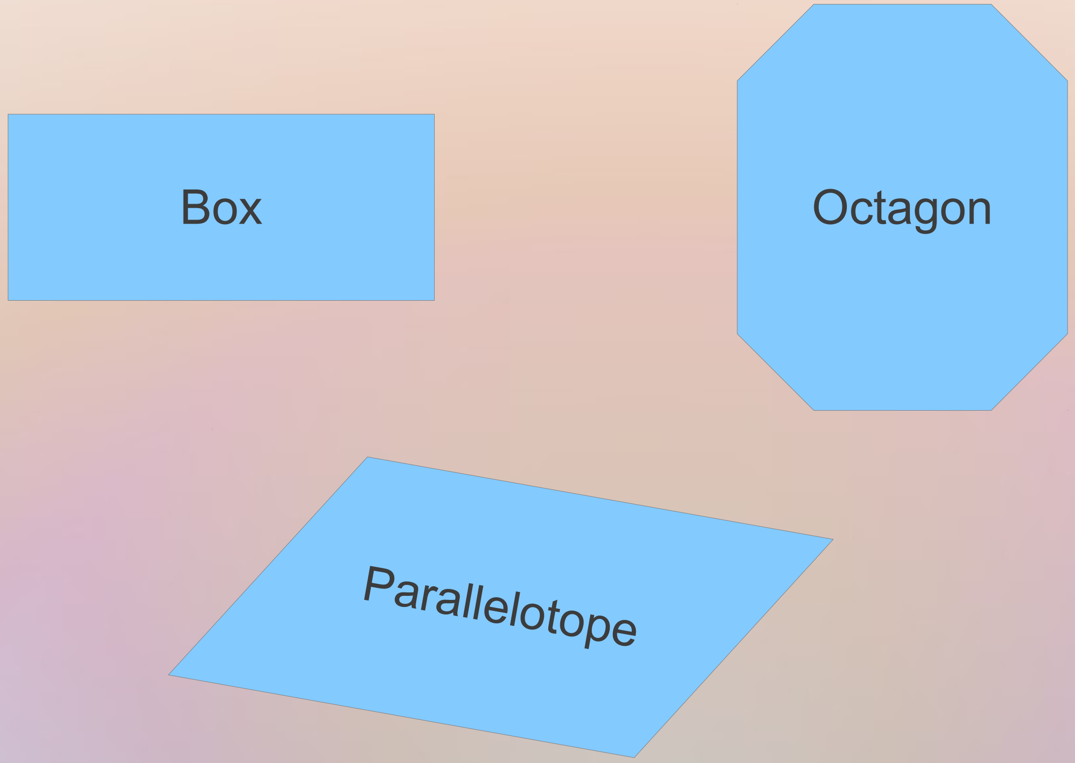
The Abstract Domain of Parallelotopes



Box

Octagon

Parallelotope

Gianluca Amato

Joint work with Francesca Scozzari
Università di Chieti-Pescara

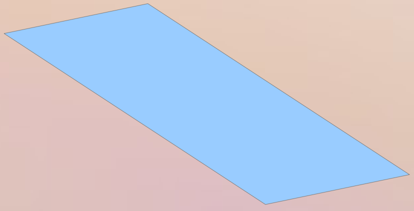
Parallelotope

- Weak relational abstract domain
  - No restriction on the single constraint
    - Any affine constraint may appear in an abstract object
  - Limitations on the number and combination of constraints
    - Linear forms of constraints should be linearly independent
  - Hence, it is not a template domain
    - Template parallelotopes (and methods to generate templates) were the topic of a previous paper [SAS 2010].

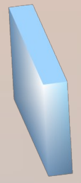
What is a parallelotope?

- A many-dimensional generalization of a parallelogram.

1-dimensional ptope
(interval)



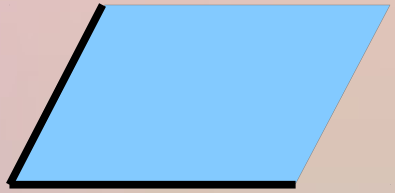
2-dimensional ptope
(parallelogram)



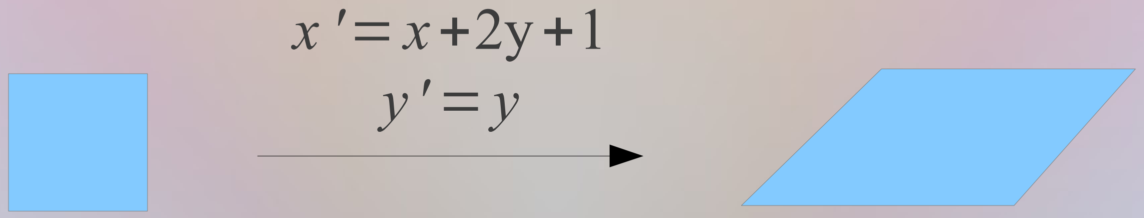
3-dimensional ptope
(parallelepiped)

What is a parallelotope?

- Several formal definitions:
  - The sum of linearly independent segments
    - Hence, a parallelotope is a ***zonotope***



  - The image of a box trough a linear transformation



$$x' = x + 2y + 1$$
$$y' = y$$

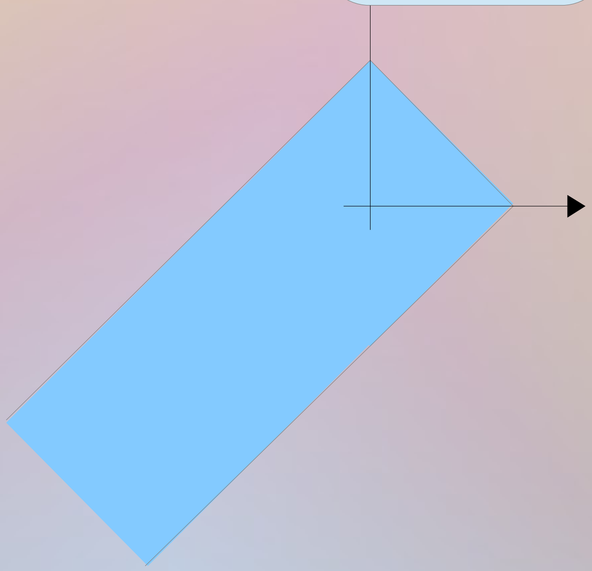
Representation of parallelotopes

- A triple <A,**m**,**M**>
  - A is a invertible m
  - **m**, **M** a vectors in
- Represents ≤ **Ax** ≤ **M** }

