Cylindrical Algebraic Decomposition Based Methods in Satisfiability Modulo Non-linear Real Arithmetic

Jasper Nalbach

RWTH Aachen University

PhD Defence
November 12, 2025

What is Real Algebra?

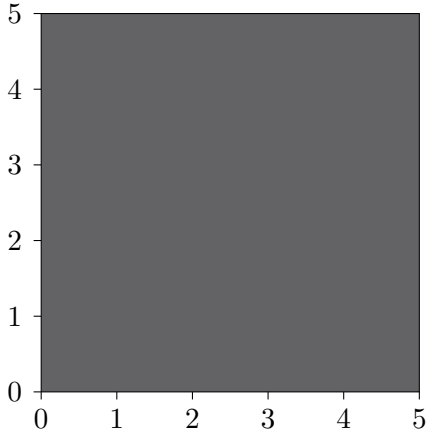


Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

What is Real Algebra?

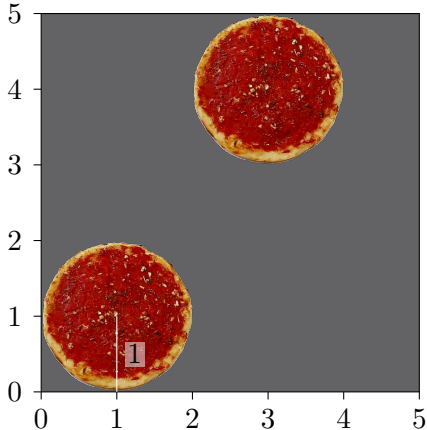
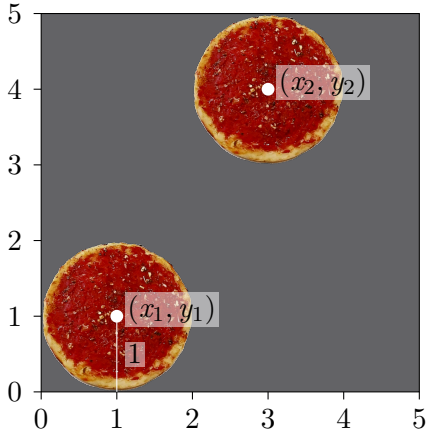


Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

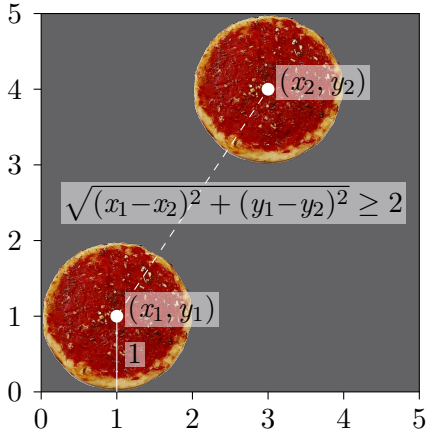
What is Real Algebra?



$$1 \leq x_1, x_2, y_1, y_2 \leq 5 - 1$$

Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

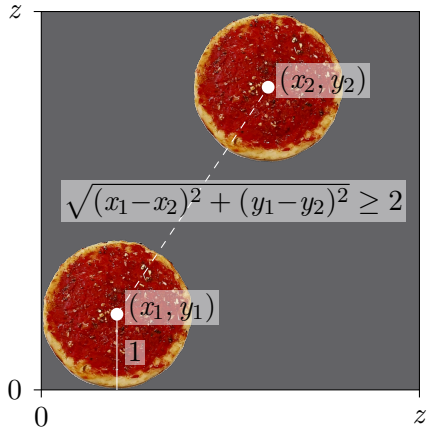
What is Real Algebra?



$$1 \leq x_1, x_2, y_1, y_2 \leq 5 - 1$$
$$\wedge\, (x_1 - x_2)^2 + (y_1 - y_2)^2 \geq 4$$

Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

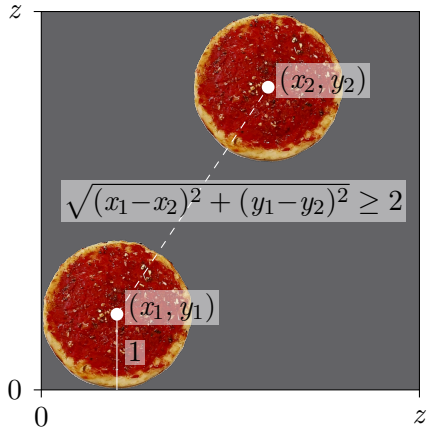
What is Real Algebra?



$$\forall z.\ 2 \leq z \leq 6 \rightarrow \exists x_1.\ \exists x_2.\ \exists y_1.\ \exists y_2.$$
$$1 \leq x_1, x_2, y_1, y_2 \leq z - 1$$
$$\wedge\ (x_1 - x_2)^2 + (y_1 - y_2)^2 \geq 4$$

Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

What is Real Algebra?



$$\exists x_1.\ \exists x_2.\ \exists y_1.\ \exists y_2.$$
$$1 \leq x_1, x_2, y_1, y_2 \leq z - 1$$
$$\wedge\, (x_1 - x_2)^2 + (y_1 - y_2)^2 \geq 4$$
$$\equiv z \geq 2 + \sqrt{2}$$

Image Credit: DinaBenedettoFerrandina, CC BY-SA 4.0, via Wikimedia Commons (modified)

History of Real Algebra

Al-Khwarizmi 820 al-Kitāb al-Mukhtaṣar fī Ḥisāb al-Jabr wal-Muqābalah (The Compendious Book on Calculation by Completion and Balancing)

History of Real Algebra

Al-Khwarizmi 820 al-Kitāb al-Mukhtaṣar fī Ḥisāb al-Jabr wal-Muqābalah (The Compendious Book on Calculation by Completion and Balancing)

Tarski's method (Tarski 1948, Seidel 1954) $\omega(2^{\cdot^{\cdot^{\cdot^{2^n}}}})$

History of Real Algebra

Al-Khwarizmi 820 al-Kitāb al-Mukhtaṣar fī Ḥisāb al-Jabr wal-Muqābalah (The Compendious Book on Calculation by Completion and Balancing)

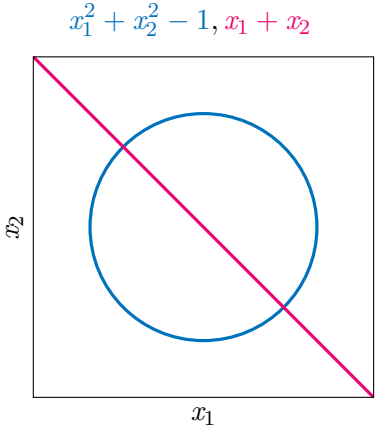
Tarski's method (Tarski 1948, Seidel 1954) $\omega(2^{\cdot^{\cdot^{\cdot^{2^n}}}})$

Cylindrical Algebraic Decomposition (Collins 1975) $\mathcal{O}(2^{2^n})$

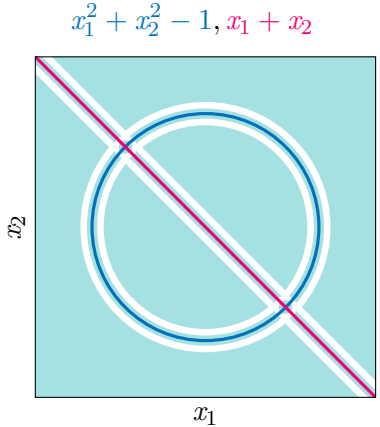
Cylindrical Algebraic Decomposition [Collins 1975]

$$\exists x_1.\ \exists x_2.\ x_1^2 + x_2^2 - 1 < 0 \wedge x_1 + x_2 > 0$$

Cylindrical Algebraic Decomposition [Collins 1975]

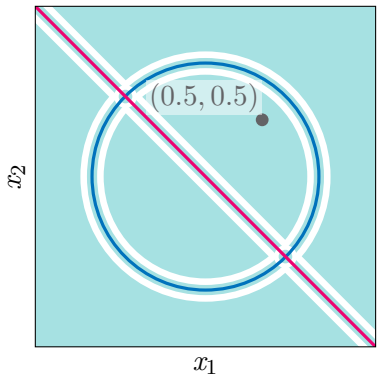


Cylindrical Algebraic Decomposition [Collins 1975]



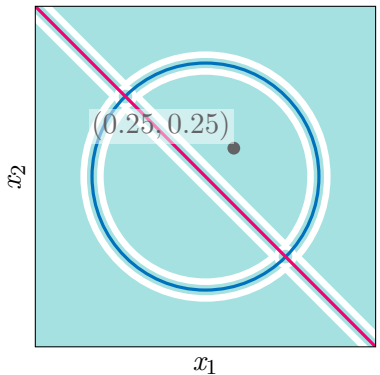
Cylindrical Algebraic Decomposition [Collins 1975]

$$0.5^2 + 0.5^2 - 1 < 0, 0.5 + 0.5 > 0$$

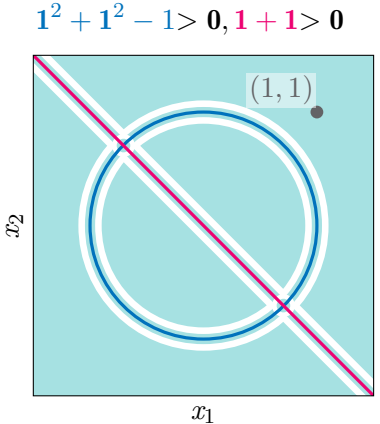


Cylindrical Algebraic Decomposition [Collins 1975]

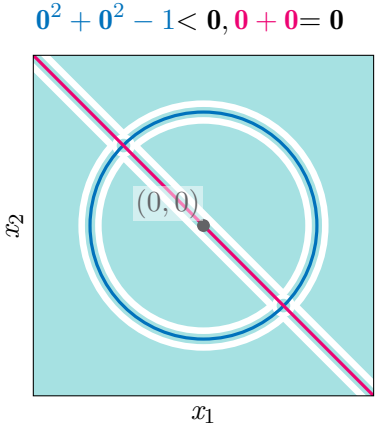
$$0.25^2 + 0.25^2 - 1 < 0, 0.25 + 0.25 > 0$$



Cylindrical Algebraic Decomposition [Collins 1975]

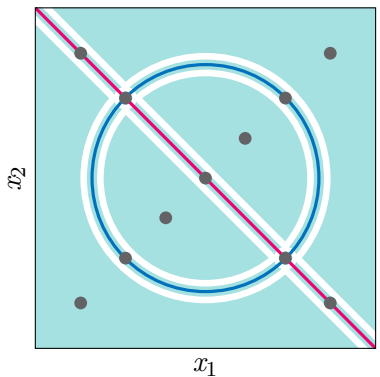


Cylindrical Algebraic Decomposition [Collins 1975]



