The Existential Theory of the Reals

Arnaud de Mesmay (CNRS, LIGM, Université Gustave Eiffel, Paris)

Graphs and complexity day, ENS Lyon, April 7, 2025

Why should I care?

The *Existential Theory of the Reals* is

1. The problem of finding whether a set of polynomial (in)equations has a solution over the reals.
2. The complexity of deciding whether a pseudo-line arrangement can be stretched.
3. The computational counterpart of the Mnëv universality theorem.

Why should I care?

The *Existential Theory of the Reals* is

1. ~~The problem of finding whether a set of polynomial (in)equations has a solution over the reals.~~
2. ~~The complexity of deciding whether a pseudo-line arrangement can be stretched.~~
3. ~~The computational counterpart of the Mnëv universality theorem.~~

This is all true but this is not the good way to start.

Why should I care?

The *Existential Theory of the Reals* is

1. ~~The problem of finding whether a set of polynomial (in)equations has a solution over the reals.~~
2. ~~The complexity of deciding whether a pseudo-line arrangement can be stretched.~~
3. ~~The computational counterpart of the Mnëv universality theorem.~~

This is all true but this is not the good way to start.

The actual “definition”

The Existential Theory of the Reals ($\exists\mathbb{R}$) is the complexity class that appears naturally for nice discrete problems that

- look like they should be in **NP**
- but there are annoying precision or algebraic issues to bound the size of the certificate.

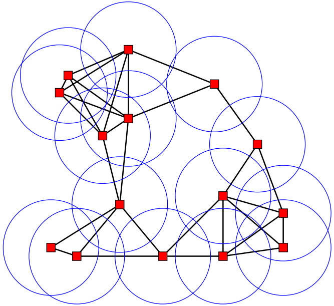
Example 1: Unit disk graphs

Unit Disk Graph Recognition

Input: A graph G.

Output: Is G the intersection graph of unit disks in the plane?

How can you certify that a graph is a unit disk graph?



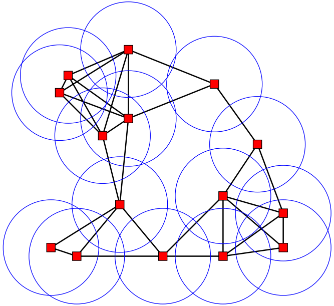
Example 1: Unit disk graphs

Unit Disk Graph Recognition

Input: A graph G.

Output: Is G the intersection graph of unit disks in the plane?

How can you certify that a graph is a unit disk graph?

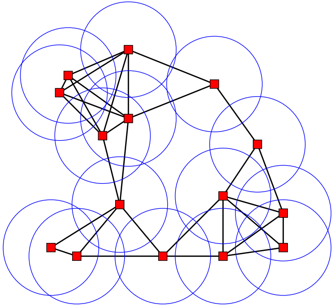


- Easy! You can "just" give the coordinates of the centers of the disks.

Example 1: Unit disk graphs

UNIT DISK GRAPH RECOGNITION

Input: A graph G.
Output: Is G the intersection graph of unit disks in the plane?



How can you certify that a graph is a unit disk graph?

- Easy! You can "just" give the coordinates of the centers of the disks.

Theorem (Kang-Muller '11)

UNIT DISK GRAPH RECOGNITION *is* $\exists\mathbb{R}$*-complete.*

Example 2: Matrix Rank problems

MINIMUM MATRIX RANK

Input: A matrix with $0, 1$ entries and some unknowns $(x_1, \ldots, x_n)$ and an integer k.

Output: Can one find real values for $(x_1, \ldots, x_n)$ so that the matrix has rank at most k?

How to certify low-rank completion of matrices?

1	0	x_1
x_3	x_2	x_2
0	1	1

Example 2: Matrix Rank problems

MINIMUM MATRIX RANK

Input: A matrix with $0, 1$ entries and some unknowns $(x_1, \dots, x_n)$ and an integer k.
Output: Can one find real values for $(x_1, \dots, x_n)$ so that the matrix has rank at most k?

1	0	x_1
x_3	x_2	x_2
0	1	1

How to certify low-rank completion of matrices?

- Easy! You can "just" give the values of the missing entries.

