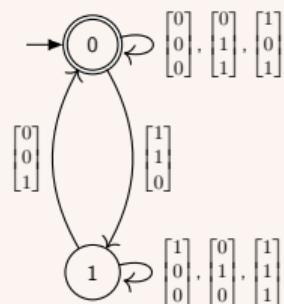


$$\psi(\mathbf{y})$$

3EXPTIME

Automata

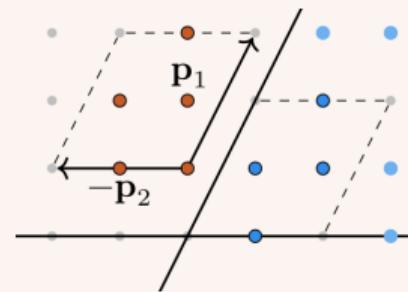
[Büchi, '60]



3EXPTIME

Geometry

[Ginsburg and Spanier, '66]



TOWER

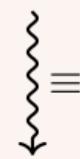
A geometric procedure for Presburger arithmetic

In this talk: We discuss an optimal algorithm to complement semilinear sets.

Quantifier elimination

[Presburger, '29]

$$\exists x : \varphi(x, \mathbf{y})$$

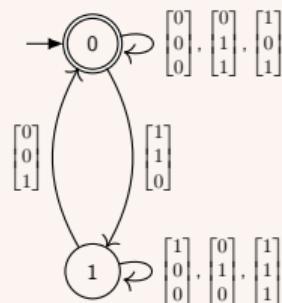


$$\psi(\mathbf{y})$$

3EXPTIME

Automata

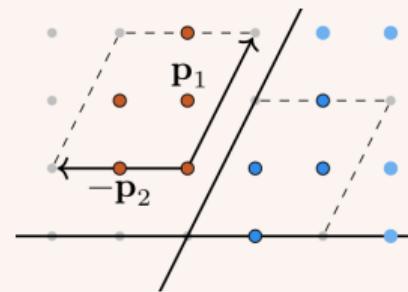
[Büchi, '60]



3EXPTIME

Geometry

[Ginsburg and Spanier, '66]



3EXPTIME

Chapter 1

In which we forget about the integers and work over the reals

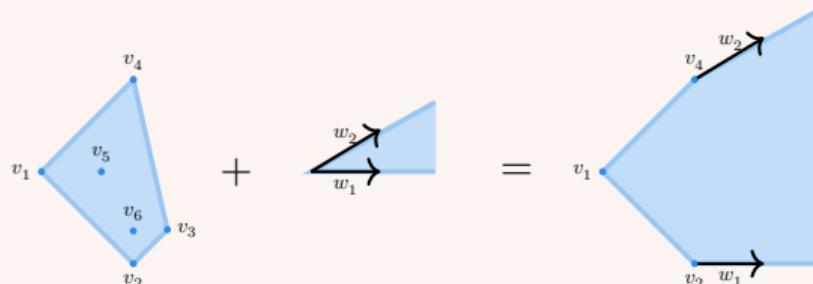
Goal: reflect on how to complement a union of polyhedra over \mathbb{R} .

The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl theorem (1897, 1935))

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

- (H) $S = \{\mathbf{x} \in \mathbb{R} : A \cdot \mathbf{x} \leq \mathbf{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\mathbf{b} \in \mathbb{Q}^d$
- (V) $S = \text{conv } V + \text{cone } W$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.



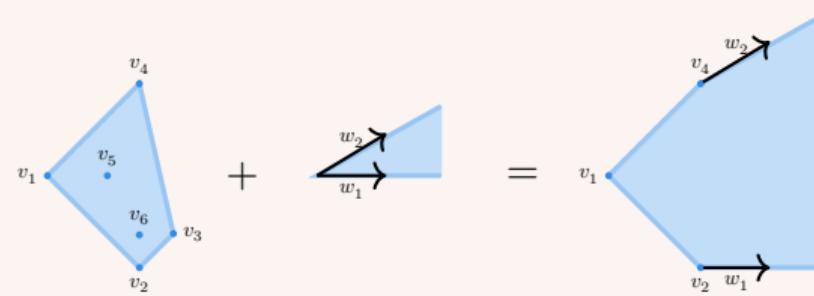
$$\text{conv}\{v_1, \dots, v_6\} \quad \text{cone}\{w_1, w_2\}$$

The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl theorem (1897, 1935))

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

- (H) $S = \{\mathbf{x} \in \mathbb{R} : A \cdot \mathbf{x} \leq \mathbf{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\mathbf{b} \in \mathbb{Q}^d$
- (V) $S = \text{conv } V + \text{cone } W$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.



$\text{conv}\{v_1, \dots, v_6\}$

$\text{cone}\{w_1, w_2\}$

Cost of switching:

bitsize of numbers:

$$\langle \text{output} \rangle \leq \text{poly}(d) \cdot \langle \text{input} \rangle$$

amount of numbers (with repetitions):

$$\#(\text{output}) \leq \#(\text{input}) \uparrow d$$

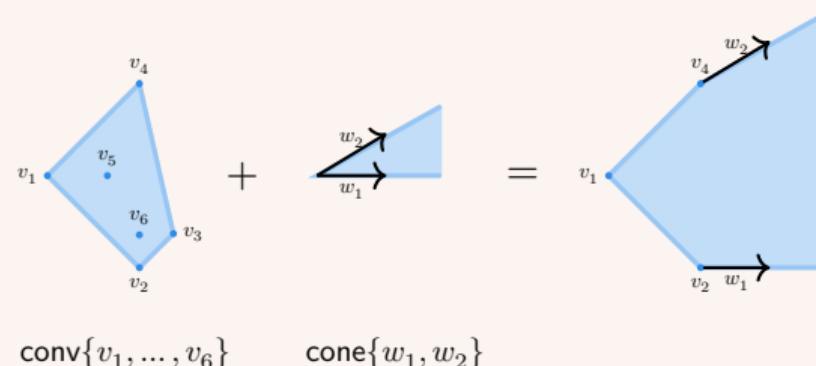
$$(a \uparrow b \uparrow c = (a+2)^{(b+2)^{\text{poly}(c)}})$$

The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl theorem (1897, 1935))

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

- (H) $S = \{\mathbf{x} \in \mathbb{R} : A \cdot \mathbf{x} \leq \mathbf{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\mathbf{b} \in \mathbb{Q}^d$
- (V) $S = \text{conv } V + \text{cone } W$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.