n = number of variables

bounds

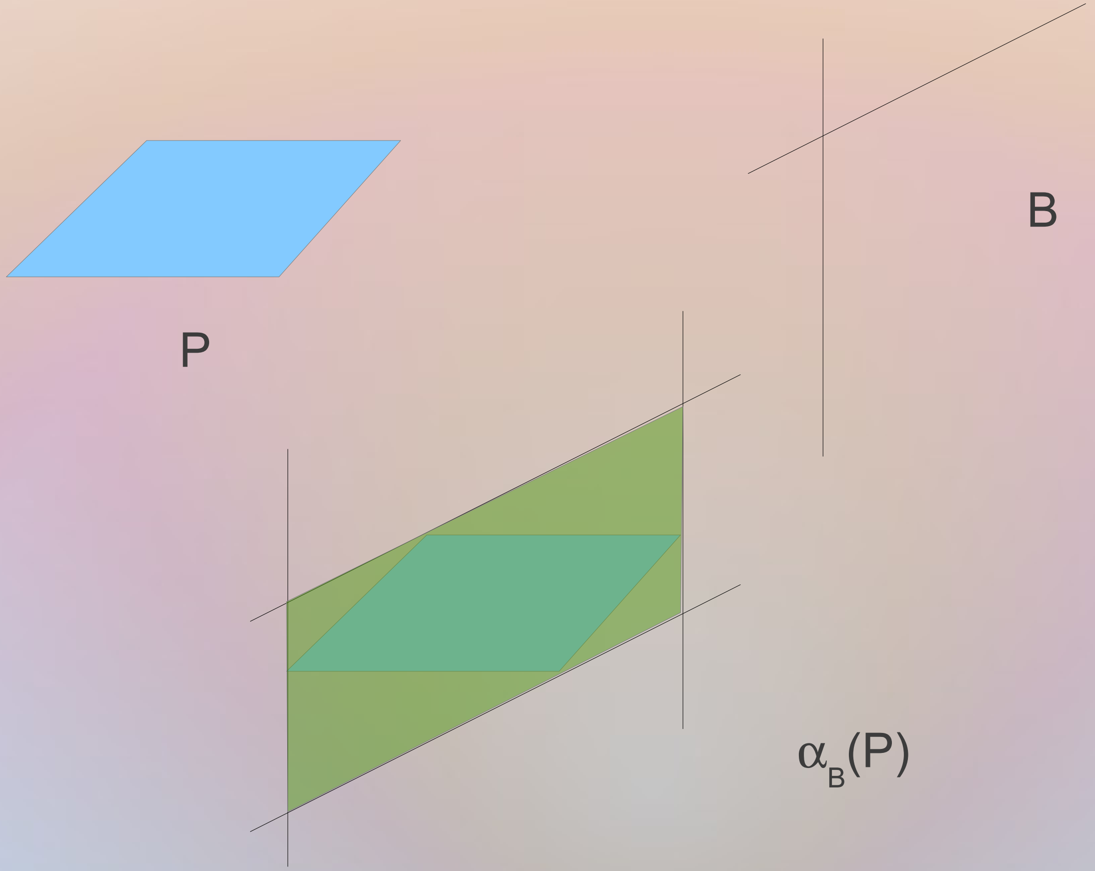
shape or template



$$\underbrace{\begin{array}{c} -\infty \leq x+y \leq 1 \\ -1 \leq x-y \leq 1 \end{array}}_{A=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \boldsymbol{m}=\begin{pmatrix} -\infty \\ -1 \end{pmatrix} \quad \boldsymbol{M}=\begin{pmatrix} 1 \\ 1 \end{pmatrix}}$$

Change of shape

- Given P=<A,**m**,**M**>, which is the least ptope containing P with shape B ?



Change of shape

- Given P=<A,**m**,**M**>, which is the least ptope containing P with shape B ?
- For each row $\mathbf{b}_i$ of B
  - Minimize/maximize scalar product $\mathbf{b}_i \cdot \mathbf{x}$ on P
  - $l_i = \inf_{\boldsymbol{x} \in P} \boldsymbol{b}_i \cdot \boldsymbol{x} = \inf_{\boldsymbol{m} \leq \boldsymbol{y} \leq \boldsymbol{M}} \boldsymbol{b}_i \cdot (A^{-1} \boldsymbol{y})$
  - $u_i = \sup_{\boldsymbol{x} \in P} \boldsymbol{b}_i \cdot \boldsymbol{x} = \sup_{\boldsymbol{m} \leq \boldsymbol{y} \leq \boldsymbol{M}} \boldsymbol{b}_i \cdot (A^{-1} \boldsymbol{y})$
- Return <B,**l**,**u**>

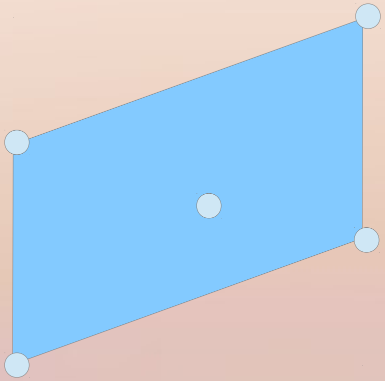
Ordering on parallelotopes

- P=<A,**m**,**M**> is a subset of P'=<A',**m'**,**M'**> ?
  - If A=A' just compare **m**/**m'** and **M**/**M'**
  - … otherwise compare $\alpha_{A'}$(P) and P'
- Normalization?
  - Several possible normalizations
  - … but we did not explore them fully

Abstraction map?

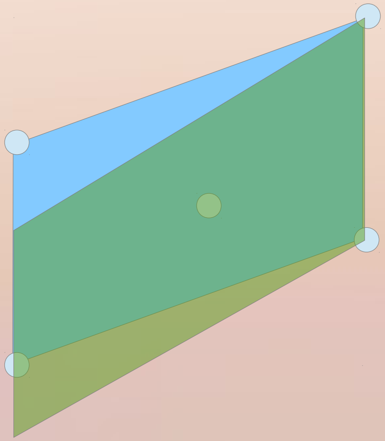
- Does an abstraction map exist to establish a Galois connection?
    - Given a set of points, is there the least ptope containing them?

Least parallelotope ?



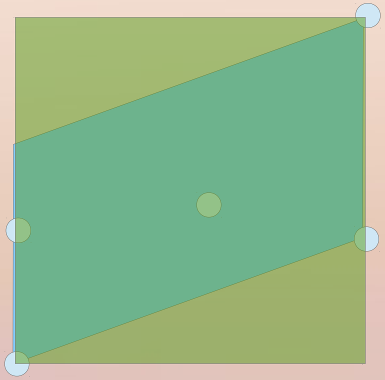
- In this case the least parallelotope exists

Minimal parallelotopes



- No least parallelotope, but many minimal ones.
- No Galois connection framework.