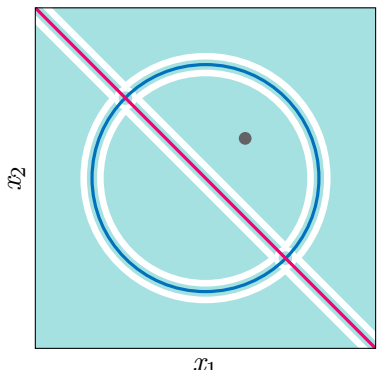
Cylindrical Algebraic Decomposition [Collins 1975]

$$\exists x_1.\ \exists x_2.\ x_1^2 + x_2^2 - 1 < 0 \wedge x_1 + x_2 > 0$$



Cylindrical Algebraic Decomposition [Collins 1975]

$$\exists x_1.\ \exists x_2.\ x_1^2 + x_2^2 - 1 < 0 \wedge x_1 + x_2 > 0$$

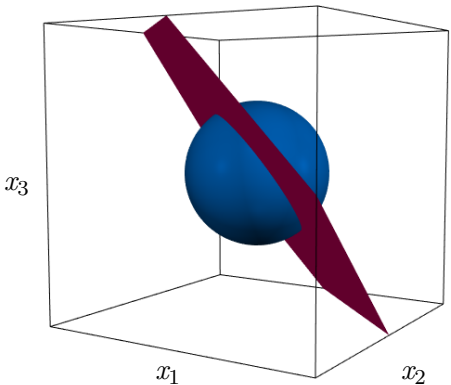


Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2 + x_3$$

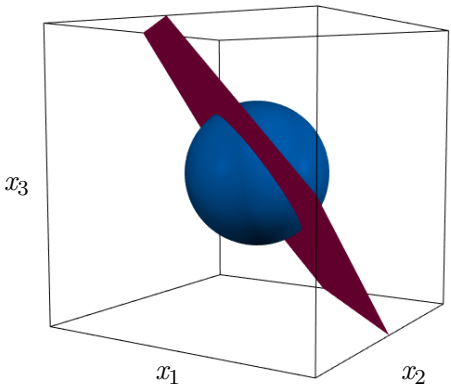
Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2 + x_3$

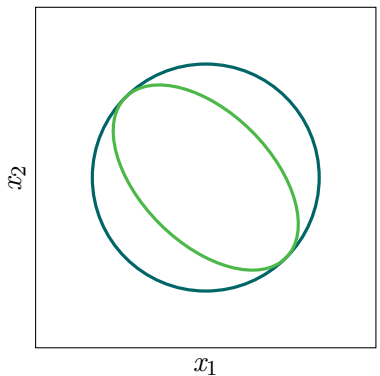


Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2 + x_3$

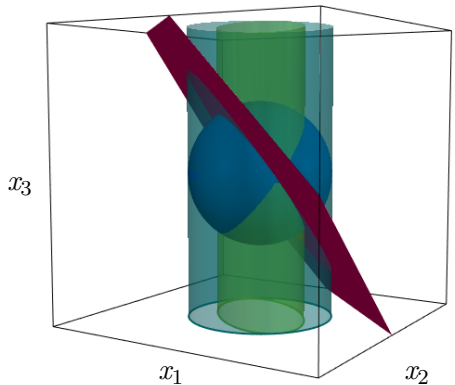


$x_1^2 + x_2^2 - 1,\ 2x_1^2 + 2x_1x_2 + 2x_2^2 - 1$

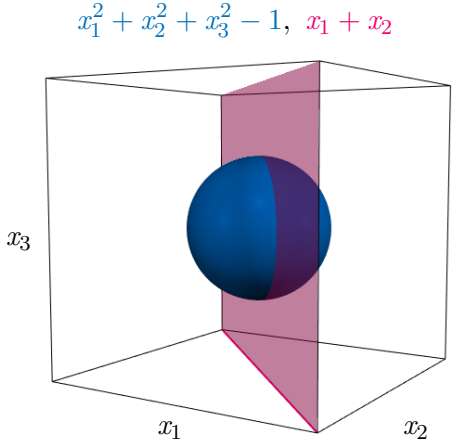


Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2 + x_3$ $\qquad$ $x_1^2 + x_2^2 - 1,\ 2x_1^2 + 2x_1x_2 + 2x_2^2 - 1$

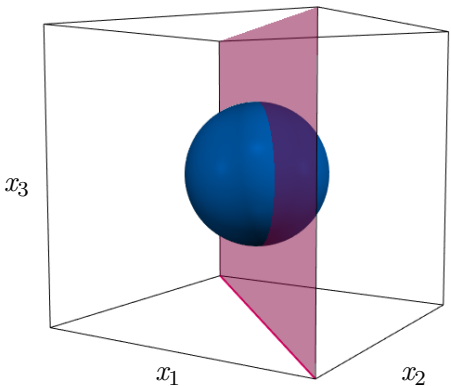


Cylindrical Algebraic Decomposition [Collins 1975]

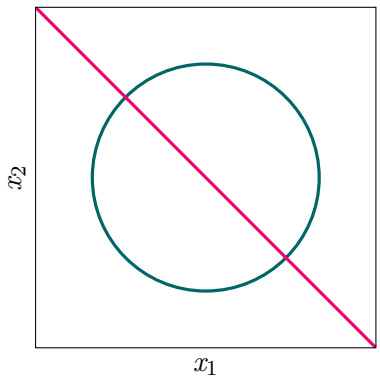


Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2$

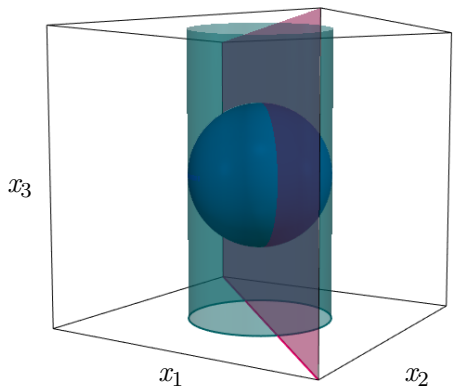


$x_1^2 + x_2^2 - 1,\ x_1 + x_2$

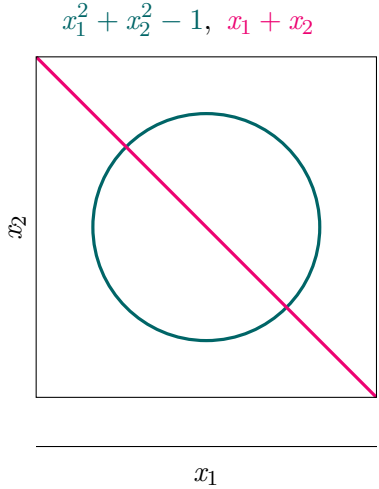


Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1 + x_2$ $\qquad$ $x_1^2 + x_2^2 - 1,\ x_1 + x_2$

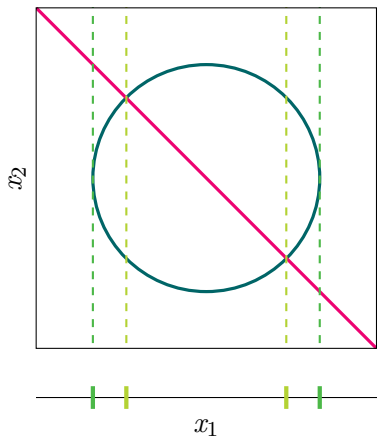


Cylindrical Algebraic Decomposition [Collins 1975]



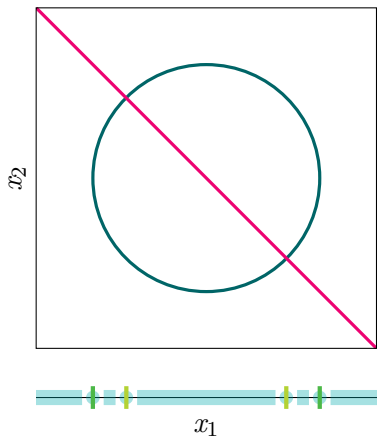
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



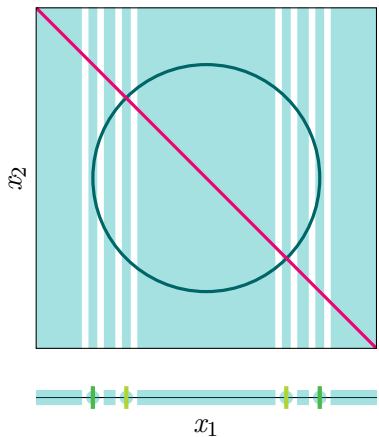
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



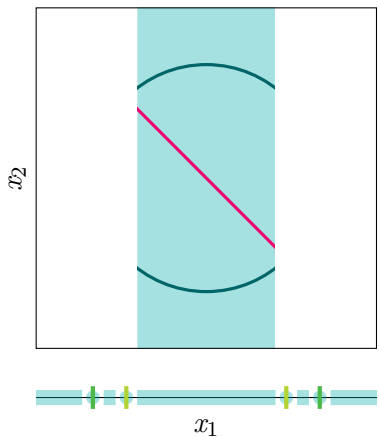
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



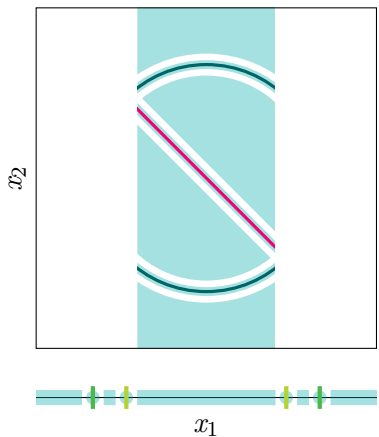
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



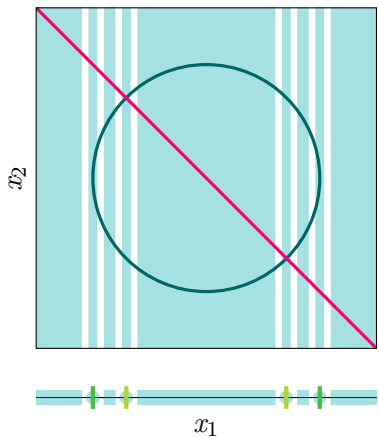
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



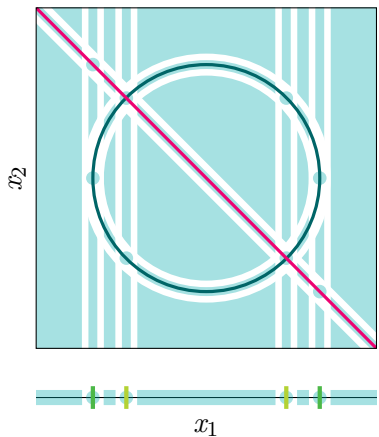
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



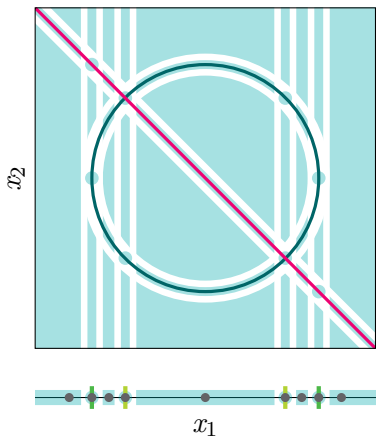
Cylindrical Algebraic Decomposition [Collins 1975]

