Incidence geometry, conditional independence and the existential theory of the reals

Tobias Boege

Aalto University
School of Science

Logic seminar
University of Helsinki
16 November 2022

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = 3/2$
- Ubiquitous in mathematical modeling.

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.
- Computer algebra allows experimentation.

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.
- Computer algebra allows experimentation.
- Atomic formulas in the language of rings.

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.
- Computer algebra allows experimentation.
- Atomic formulas in the language of rings.

The first-order theory of algebraically closed fields has quantifier elimination in the language of rings.

Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.
- Computer algebra allows experimentation.
- Atomic formulas in the language of rings.

The first-order theory of algebraically closed fields has quantifier elimination in the language of rings.

But algebraic statistics, polynomial optimization, computational geometry, . . . need the real numbers.

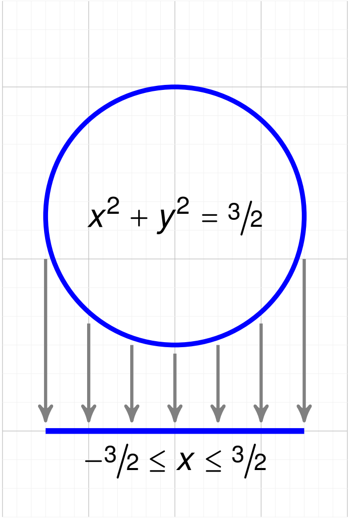
Non-linear algebra

Systems of polynomial equations:

- $x^2 + y^2 = {}^3\!/_2$
- Ubiquitous in mathematical modeling.
- Lots of structure but practically challenging.
- Computer algebra allows experimentation.
- Atomic formulas in the language of rings.

The first-order theory of algebraically closed fields has quantifier elimination in the language of rings.

But algebraic statistics, polynomial optimization, computational geometry, . . . need the real numbers.



The feasibility problem in $(\mathbb{R}, +, \cdot, <, 0, 1)$

Tarski–Seidenberg Theorem

Real-closed fields have quantifier elimination in the language of ordered rings.

The definable sets in this language are the semialgebraic sets.

The feasibility problem in $(\mathbb{R}, +, \cdot, <, 0, 1)$

Tarski–Seidenberg Theorem

Real-closed fields have quantifier elimination in the language of ordered rings.

The definable sets in this language are the semialgebraic sets.

The feasibility problem ETR

Given a quantifier-free formula, decide if it is satisfiable in $\mathbb{R}$.
Equivalently: decide if an explicitly given semialgebraic set is inhabited.

The feasibility problem in $(\mathbb{R}, +, \cdot, <, 0, 1)$

Tarski–Seidenberg Theorem

Real-closed fields have quantifier elimination in the language of ordered rings.

The definable sets in this language are the semialgebraic sets.

The feasibility problem ETR

Given a quantifier-free formula, decide if it is satisfiable in $\mathbb{R}$.
Equivalently: decide if an explicitly given semialgebraic set is inhabited.

$$x^2 + y^2 = 0 \wedge x < y \ ?$$

ETR modulo polytime = $\exists\mathbb{R}$

The complexity class $\exists\mathbb{R}$ consists of all decision problems which (many-one) reduce to ETR in polynomial time. Input length is formula length*. Canny (1988): ETR $\in$ PSPACE.

Lemma

The special case of ETR *for varieties (conjunctions of equations) is* $\exists\mathbb{R}$*-complete.*

Proof.

Given any boolean combination of polynomial constraints $f \bowtie 0$ with $\bowtie \in \{=, \neq, <, \leq, \geq, >\}$:

ETR modulo polytime = $\exists\mathbb{R}$

The complexity class $\exists\mathbb{R}$ consists of all decision problems which (many-one) reduce to ETR in polynomial time. Input length is formula length*. Canny (1988): ETR $\in$ PSPACE.

Lemma

The special case of ETR *for varieties (conjunctions of equations) is $\exists\mathbb{R}$-complete.*

Proof.

Given any boolean combination of polynomial constraints $f \bowtie 0$ with $\bowtie \in \{=, \neq, <, \leq, \geq, >\}$:

- Use the Tseitin transform to derive a CNF for it.

