A New Encoding of Not Necessarily Closed Convex Polyhedra

Roberto BAGNARA, Patricia M. HILL, Enea ZAFFANELLA
University of Parma, Italy
University of Leeds, United Kingdom

http://www.cs.unipr.it/ppl/

Convex Polyhedra: What and Why

What?

- ➜ regions of $\mathbb{R}^n$ bounded by a finite set of hyperplanes.

Why? Solving Classical Data-Flow Analysis Problems!

- ➜ array bound checking and compile-time overflow detection;
- ➜ loop invariant computations and loop induction variables.

Why? Verification of Concurrent and Reactive Systems!

- ➜ synchronous languages;
- ➜ linear hybrid automata (roughly, FSMs with time requirements);
- ➜ systems based on temporal specifications.

And Again: Many Other Applications...

- ➜ inferring argument size relationships in logic programs;
- ➜ termination inference for Prolog programs;
- ➜ string cleanness for C programs.

NOT NECESSARILY CLOSED POLYHEDRA

Constraint Representation: $\mathrm{con}(\mathcal{C})$

- If $\boldsymbol{a} \in \mathbb{R}^n$, $\boldsymbol{a} \neq \boldsymbol{0}$, and $b \in \mathbb{R}$, the linear non-strict (resp., strict) inequality constraint $\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b$ (resp., $\langle \boldsymbol{a}, \boldsymbol{x} \rangle > b$) defines a closed (resp., open) affine half-space.
- Mixed constraint systems $\Longleftrightarrow$ NNC polyhedra.

Not Necessarily Closed Polyhedra

Constraint Representation: $\mathrm{con}(\mathcal{C})$

- If $\boldsymbol{a} \in \mathbb{R}^n$, $\boldsymbol{a} \neq \mathbf{0}$, and $b \in \mathbb{R}$, the linear non-strict (resp., strict) inequality constraint $\langle \boldsymbol{a}, \boldsymbol{x} \rangle \geq b$ (resp., $\langle \boldsymbol{a}, \boldsymbol{x} \rangle > b$) defines a closed (resp., open) affine half-space.
- Mixed constraint systems $\Longleftrightarrow$ NNC polyhedra.

Generator Representation: $\mathrm{gen}(\mathcal{G})$, where $\mathcal{G} = (R, P, C)$

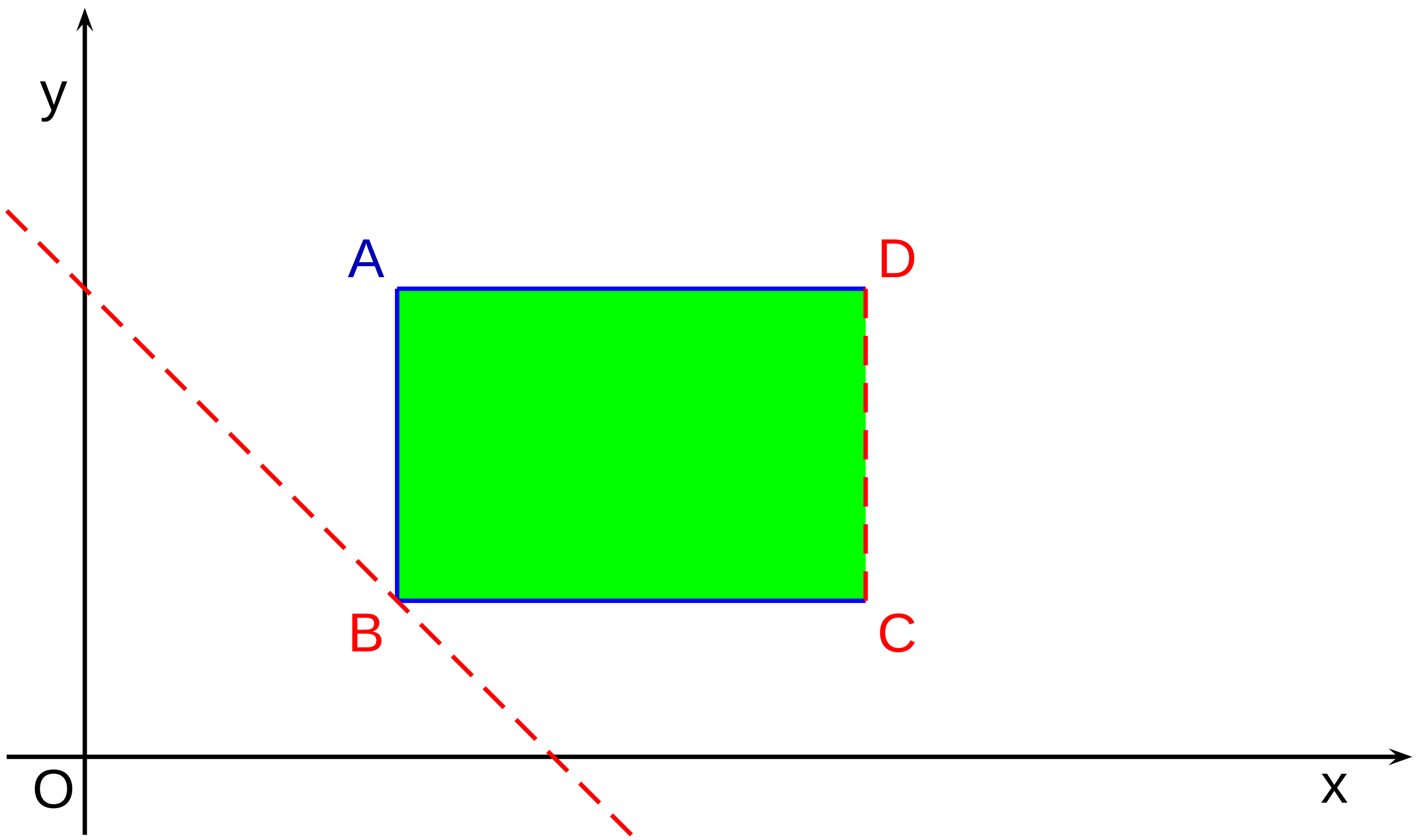
- $\boldsymbol{r} \in \mathbb{R}^n$ is a ray of $\mathcal{P} \subseteq \mathbb{R}^n$ iff it is a direction of infinity for $\mathcal{P}$;
- $\boldsymbol{p} \in \mathbb{R}^n$ is a point of $\mathcal{P} \subseteq \mathbb{R}^n$ iff $\boldsymbol{p} \in \mathcal{P}$.
- $\boldsymbol{c} \in \mathbb{R}^n$ is a closure point of $\mathcal{P} \subseteq \mathbb{R}^n$ iff $\boldsymbol{c} \in \mathbb{C}(\mathcal{P})$.
- All NNC polyhedra can be expressed as

$$\left\{ R\boldsymbol{\rho} + P\boldsymbol{\pi} + C\boldsymbol{\gamma} \in \mathbb{R}^n \;\middle|\; \begin{array}{l} \boldsymbol{\rho} \in \mathbb{R}^r_+, \boldsymbol{\pi} \in \mathbb{R}^p_+, \boldsymbol{\gamma} \in \mathbb{R}^c_+, \\ \boldsymbol{\pi} \neq \mathbf{0}, \sum_{i=1}^p \pi_i + \sum_{i=1}^c \gamma_i = 1 \end{array} \right\}.$$

- Extended generator systems $\Longleftrightarrow$ NNC polyhedra.