Relatively optimal parallelotope



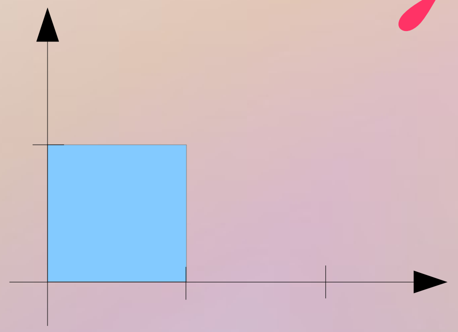
- The green square is not minimal
- …. however, its the least correct one *of the given shape*
- We call it **relatively optimal**

Semantic Transformers

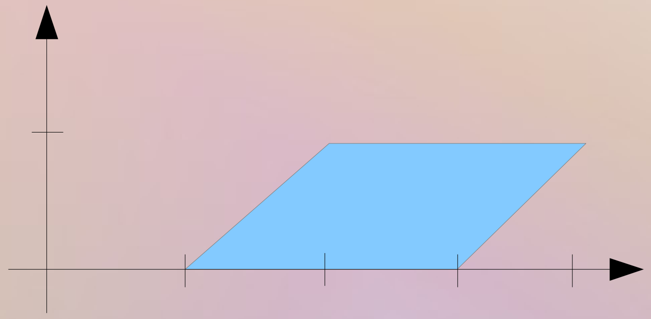
- Concrete transformers
  - Affine assignment
    - Invertible, Non-invertible
  - Non-deterministic assignment
  - Refinement by linear inequality (test)
  - Union
- We strive to find abstract transformers which are
  - γ-complete
  - Minimal
  - Relatively optimal

Inv. Assignment: x'=x+2y+1

- Invertible affine transformations map parallelotopes to parallelotopes.