Theorem (Buss-Frandsen-Shallit '99)

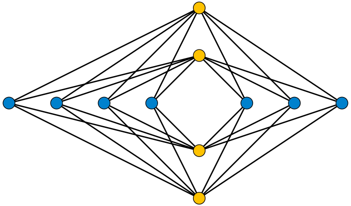
MINIMUM MATRIX RANK *is* $\exists\mathbb{R}$*-complete.*

Example 3: Crossing Numbers

Rectilinear Crossing Number

Input: A graph G and an integer k.

Output: Is there a straight-line drawing of G with at most k crossings?



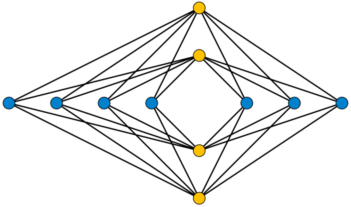
How can you certify that there is a drawing with few crossings?

Example 3: Crossing Numbers

RECTILINEAR CROSSING NUMBER

Input: A graph G and an integer k.

Output: Is there a straight-line drawing of G with at most k crossings?



How can you certify that there is a drawing with few crossings?

- Easy! You can "just" give the vertex coordinates.

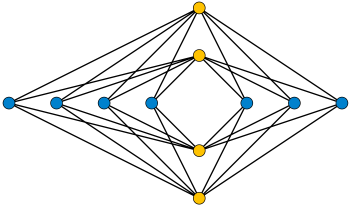
Theorem (Bienstock '91)

RECTILINEAR CROSSING NUMBER *is* $\exists\mathbb{R}$*-complete.*

Example 3: Crossing Numbers

RECTILINEAR CROSSING NUMBER

Input: A graph G and an integer k.
Output: Is there a straight-line drawing of G with at most k crossings?



How can you certify that there is a drawing with few crossings?

- Easy! You can "just" give the vertex coordinates.

Theorem (Bienstock '91)

RECTILINEAR CROSSING NUMBER *is* $\exists\mathbb{R}$*-complete.*

Corollary

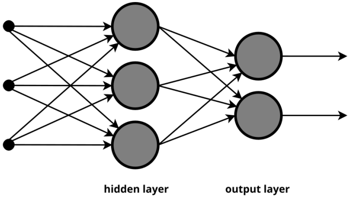
The crossing number and the rectilinear crossing number of a graph can be different *(if $\exists\mathbb{R} \neq$ **NP**).*

Example 4: The AI slide

Training Neural Networks

Input: A set of data points, a neural network architecture, a cost function, a threshold.

Output: Are there biases and weights such that the total error is below the threshold?

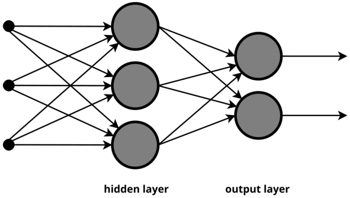


How can you certify that there is a good choice of weights and biases?

Example 4: The AI slide

Training Neural Networks

Input: A set of data points, a neural network architecture, a cost function, a threshold.
Output: Are there biases and weights such that the total error is below the threshold?



How can you certify that there is a good choice of weights and biases?

- Easy! You can "just" give them.

Theorem (Abrahamsen-Kleist-Miltzow '21, BHJMW '22)

Training Neural Networks *is* $\exists\mathbb{R}$*-complete.*

Back to the first slide

The *Existential Theory of the Reals* is

1. The problem of finding whether a set of polynomial (in)equations has a solution over the reals.
2. The complexity of deciding whether a pseudo-line arrangement can be stretched.
3. The computational counterpart of the Mnëv universality theorem.

Plan of the talk

The *plan of the talk* is

1. Algebraic aspects (a.k.a. how to prove $\exists\mathbb{R}$-membership).
2. Stretchability (a.k.a. how to prove $\exists\mathbb{R}$-hardness).
3. Some more things to know about $\exists\mathbb{R}$.

1. Algebraic aspects

Existential Theory of the Reals (ETR)

Input: A system of polynomial (in)equations.
Output: Is there a solution over the reals?

The complexity of the equations (degree, size of the coefficients, number of summands) is counted in the input.

$$\begin{aligned} x^4 + y^2 + 24 \geq &\quad 0 \\ x^3 + z = &\quad 22 \\ x^4 + x^7 + x^5 = &\quad 5 \end{aligned}$$

1. Algebraic aspects

Existential Theory of the Reals (ETR)

Input: A system of polynomial (in)equations.
Output: Is there a solution over the reals?