$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$



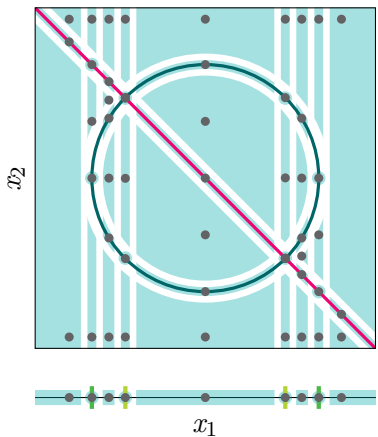
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



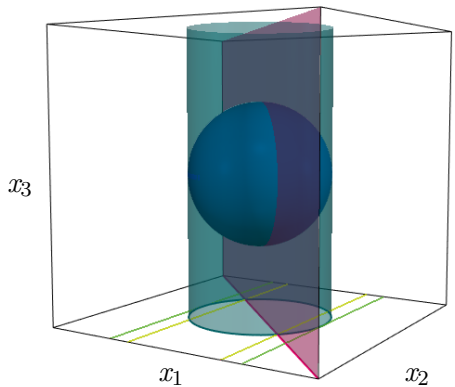
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



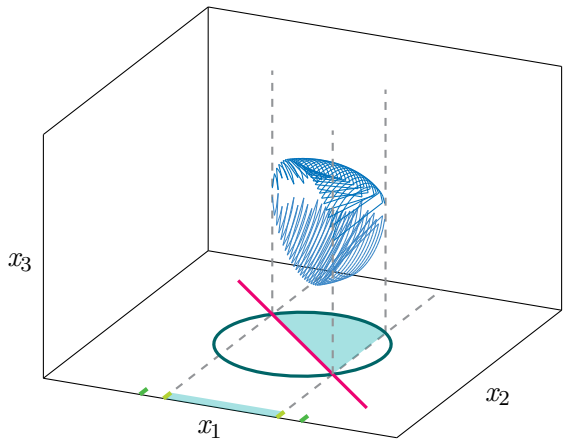
Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



Cylindrical Algebraic Decomposition [Collins 1975]

$$x_1^2 + x_2^2 + x_3^2 - 1,\ x_1^2 + x_2^2 - 1,\ x_1 + x_2,\ x_1^2 - 1,\ 2x_1^2 - 1$$



Limitations of CAD

Cylindrical Algebraic Decomposition (Collins 1975) First tractable approach. Doubly exponential in the number of variables.

Limitations of CAD

Cylindrical Algebraic Decomposition (Collins 1975) First tractable approach. Doubly exponential in the number of variables.

2^n

2^{2^n}

Image: Terezo del Río

Limitations of CAD

Cylindrical Algebraic Decomposition (Collins 1975) First tractable approach. Doubly exponential in the number of variables.

Davenport, Heintz 1988 *Real Quantifier Elimination is Doubly Exponential* in the number of quantifier alternations.

Limitations of CAD

Cylindrical Algebraic Decomposition (Collins 1975) First tractable approach. Doubly exponential in the number of variables.

Davenport, Heintz 1988 *Real Quantifier Elimination is Doubly Exponential* in the number of quantifier alternations.

Basu, Pollack, Roy 1996 Singly exponential in the number of variables. Doubly exponential in the number of quantifier alternations.

Why use CAD at all then?

Hong 1991 *Comparison of Several Decision Algorithms for the Existential Theory of the Reals.*

Algorithm	Theoretical	$n = m = d = L = 2$
Collins	$L^3(md)^{2^{O(n)}}$	$\ll 1$ second
Grigor′ev/Vorobjov	$L(md)^{n^2}$	$\gg 1$ million years
Renegar	$L(\log L)(\log\log L)(md)^{O(n)}$	$\gg 1$ million years

Why use CAD at all then?

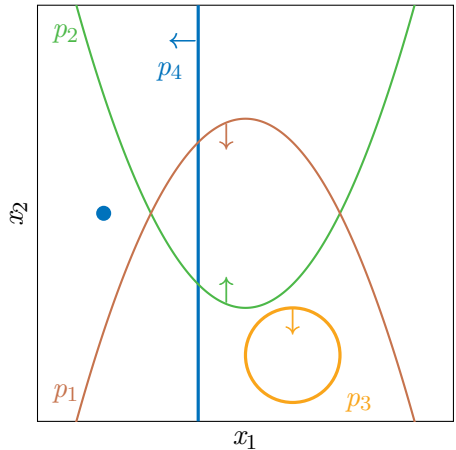
Hong 1991 *Comparison of Several Decision Algorithms for the Existential Theory of the Reals.*

Algorithm	Theoretical	$n = m = d = L = 2$
Collins	$L^3(md)^{2^{O(n)}}$	$\ll 1$ second
Grigor′ev/Vorobjov	$L(md)^{n^2}$	$\gg 1$ million years
Renegar	$L(\log L)(\log\log L)(md)^{O(n)}$	$\gg 1$ million years

CAD solves real-world problems!

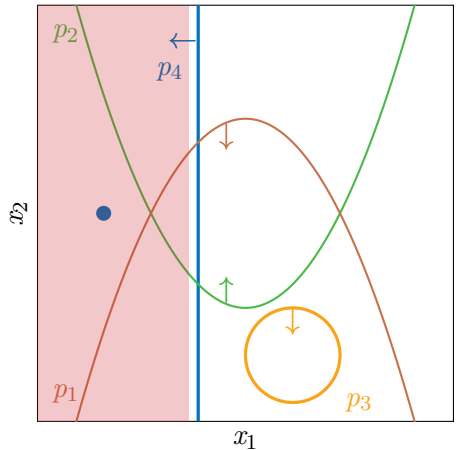
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\ \ p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$



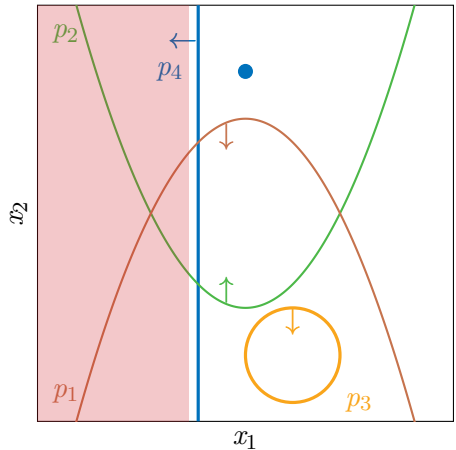
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\ \ p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$



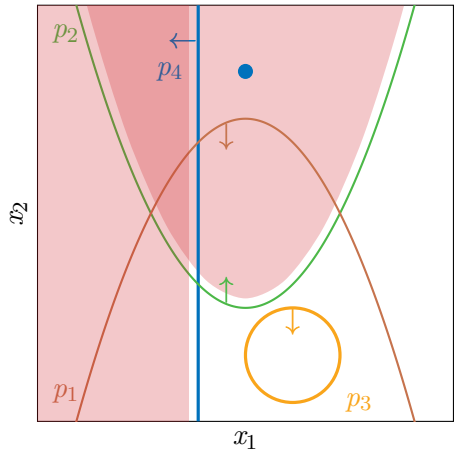
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\ \ p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$



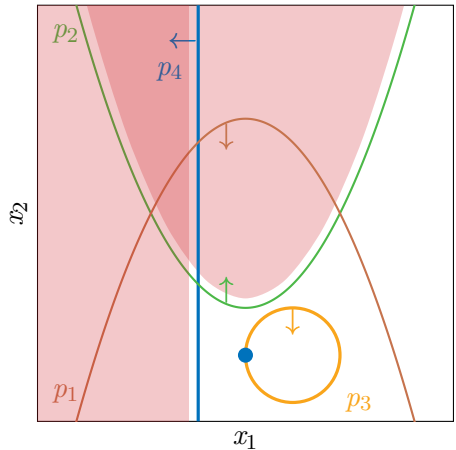
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\ \ p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$



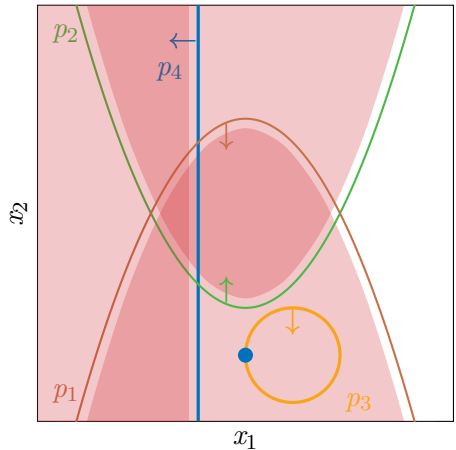
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\quad p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$



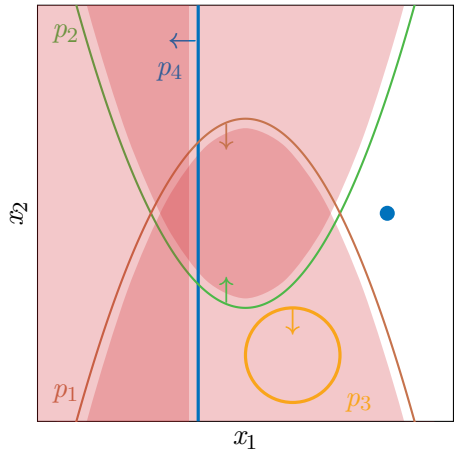
Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\quad p_1 < 0 \wedge p_2 > 0 \wedge p_3 \geq 0 \wedge p_4 \geq 0$$

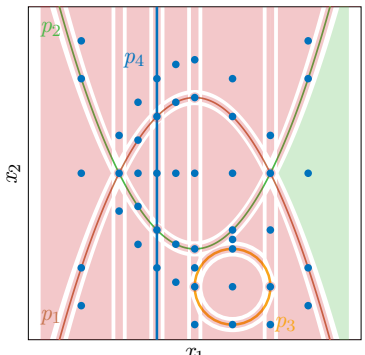


Exploration-guided Algorithms

$$\exists x_1.\exists x_2.\quad p_1 < 0 \;\wedge\; p_2 > 0 \;\wedge\; p_3 \geq 0 \;\wedge\; p_4 \geq 0$$

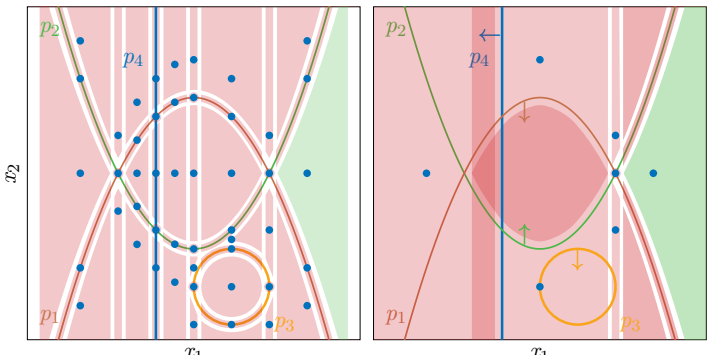


Exploration-guided Algorithms



Cylindrical Algebraic Decomposition (CAD) [Collins 1975]