ETR modulo polytime = $\exists\mathbb{R}$

The complexity class $\exists\mathbb{R}$ consists of all decision problems which (many-one) reduce to ETR in polynomial time. Input length is formula length*. Canny (1988): ETR $\in$ PSPACE.

Lemma

The special case of ETR *for varieties (conjunctions of equations) is $\exists\mathbb{R}$-complete.*

Proof.

Given any boolean combination of polynomial constraints $f \bowtie 0$ with $\bowtie \in \{=, \neq, <, \leq, \geq, >\}$:

- Use the Tseitin transform to derive a CNF for it.
- Replace $f \neq 0 \rightarrow yf = 1$, $f > 0 \rightarrow y^2 f = 1$ and $f \geq 0 \rightarrow f = y^2$.

ETR modulo polytime = $\exists\mathbb{R}$

The complexity class $\exists\mathbb{R}$ consists of all decision problems which (many-one) reduce to ETR in polynomial time. Input length is formula length*. Canny (1988): ETR $\in$ PSPACE.

Lemma

The special case of ETR *for varieties (conjunctions of equations) is $\exists\mathbb{R}$-complete.*

Proof.

Given any boolean combination of polynomial constraints $f \bowtie 0$ with $\bowtie \in \{=, \neq, <, \leq, \geq, >\}$:

- Use the Tseitin transform to derive a CNF for it.
- Replace $f \neq 0 \;\rightarrow\; yf = 1,\;\; f > 0 \rightarrow y^2 f = 1$ and $f \geq 0 \rightarrow f = y^2$.
- Dissolve disjunctions $\bigvee_i [f_i = 0]$ into $\bigwedge_i [y_i = f_i] \wedge [\prod_i y_i = 0]$. □

Incidence geometry

The projective plane over $\mathbb{R}$ is the space $\mathbb{P}^2$ which extends the affine plane $\mathbb{R}^2$ by a line at infinity. A point $p \in \mathbb{P}^2$ is given by its homogeneous coordinates $p = [x : y : z]$:

- Not all of x, y, z are zero, and
- $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for $\lambda \neq 0$.

Incidence geometry

The projective plane over $\mathbb{R}$ is the space $\mathbb{P}^2$ which extends the affine plane $\mathbb{R}^2$ by a line at infinity. A point $p \in \mathbb{P}^2$ is given by its homogeneous coordinates $p = [x : y : z]$:

- Not all of x, y, z are zero, and
- $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for $\lambda \neq 0$.

A triple of homogeneous coordinates $[a : b : c]$ dually also represents a line in $\mathbb{P}^2$ with the equation $ax + by + cz = 0$.

Incidence geometry

The projective plane over $\mathbb{R}$ is the space $\mathbb{P}^2$ which extends the affine plane $\mathbb{R}^2$ by a line at infinity. A point $p \in \mathbb{P}^2$ is given by its homogeneous coordinates $p = [x : y : z]$:

- Not all of x, y, z are zero, and
- $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for $\lambda \neq 0$.

A triple of homogeneous coordinates $[a : b : c]$ dually also represents a line in $\mathbb{P}^2$ with the equation $ax + by + cz = 0$.

In the projective plane...

Every pair of distinct points p, p' has a unique line $p \vee p'$ which contains them both.
Every pair of distinct lines ℓ, ℓ' has a unique point $\ell \wedge \ell'$ which lies on both of them.

Both, $\vee$ and $\wedge$, are the cross product $\times$ in $\mathbb{R}^3$ operating on homogeneous coordinates.

Incidence geometry

Let $p = [x : y : z]$ be a point and $\ell = [a : b : c]$ be a line.
Then p lies on ℓ if and only if $0 = \langle p, \ell \rangle = ax + by + cz$.

Incidence geometry

Let $p = [x : y : z]$ be a point and $\ell = [a : b : c]$ be a line.
Then p lies on ℓ if and only if $0 = \langle p, \ell \rangle = ax + by + cz$.

An incidence structure is a combinatorial object consisting of

- finitely many (labels for) points $\mathcal{P}$,
- finitely many (labels for) lines $\mathcal{L}$, and
- a set $\mathcal{I}$ of incidence constraints $p \in \ell$ or $p \notin \ell$ for some $p \in \mathcal{P}$ and $\ell \in \mathcal{L}$.