Example Using Constraints

$\mathcal{P} = \mathrm{con}\big(\{2 \leq x, x < 5, 1 \leq y \leq 3, x + y > 3\}\big).$

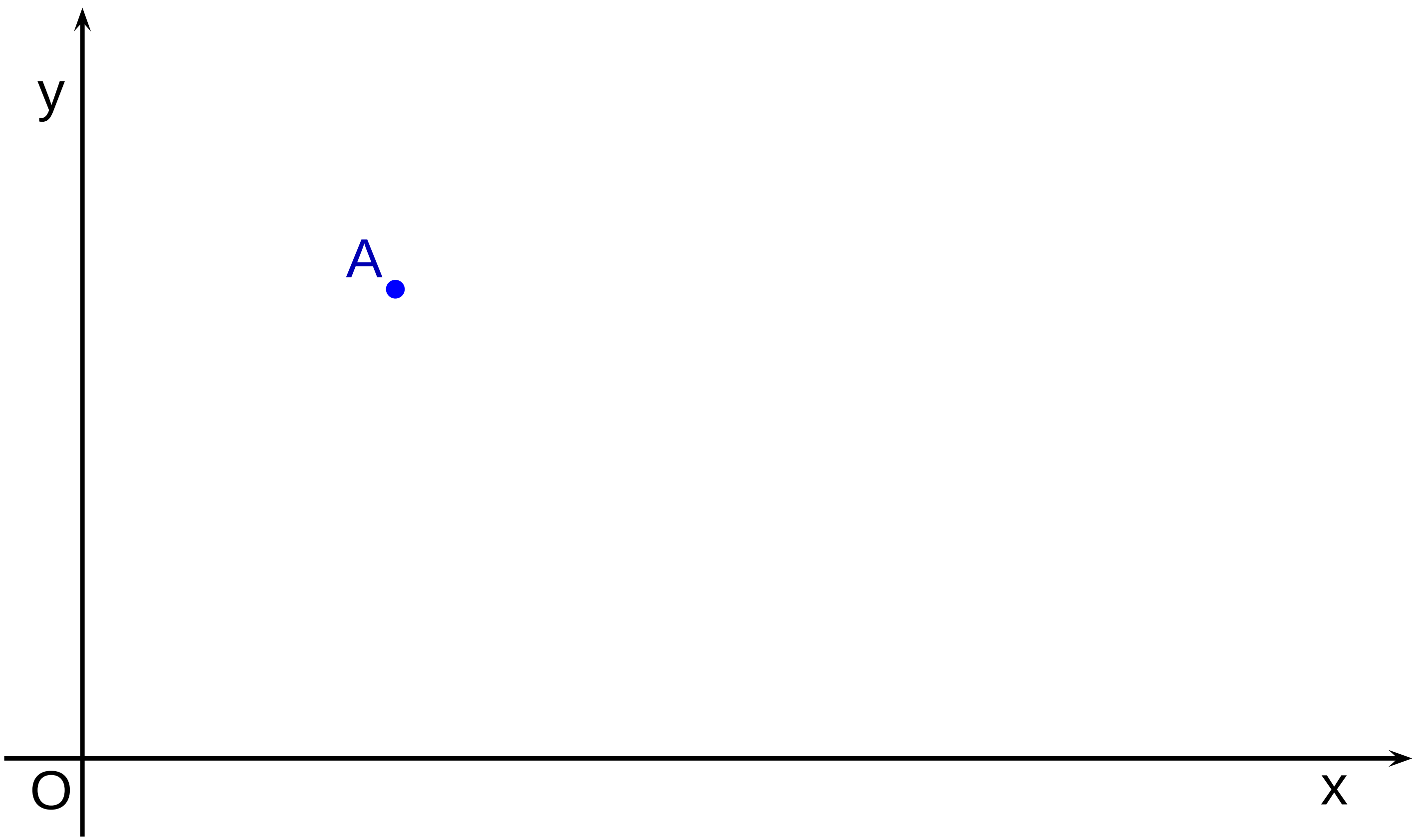


Same Example Using Generators (i)

$$\mathcal{P} = \mathrm{gen}\big((R, P, C)\big) = \mathrm{gen}\big((\varnothing, \varnothing, \varnothing)\big).$$

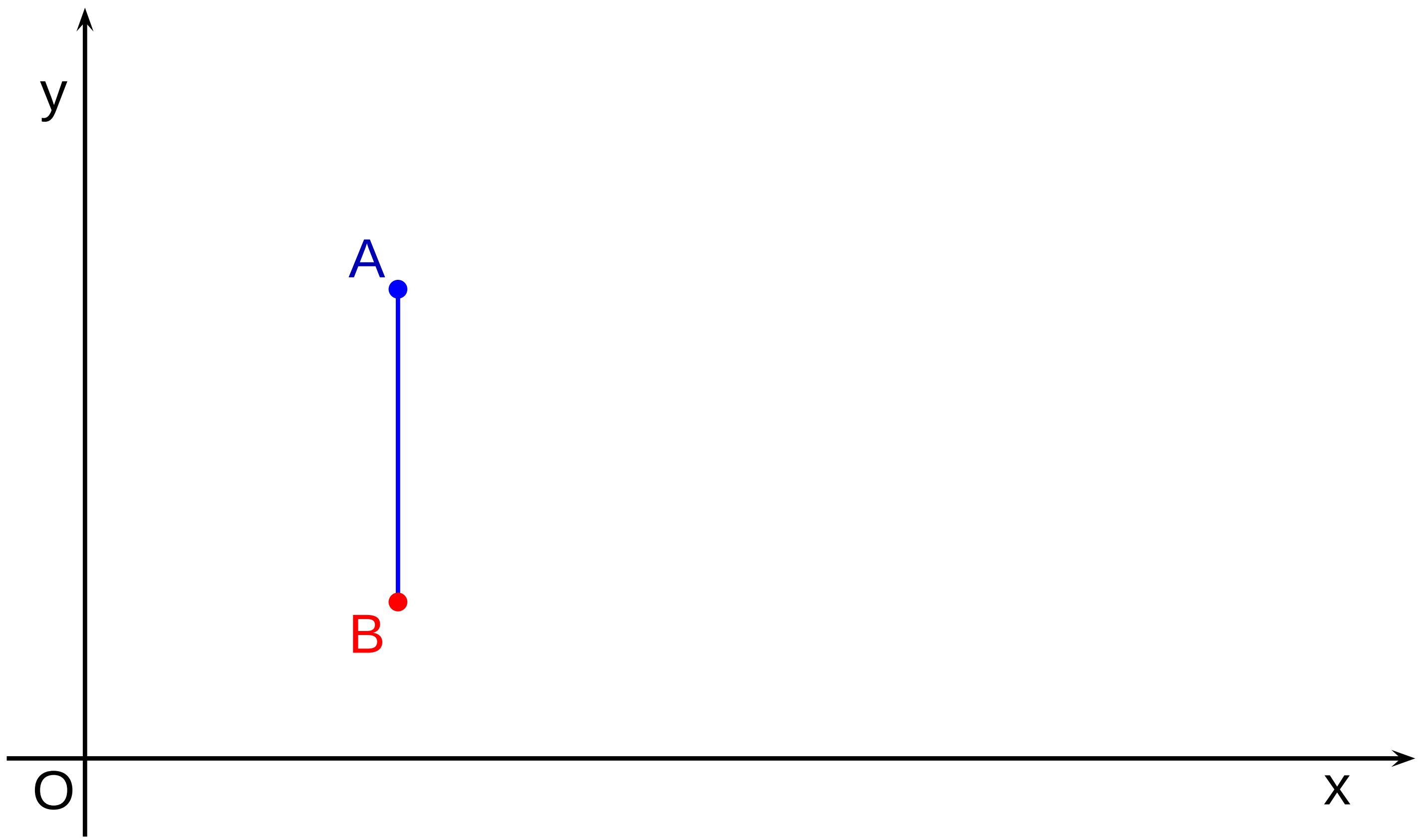
Same Example Using Generators (ii)