Cost of switching: (V) \rightarrow (H)

bitsize of numbers:

$$\langle A \rangle, \langle \mathbf{b} \rangle \leq \text{poly}(d) \cdot \max(\langle V \rangle, \langle W \rangle)$$

amount of numbers (with repetitions):

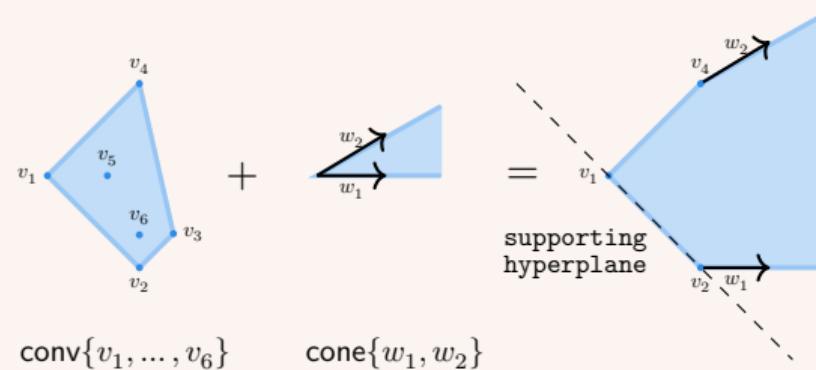
$$\#[A \mid \mathbf{b}] \leq (\#V + \#W) \uparrow d$$

The geometry of a system of inequalities over the **reals**

Theorem (Minkowski-Weyl theorem (1897, 1935))

Consider $S \subseteq \mathbb{R}^d$. The two following statements are equivalent:

- (H) $S = \{\mathbf{x} \in \mathbb{R} : A \cdot \mathbf{x} \leq \mathbf{b}\}$ for some matrix $A \in \mathbb{Q}^{n \times d}$ and vector $\mathbf{b} \in \mathbb{Q}^d$
- (V) $S = \text{conv } V + \text{cone } W$ for some finite sets $V, W \subseteq \mathbb{Q}^d$.



Cost of switching: (V) \rightarrow (H)

bitsize of numbers:

$$\langle A \rangle, \langle \mathbf{b} \rangle \leq \text{poly}(d) \cdot \max(\langle V \rangle, \langle W \rangle)$$

amount of numbers (with repetitions):

$$\#[A | \mathbf{b}] \leq (\#V + \#W) \uparrow d$$

Cutting \mathbb{R}^d using hyperplanes

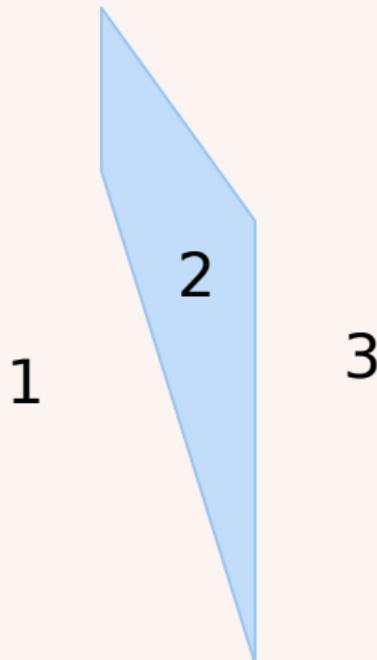
Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.

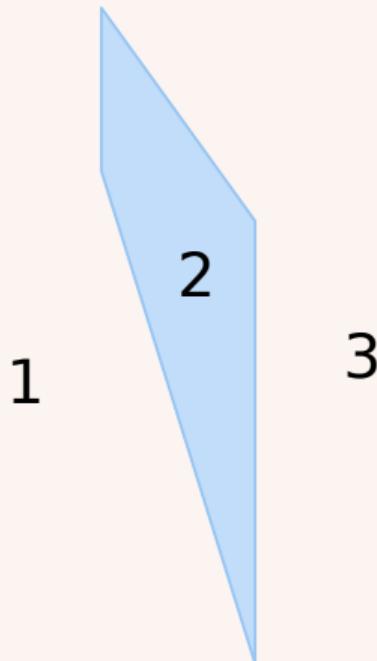


$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.



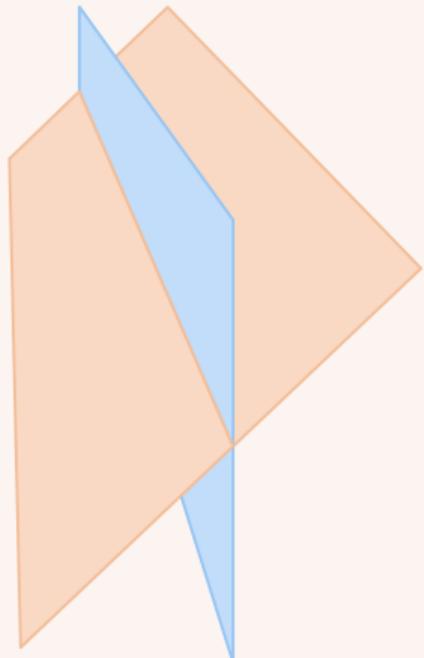
$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

$$\left\{ \begin{array}{l} \Phi(0, n) = \Phi(d, 0) = 1 \\ \end{array} \right.$$

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.



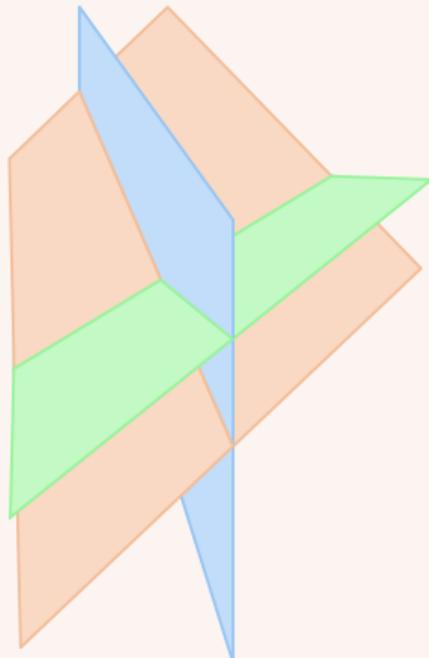
$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

$$\begin{cases} \Phi(0, n) = \Phi(d, 0) = 1 \\ \Phi(d+1, n+1) \leq \Phi(d+1, n) + 2\Phi(d, n) \end{cases}$$

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.



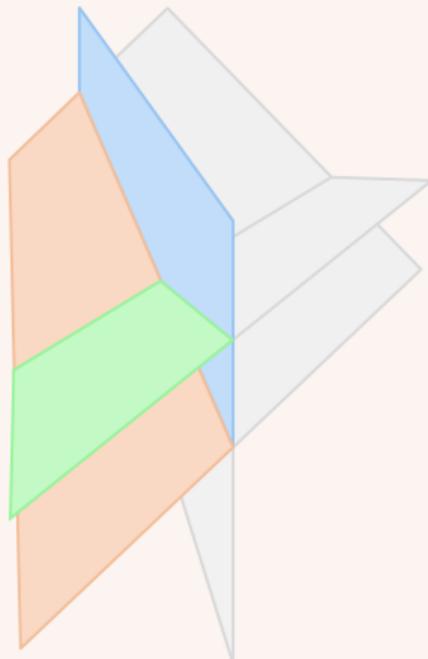
$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

$$\begin{cases} \Phi(0, n) = \Phi(d, 0) = 1 \\ \Phi(d+1, n+1) \leq \Phi(d+1, n) + 2\Phi(d, n) \end{cases}$$

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.



$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

$$\begin{cases} \Phi(0, n) = \Phi(d, 0) = 1 \\ \Phi(d+1, n+1) \leq \Phi(d+1, n) + 2\Phi(d, n) \end{cases}$$

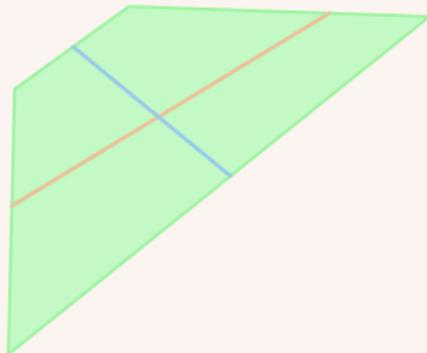
The $(n + 1)$ -th hyperplane cuts
the parts it intersects in three.