The complexity of the equations (degree, size of the coefficients, number of summands) is counted in the input.

$$\begin{aligned} x^4 + y^2 + 24 \geq {} & 0 \\ x^3 + z = {} & 22 \\ x^4 + x^7 + x^5 = {} & 5 \end{aligned}$$

The Existential Theory of the Reals as a complexity class

The Existential Theory of the Reals ($\exists\mathbb{R}$) is the complexity class made of all problems that can be (many-to-one) reduced to the Existential Theory of the Reals (ETR).

Intuitively, $\exists\mathbb{R}$ is the set of problems that can be encoded as the real solutions of polynomial inequations.

1. Algebraic aspects

EXISTENTIAL THEORY OF THE REALS (ETR)

Input: A system of polynomial (in)equations.
Output: Is there a solution over the reals?

The complexity of the equations (degree, size of the coefficients, number of summands) is counted in the input.

$$
\begin{aligned}
x^4 + y^2 + 24 &\geq 0 \\
x^3 + z &= 22 \\
x^4 + x^7 + x^5 &= 5
\end{aligned}
$$

The Existential Theory of the Reals as a complexity class

The Existential Theory of the Reals ($\exists\mathbb{R}$) is the complexity class made of all problems that can be (many-to-one) reduced to the EXISTENTIAL THEORY OF THE REALS (ETR).

Intuitively, $\exists\mathbb{R}$ is the set of problems that can be encoded as the real solutions of polynomial inequations.

Corollary

The Existential Theory of the Reals is complete for the Existential Theory of the Reals.

1. Algebraic aspects

Existential Theory of the Reals (ETR)

Input: A system of polynomial (in)equations.
Output: Is there a solution over the reals?

The complexity of the equations (degree, size of the coefficients, number of summands) is counted in the input.

$$\begin{aligned} x^4 + y^2 + 24 \geq & \quad 0 \\ x^3 + z = & \quad 22 \\ x^4 + x^7 + x^5 = & \quad 5 \end{aligned}$$

The Existential Theory of the Reals as a complexity class

The Existential Theory of the Reals ($\exists\mathbb{R}$) is the complexity class made of all problems that can be (many-to-one) reduced to the Existential Theory of the Reals (ETR).

Intuitively, $\exists\mathbb{R}$ is the set of problems that can be encoded as the real solutions of polynomial inequations.

Corollary

ETR *is* $\exists\mathbb{R}$*-complete.*

Where is $\exists\mathbb{R}$? (1)

Theorem

$$\mathbf{NP} \subseteq \exists\mathbb{R}.$$

Where is $\exists\mathbb{R}$? (1)

Theorem

$$\mathbf{NP} \subseteq \exists\mathbb{R}.$$

Proof:

- We encode 3-SAT variables as 0 or 1.
- We enforce these values with equations $x(x-1)=0$.
- We encode variable negation with $y = 1 - x$.
- We encode 3-SAT clauses $x \vee y \vee z$ as $x + y + z \geq 1$

That's it.

Where is $\exists\mathbb{R}$? (2)

Theorem

$$\exists\mathbb{R} \subseteq \textbf{PSPACE}.$$

Where is $\exists\mathbb{R}$? (2)

Theorem

$$\exists\mathbb{R} \subseteq \textbf{PSPACE}.$$

Wait, what? I was told in high school that we cannot solve equations like $x^4 + x^7 + x^5 = 5$!

Theorem (Abel-Ruffini)

There is no solution in radicals (square roots, cubic roots, etc.) to general polynomial equations of degree five or higher.

Where is $\exists\mathbb{R}$? (2)

Theorem

$$\exists\mathbb{R} \subseteq \mathbf{PSPACE}.$$

Wait, what? I was told in high school that we cannot solve equations like $x^4 + x^7 + x^5 = 5$!

Theorem (Abel-Ruffini)

There is no solution in radicals (square roots, cubic roots, etc.) to general polynomial equations of degree five or higher.

- But ETR is not about *finding* solutions, just about *deciding* if there is one.
- For example, $ax^2 + bx + c = 0$ with $a \neq 0$ has a real solution if and only if $b^2 - 4ac \geq 0$.
- Note that this involves no radicals.
- We have reduced the *existential* equation $\exists x, ax^2 + bx + c = 0$ to the *quantifier-free* equation $b^2 - 4ac \geq 0$.