$$\mathcal{P} = \text{gen}\big((R, P, C)\big) = \text{gen}\Big(\big(\varnothing, \{A\}, \varnothing\big)\Big).$$



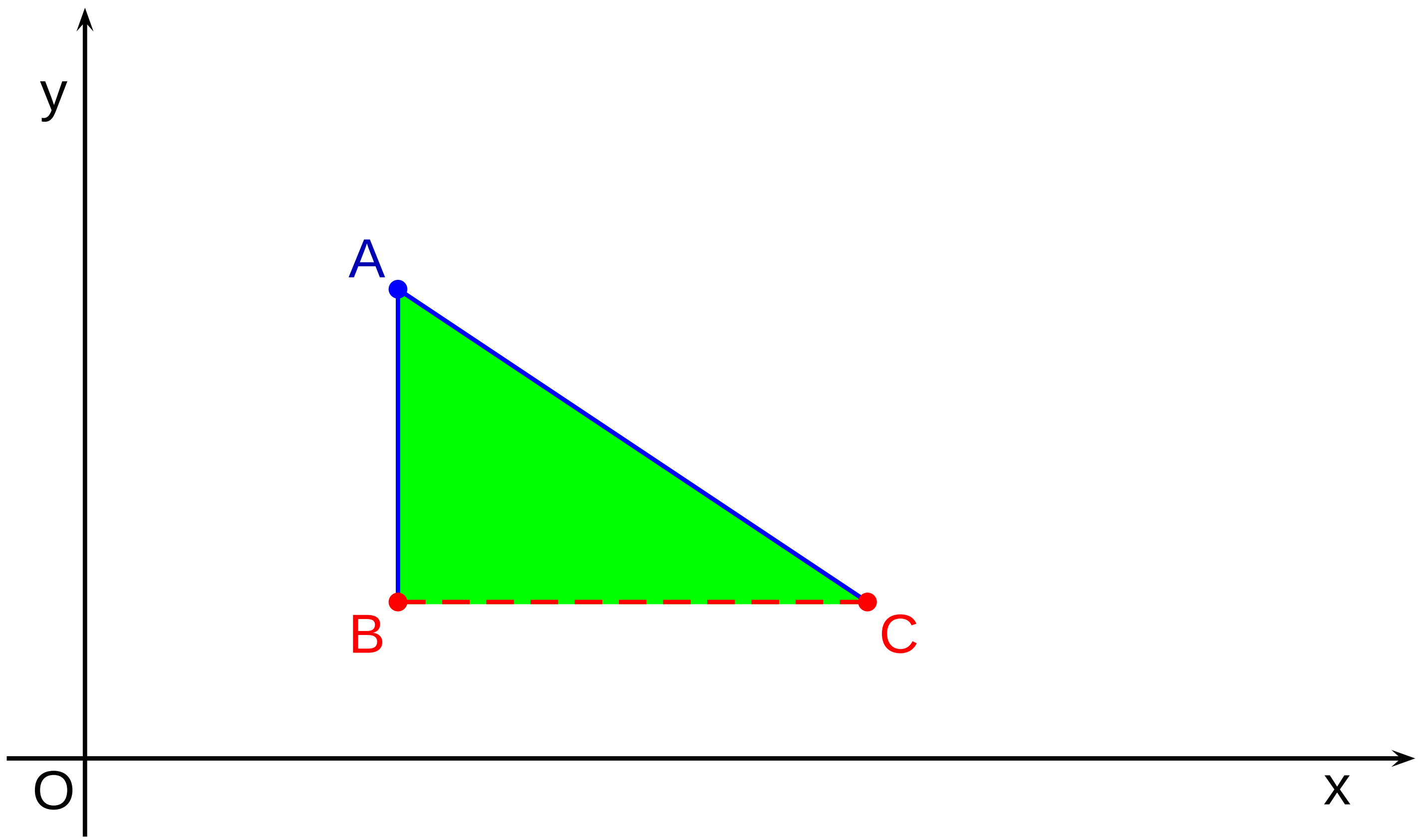
Same Example Using Generators (iii)

$$\mathcal{P} = \mathrm{gen}\big((R,P,C)\big) = \mathrm{gen}\Big(\big(\varnothing,\{A\},\{B\}\big)\Big).$$