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.

$$\Phi(d, 1) = 3 \quad (d \geq 1)$$



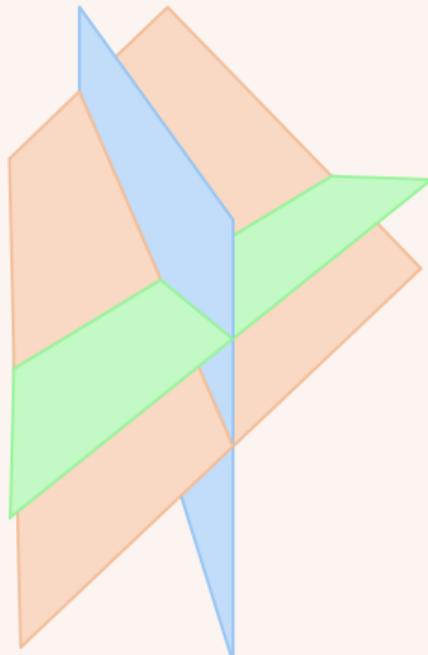
$$\begin{cases} \Phi(0, n) = \Phi(d, 0) = 1 \\ \Phi(d+1, n+1) \leq \Phi(d+1, n) + 2\Phi(d, n) \end{cases}$$

The $(n + 1)$ -th hyperplane cuts
the parts it intersects in three.

Cutting \mathbb{R}^d using hyperplanes

Question: In how many parts can we cut \mathbb{R}^d using n hyperplanes?

$\Phi(d, n) :=$ maximal number of parts, in dimension d and using n hyperplanes.



$$\Phi(d, 1) = 3 \quad (d \geq 1)$$

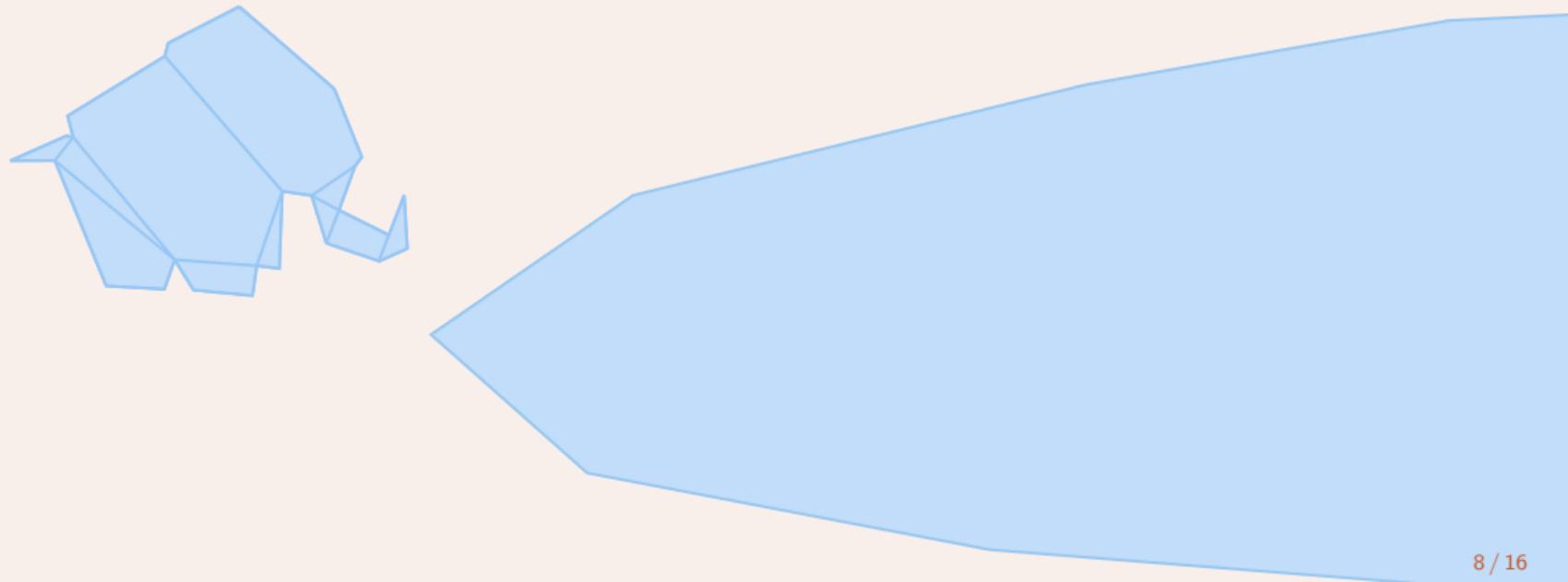
$$\begin{cases} \Phi(0, n) = \Phi(d, 0) = 1 \\ \Phi(d+1, n+1) \leq \Phi(d+1, n) + 2\Phi(d, n) \end{cases}$$

$$\Rightarrow \Phi(d, n) \leq (2n)^d + 1$$

“ n^d cutting lemma”

Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?



Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

1. Find a family of (supporting) hyperplanes \mathcal{H} that **carves out** all polyhedra



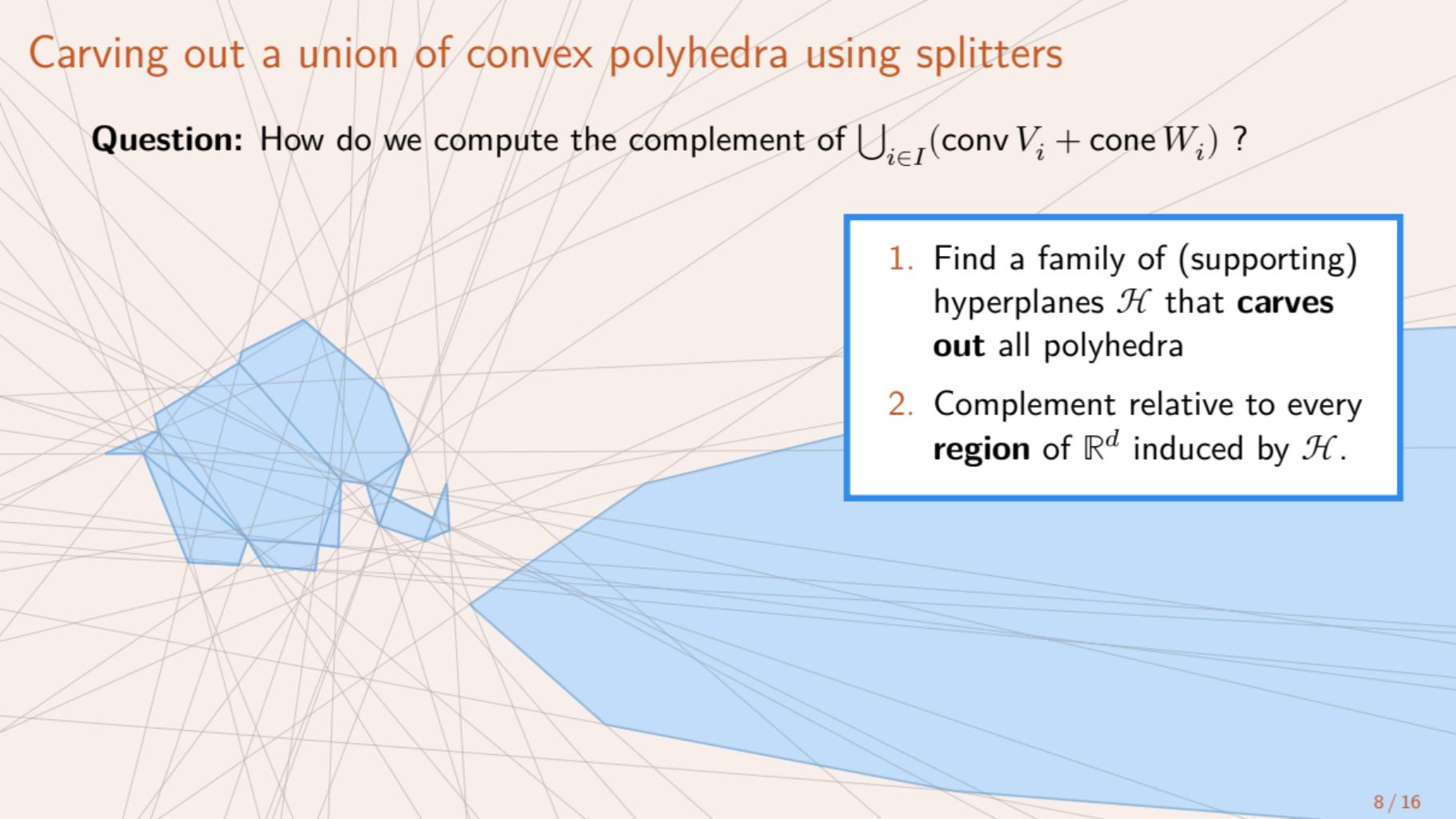
Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

1. Find a family of (supporting) hyperplanes \mathcal{H} that **carves out** all polyhedra
2. Complement relative to every **region** of \mathbb{R}^d induced by \mathcal{H} .

Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

- 
1. Find a family of (supporting) hyperplanes \mathcal{H} that **carves out** all polyhedra
 2. Complement relative to every **region** of \mathbb{R}^d induced by \mathcal{H} .

Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

An **(\mathbb{R} -)splitter** for a family of convex polyhedra \mathcal{P} is a family of convex polyhedra \mathcal{R} s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Claim: Given \mathcal{R} it is easy to compute $\mathbb{R}^d \setminus \bigcup \mathcal{P}$.

Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

An **(\mathbb{R} -)splitter** for a family of convex polyhedra \mathcal{P} is a family of convex polyhedra \mathcal{R} s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Claim: Given \mathcal{R} it is easy to compute $\mathbb{R}^d \setminus \bigcup \mathcal{P}$.

Theorem

Every $\mathcal{P} = \{\text{conv } V_i + \text{cone } W_i\}_{i \in I}$ has an \mathbb{R} -splitter $\mathcal{R} = \{\text{conv } C_j + \text{cone } Q_j\}_{j \in J}$ s.t.

$$\langle \mathcal{R} \rangle \leq \text{poly}(d) \cdot \langle \mathcal{P} \rangle \quad \text{and} \quad \#\mathcal{R} \leq (2 \cdot \#\mathcal{P}) \uparrow d.$$

Carving out a union of convex polyhedra using splitters

Question: How do we compute the complement of $\bigcup_{i \in I} (\text{conv } V_i + \text{cone } W_i)$?

An **(\mathbb{R} -)splitter** for a family of convex polyhedra \mathcal{P} is a family of convex polyhedra \mathcal{R} s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Claim: Given \mathcal{R} it is easy to compute $\mathbb{R}^d \setminus \bigcup \mathcal{P}$.

Theorem

Minkowski-Weyl theorem + n^d cutting lemma

Every $\mathcal{P} = \{\text{conv } V_i + \text{cone } W_i\}_{i \in I}$ has an \mathbb{R} -splitter $\mathcal{R} = \{\text{conv } C_j + \text{cone } Q_j\}_{j \in J}$ s.t.

$$\langle \mathcal{R} \rangle \leq \text{poly}(d) \cdot \langle \mathcal{P} \rangle \quad \text{and} \quad \#\mathcal{R} \leq (2 \cdot \#\mathcal{P}) \uparrow d.$$

Chapter 2

In which we reintroduce the integers

Goal: refine the notion of splitter to work over \mathbb{Z} .

The geometry of a system of inequalities over the integers

Theorem (von zur Gathen & Sieveking, '78)

Consider $S \subseteq \mathbb{Z}^d$. Then, below (H) implies (V), but not vice versa:

(H) $S = \{\mathbf{x} \in \mathbb{Z}^d : A \cdot \mathbf{x} \leq \mathbf{c}\}$ for some $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^m$

(V) $S = \bigcup_{\mathbf{b} \in B} L(\mathbf{b}, P)$ for some finite sets $B, P \subseteq \mathbb{Z}^d$.

$$B \quad + \quad P \cdot \mathbb{N} \quad = \quad \begin{array}{c} b_4 \\ b_1 \\ b_2 \\ b_3 \end{array} + \begin{array}{c} p_2 \\ p_1 \end{array} \cdot \begin{array}{c} \vdots \\ \vdots \end{array} = \begin{array}{c} b_4 \\ b_1 \\ b_2 \\ b_3 \end{array} \begin{array}{c} \nearrow \\ \searrow \end{array} \begin{array}{c} \vdots \\ \vdots \end{array}$$

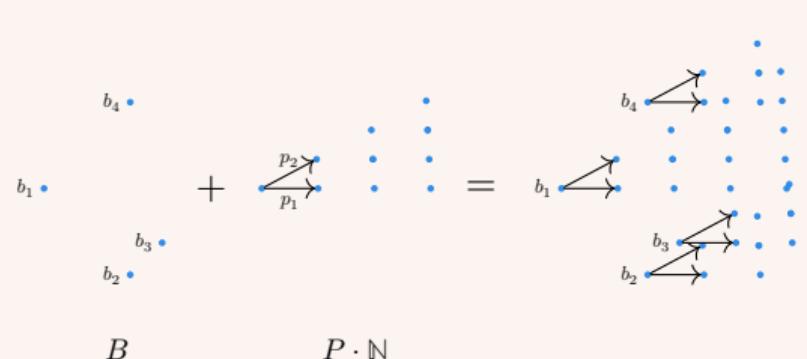
The geometry of a system of inequalities over the integers

Theorem (von zur Gathen & Sieveking, '78)

Consider $S \subseteq \mathbb{Z}^d$. Then, below (H) implies (V), but not vice versa:

(H) $S = \{\mathbf{x} \in \mathbb{Z}^d : A \cdot \mathbf{x} \leq \mathbf{c}\}$ for some $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^m$

(V) $S = \bigcup_{\mathbf{b} \in B} L(\mathbf{b}, P)$ for some finite sets $B, P \subseteq \mathbb{Z}^d$.