We assume that there are four points in $\mathcal{P}$ no three of which are collinear.
They form a projective basis.

Incidence geometry

Let $p = [x : y : z]$ be a point and $\ell = [a : b : c]$ be a line.
Then p lies on ℓ if and only if $0 = \langle p, \ell \rangle = ax + by + cz$.

An incidence structure is a combinatorial object consisting of

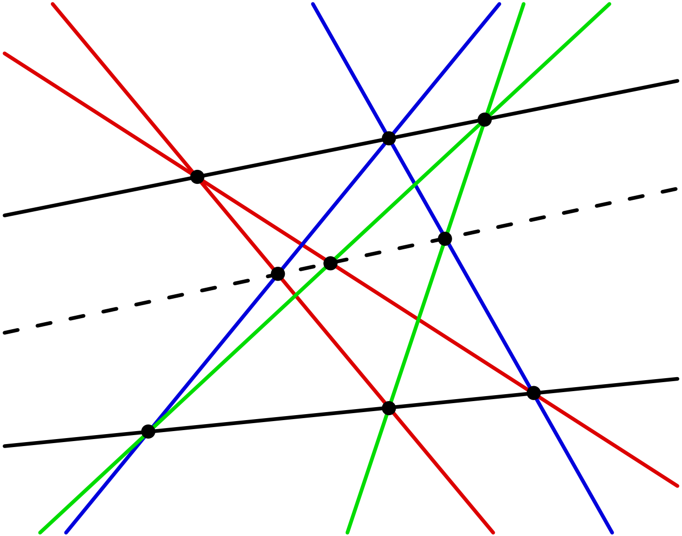
- finitely many (labels for) points $\mathcal{P}$,
- finitely many (labels for) lines $\mathcal{L}$, and
- a set $\mathcal{I}$ of incidence constraints $p \in \ell$ or $p \notin \ell$ for some $p \in \mathcal{P}$ and $\ell \in \mathcal{L}$.

We assume that there are four points in $\mathcal{P}$ no three of which are collinear.
They form a projective basis.

Realizability problem for incidence structures PLR

Given an incidence structure, decide if it can be realized in $\mathbb{P}^2$.

PLR is not straightforward



A technique for $\exists\mathbb{R}$-completeness

The coordinates of all points in $\mathcal{P}$ and of all lines in $\mathcal{L}$ are finitely many variables and we have (short!) polynomial equations ($p \in \ell$) and inequations ($p \notin \ell$) in them:

$$\mathsf{PLR} \in \exists\mathbb{R}.$$

A technique for $\exists\mathbb{R}$-completeness

The coordinates of all points in $\mathcal{P}$ and of all lines in $\mathcal{L}$ are finitely many variables and we have (short!) polynomial equations ($p \in \ell$) and inequations ($p \notin \ell$) in them:

$$\text{PLR} \in \exists\mathbb{R}.$$

Theorem (von Staudt 1857)

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

Recall: It suffices to reduce the variety case of ETR. We will show how to encode one polynomial equation $f = 0$ as an incidence structure.

A technique for $\exists\mathbb{R}$-completeness

The coordinates of all points in $\mathcal{P}$ and of all lines in $\mathcal{L}$ are finitely many variables and we have (short!) polynomial equations ($p \in \ell$) and inequations ($p \notin \ell$) in them:

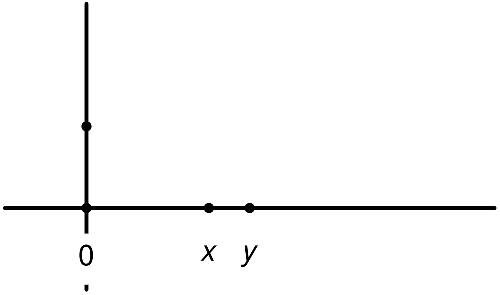
$$\text{PLR} \in \exists\mathbb{R}.$$

Theorem (von Staudt 1857)

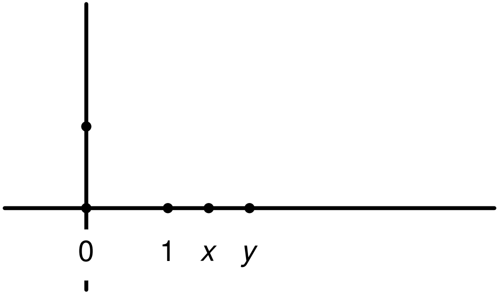
PLR *is* $\exists\mathbb{R}$*-complete.*

Recall: It suffices to reduce the variety case of ETR. We will show how to encode one polynomial equation $f = 0$ as an incidence structure. In fact, the polynomials $z = x + y$ and $z = x \cdot y$ are sufficient.