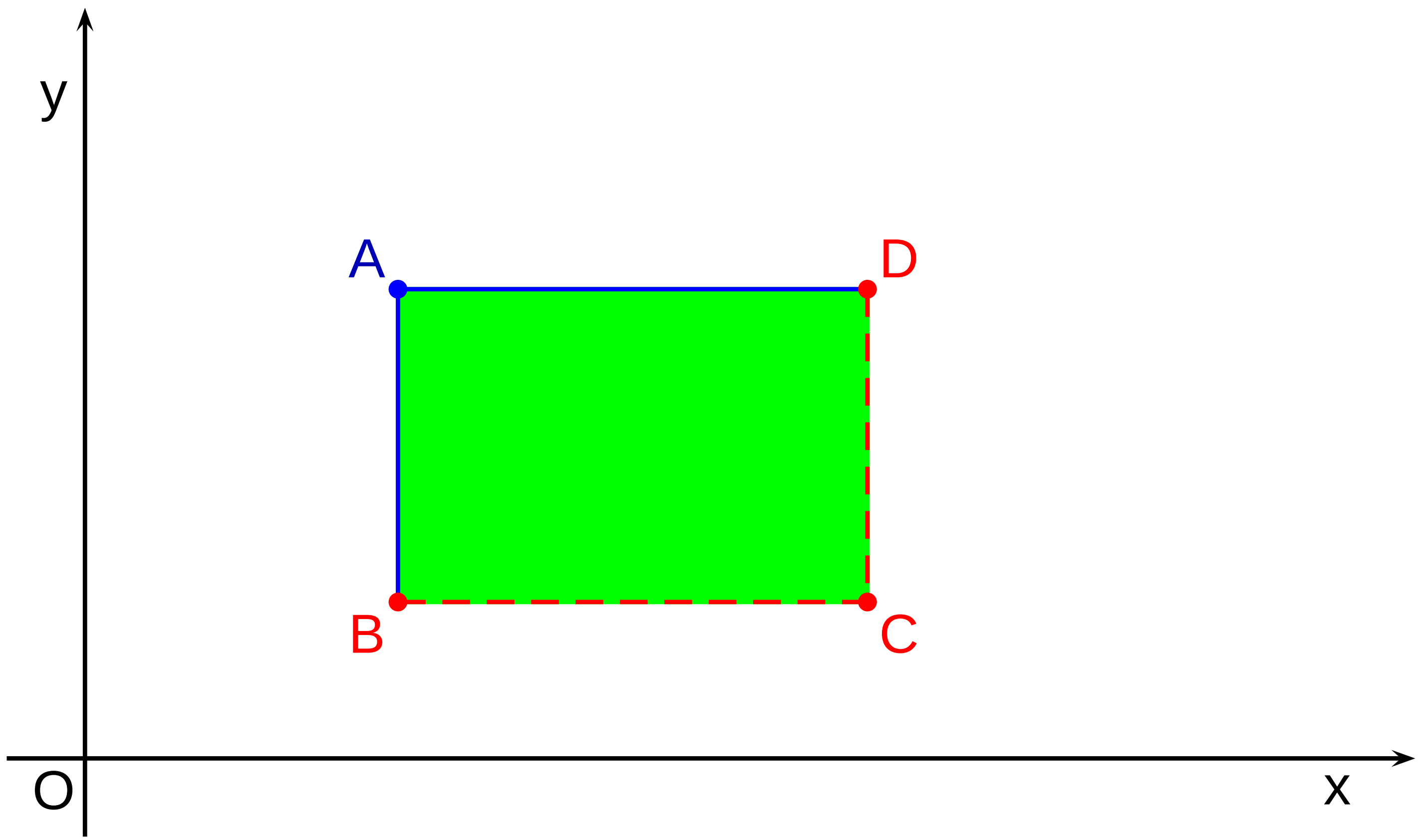
Same Example Using Generators (iv)

$$\mathcal{P} = \text{gen}\big((R, P, C)\big) = \text{gen}\Big(\big(\varnothing, \{A\}, \{B, C\}\big)\Big).$$



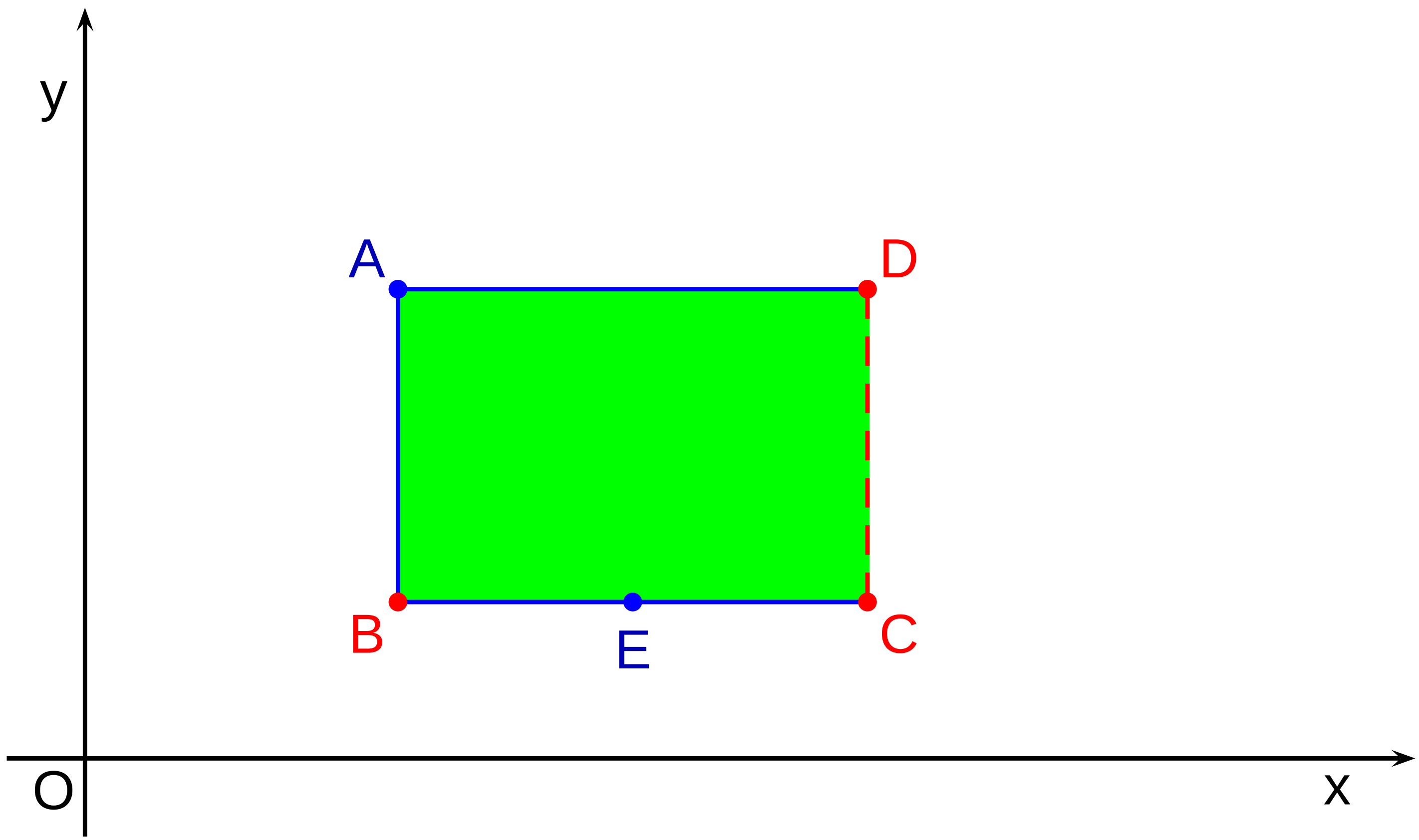
Same Example Using Generators (v)

$$\mathcal{P} = \mathrm{gen}\big((R,P,C)\big) = \mathrm{gen}\Big(\big(\varnothing,\{A\},\{B,C,D\}\big)\Big).$$



Same Example Using Generators (vi)

$$\mathcal{P} = \text{gen}\big((R, P, C)\big) = \text{gen}\Big(\big(\varnothing, \{A, E\}, \{B, C, D\}\big)\Big).$$