Quantifier elimination

The simple degree-two example generalizes completely:

Theorem (Tarski-Seideberg quantifier elimination)

Any formula construction with polynomial equations, inequations, logical connections $\vee$, $\wedge$, $\neg$ *and quantifiers* $\exists$ *and* $\forall$ *is equivalent to a similar formula without quantifiers.*

- The proof is constructive, and therefore reduces ETR to computing a single algebraic expression (as in $b^2 - 4ac \geq 0$).

Quantifier elimination

The simple degree-two example generalizes completely:

Theorem (Tarski-Seideberg quantifier elimination)

Any formula construction with polynomial equations, inequations, logical connections $\vee$, $\wedge$, $\neg$ and quantifiers $\exists$ and $\forall$ is equivalent to a similar formula without quantifiers.

- The proof is constructive, and therefore reduces ETR to computing a single algebraic expression (as in $b^2 - 4ac \geq 0$).
- The best algorithms for this rely on *cylindrical algebraic decomposition* and run in *double-exponential time*.

Quantifier elimination

The simple degree-two example generalizes completely:

Theorem (Tarski-Seideberg quantifier elimination)

Any formula construction with polynomial equations, inequations, logical connections $\vee$, $\wedge$, $\neg$ and quantifiers $\exists$ and $\forall$ is equivalent to a similar formula without quantifiers.

- The proof is constructive, and therefore reduces ETR to computing a single algebraic expression (as in $b^2 - 4ac \geq 0$).
- The best algorithms for this rely on *cylindrical algebraic decomposition* and run in *double-exponential time*.
- When there are only *existential quantifiers*, which is the case for ETR, the complexity improves to **PSPACE** [Canny '88].

Quantifier elimination

The simple degree-two example generalizes completely:

Theorem (Tarski-Seideberg quantifier elimination)

Any formula construction with polynomial equations, inequations, logical connections $\vee$, $\wedge$, $\neg$ and quantifiers $\exists$ and $\forall$ is equivalent to a similar formula without quantifiers.

- The proof is constructive, and therefore reduces ETR to computing a single algebraic expression (as in $b^2 - 4ac \geq 0$).
- The best algorithms for this rely on *cylindrical algebraic decomposition* and run in *double-exponential time*.
- When there are only *existential quantifiers*, which is the case for ETR, the complexity improves to **PSPACE** [Canny '88].

Be careful

Quantifier elimination may turn equalities into inequalities.

So, where is $\exists\mathbb{R}$?

Theorem

$$\mathbf{NP} \subseteq \exists\mathbb{R} \subseteq \mathbf{PSPACE}.$$

It is widely conjectured that the two inclusions are strict, but nothing is known about that.

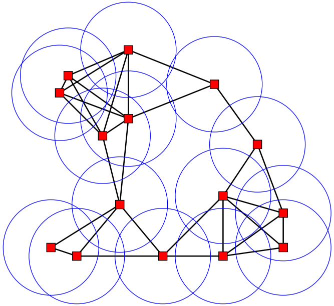
How to prove $\exists\mathbb{R}$ membership?

By definition, to prove $\exists\mathbb{R}$membership, it suffices to encode the problem as a set of algebraic (in)equations.

Example: Unit Disk Graph Recognition

Given a graph $G = (V, E)$:

- For each vertex v_i, use a pair of unknowns (x_i, y_i).
- For each edge $e = (v_i, v_j)$, use an equation $(x_i - x_j)^2 + (y_i - y_j)^2 \leq 1$.
- For each non-edge $\neg e = (v_i, v_j)$, use an equation $(x_i - x_j)^2 + (y_i - y_j)^2 > 1$.



Theorem

Unit Disk Graph Recognition $\in \exists\mathbb{R}$.

How to prove $\exists\mathbb{R}$ membership faster?

- When proving NP-membership, we generally do not write a SAT-formula encoding the problem. Instead, we prove that it is easy to certify a solution, i.e., that it can recognized by a non-deterministic Turing machine in polynomial time.

How to prove $\exists\mathbb{R}$ membership faster?