$$\xrightarrow{x' = x + 2y + 1}$$



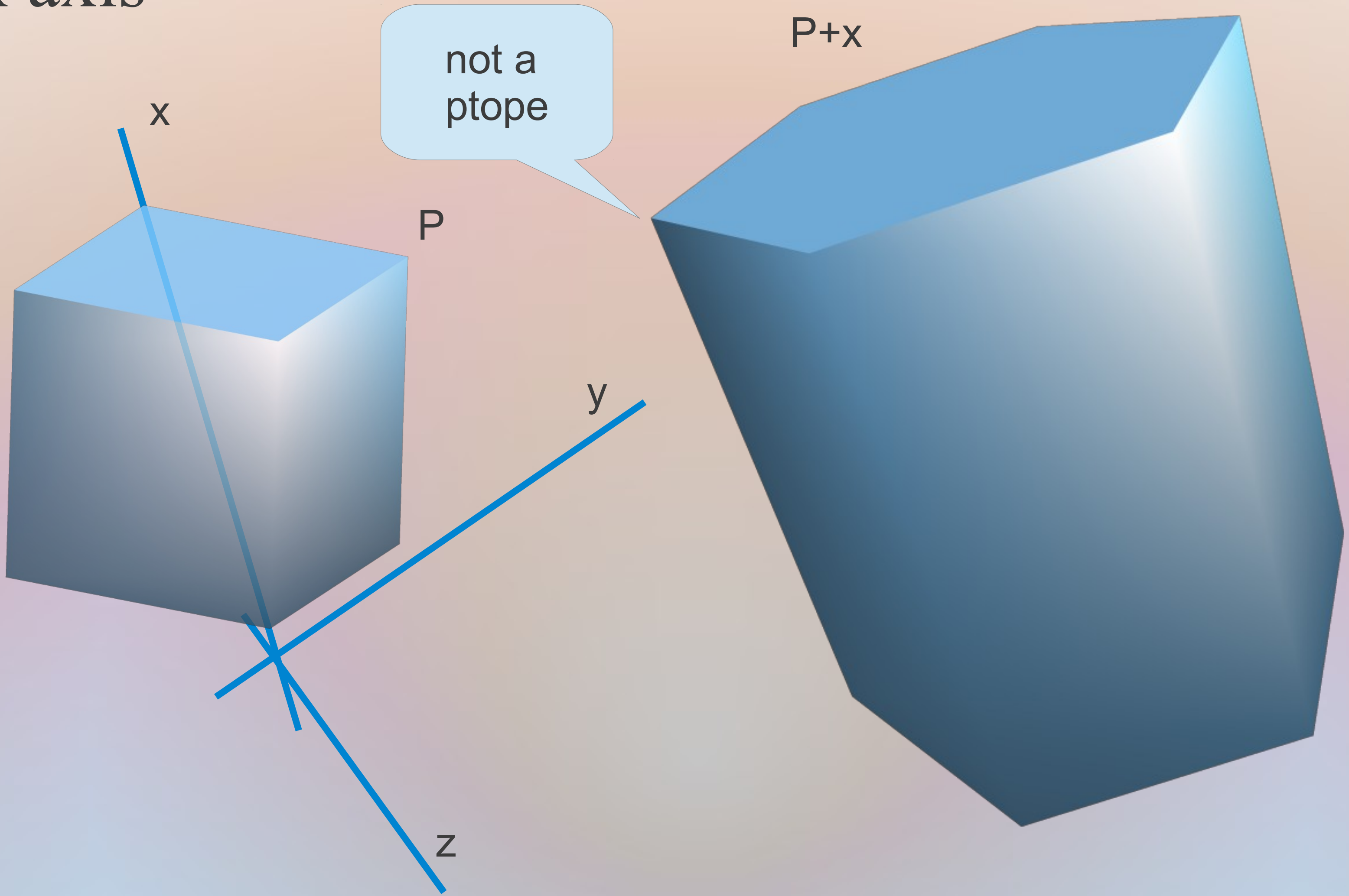
$$0 \leq x \leq 1$$
$$0 \leq y \leq 1$$

$$0 \leq x' - 2y + 1 \leq 2$$
$$0 \leq y \leq 1$$

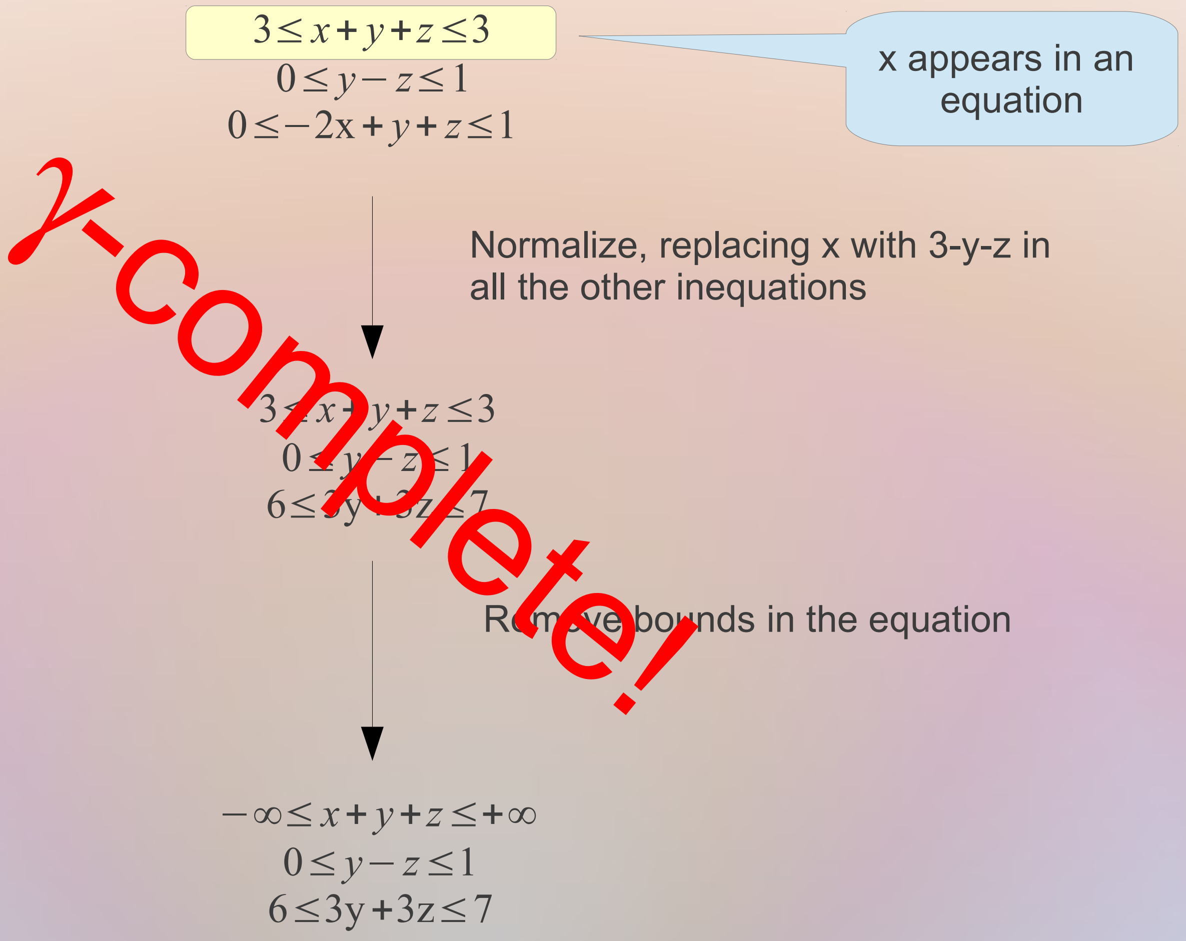
γ-complete!

Non-deterministic assignment: x=?

- Sum of the parallelotope with the line corresponding to x axis



Non-det. assignment: x=? (good case)



$$3 \le x + y + z \le 3$$
$$0 \le y - z \le 1$$
$$0 \le -2x + y + z \le 1$$

x appears in an equation

Normalize, replacing x with 3-y-z in all the other inequations

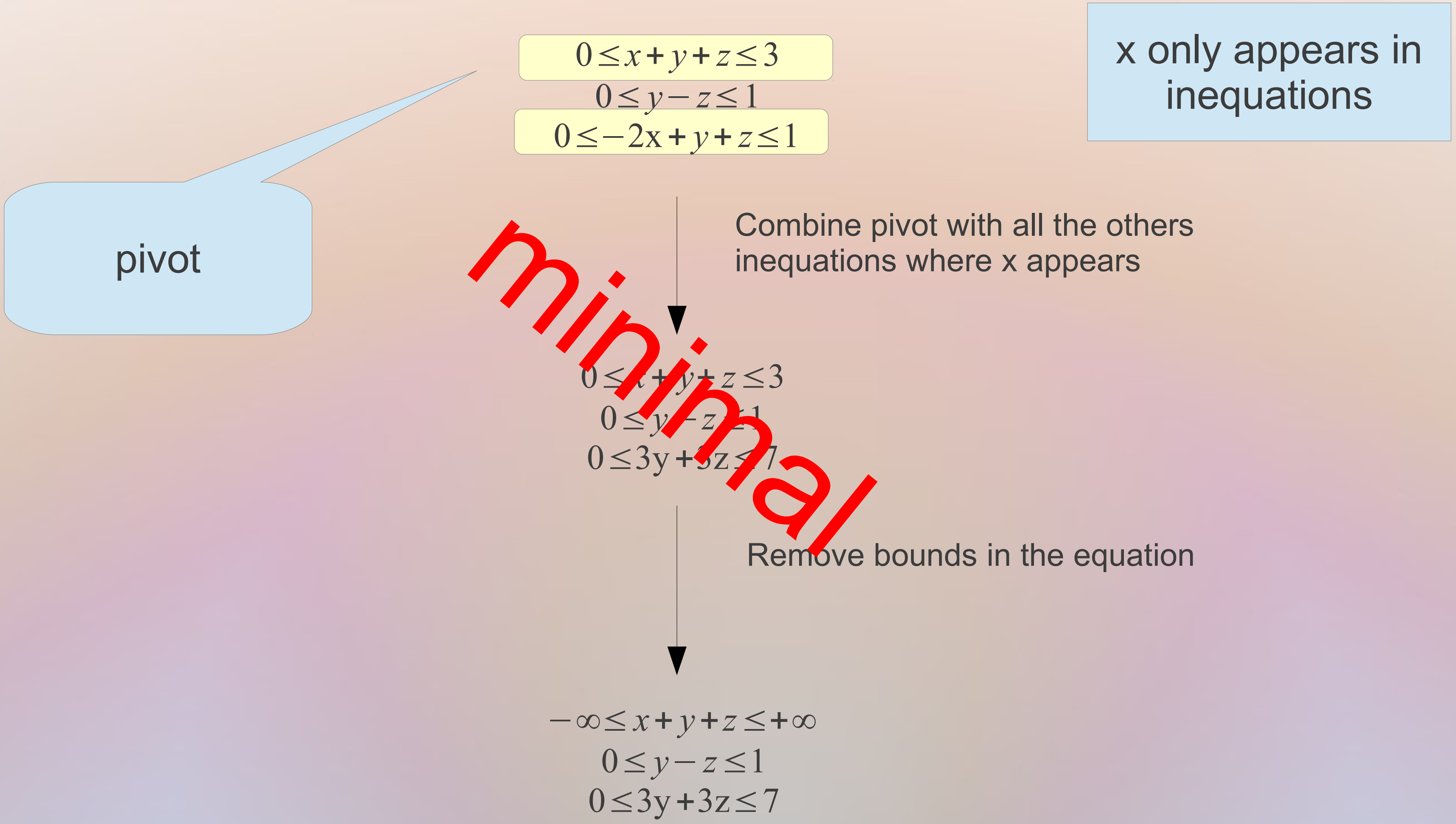
$$3 \le x + y + z \le 3$$
$$0 \le y - z \le 1$$
$$6 \le 3y + 3z \le 7$$

Remove bounds in the equation

$$-\infty \le x + y + z \le +\infty$$
$$0 \le y - z \le 1$$
$$6 \le 3y + 3z \le 7$$

γ-complete!