Encoding NNC Polyhedra as C Polyhedra

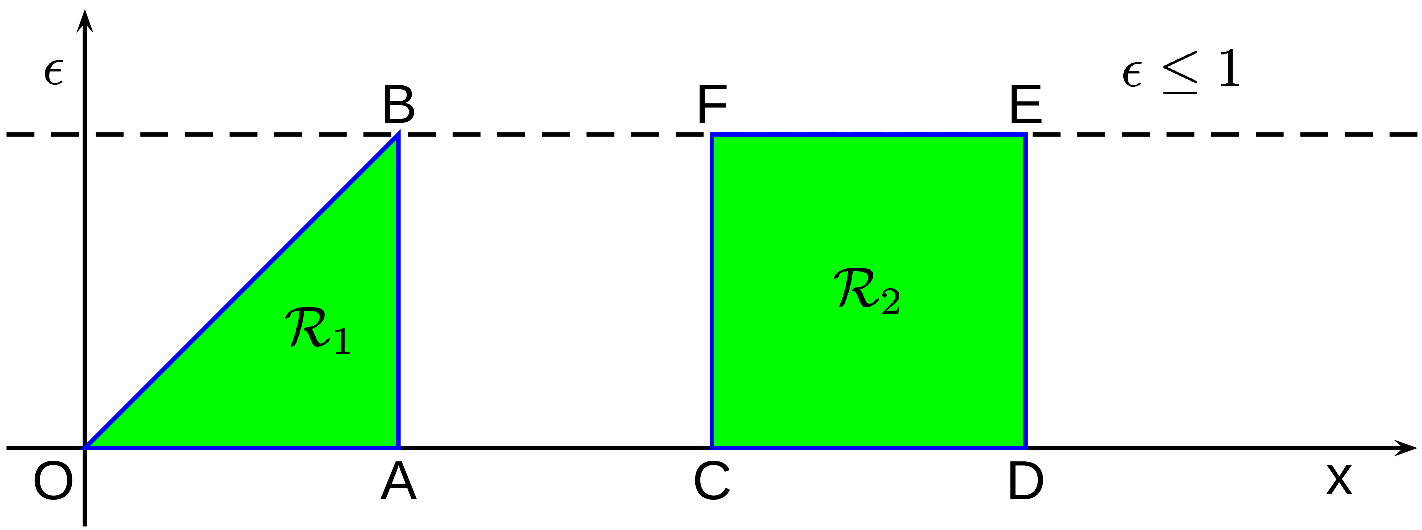
- Let $\mathbb{P}_n$ and $\mathbb{CP}_n$ be the sets of all NNC and closed polyhedra, respectively: each $\mathcal{P} \in \mathbb{P}_n$ can be embedded into $\mathcal{R} \in \mathbb{CP}_{n+1}$.
- A new dimension is added, the ϵ coordinate:
  - to distinguish between strict and non-strict constraints;
  - to distinguish between points and closure points.
- (Will denote by e the coefficient of the ϵ coordinate.)
- The encoded NNC polyhedron:

$$\mathcal{P} = [\![\mathcal{R}]\!] \stackrel{\text{def}}{=} \left\{ \boldsymbol{v} \in \mathbb{R}^n \;\middle|\; \exists e > 0 \,.\, (\boldsymbol{v}^{\mathrm{T}}, e)^{\mathrm{T}} \in \mathcal{R} \right\}.$$

Example: Encoding $\mathbb{P}_1$ Into $\mathbb{CP}_2$

$\mathcal{R}_1$ encodes $\mathcal{P}_1 = \mathrm{con}\big(\{0 < x \leq 1\}\big)$,

$\mathcal{R}_2$ encodes $\mathcal{P}_2 = \mathrm{con}\big(\{2 \leq x \leq 3\}\big)$.



The Approach by Halbwachs et al.

➜ If $\mathcal{P} \in \mathbb{P}_n$ and $\mathcal{P} = \mathrm{con}(\mathcal{C})$, where

$$\mathcal{C} = \bigl\{\, \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle \bowtie_i b_i \bigm| i \in \{1, \ldots, m\}, \boldsymbol{a}_i \in \mathbb{R}^n, \bowtie_i \in \{\geq, >\}, b_i \in \mathbb{R} \,\bigr\},$$

then $\mathcal{R} \in \mathbb{CP}_{n+1}$ is defined by $\mathcal{R} = \mathrm{con}\bigl(\mathrm{con\_repr}(\mathcal{C})\bigr)$, where

$$\begin{aligned} \mathrm{con\_repr}(\mathcal{C}) \stackrel{\mathrm{def}}{=} {} & \bigl\{0 \leq \epsilon \leq 1\bigr\} \\ & \cup \bigl\{\, \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle - 1 \cdot \epsilon \geq b_i \bigm| i \in \{1, \ldots, m\}, \bowtie_i \in \{>\} \,\bigr\} \\ & \cup \bigl\{\, \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle + 0 \cdot \epsilon \geq b_i \bigm| i \in \{1, \ldots, m\}, \bowtie_i \in \{\geq\} \,\bigr\}. \end{aligned}$$

➜ If $\mathcal{P} \in \mathbb{P}_n$ and $\mathcal{P} = \mathrm{gen}(\mathcal{G})$, where $\mathcal{G} = (R, P, C)$, then $\mathcal{R} \in \mathbb{CP}_{n+1}$ is defined by $\mathcal{R} = \mathrm{gen}\bigl(\mathrm{gen\_repr}(\mathcal{G})\bigr) = \mathrm{gen}\bigl((R', P')\bigr)$, where

$$\begin{aligned} R' &= \bigl\{\, (\boldsymbol{r}^{\mathrm{T}}, 0)^{\mathrm{T}} \bigm| \boldsymbol{r} \in R \,\bigr\}, \\ P' &= \bigl\{\, (\boldsymbol{p}^{\mathrm{T}}, 1)^{\mathrm{T}}, (\boldsymbol{p}^{\mathrm{T}}, 0)^{\mathrm{T}} \bigm| \boldsymbol{p} \in P \,\bigr\} \cup \bigl\{\, (\boldsymbol{c}^{\mathrm{T}}, 0)^{\mathrm{T}} \bigm| \boldsymbol{c} \in C \,\bigr\}. \end{aligned}$$

The Approach by Halbwachs et al. (cont'd)