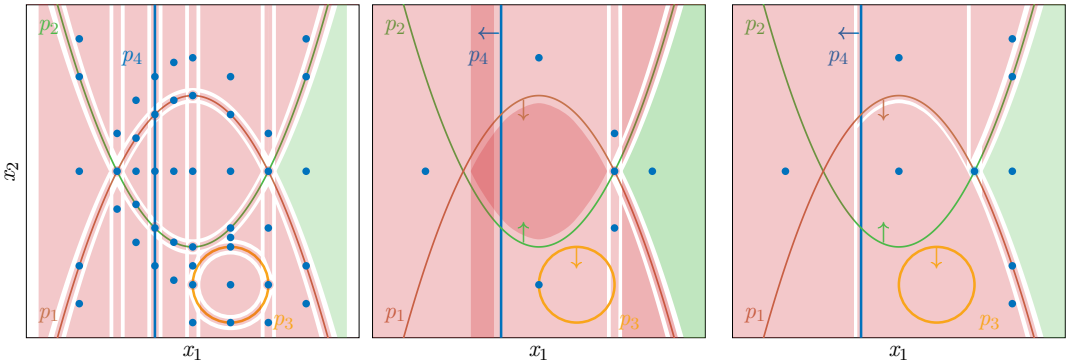
Exploration-guided Algorithms



Cylindrical Algebraic Decomposition (CAD) [Collins 1975]

NLSAT [Jovanović, de Moura 2012], Cylindrical Algebraic Covering (CAIC) [Ábrahám et al. 2021]

Exploration-guided Algorithms

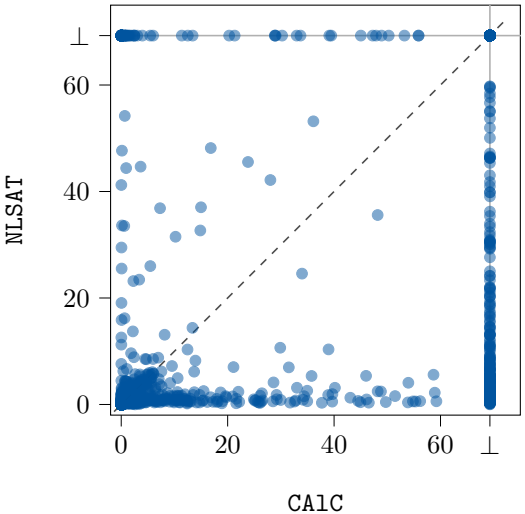


Cylindrical Algebraic Decomposition (CAD) [Collins 1975]

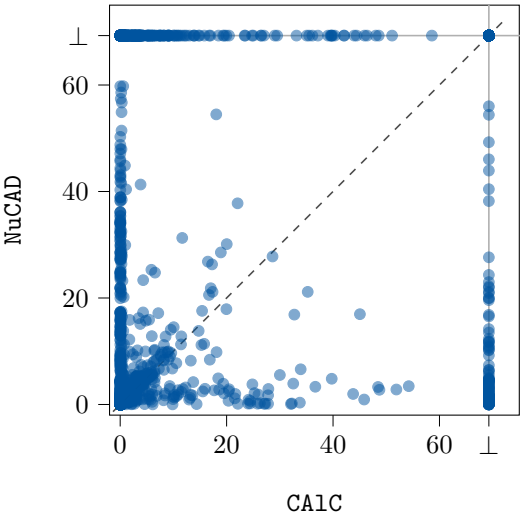
NLSAT [Jovanović, de Moura 2012], Cylindrical Algebraic Covering (CAIC) [Ábrahám et al. 2021]

Non-uniform CAD (NuCAD) [Brown 2015]

Comparison of Running Times

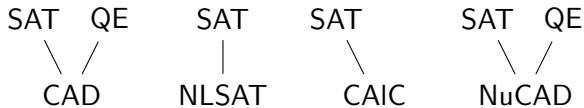


Satisfiability Checking



Quantifier Elimination

Contributions



Contributions

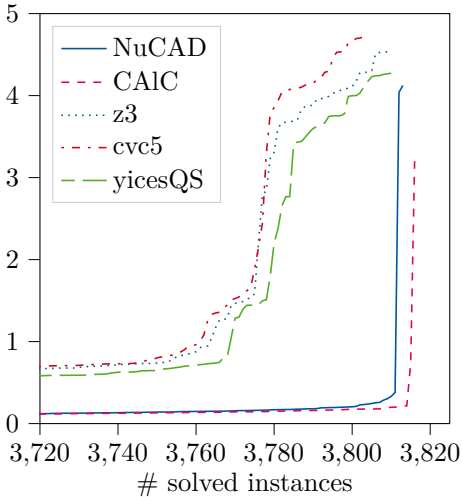
Quantifier Elimination

$$\exists x_1.\ \exists x_2.\ \exists y_1.\ \exists y_2.\ 1 \leq x_1, x_2, y_1, y_2 \leq z - 1 \wedge (x_1 - x_2)^2 + (y_1 - y_2)^2 \geq 4$$

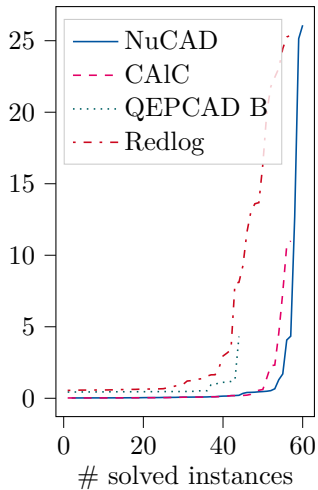
Quantifier Elimination

$$\exists x_1.\ \exists x_2.\ \exists y_1.\ \exists y_2.\ 1 \leq x_1, x_2, y_1, y_2 \leq z - 1 \wedge (x_1 - x_2)^2 + (y_1 - y_2)^2 \geq 4$$
$$\equiv z \geq 2 + \sqrt{2}$$

Quantifier Elimination [Nalbach, Kremer 2024; Nalbach, Ábrahám 2025]

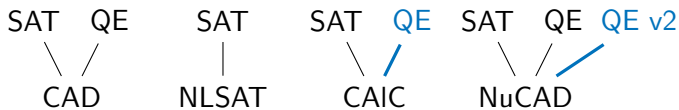


Satisfiability Checking with Quantifiers

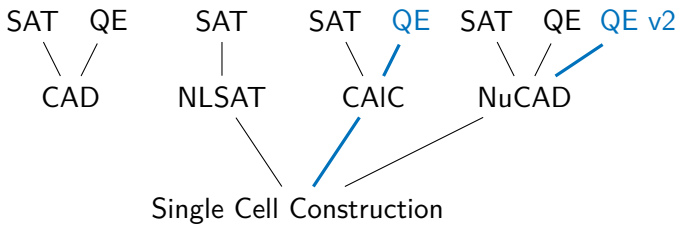


Quantifier Elimination

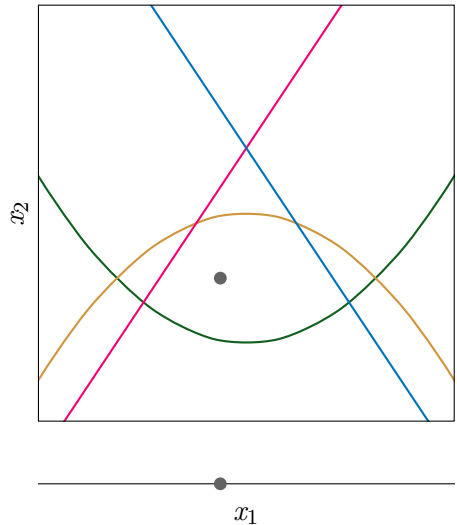
Contributions



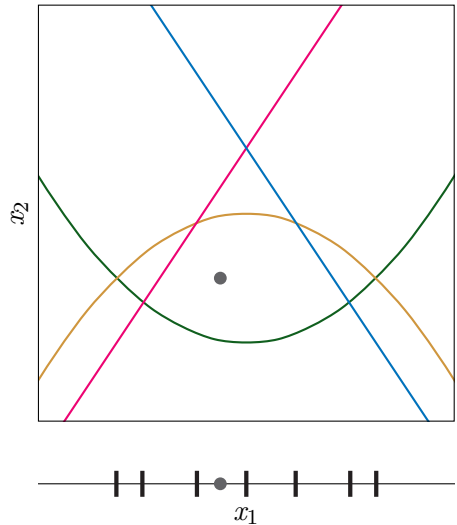
Contributions



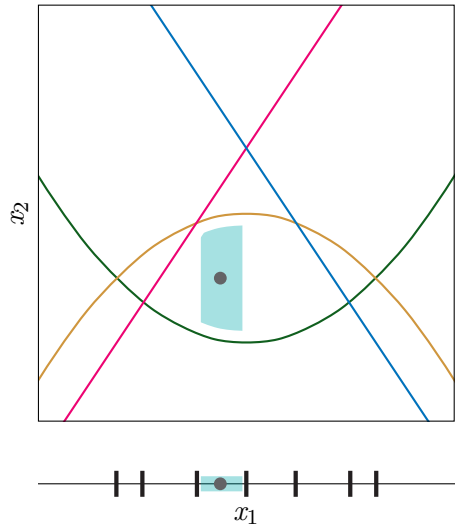
Single Cell Construction [Brown 2015]



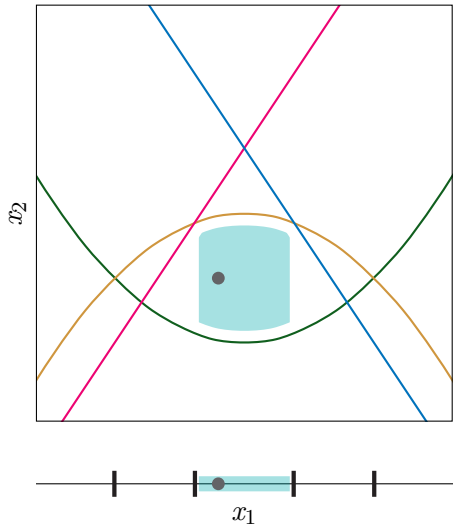
Single Cell Construction [Brown 2015]



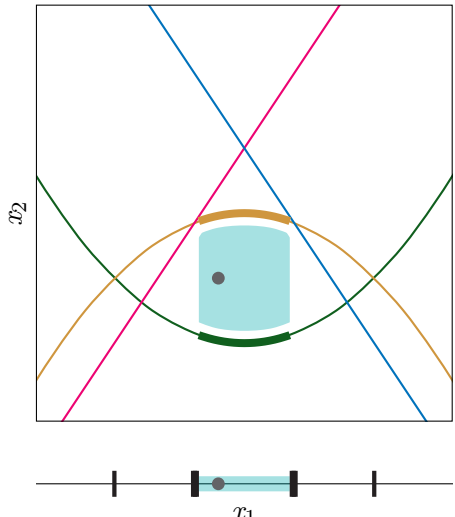
Single Cell Construction [Brown 2015]