Non-det. Assignment: x=? (bad case)



x only appears in inequations

$$0 \le x + y + z \le 3$$
$$0 \le y - z \le 1$$
$$0 \le -2x + y + z \le 1$$

pivot

Combine pivot with all the others inequations where x appears

minimal

$$0 \le x + y + z \le 3$$
$$0 \le y - z \le 1$$
$$0 \le 3y + 3z \le 7$$

Remove bounds in the equation

$$-\infty \le x + y + z \le +\infty$$
$$0 \le y - z \le 1$$
$$0 \le 3y + 3z \le 7$$

Non-invertible Assignment: x=2y+z-1

$$\begin{array}{c} 0 \le x+y+z \le 3 \\ 0 \le y-z \le 1 \\ 0 \le -2x+y+z \le 1 \end{array} \longrightarrow \begin{array}{c} -\infty \le x+y+z \le +\infty \\ 0 \le y-z \le 1 \\ 6 \le -y-z \le 7 \end{array} \longrightarrow \begin{array}{c} -1 \le x-2y-z \le -1 \\ 0 \le y-z \le 1 \\ 6 \le -y-z \le 7 \end{array}$$

non-det. assignment

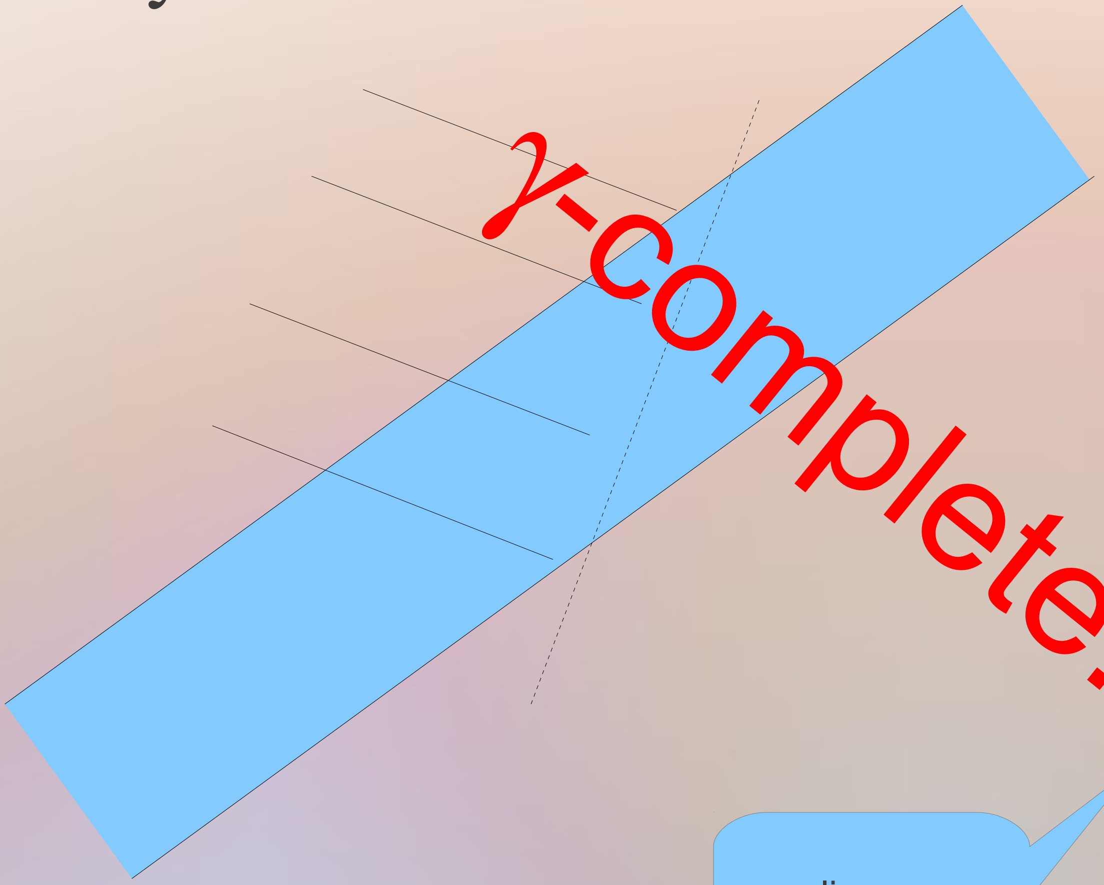
replace the only row containing x with the new equation

minimal or

γ-complete

Linear refinement: -2x+y ≥ 0

- Easy case:



γ-complete!