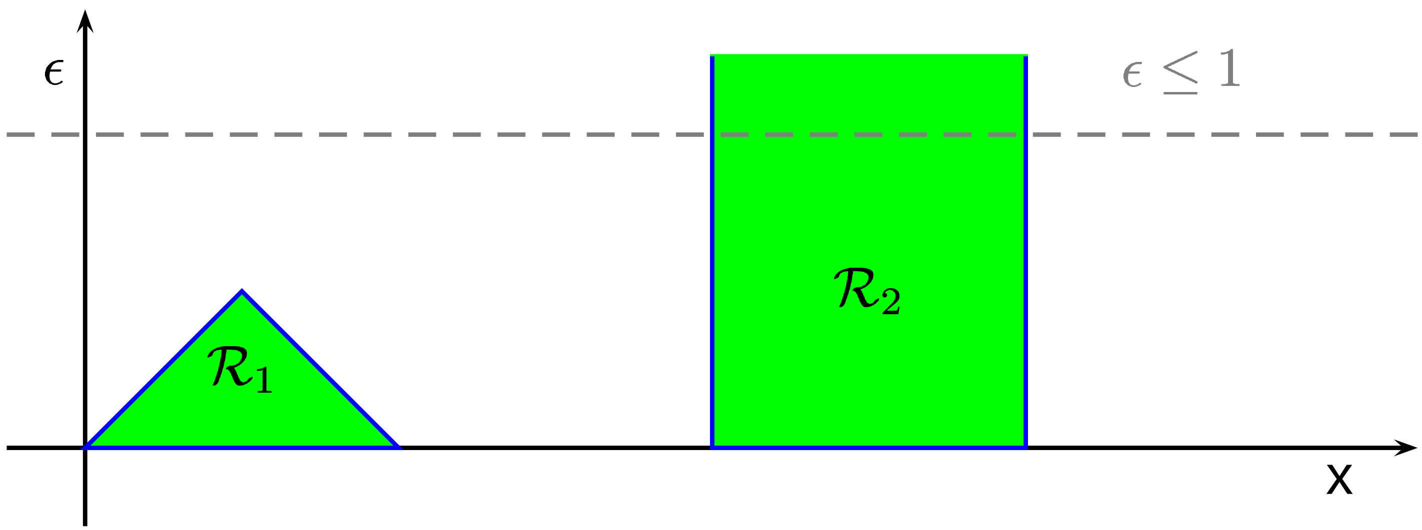
- With a little precaution the operations on representations do (or can be slightly modified to do) what is expected:
  - intersection;
  - convex polyhedral hull;
  - affine image and preimage;
  - ...
- This encoding is used in the New Polka library by B. Jeannet and in the Parma Polyhedra Library.
- Is this approach the only possible one?
- Can we generalize this construction so as to preserve its good qualities?

The Constraint $\epsilon \leq \delta$ is Needed . . .

Suppose we do not add any ϵ-upper-bound constraint:

$\mathcal{R}_1$ encodes $\mathcal{P}_1 = \mathrm{con}\big(\{0 < x < 1\}\big)$,

$\mathcal{R}_2$ encodes $\mathcal{P}_2 = \mathrm{con}\big(\{2 \leq x \leq 3\}\big)$.

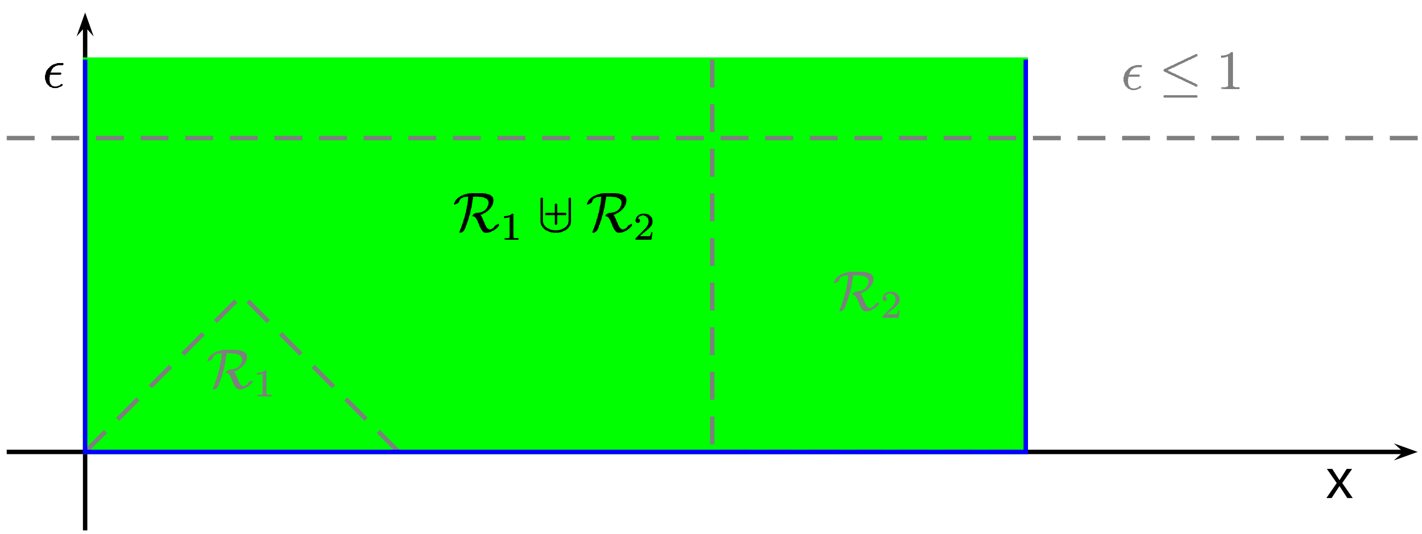


. . . Because Otherwise the Poly-Hull is Not Correct

The poly-hull $\mathcal{P}_1 \uplus \mathcal{P}_2$ is not represented correctly by $\mathcal{R}_1 \uplus \mathcal{R}_2$.

$$\mathcal{P}_1 \uplus \mathcal{P}_2 \stackrel{\text{def}}{=} \text{con}\big(\{0 < x \leq 3\}\big),$$

$\mathcal{R}_1 \uplus \mathcal{R}_2$ encodes $\mathcal{P}' = \text{con}\big(\{0 \leq x \leq 3\}\big)$.