Cost of switching: (H) \rightarrow (V)

$$\langle B \rangle, \langle P \rangle \leq \text{poly}(d) \cdot \langle [A|\mathbf{c}] \rangle$$

$$\#P \leq \#[A|\mathbf{c}] \uparrow d$$

$$\#B \leq 2 \uparrow (d \cdot \langle B \rangle)$$

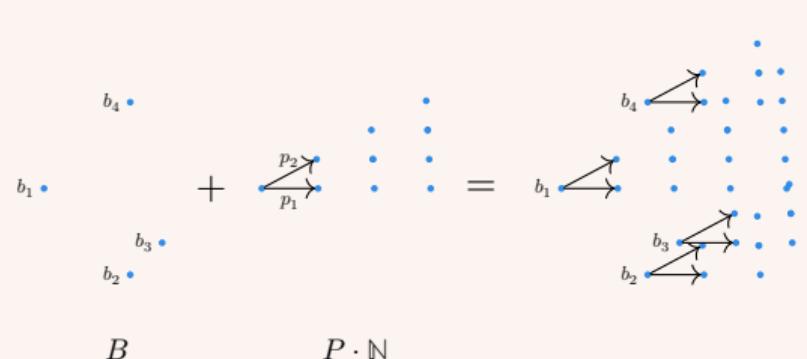
The geometry of a system of inequalities over the integers

Theorem (von zur Gathen & Sieveking, '78)

Consider $S \subseteq \mathbb{Z}^d$. Then, below (H) implies (V), but not vice versa:

(H) $S = \{\mathbf{x} \in \mathbb{Z}^d : A \cdot \mathbf{x} \leq \mathbf{c}\}$ for some $A \in \mathbb{Z}^{n \times d}$ and $\mathbf{c} \in \mathbb{Z}^m$

(V) $S = \bigcup_{\mathbf{b} \in B} L(\mathbf{b}, P)$ for some finite sets $B, P \subseteq \mathbb{Z}^d$.



Cost of switching: (H) \rightarrow (V)

$$\langle B \rangle, \langle P \rangle \leq \text{poly}(d) \cdot \langle [A|\mathbf{c}] \rangle$$

$$\#P \leq \#[A|\mathbf{c}] \uparrow d$$

$$\#B \leq 2 \uparrow (d \cdot \langle B \rangle)$$

We call $L(B, P) \stackrel{\text{def}}{=} \bigcup_{\mathbf{b} \in B} L(\mathbf{b}, P)$ an **hybrid linear set**.

Semilinear sets (again)

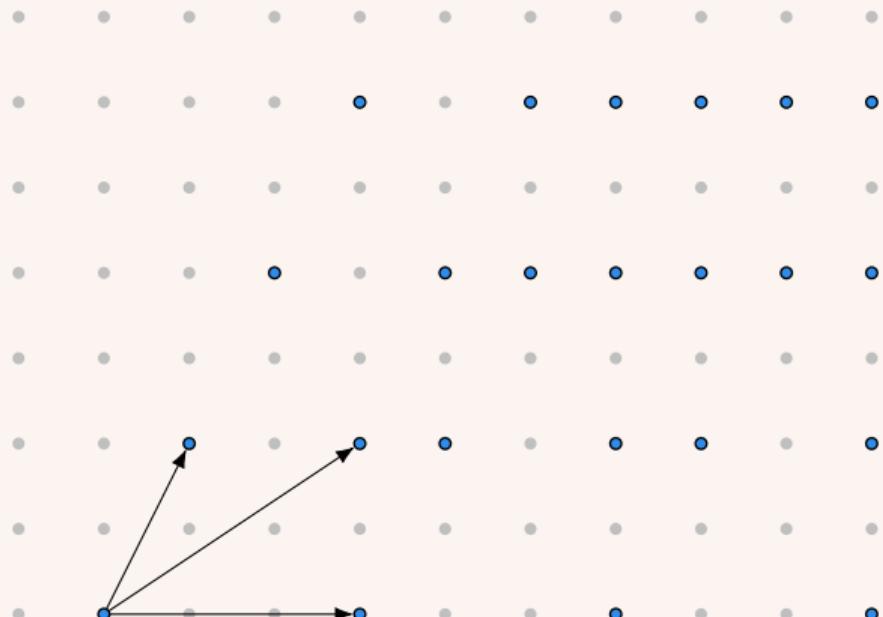
Arithmetic progression



$b + i \cdot p$, where $i \in \mathbb{N}$

b base point, p period

Semilinear sets (again)



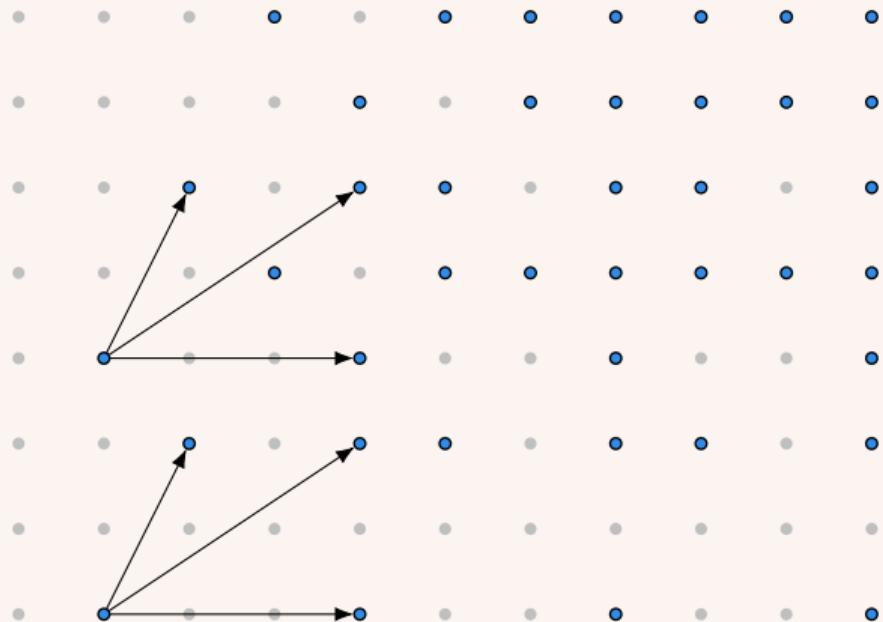
Linear set

(arithmetic progression
in multiple dimensions)

$$L(\mathbf{b}, P)$$

\mathbf{b} base, P periods

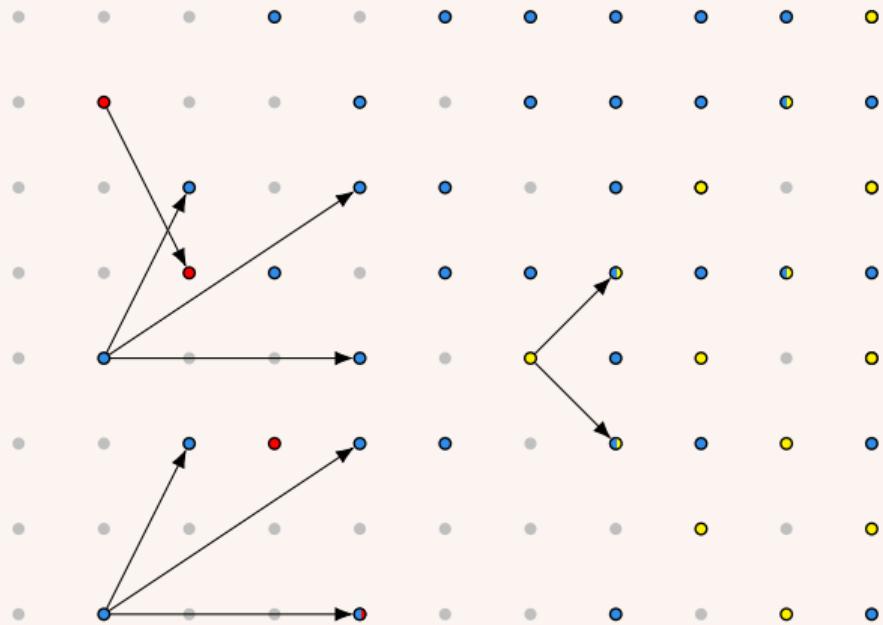
Semilinear sets (again)