choose an unbounded line

$$-\infty \le x+y \le +\infty$$
$$-1 \le x-y \le 1$$

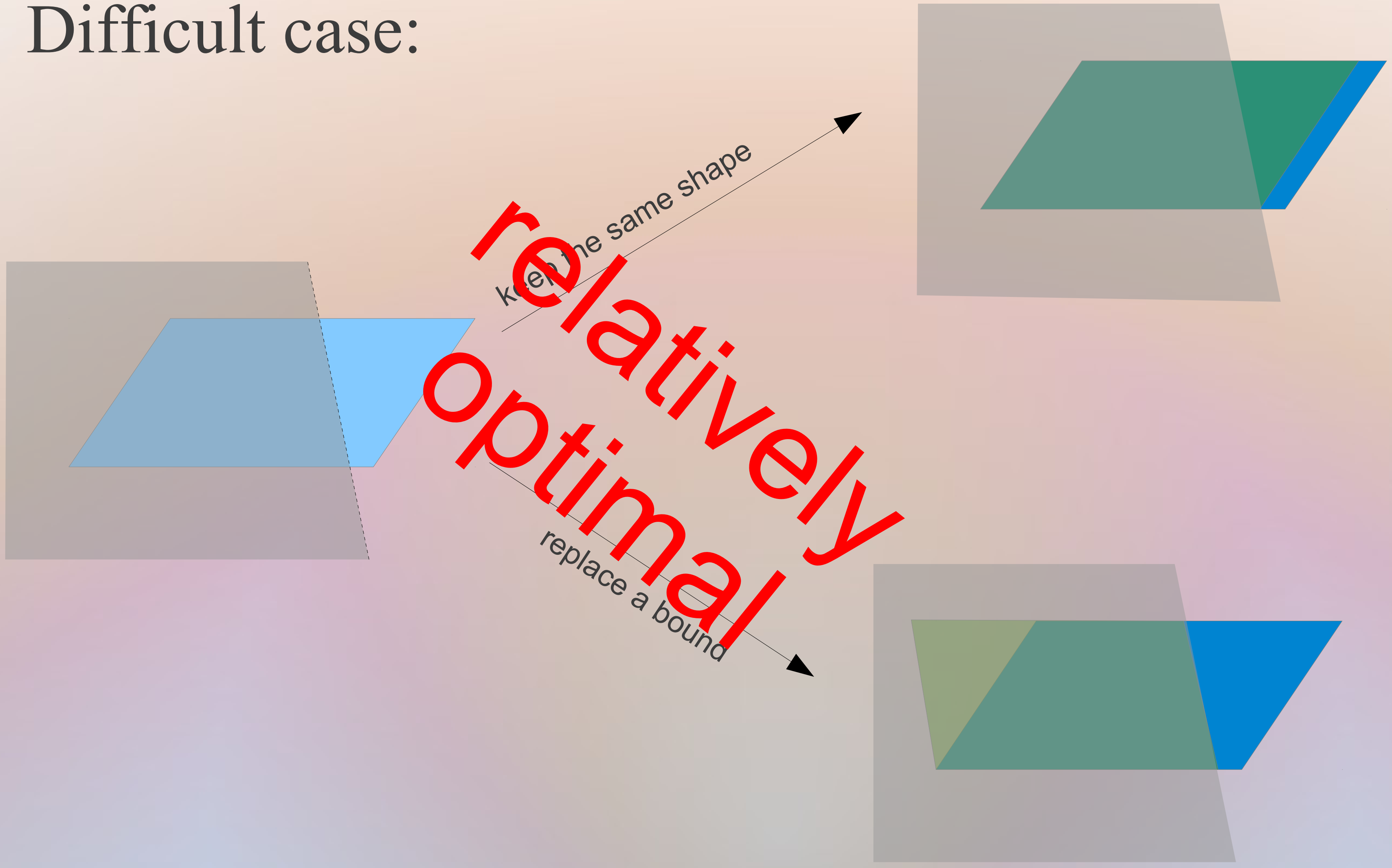
↓

$$0 \le -2x+y \le +\infty$$
$$-1 \le x-y \le 1$$

linear independent

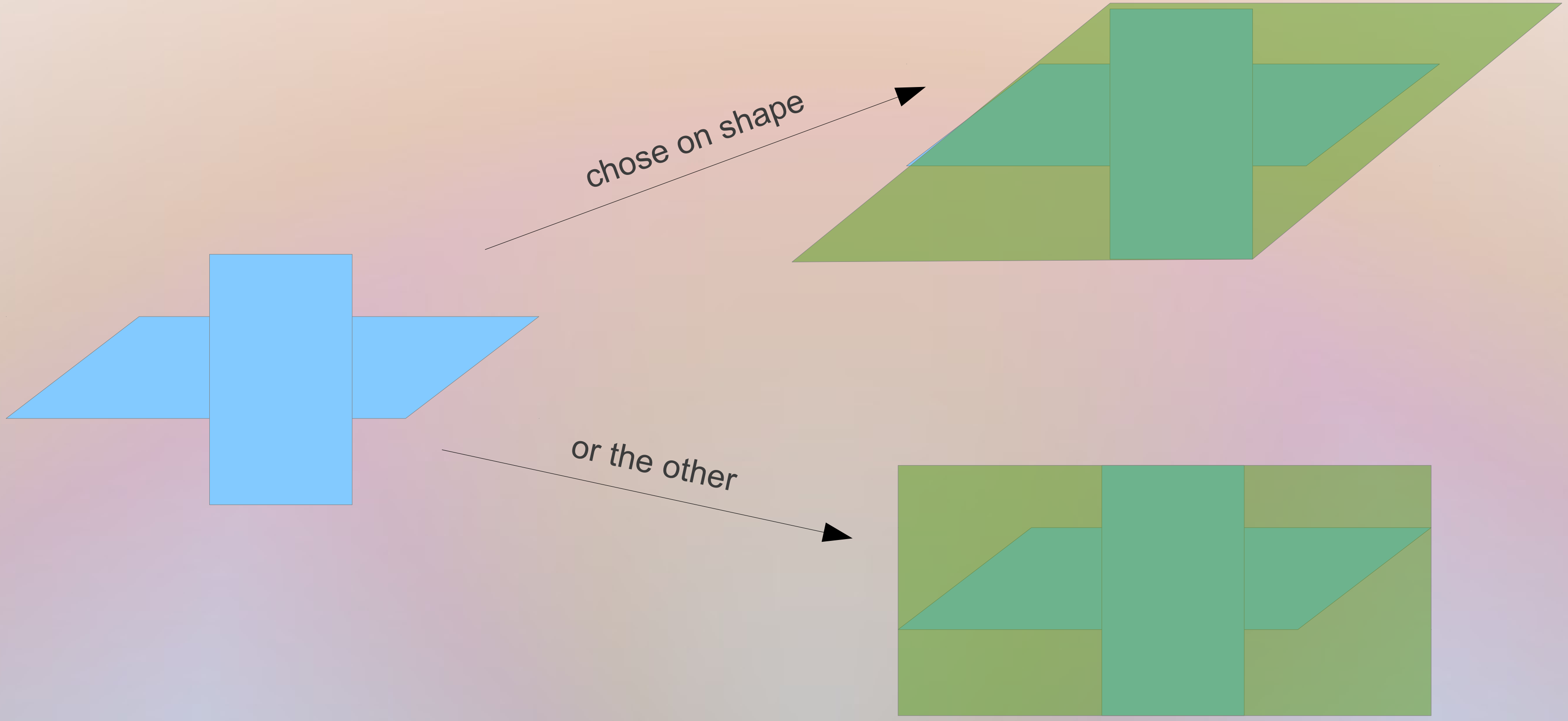
Linear refinement

- Difficult case:



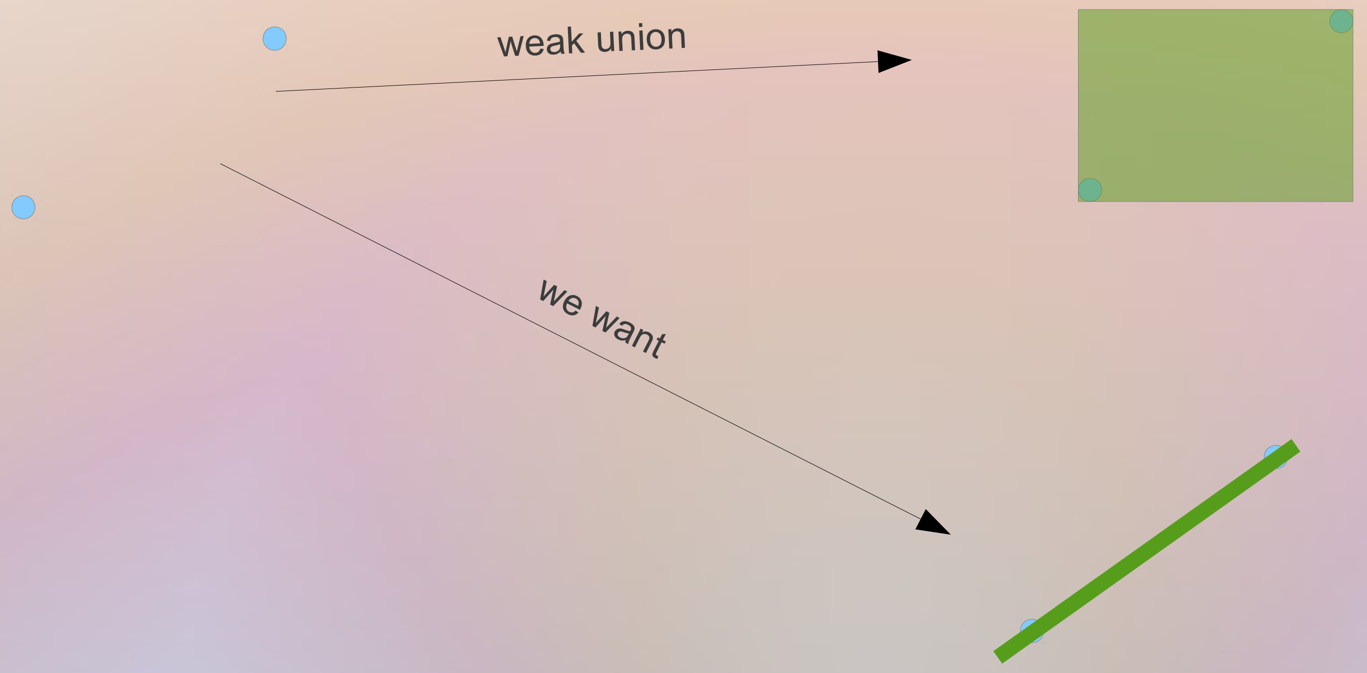
Union (weak)

- The weak union is similar to join of template polyhedra.



Union (weak)

- Weak union never creates new constraints

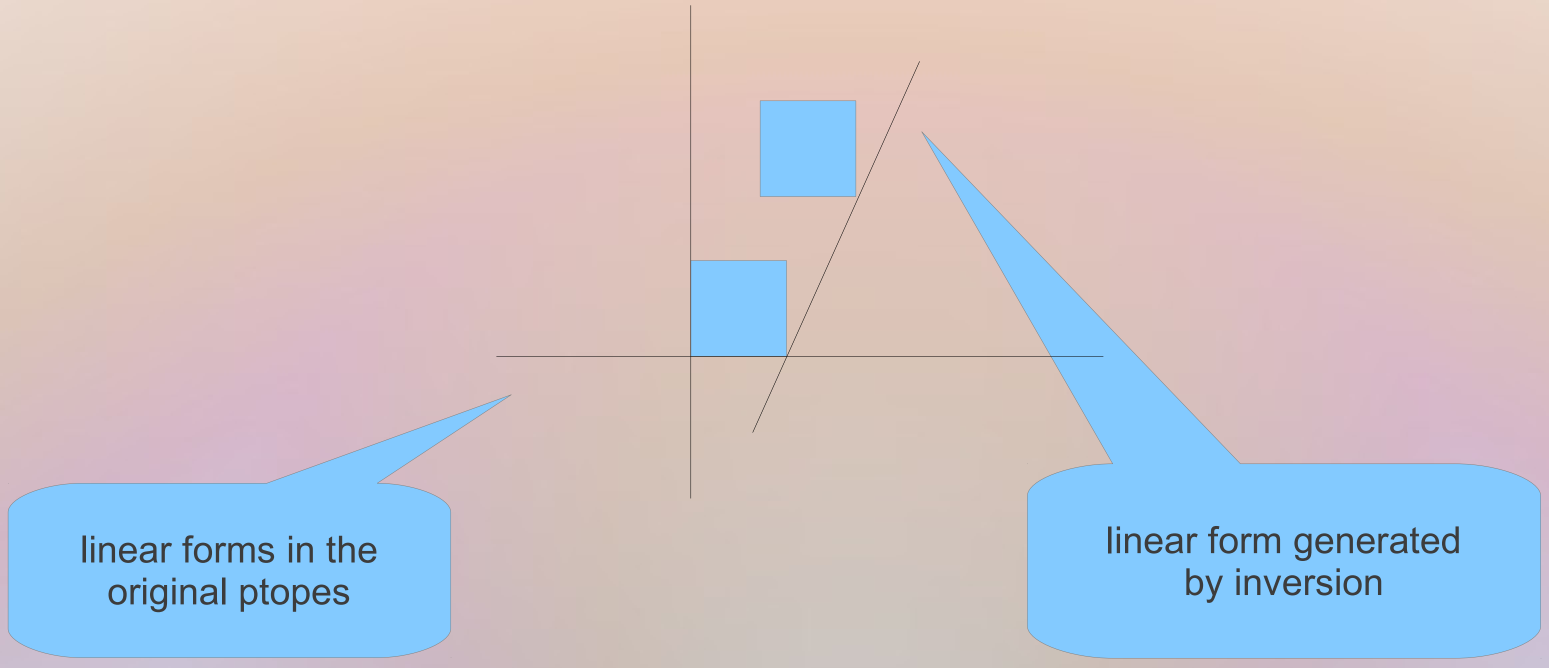


- Useful for widening

Union (inversion based)