- When proving NP-membership, we generally do not write a SAT-formula encoding the problem. Instead, we prove that it is easy to certify a solution, i.e., that it can recognized by a non-deterministic Turing machine in polynomial time.
- Likewise:

Theorem (Erickson, van der Hoog, Miltzow '20)

$\exists\mathbb{R}$ *membership is equivalent to being able to verify a solution in polynomial time on a Real RAM machine.*

Intuitively, a real RAM machine is like a word RAM model (or a Turing machine) that is allowed to

- manipulate real numbers, and
- operations on them (addition, multiplication, substraction, division, square roots)

in constant time.

It is unwise to allow downcasting reals to integers (e.g., allowing the floor function $\lfloor x \rfloor$).

2. Proving $\exists\mathbb{R}$-hardness

- As for every complexity class, one proves $\exists\mathbb{R}$-hardness of a problem P by reducing an $\exists\mathbb{R}$-complete problem to it.
- Recall that ETR is $\exists\mathbb{R}$-complete. This is not impractical and for example can be used to prove $\exists\mathbb{R}$-hardness of
  - Example 2: Minimum Matrix Rank
  - Example 4: Training Neural Networks

2. Proving $\exists\mathbb{R}$-hardness

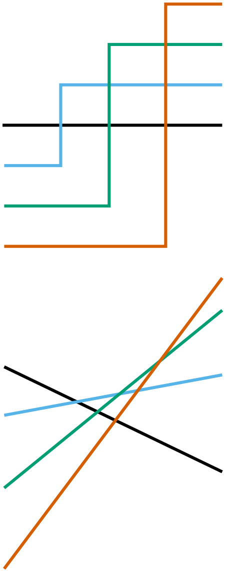
- As for every complexity class, one proves $\exists\mathbb{R}$-hardness of a problem P by reducing an $\exists\mathbb{R}$-complete problem to it.
- Recall that ETR is $\exists\mathbb{R}$-complete. This is not impractical and for example can be used to prove $\exists\mathbb{R}$-hardness of
  - Example 2: Minimum Matrix Rank
  - Example 4: Training Neural Networks
- But for most problems, in particular for those of a *geometric* nature, it is more common to reduce from another problem: Stretchability.

Stretchability of pseudoline arrangements

A *pseudoline arrangement* is a collection of x-monotone curves in the plane that each cross pairwise exactly once.

STRETCHABILITY

Input: A pseudoline arrangement (for example described with polygonal lines).
Output: Is it *homeomorphic* to an arrangement of straight lines?



Stretchability of pseudoline arrangements

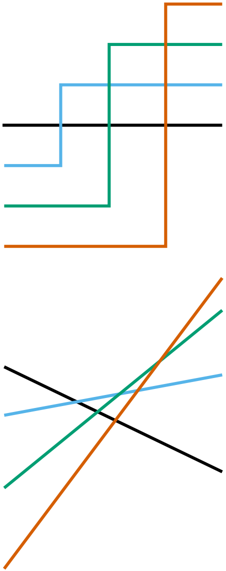
A *pseudoline arrangement* is a collection of x-monotone curves in the plane that each cross pairwise exactly once.

Stretchability

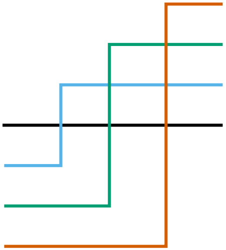
Input: A pseudoline arrangement (for example described with polygonal lines).

Output: Is it *homeomorphic* to an arrangement of straight lines?

What an oddly specific problem.



Stretchability of pseudoline arrangements



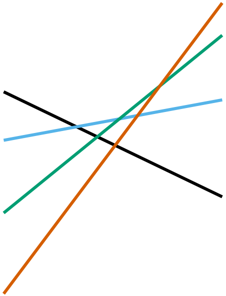
A *pseudoline arrangement* is a collection of x-monotone curves in the plane that each cross pairwise exactly once.

Stretchability

Input: A pseudoline arrangement (for example described with polygonal lines).
Output: Is it *homeomorphic* to an arrangement of straight lines?

What an oddly specific problem.

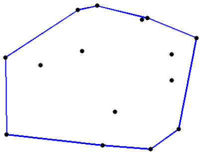
Who cares??



Parenthesis on abstract data structures in computational geometry

- *Computational geometry* investigates algorithms with geometric input.