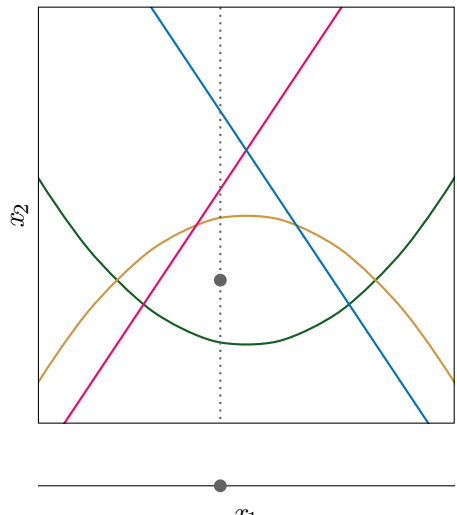
Single Cell Construction [Brown 2015]



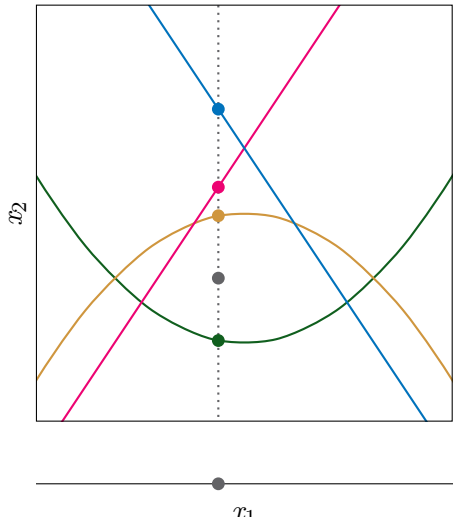
Single Cell Construction [Brown 2015]



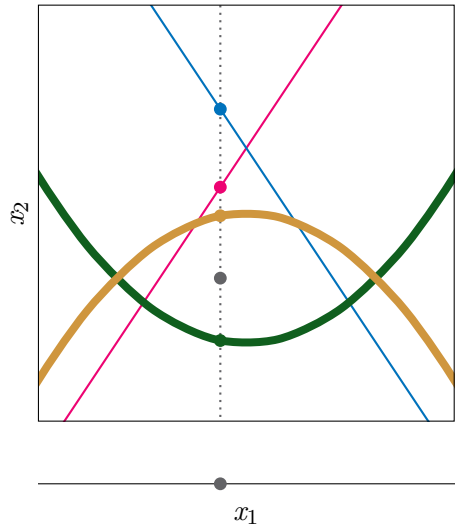
Single Cell Construction [Brown 2015, Nalbach et al. 2024]



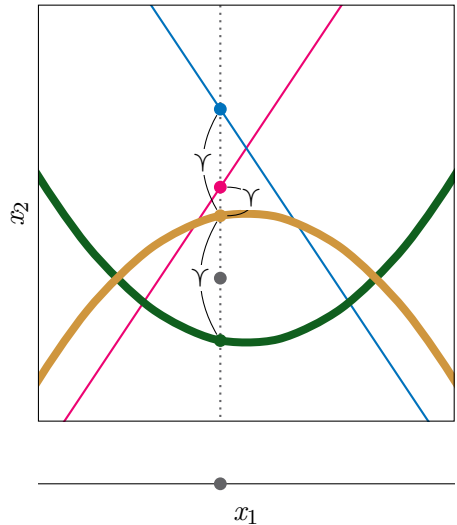
Single Cell Construction [Brown 2015, Nalbach et al. 2024]



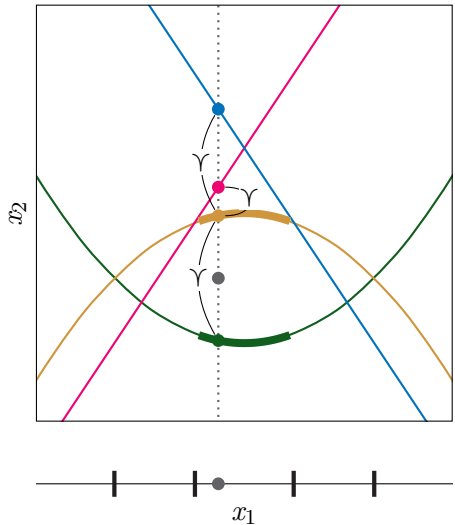
Single Cell Construction [Brown 2015, Nalbach et al. 2024]



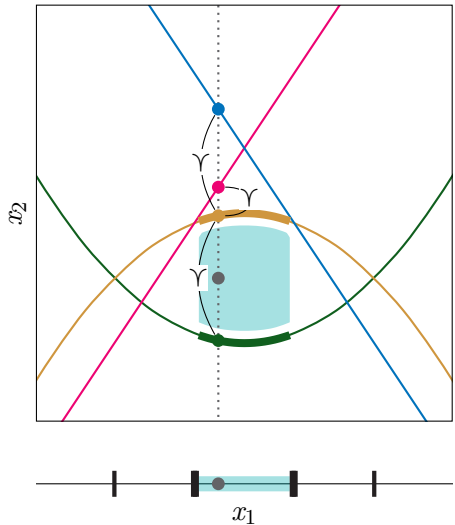
Single Cell Construction [Brown 2015, Nalbach et al. 2024]



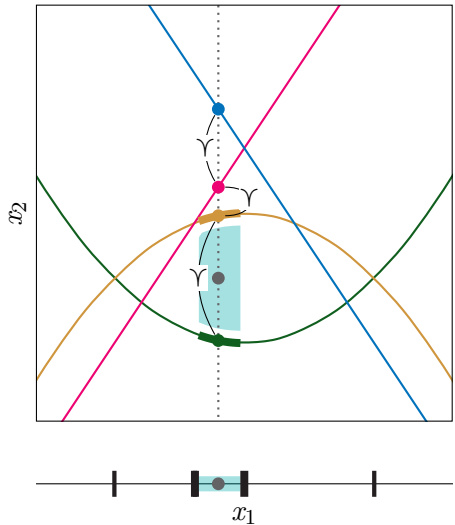
Single Cell Construction [Brown 2015, Nalbach et al. 2024]



Single Cell Construction [Brown 2015, Nalbach et al. 2024]



Single Cell Construction [Brown 2015, Nalbach et al. 2024]

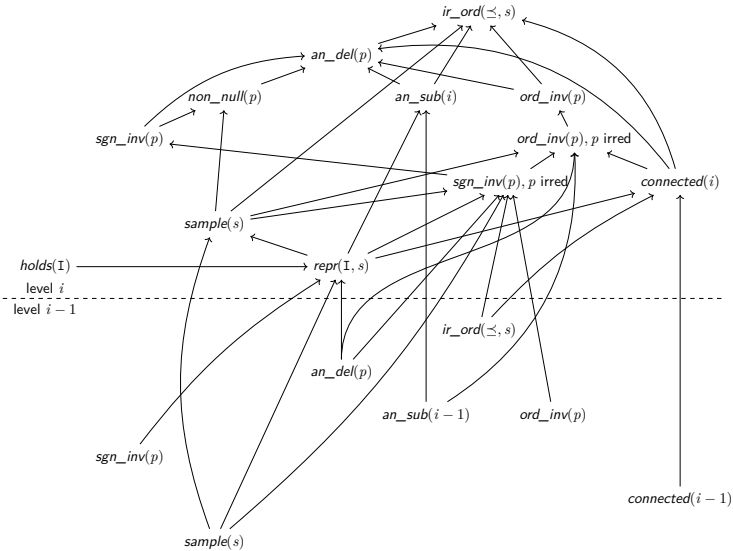


A Proof System for Exploration-Guided Algorithms

Rule. Let $i \in \mathbb{N}_{>0}$, $R \subseteq \mathbb{R}^i$, $p \in \mathbb{Q}[x_1, \ldots, x_i]$, $\mathsf{level}(p) = i$, p reducible, $\mathsf{factors}(p) = \{q_1, \ldots, q_k\}$.

$$\mathsf{sgn\_inv}(q_1)(R),\ \ldots,\ \mathsf{sgn\_inv}(q_k)(R) \qquad \vdash \mathsf{sgn\_inv}(p)(R)$$

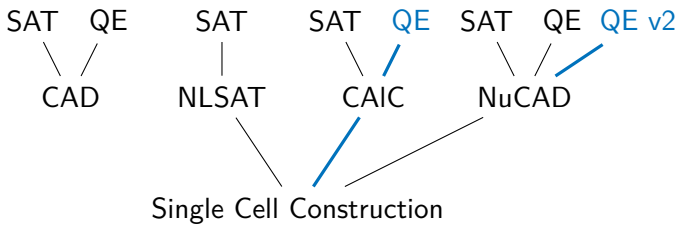
A Proof System for Exploration-Guided Algorithms



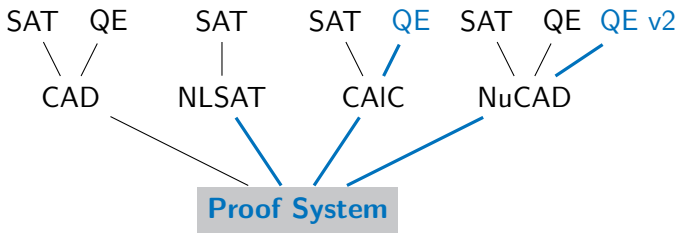
A Proof System for Exploration-Guided Algorithms

$$
\begin{aligned}
\boxed{\mathit{sgn\_inv}(p_1)} &\to \mathit{sample}(s), \mathit{repr}(\mathtt{I}_2, s_1), \mathit{ir\_ord}(\preceq, s_1), \mathit{an\_del}(p_1), \mathit{an\_sub}(1), \mathit{connected}(1)\\
\boxed{\mathit{sgn\_inv}(p_2)} &\to \mathit{sample}(s), \mathit{repr}(\mathtt{I}_2, s_1), \mathit{ir\_ord}(\preceq, s_1), \mathit{an\_del}(p_2), \mathit{an\_sub}(1), \mathit{connected}(1)\\
\boxed{\mathit{sgn\_inv}(p_3)} &\to \mathit{sample}(s), \mathit{repr}(\mathtt{I}_2, s_1), \mathit{ir\_ord}(\preceq, s_1), \mathit{an\_del}(p_3), \mathit{an\_sub}(1), \mathit{connected}(1)\\
\mathit{sample}(s) &\to \mathit{repr}(\mathtt{I}_2, s_1), \mathit{sample}(s_1)\\
\mathit{repr}(\mathtt{I}_2, s_1) &\to \boxed{R = R{\downarrow_{[1]}} \times \mathtt{I}_2}, \mathit{an\_del}(p_2), \mathit{an\_del}(p_3), \mathit{sample}(s_1)\\
\mathit{ir\_ord}(\preceq, s_1) &\to \mathit{an\_del}(p_1), \mathit{an\_del}(p_2), \mathit{an\_del}(p_3), \mathit{ord\_inv}(\mathrm{res}_{x_2}(p_3, p_1)), \mathit{ord\_inv}(\mathrm{res}_{x_2}(p_3, p_2)),\\
&\qquad \mathit{an\_sub}(1), \mathit{connected}(1), \mathit{sample}(s_1)\\
\mathit{an\_del}(p_1) &\to \mathit{non\_null}(p_1), \mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_1)), \mathit{an\_sub}(1), \mathit{connected}(1), \mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_1))\\
\mathit{an\_del}(p_2) &\to \mathit{non\_null}(p_2), \mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_2)), \mathit{an\_sub}(1), \mathit{connected}(1), \mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_2))\\
\mathit{an\_del}(p_3) &\to \mathit{non\_null}(p_3), \mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_3)), \mathit{an\_sub}(1), \mathit{connected}(1), \mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_3))\\
\mathit{non\_null}(p_1) &\to \mathit{trivial}\\
\mathit{non\_null}(p_2) &\to \mathit{trivial}\\
\mathit{non\_null}(p_3) &\to \mathit{trivial}\\
\mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_1)) &\to \mathit{trivial}\\
\mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_2)) &\to \mathit{sgn\_inv}(p_4), \mathit{sample}(s_1)\\
\mathit{ord\_inv}(\mathrm{disc}_{x_2}(p_3)) &\to \mathit{trivial}\\
\mathit{sgn\_inv}(p_4) &\to \mathit{repr}(\mathtt{I}_1)\\
\mathit{ord\_inv}(\mathrm{res}_{x_2}(p_3, p_1)) &\to \mathit{trivial}\\
\mathit{ord\_inv}(\mathrm{res}_{x_2}(p_3, p_2)) &\to \mathit{sgn\_inv}(p_5), \mathit{sample}(s_1)
\end{aligned}
\qquad
\begin{aligned}
\mathit{sgn\_inv}(p_5) &\to \mathit{repr}(\mathtt{I}_1)\\
\mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_1)) &\to \mathit{trivial}\\
\mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_2)) &\to \mathit{trivial}\\
\mathit{sgn\_inv}(\mathrm{ldcf}_{x_2}(p_3)) &\to \mathit{trivial}\\
\mathit{an\_sub}(1) &\to \mathit{repr}(\mathtt{I}_1)\\
\mathit{connected}(1) &\to \mathit{trivial}\\
\mathit{sample}(s_1) &\to \mathit{repr}(\mathtt{I}_1)\\
\mathit{repr}(\mathtt{I}_1) &\to \boxed{R{\downarrow_{[1]}} = \mathtt{I}_1}
\end{aligned}
$$