- A smarter union based on inverse join
  - collect all the linear forms of the bounding hyperplanes
    - for the original parallelotopes
    - generated by inversion
  - prioritize them according to some heuristics
  - choose a subset of linear forms which is a basis of the vector space and which maximizes priorities
  - compute the relatively optimal parallelotope with the shape given by the chosen linear forms

Collecting linear forms

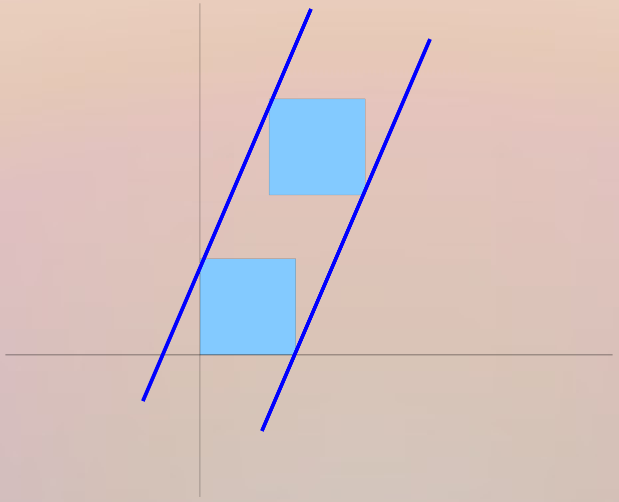


linear forms in the original ptopes

linear form generated by inversion

Prioritizing linear forms

- For each linear form, compute the bounds for the original parallelotopes

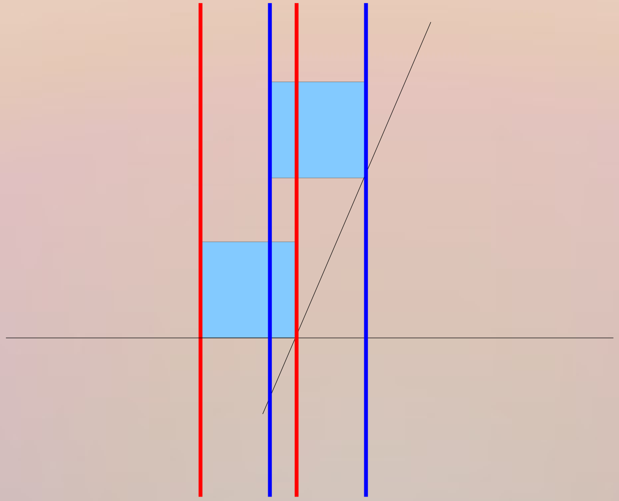


Bounds are the same
Priority 1

lower values are higher priority

Prioritizing linear forms

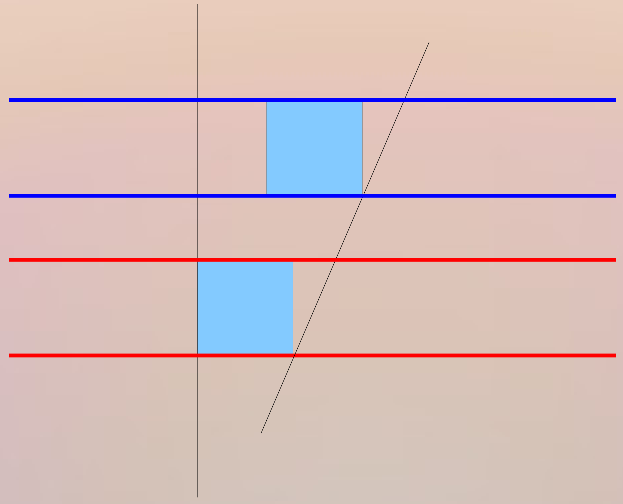
- For each linear form, compute the bounds for the original parallelotopes



Bounds intersect
Priority 2

Prioritizing linear forms

- For each linear form, compute the bounds for the original parallelotopes



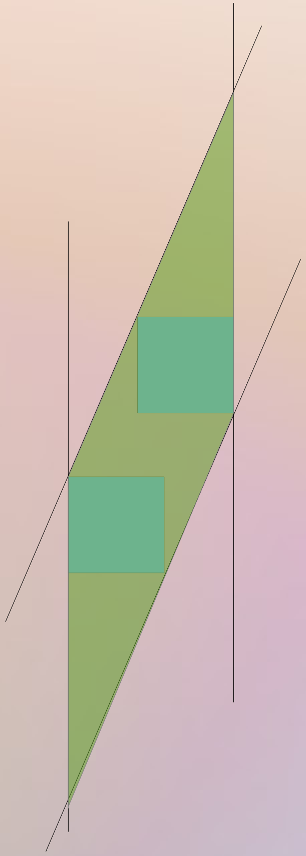
Bounds do not intersect
Priority 3

Choose linear forms

- Collect
  - In order of priority
  - Until we get a linearly independent set
- Easy in this case
- In the general case, follow
  - Gaussian elimination
  - or QR factorization

  and use pivots

relatively optimal



Precision

- Parallelotope is
  - More precise than Karr's analysis
  - Less precise than polyhedra
    - with standard join or inverse join
  - Incomparable with all the other domains
    - even with interval domain

Complexity

Operation	Parallelotopes	Karr's lin. eq.	Octagons (with normal.)
Check equality	n^3	n^2	n^2
Assignment	n^2	n^2	n^2
n.d. Assignment	n^2	n^2	n
Refinement	n^3	n^2 (equality)	n^3
Union	n^4	n^3	n^2
Widening	n^3	--	n^3

Example

```
i = 2
j = k+5
While (TRUE)
{
   i = i+1
   j = j+3
}
```

- Invariants
  - $3i - j + k = 1$
  - $2 \leq i$
  - $k+5 \leq j$

Found by parallelotope analysis

implied by the first twos

Example

```
i = 2
j = 0
while (TRUE)
{
    if (i*i==4)
        i = i+4
    else {
        j = j+1
        i = i+2
    }
}
```

- Invariants:
  - $i+2j \leq 6$
  - $0 \leq j$
  - $2j - i \leq -2$

Found by parallelotope analysis

found during inversion join, but discharged in favor of the first twos

Strong and weak points

- Strong points
  - No limits on the complexity of constraints
  - Reasonably fast
- Weak points
  - Few constraints may be handled simultaneously
  - Require rational arithmetic when analyzing floating point variables
    - but we didn't try very hard to use floating points

How to improve

- Parallelotope as an auxiliary domain
  - To be combined with domains such as *Octagon*, *TVPI*, *Interval*
  - The base domain compute the “standard invariants”
  - For constraints outside the reach of the standard domain, parallelotopes may help
- How to combine?
  - Reduced product? Difficult
  - Transfer function between the two domains
  - Need to tune Parallelotope to avoid invariants handled by the base domain