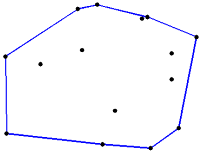
Example: Given a set of points in $\mathbb{R}^2$, compute their convex hull.



Parenthesis on abstract data structures in computational geometry

- *Computational geometry* investigates algorithms with geometric input.

Example: Given a set of points in $\mathbb{R}^2$, compute their convex hull.

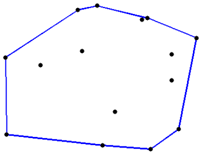


- Most of these problems do not actually rely on the coordinates of the points, but only on *orientation predicates*: is A to the left, on or to the right of the line (BC)?
- So it makes sense to use these predicates as the data structure to work with. This is called a *chirotope*, or *abstract order type*, or *oriented matroid of rank* 3.

Parenthesis on abstract data structures in computational geometry

- *Computational geometry* investigates algorithms with geometric input.

Example: Given a set of points in $\mathbb{R}^2$, compute their convex hull.

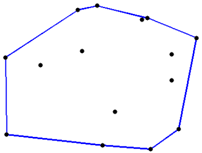


- Most of these problems do not actually rely on the coordinates of the points, but only on *orientation predicates*: is A to the left, on or to the right of the line (BC)?
- So it makes sense to use these predicates as the data structure to work with. This is called a *chirotope*, or *abstract order type*, or *oriented matroid of rank* 3.
- Then the question arises: given a chirotope, does it correspond to an actual set of points?

Parenthesis on abstract data structures in computational geometry

- *Computational geometry* investigates algorithms with geometric input.

Example: Given a set of points in $\mathbb{R}^2$, compute their convex hull.



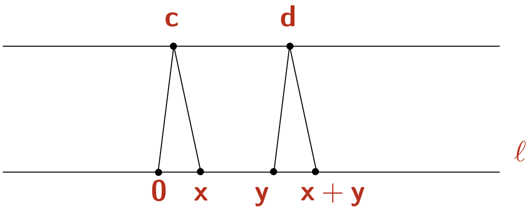
- Most of these problems do not actually rely on the coordinates of the points, but only on *orientation predicates*: is A to the left, on or to the right of the line (BC)?
- So it makes sense to use these predicates as the data structure to work with. This is called a *chirotope*, or *abstract order type*, or *oriented matroid of rank* 3.
- Then the question arises: given a chirotope, does it correspond to an actual set of points?
- Via the duality $(a, b) \mapsto ax - b$ mapping points to lines, this is equivalent to the STRETCHABILITY problem.

$\exists\mathbb{R}$-completeness of STRETCHABILITY

Theorem (Mnëv '88, Shor '91)

STRETCHABILITY *is* $\exists\mathbb{R}$*-complete.*

- The key insight comes from the *von Staudt constructions*, allowing to encode algebraic operations in line arrangements.

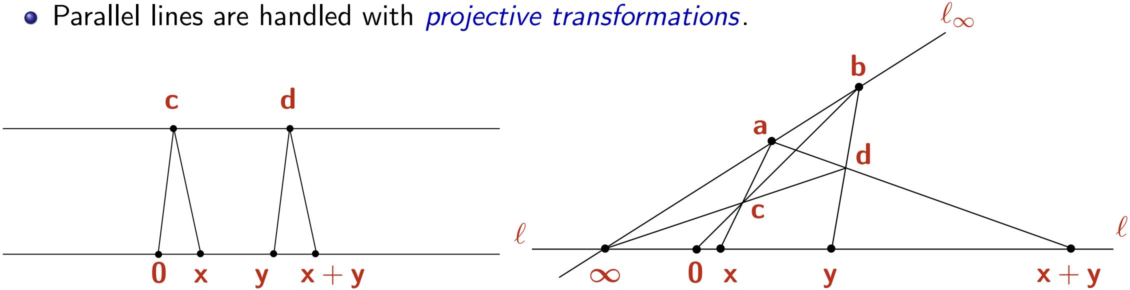


$\exists\mathbb{R}$-completeness of STRETCHABILITY

Theorem (Mnëv '88, Shor '91)

STRETCHABILITY *is* $\exists\mathbb{R}$*-complete.*

- The key insight comes from the *von Staudt constructions*, allowing to encode algebraic operations in line arrangements.
- Parallel lines are handled with *projective transformations*.