Hybrid linear set
(finite union of linear sets having the same periodic behaviour)

$L(B, P)$
 B bases, P periods

Semilinear sets (again)



Semilinear set
(finite union of
hybrid linear sets)

$$\bigcup_{i \in I} L(B_i, P_i)$$

I finite set of indices

\mathbb{Z} -splitters

An (\mathbb{R} -)splitter for a family of convex polyhedra \mathcal{P} is a family of convex polyhedra \mathcal{R} s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Claim: Given \mathcal{R} it is easy to compute $\mathbb{R}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

An ~~(\mathbb{R})splitter~~ for a family of ~~convex polyhedra~~ \mathcal{P} is a family of ~~convex polyhedra~~ \mathcal{R} s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Claim: Given \mathcal{R} it is easy to compute $\mathbb{R}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces
2. for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. ~~$\bigcup \mathcal{R} = \mathbb{R}^d$ and \mathcal{R} is closed under taking faces~~
2. ~~for every $R_1, R_2 \in \mathcal{R}$, the set $R_1 \cap R_2$ is either \emptyset or a face of both R_1 and R_2~~
3. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. ~~for every $R \in \mathcal{R}$ and $P \in \mathcal{P}$ the set $R \cap P$ is either \emptyset or a face of R~~

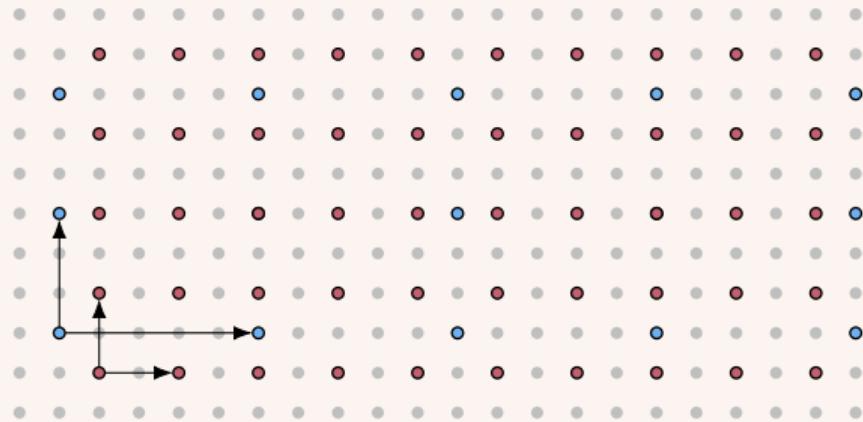
Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

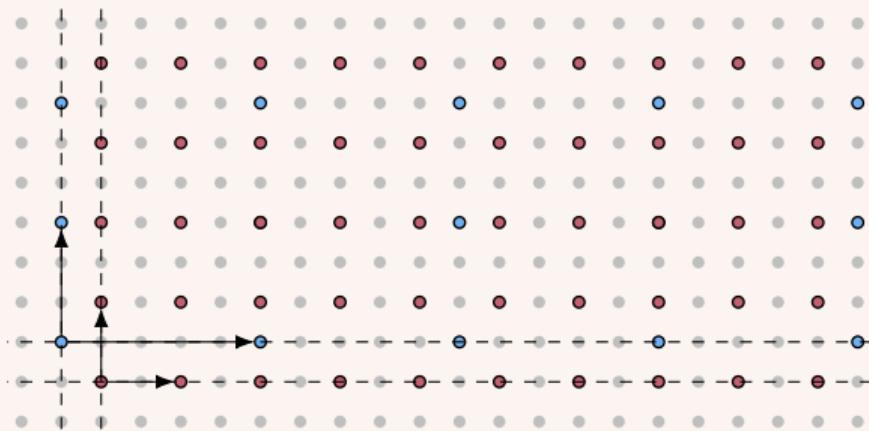


\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.



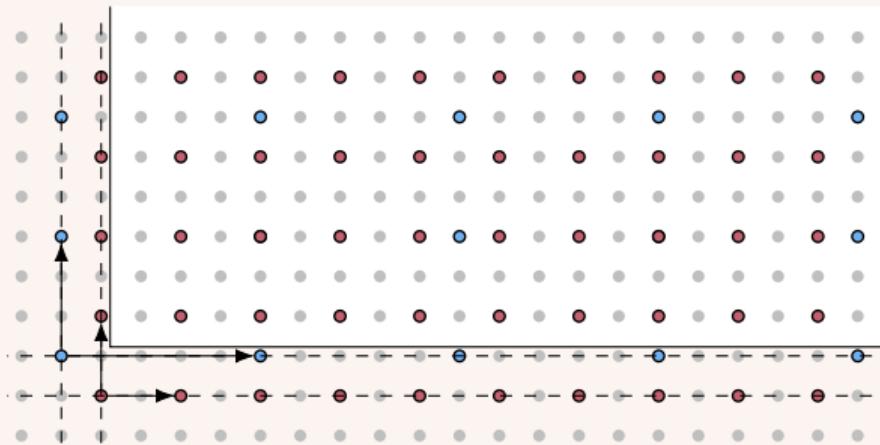
\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

The region Z characterises a portion of \mathbb{Z}^d



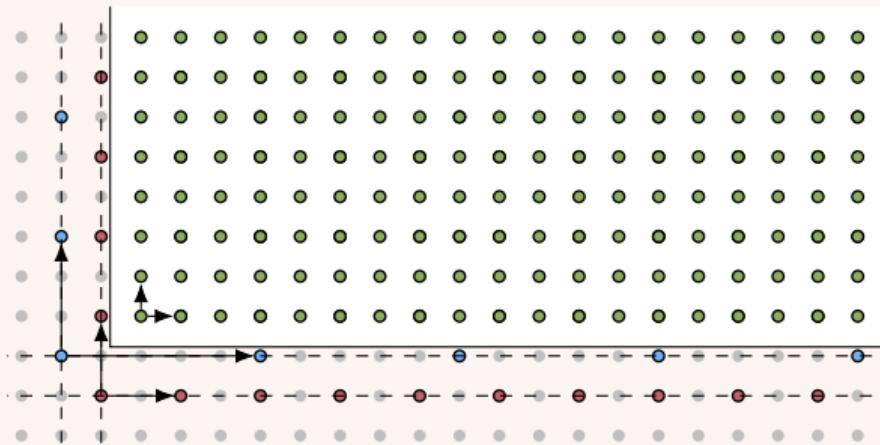
\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

The region Z characterises a portion of \mathbb{Z}^d



Not all hybrid linear sets agree with our goal!