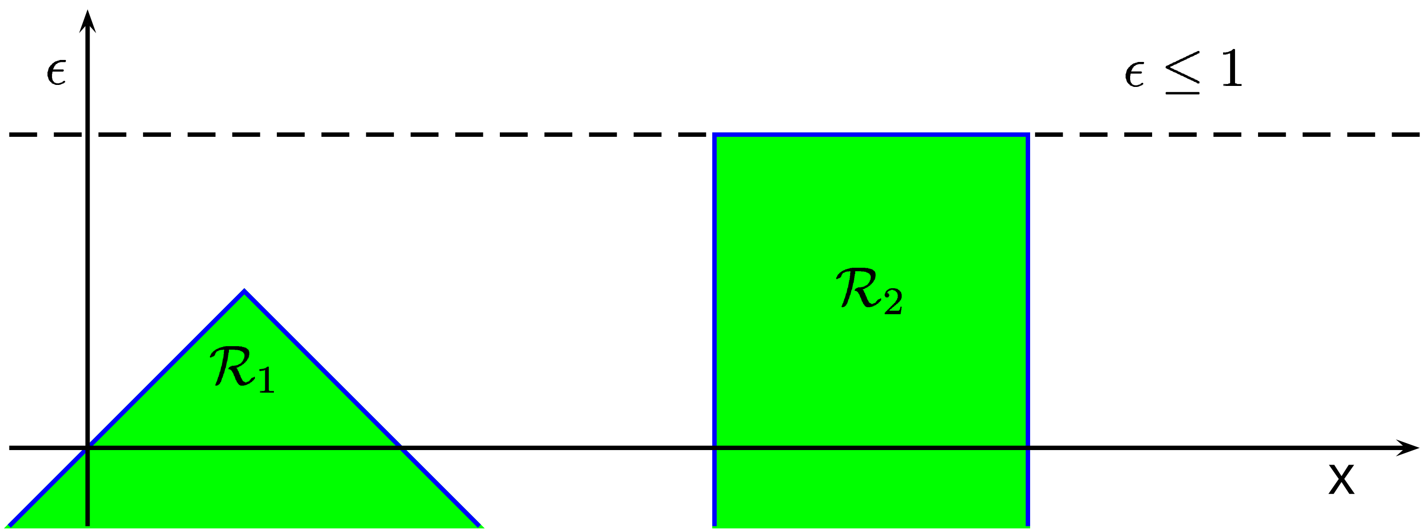


The Constraint $\epsilon \geq 0$ is Needed ...

Suppose we do not add the non-negativity constraint for ϵ:

$\mathcal{R}_1$ encodes $\mathcal{P}_1 = \mathrm{con}\big(\{0 < x < 1\}\big)$,

$\mathcal{R}_2$ encodes $\mathcal{P}_2 = \mathrm{con}\big(\{2 \leq x \leq 3\}\big)$.

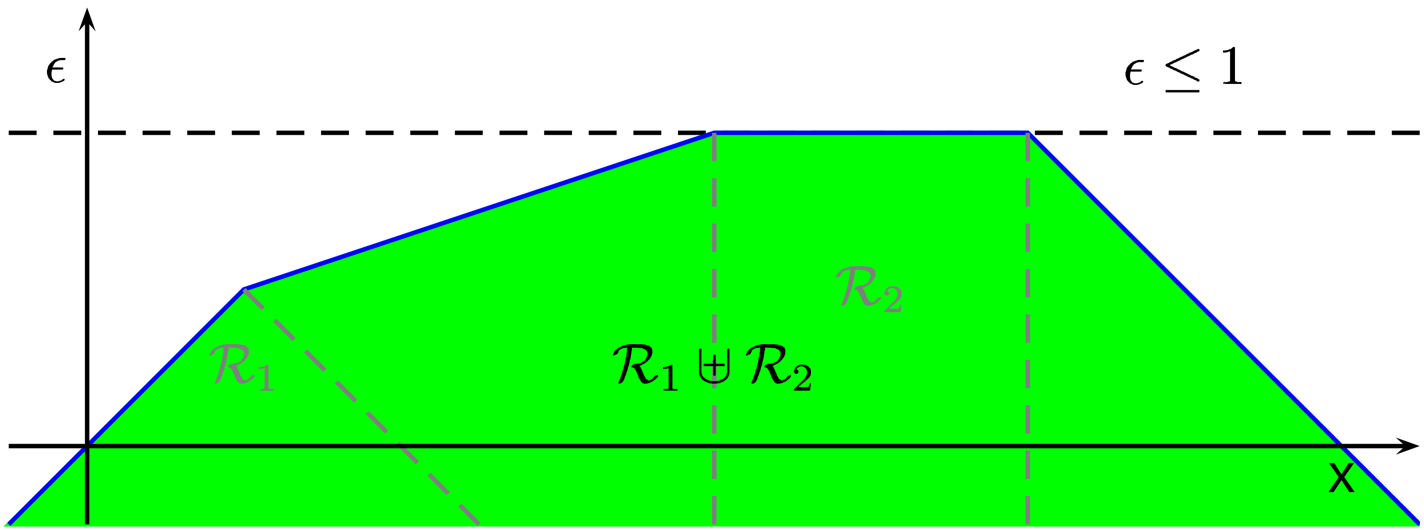


... For the Same Reason ...

The poly-hull $\mathcal{P}_1 \uplus \mathcal{P}_2$ is not represented correctly by $\mathcal{R}_1 \uplus \mathcal{R}_2$.

$$\mathcal{P}_1 \uplus \mathcal{P}_2 \stackrel{\text{def}}{=} \operatorname{con}\bigl(\{0 < x \leq 3\}\bigr),$$

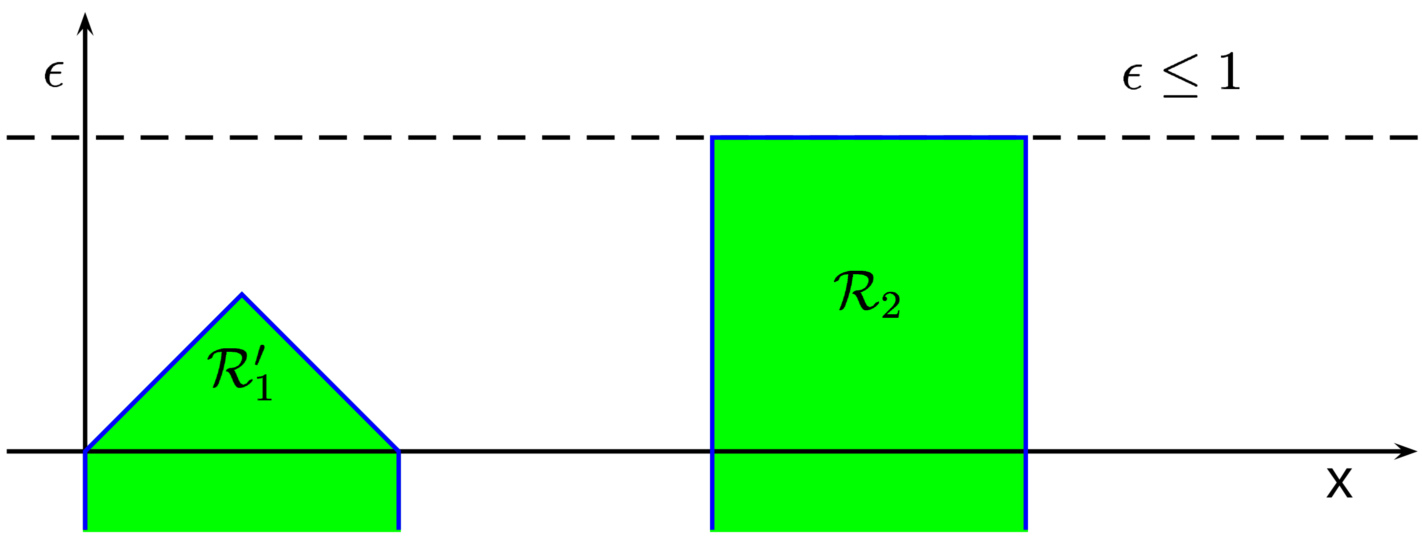
$\mathcal{R}_1 \uplus \mathcal{R}_2$ encodes $\mathcal{P}'' = \operatorname{con}\bigl(\{0 < x < 4\}\bigr)$.