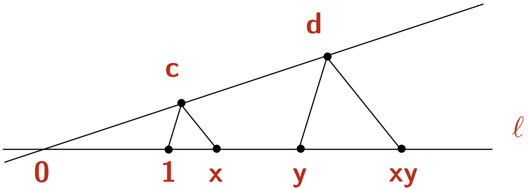


$\exists\mathbb{R}$-completeness of STRETCHABILITY

Theorem (Mnëv '88, Shor '91)

STRETCHABILITY *is* $\exists\mathbb{R}$*-complete.*

- The key insight comes from the *von Staudt constructions*, allowing to encode algebraic operations in line arrangements.
- Parallel lines are handled with *projective transformations*.

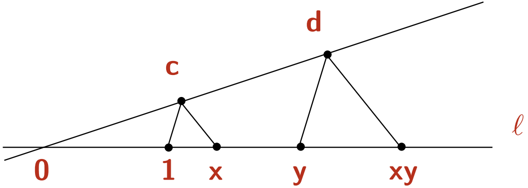


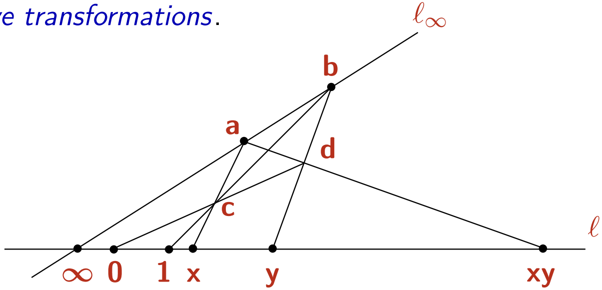
$\exists\mathbb{R}$-completeness of STRETCHABILITY

Theorem (Mnëv '88, Shor '91)

STRETCHABILITY *is* $\exists\mathbb{R}$*-complete.*

- The key insight comes from the *von Staudt constructions*, allowing to encode algebraic operations in line arrangements.
- Parallel lines are handled with *projective transformations*.

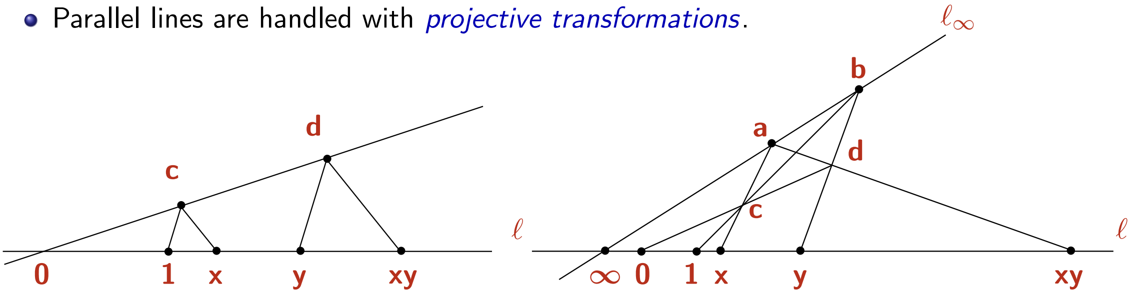




Theorem (Mnëv '88, Shor '91)

Stretchability *is ∃ℝ-complete.*

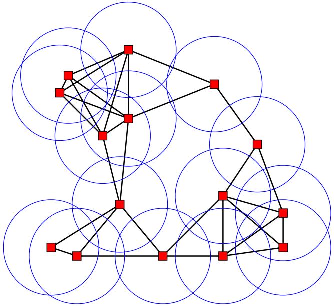
- The key insight comes from the *von Staudt constructions*, allowing to encode algebraic operations in line arrangements.
- Parallel lines are handled with *projective transformations*.



Using these gadgets, the solvability of an ETR formula translates into the stretchability of some line arrangement, but there are **many** tricky details.

3. A few more things to know about $\exists\mathbb{R}$: Precision issues

How precise do you need to be if you actually want to describe the coordinates of a unit disk graph?



$\exists\mathbb{R}$-complete problems generally require *doubly exponential precision*.