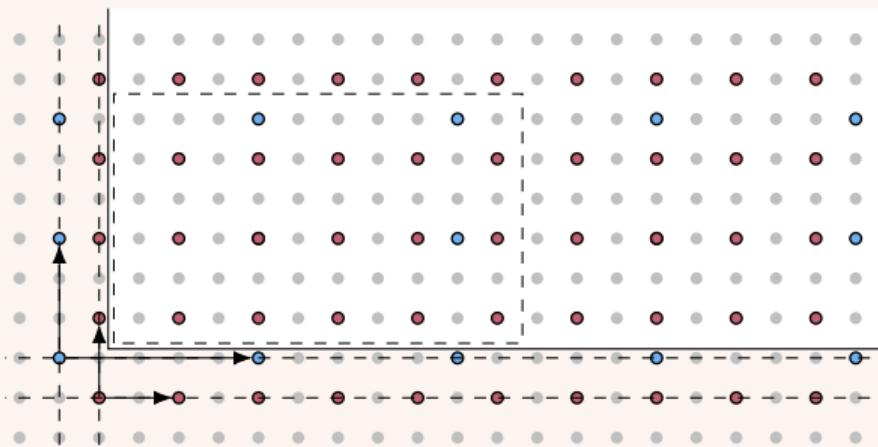
\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

The region Z characterises a portion of \mathbb{Z}^d



Idea: find C and Q such that

- $Z = L(C, Q)$
- $L(C, Q) \cap L(\mathbf{b}, P_i) = L(C \cap L(\mathbf{b}, P_i), Q)$
for every $i \in I$ and $\mathbf{b} \in B_i$

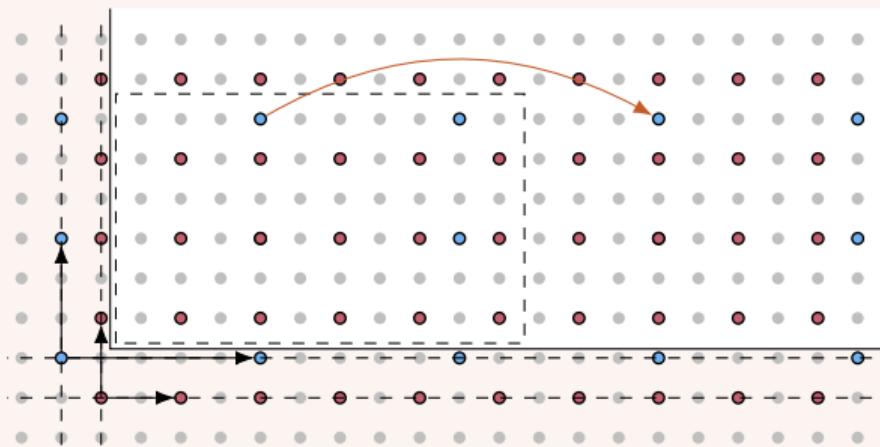
\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

The region Z characterises a portion of \mathbb{Z}^d



Idea: find C and Q such that

- $Z = L(C, Q)$
- $L(C, Q) \cap L(\mathbf{b}, P_i) = L(C \cap L(\mathbf{b}, P_i), Q)$
for every $i \in I$ and $\mathbf{b} \in B_i$

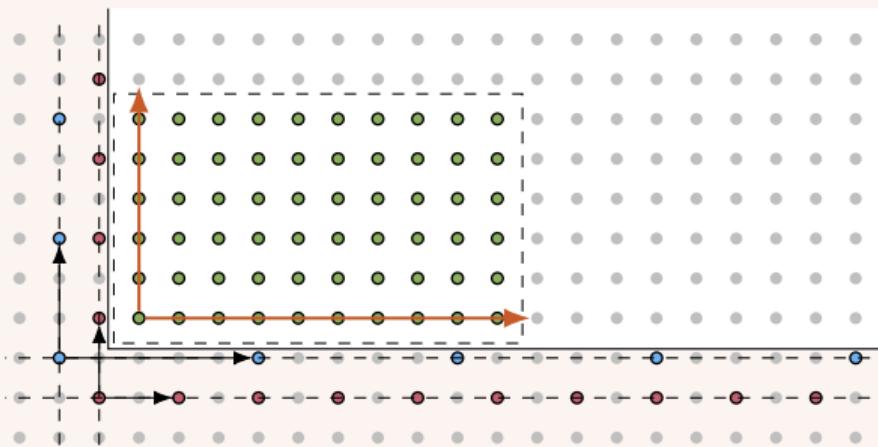
\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Goal: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

The region Z characterises a portion of \mathbb{Z}^d



Idea: find C and Q such that

- $Z = L(C, Q)$
- $L(C, Q) \cap L(\mathbf{b}, P_i) = L(C \cap L(\mathbf{b}, P_i), Q)$
for every $i \in I$ and $\mathbf{b} \in B_i$

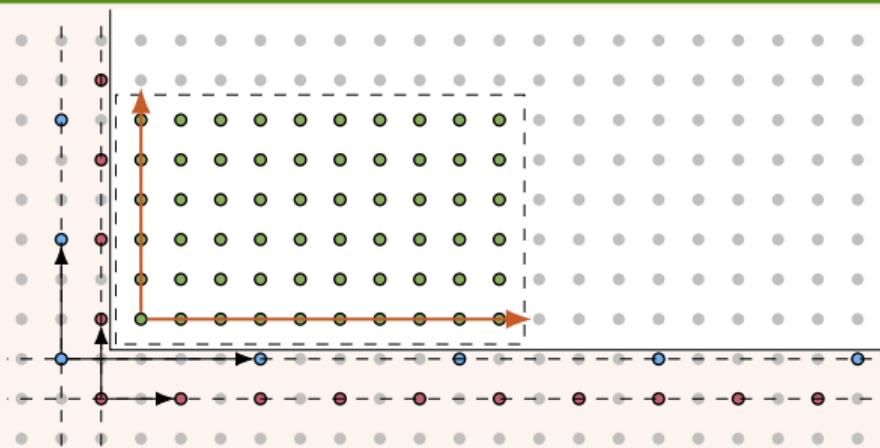
$$\Rightarrow Z \setminus \bigcup \mathcal{P} = L(C \setminus \bigcup \mathcal{P}, Q)$$

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$
3. for every $j \in J$, the set Q_j is proper (i.e. made of linearly independent vectors)
4. if $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ then $Q_j \subseteq L(\mathbf{0}, P_i) \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Claim: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.



Idea: find C and Q such that

- $Z = L(C, Q)$
- $L(C, Q) \cap L(\mathbf{b}, P_i) = L(C \cap L(\mathbf{b}, P_i), Q)$
for every $i \in I$ and $\mathbf{b} \in B_i$

$$\Rightarrow Z \setminus \bigcup \mathcal{P} = L(C \setminus \bigcup \mathcal{P}, Q)$$

\mathbb{Z} -splitters

A **\mathbb{Z} -splitter** for a family $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ is a family $\mathcal{Z} = \{Z_j := L(C_j, Q_j)\}_{j \in J}$ s.t.