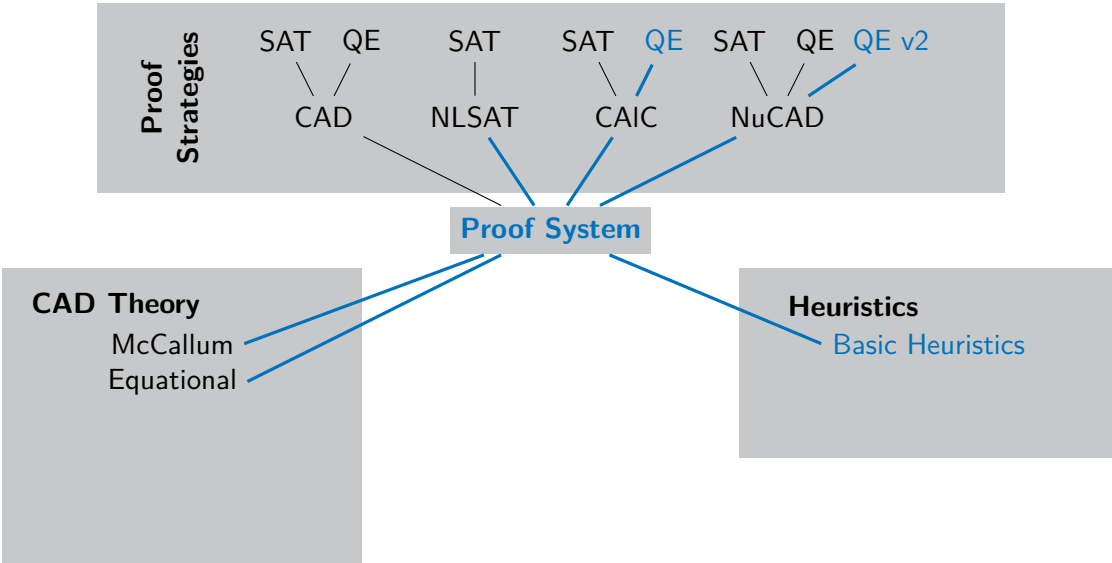
Contributions



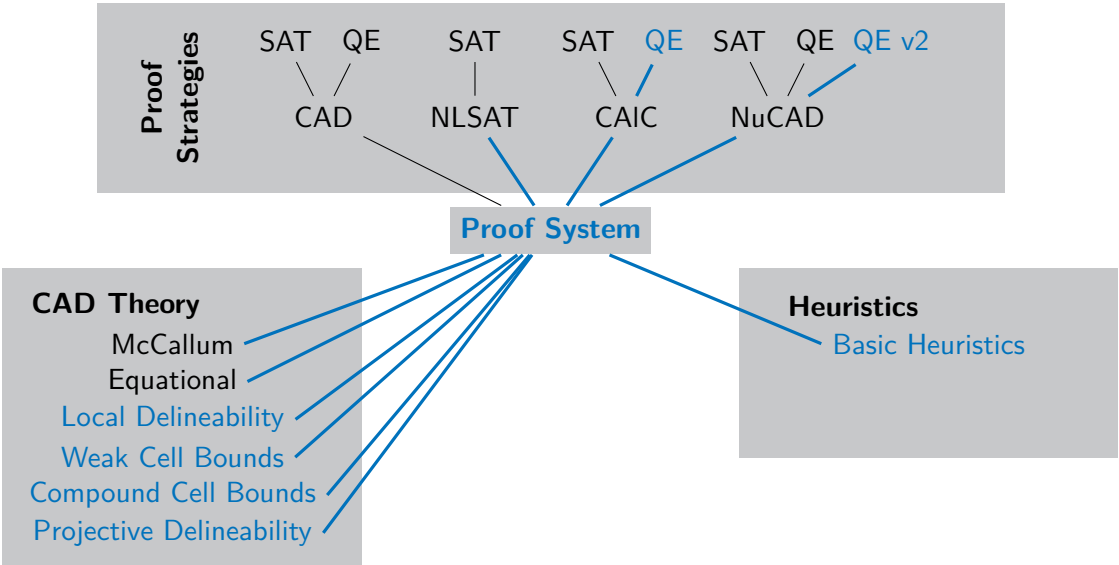
Contributions



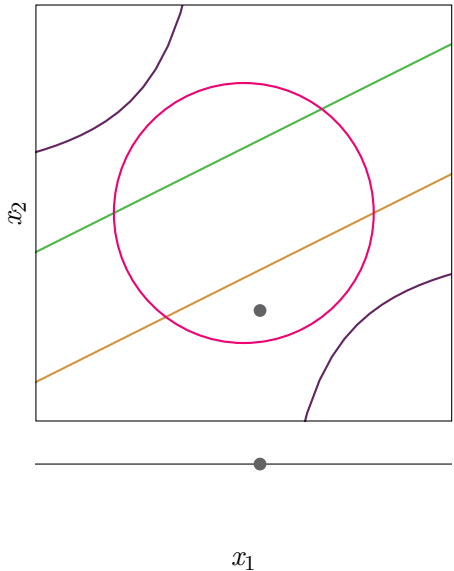
Contributions



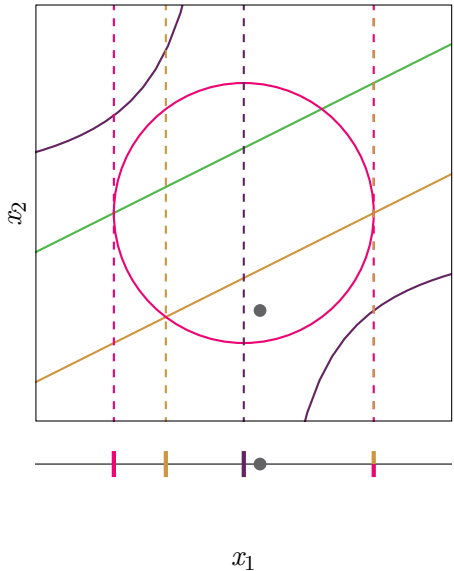
Contributions



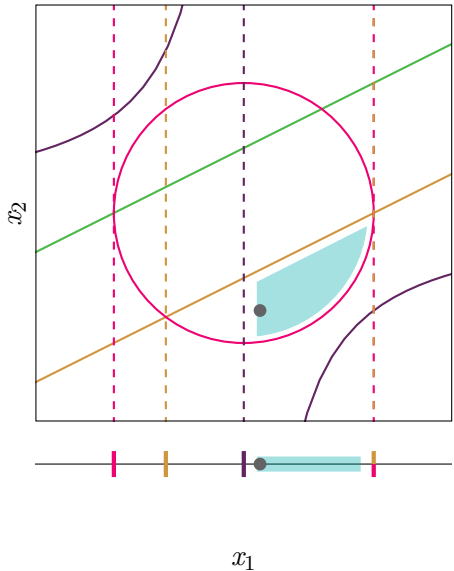
Projective Delineability [Michel et al. 2024, Nalbach et al. 2025]



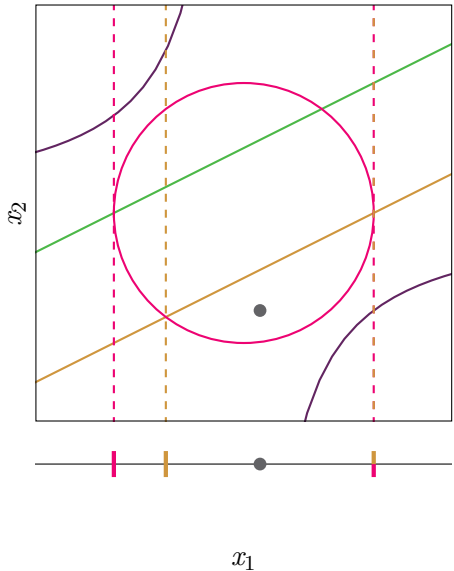
Projective Delineability [Michel et al. 2024, Nalbach et al. 2025]

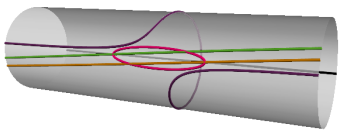


Projective Delineability [Michel et al. 2024, Nalbach et al. 2025]

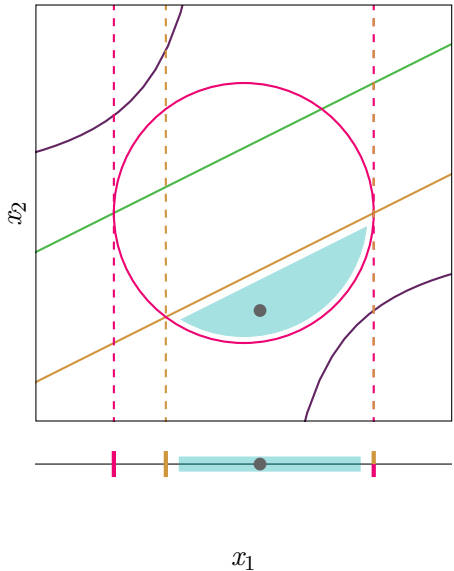


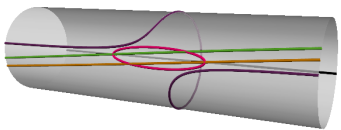
Projective Delineability [Michel et al. 2024, Nalbach et al. 2025]