. . . But This Time There is a Workaround!

In the encoding, for each strict inequality constraint, do also add the corresponding non-strict inequality.

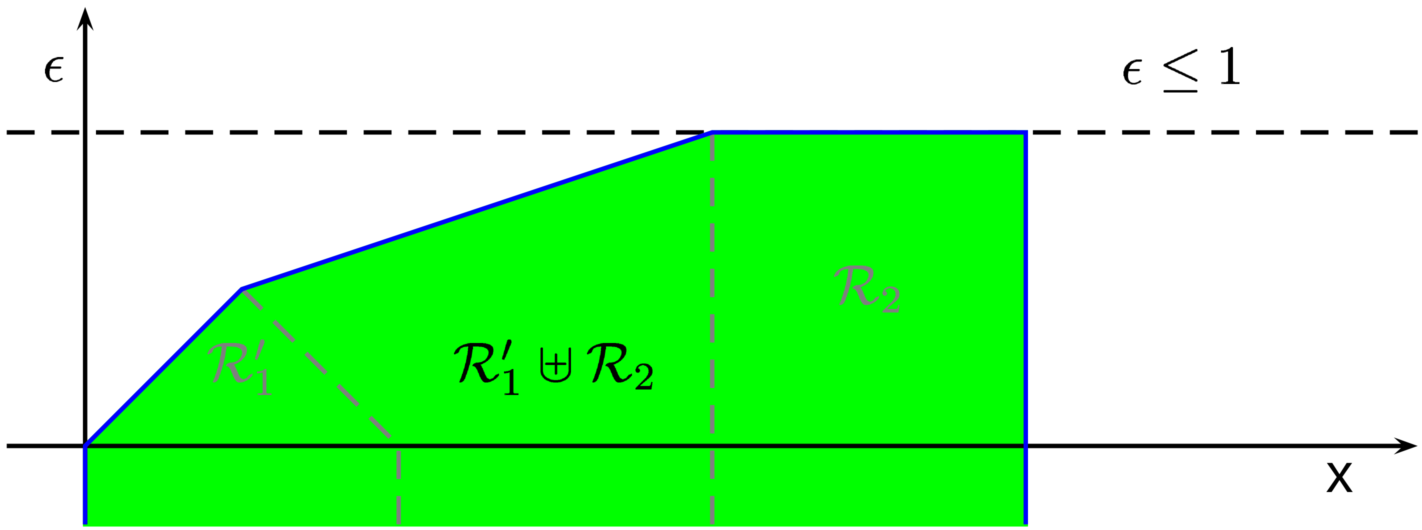
$$\mathcal{R}_1' \stackrel{\text{def}}{=} \text{con}\big(\{\epsilon \le 1, x - \epsilon \ge 0, x \ge 0, -x - \epsilon \ge -1, -x \ge -1\}\big).$$



... But This Time There is a Workaround!

In the encoding, for each strict inequality constraint, do also add the corresponding non-strict inequality.

$$\mathcal{R}_1' \stackrel{\text{def}}{=} \operatorname{con}\big(\{\epsilon \leq 1, x - \epsilon \geq 0, x \geq 0, -x - \epsilon \geq -1, -x \geq -1\}\big).$$



The Alternative Encoding

- If $\mathcal{P} \in \mathbb{P}_n$ and $\mathcal{P} = \mathrm{con}(\mathcal{C})$, where

$$\mathcal{C} = \left\{ \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle \bowtie_i b_i \;\middle|\; i \in \{1, \ldots, m\}, \boldsymbol{a}_i \in \mathbb{R}^n, \bowtie_i \in \{\geq, >\}, b_i \in \mathbb{R} \right\},$$

then $\mathcal{R} \in \mathbb{CP}_{n+1}$ is defined by $\mathcal{R} = \mathrm{con}\bigl(\mathrm{con\_repr}(\mathcal{C})\bigr)$, where

$$\begin{aligned} \mathrm{con\_repr}(\mathcal{C}) \stackrel{\mathrm{def}}{=} \{\epsilon \leq 1\} & \\ & \cup \left\{ \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle - 1 \cdot \epsilon \geq b_i \;\middle|\; i \in \{1, \ldots, m\}, \bowtie_i \in \{>\} \right\} \\ & \cup \left\{ \langle \boldsymbol{a}_i, \boldsymbol{x} \rangle + 0 \cdot \epsilon \geq b_i \;\middle|\; i \in \{1, \ldots, m\}, \bowtie_i \in \{\geq, >\} \right\}. \end{aligned}$$

- If $\mathcal{P} \in \mathbb{P}_n$ and $\mathcal{P} = \mathrm{gen}(\mathcal{G})$, where $\mathcal{G} = (R, P, C)$, then $\mathcal{R} \in \mathbb{CP}_{n+1}$ is defined by $\mathcal{R} = \mathrm{gen}\bigl(\mathrm{gen\_repr}(\mathcal{G})\bigr) = \mathrm{gen}\bigl((R', P')\bigr)$, where

$$\begin{aligned} R' &= \left\{(\boldsymbol{0}^{\mathrm{T}}, -1)^{\mathrm{T}}\right\} \cup \left\{ (\boldsymbol{r}^{\mathrm{T}}, 0)^{\mathrm{T}} \;\middle|\; \boldsymbol{r} \in R \right\}, \\ P' &= \left\{ (\boldsymbol{p}^{\mathrm{T}}, 1)^{\mathrm{T}} \;\middle|\; \boldsymbol{p} \in P \right\} \cup \left\{ (\boldsymbol{q}^{\mathrm{T}}, 0)^{\mathrm{T}} \;\middle|\; \boldsymbol{q} \in C \right\}. \end{aligned}$$

CONSTRAINT-BIASED VS GENERATOR-BIASED REPRESENTATIONS

- ➜ The alternative encoding has dual properties with respect to the original by Halbwachs et al.
  - ➜ With the original, the encoding of an NNC polyhedron may require a similar number of constraints but about twice the number of generators: it is *constraint-biased*.
  - ➜ With the alternative, it may require a similar number of generators but twice the number of constraints: this encoding is *generator-biased*.

$\Longrightarrow$ Due to the use of exponential algorithms, their computational behavior can vary wildly depending on the operation and on the actual polyhedra being manipulated.

$\Longrightarrow$ It seems likely that the performance of one encoding with respect to the other will heavily depend on the particular application.

FUTURE WORK

- An implementation of the proposed techniques is ongoing.
  - Interested? Go to `http://www.cs.unipr.it/ppl/`, learn how to access the CVS repository anonymously, and check out the `alt_nnc` development branch!
- Can we devise efficient techniques so as to use both constraint- and generator-biased encodings, switching dynamically from one to the other in an attempt to maximize performance?
- A minimized encoding may represent a non-minimized NNC polyhedron:
  - this is true for both encodings;
  - in our SAS'02 paper we propose a stronger form of minimization;
  - we are working on a generalization of this idea that encompasses both the constraint- and the generator-biased encodings.