1. $\bigcup \mathcal{Z} = \mathbb{Z}^d$, where the union is disjoint
2. either $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ or $Z_j \cap (\mathbf{b} + \text{cone } P_i) = \emptyset \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$
3. for every $j \in J$, the set Q_j is proper (i.e. made of linearly independent vectors)
4. if $Z_j \subseteq (\mathbf{b} + \text{cone } P_i)$ then $Q_j \subseteq L(\mathbf{0}, P_i) \quad \forall i \in I, \mathbf{b} \in B_i, j \in J$

Claim: Given \mathcal{Z} it is easy to compute $\mathbb{Z}^d \setminus \bigcup \mathcal{P}$.

Theorem

Every $\mathcal{P} = \{L(B_i, P_i)\}_{i \in I}$ has a \mathbb{Z} -splitter $\mathcal{Z} = \{L(C_j, Q_j)\}_{j \in J}$ such that

$$\langle \mathcal{Z} \rangle \leq \text{poly}(d) \cdot \#I \cdot \langle \mathcal{P} \rangle \quad \text{and} \quad \#(\bigcup_{j \in J} Q_j) \leq (\#I \cdot \max_{i \in I} \#P_i) \uparrow d .$$

Chapter 3

Complementation

Goal: Complementation.

The procedure

Input: a semilinear set M

Output: the complement $\mathbb{Z}^d \setminus M$ as a semilinear set

1. update M to $\bigcup_{i \in I} L(B_i, P_i)$
where each P_i is proper
2. compute $\mathcal{Z} = \{L(C_j, Q_j)\}_{j \in J}$
 \mathbb{Z} -splitter for $\{L(B_i, P_i)\}_{i \in I}$
3. **for** $j \in J$ **do**
4. $E_j \leftarrow C_j \setminus M$
5. $\mathcal{Q} \leftarrow \{Q_j\}_{j \in J}$
6. **for** $Q \in \mathcal{Q}$ **do**
7. $\mathcal{E}_Q \leftarrow \{E_j : j \in J, Q_j = Q\}$
8. **return** $\bigcup_{Q \in \mathcal{Q}} L((\bigcup \mathcal{E}_Q), Q)$

Discrete Carathéodory's theorem
[Chistikov and Haase, ICALP'16]

Complement M region-wise

Merge hybrid linear sets
having the same period sets
 $L(B, P) \cup L(C, P) = L(B \cup C, P)$

Running time and bounds on the complement

Theorem

Let $M = \bigcup_{i \in I} L(B_i, P_i) \subseteq \mathbb{Z}^d$. Then, $\mathbb{Z}^d \setminus M = N = \bigcup_{j \in J} L(C_j, Q_j)$ s.t.

$$\#J \leq (\#I \cdot \max_{i \in I} \#P_i) \uparrow d \quad \langle N \rangle \leq \text{poly}(d) \cdot \#I \cdot \langle M \rangle \quad \text{and} \quad Q_j \text{ is proper.}$$

The family $\{(C_j, Q_j)\}_{j \in J}$ can be computed in time $2 \uparrow (\langle M \rangle \cdot \#I) \uparrow d$.

Running time and bounds on the complement

Theorem

Let $M = \bigcup_{i \in I} L(B_i, P_i) \subseteq \mathbb{Z}^d$. Then, $\mathbb{Z}^d \setminus M = N = \bigcup_{j \in J} L(C_j, Q_j)$ s.t.

$$\#J \leq (\#I \cdot \max_{i \in I} \#P_i) \uparrow d \quad \langle N \rangle \leq \text{poly}(d) \cdot \#I \cdot \langle M \rangle \quad \text{and} \quad Q_j \text{ is proper.}$$

The family $\{(C_j, Q_j)\}_{j \in J}$ can be computed in time $2 \uparrow (\langle M \rangle \cdot \#I) \uparrow d$.

Theorem (A geometric procedure for Presburger arithmetic)

There is an algorithm that given Φ in PA, computes a family $\{(B_i, P_i)\}_{i \in I}$ such that $\llbracket \Phi \rrbracket = \bigcup_{i \in I} L(B_i, P_i)$. The algorithm runs in time $2 \uparrow \langle \Phi \rangle \uparrow d \uparrow h$ and ensures:

$$\#I \leq 2 \uparrow d \uparrow h \quad \langle B_i \rangle, \langle P_i \rangle \leq \langle \Phi \rangle \uparrow d \uparrow h \quad \text{and} \quad P_i \text{ proper,}$$

where h is the depth of the formula and d is the number of its variables.

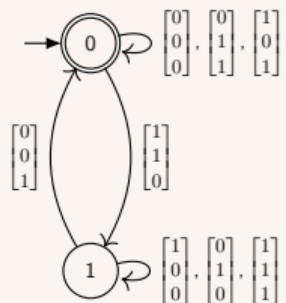
Concluding remarks

Quantifier elimination [Presburger, '29]

$$\exists x : \varphi(x, \mathbf{y}) \equiv \psi(\mathbf{y})$$

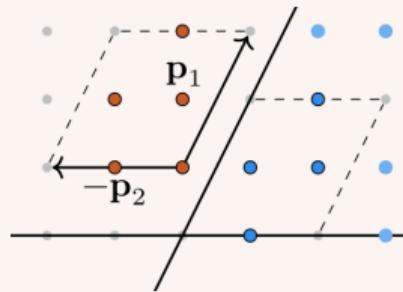
3EXPTIME

Automata [Büchi, '60]



3EXPTIME

Geometry [Ginsburg and Spanier, '66]



3EXPTIME

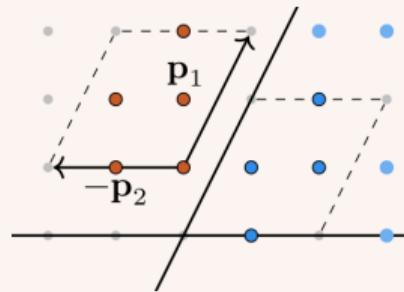
Concluding remarks

Key notion: \mathbb{Z} -splitters.

A decomposition of \mathbb{Z}^d with many interesting properties.

Geometry

[Ginsburg and Spanier, '66]



3EXPTIME

Concluding remarks

Key notion: \mathbb{Z} -splitters.

A decomposition of \mathbb{Z}^d with many interesting properties.

From our procedure:

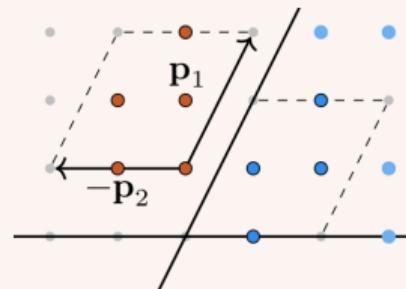
$$[\Phi] = \bigcup_{i \in I} L(B_i, P_i) \text{ where } \#I \leq 2 \uparrow d \uparrow h.$$

From this bound we conclude that the VC dimension of PA is doubly exponential.

For details see the paper: “*Geometric decision procedures and the VC dimension of linear arithmetic theories*”, Chistikov, Haase, Mansutti, LICS’22

Geometry

[Ginsburg and Spanier, ‘66]



3EXPTIME