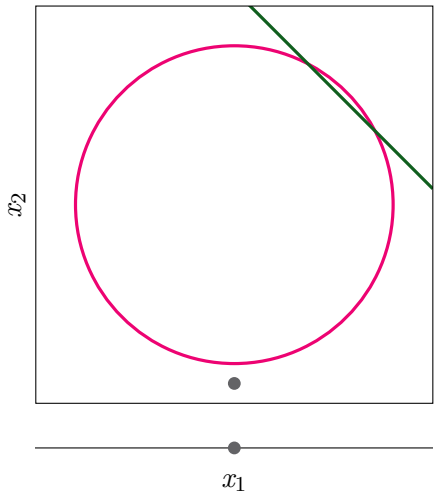


Projective Delineability [Michel et al. 2024, Nalbach et al. 2025]

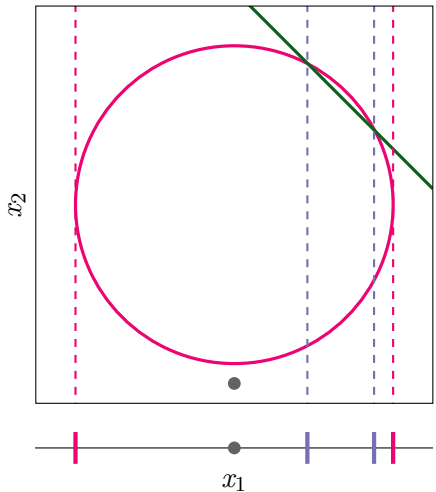




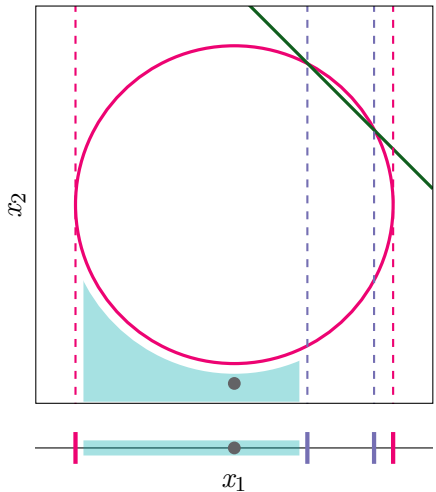
Irrelevant Intersections [Nalbach, Ábrahám 2024]



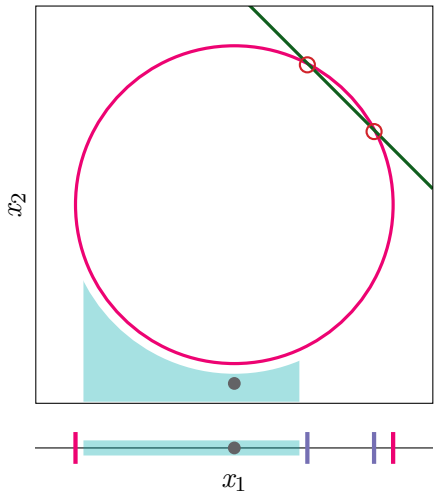
Irrelevant Intersections [Nalbach, Ábrahám 2024]



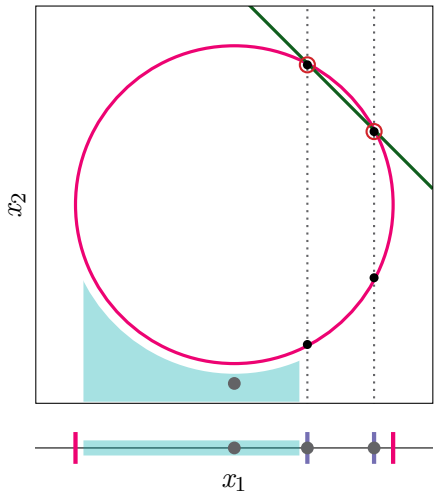
Irrelevant Intersections [Nalbach, Ábrahám 2024]



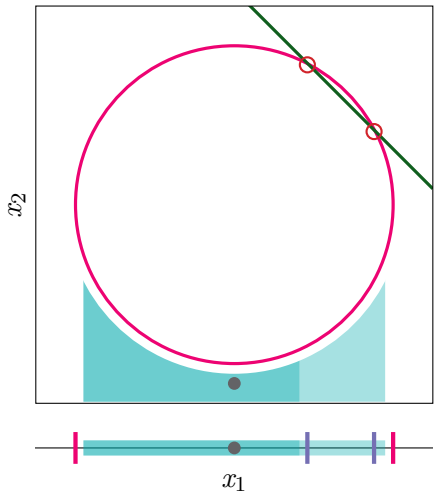
Irrelevant Intersections [Nalbach, Ábrahám 2024]



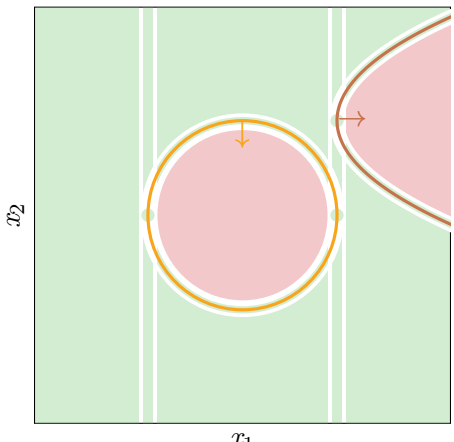
Irrelevant Intersections [Nalbach, Ábrahám 2024]



Irrelevant Intersections [Nalbach, Ábrahám 2024]

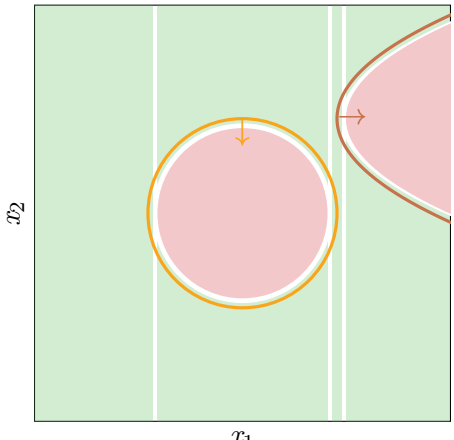


Weak Cell Bounds [Nalbach, Ábrahám 2024; Nalbach, Ábrahám 2025]



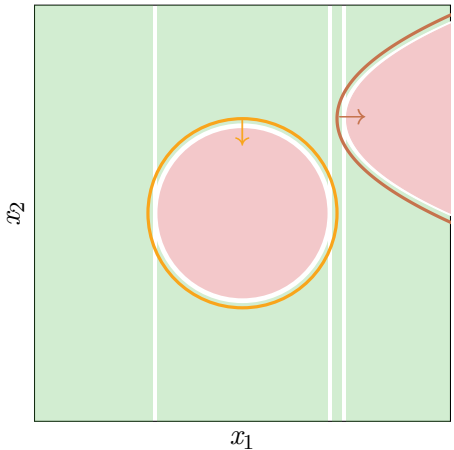
NuCAD Example

Weak Cell Bounds [Nalbach, Ábrahám 2024; Nalbach, Ábrahám 2025]

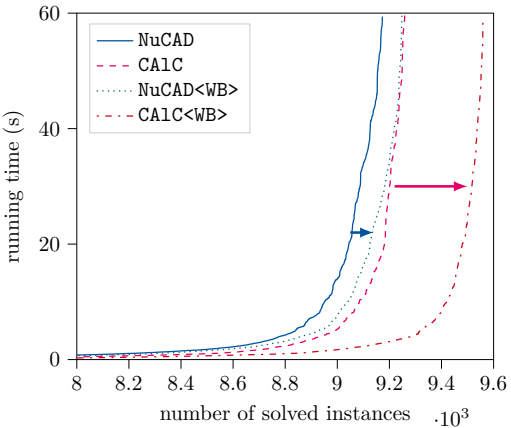


NuCAD Example
from 19 to 8 cells

Weak Cell Bounds [Nalbach, Ábrahám 2024; Nalbach, Ábrahám 2025]