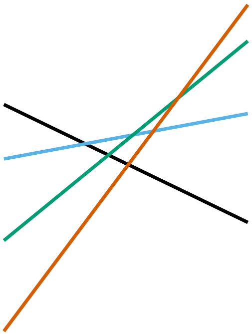
- This comes from the fact that one can encode numbers of size 2^{2^n} or $2^{2^{-n}}$ with only n equations.
- Conversely, real algebraic geometric theorems shows that for open sets, doubly exponential precision is generally enough.
- Similarly, for closed sets, irrational numbers are generally required.

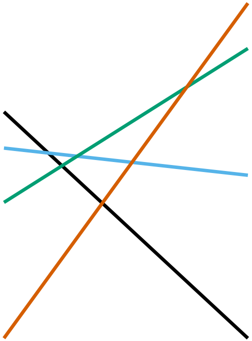
3. A few more things to know about $\exists\mathbb{R}$: Universality

Conjecture (Ringel '56)

If two line arrangements have the same chirotope, then they are isotopic, i.e., one can be deformed into the other.

Seems intuitive...





3. A few more things to know about $\exists\mathbb{R}$: Universality

Conjecture (Ringel '56)

If two line arrangements have the same chirotope, then they are isotopic, i.e., one can be deformed into the other.

Seems intuitive... but

Theorem (Mnëv '86)

Any semi-algebraic variety is stably equivalent to the realization space of some pseudoline arrangement.

- A semi-algebraic variety is just a set of solutions of an ETR formula.
- Stable equivalence would bring us beyond the scope of this tutorial, but ...
- ... in a nutshell, universality means that the solution space of $\exists\mathbb{R}$-complete problems is generally *horribly complicated* from an algebraic, geometric and topological point of view.
- In particular, it is in general **not** connected, nor simply connected, nor contractible or anything like that.

3. A few more things to know about $\exists\mathbb{R}$: Problems that are not $\exists\mathbb{R}$-complete

The actual "definition"

The Existential Theory of the Reals ($\exists\mathbb{R}$) is the complexity class that appears naturally for nice discrete problems that

- look like they should be in **NP**
- but there are annoying precision or algebraic issues to bound the size of the certificate.

Some non-examples:

- Problems that are *overconstrained*: for example, deciding whether a weighted graph represents distances in $\mathbb{R}^d$ is $\exists\mathbb{R}$-complete, but not if the graph is complete.
- Problems easy to optimize. For example, computing the geometric median (point that minimizes sums of distances) of points in $\mathbb{R}^d$ runs into algebraic issues, but it is probably not $\exists\mathbb{R}$-complete.
- In particular, the famous SUM OF SQUARE ROOTS PROBLEM: given integers $a_1, \ldots, a_n$ and k, is $\sum \sqrt{a_i} \geq k$? is **not** believed to be $\exists\mathbb{R}$-complete.

Some concluding words

- There are a **lot** of very different $\exists\mathbb{R}$-complete problems.
- Still a **lof** of open questions.
- Many topics I have not touched on, among them:
  - $\forall\exists\mathbb{R}$-completeness and higher levels of the hierarchy,
  - connections to Blum-Shub-Smale models,
  - $\exists\mathbb{Z}$ (undecidable), $\exists\mathbb{C}$ (easier), $\exists\mathbb{Q}$ (unknown decidability),
  - actual algorithms to solve systems of polynomial inequations,
  - ...
- To learn more about this topic: read
  - The Existential Theory of the Reals as a Complexity Class: A Compendium, by Schaefer, Cardinal and Miltzow
  - Segment intersections graphs and $\exists\mathbb{R}$, by Matoušek

Some concluding words

- There are a **lot** of very different $\exists\mathbb{R}$-complete problems.
- Still a **lof** of open questions.
- Many topics I have not touched on, among them:
  - $\forall\exists\mathbb{R}$-completeness and higher levels of the hierarchy,
  - connections to Blum-Shub-Smale models,
  - $\exists\mathbb{Z}$ (undecidable), $\exists\mathbb{C}$ (easier), $\exists\mathbb{Q}$ (unknown decidability),
  - actual algorithms to solve systems of polynomial inequations,
  - ...
- To learn more about this topic: read
  - The Existential Theory of the Reals as a Complexity Class: A Compendium, by Schaefer, Cardinal and Miltzow
  - Segment intersections graphs and $\exists\mathbb{R}$, by Matoušek

Thank you! Any questions?