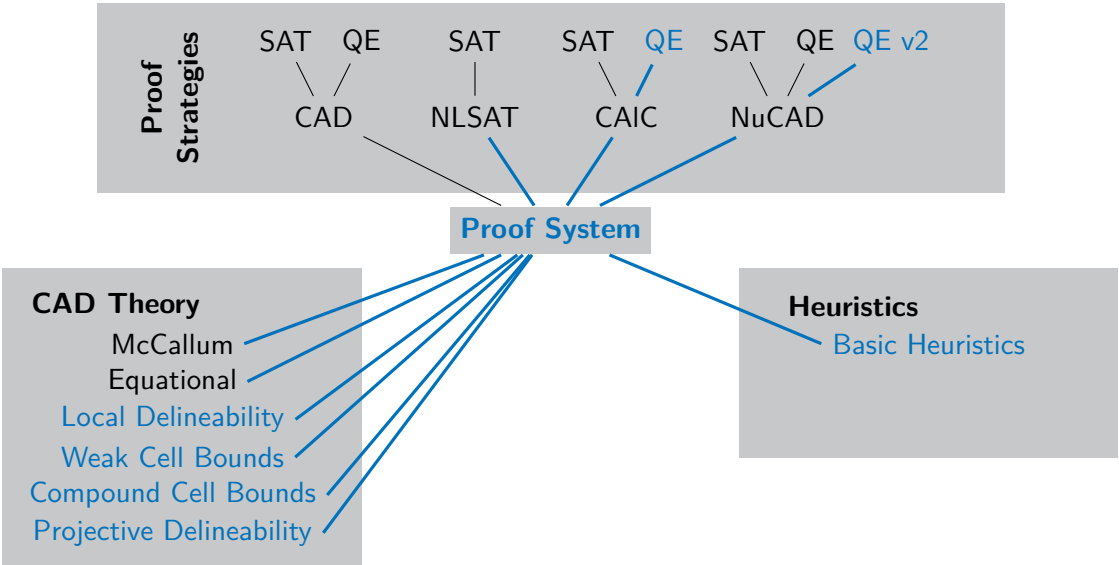


NuCAD Example
from 19 to 8 cells

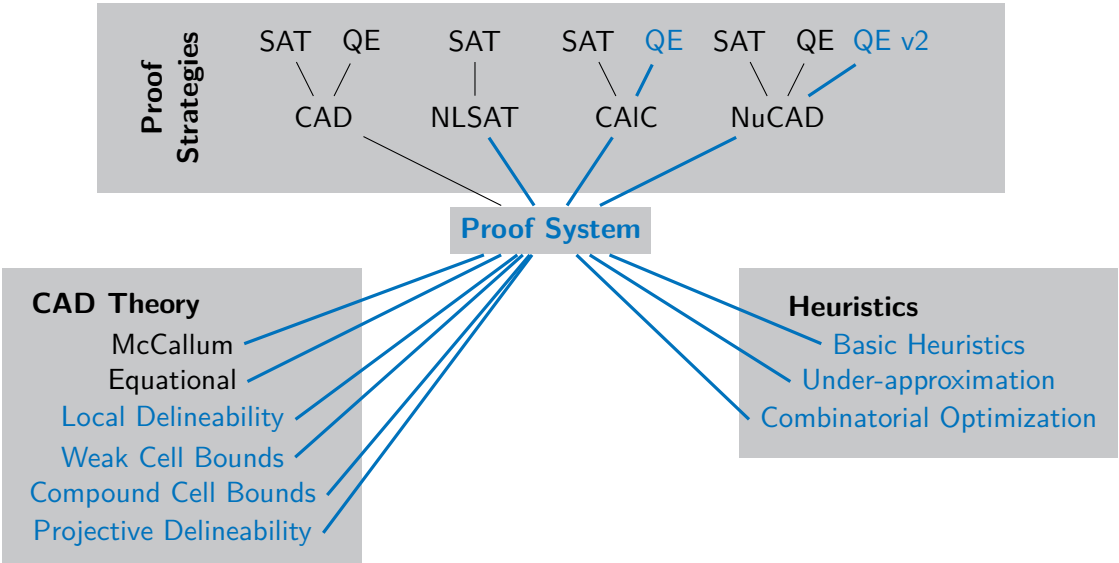


Quantifier Elimination

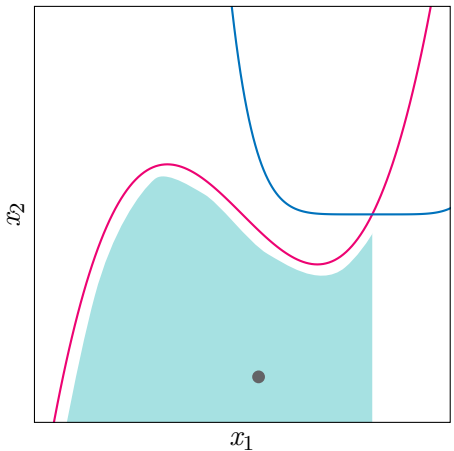
Contributions



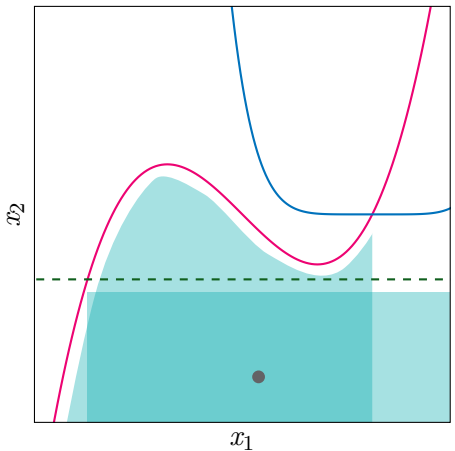
Contributions



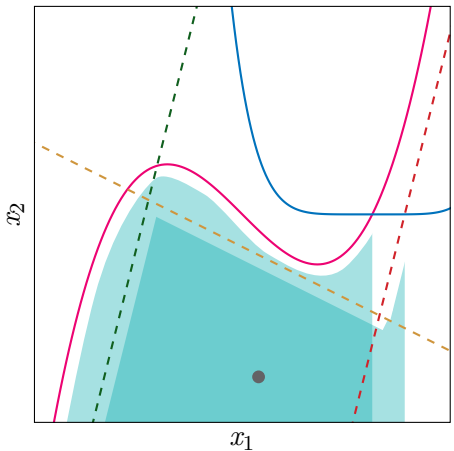
Under-approximation of Cell Bounds [Promies et al. 2025]



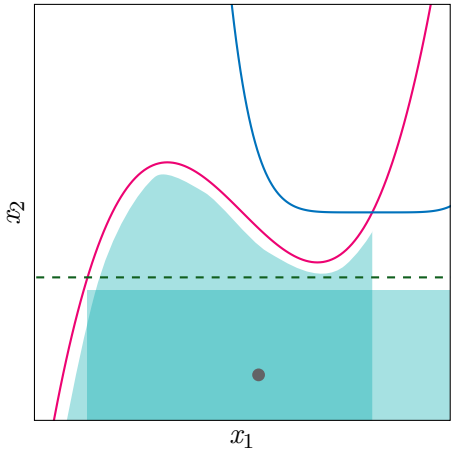
Under-approximation of Cell Bounds [Promies et al. 2025]

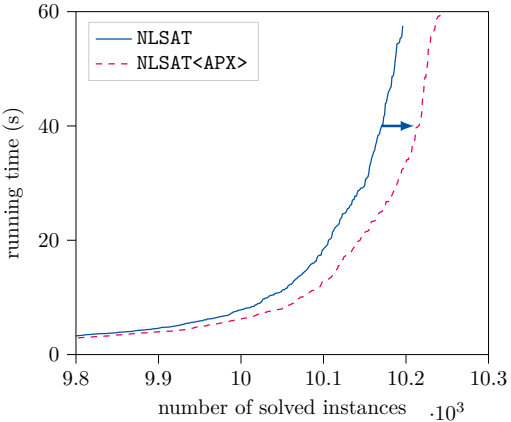


Under-approximation of Cell Bounds [Promies et al. 2025]

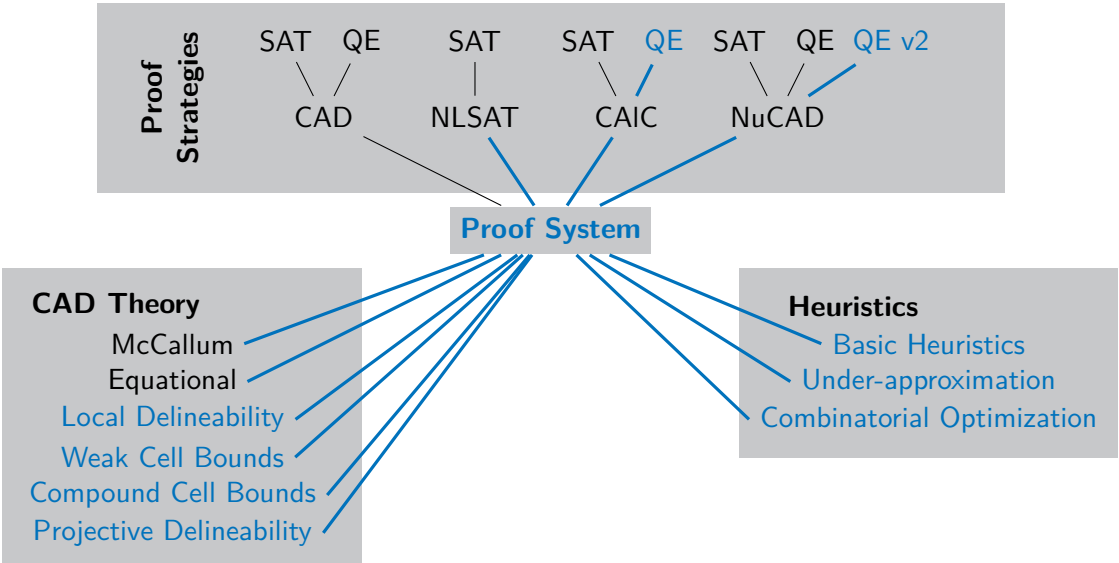


Under-approximation of Cell Bounds [Promies et al. 2025]

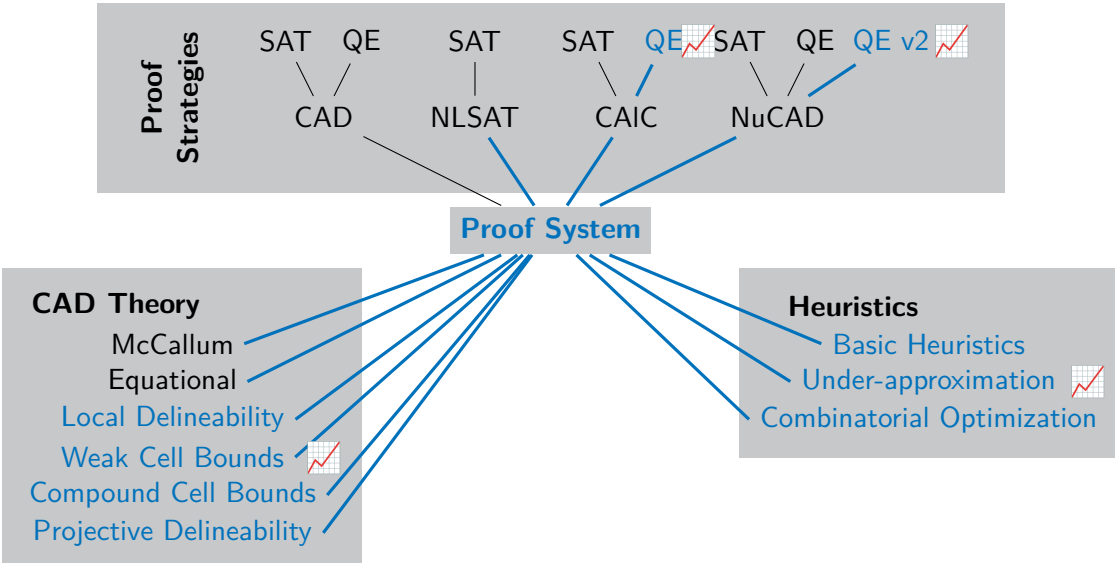




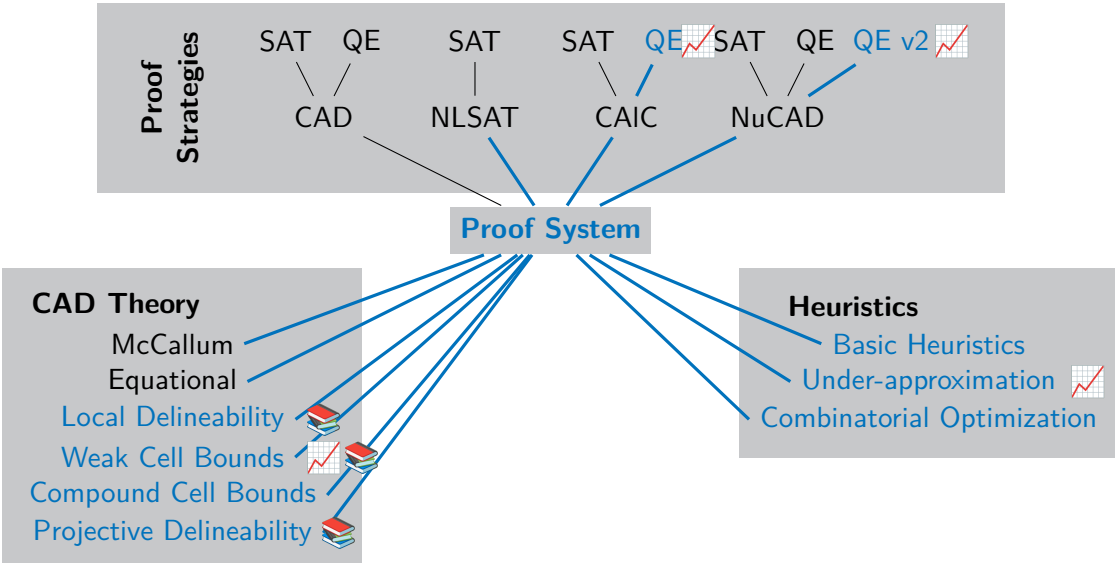
Contributions



Contributions



Contributions



Contributions