Von Staudt constructions

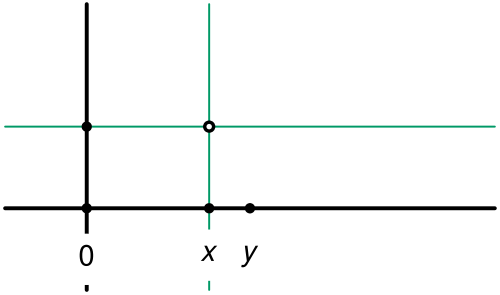


Addition

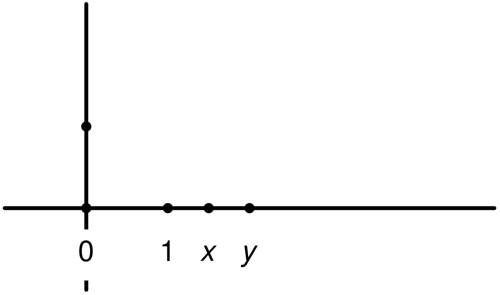


Multiplication

Von Staudt constructions

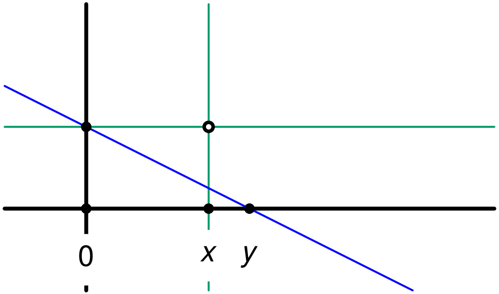


Addition

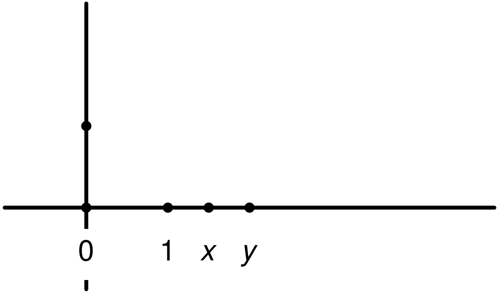


Multiplication

Von Staudt constructions

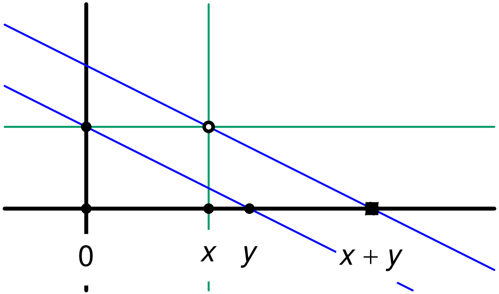


Addition

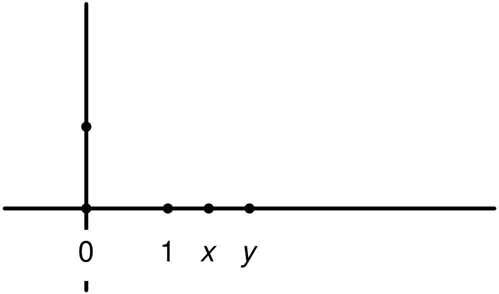


Multiplication

Von Staudt constructions

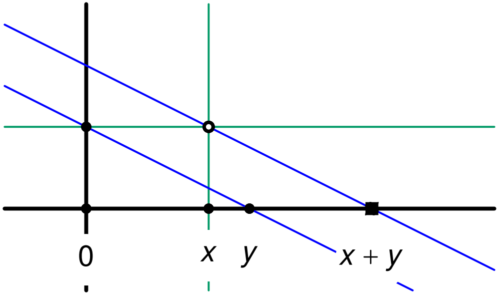


Addition

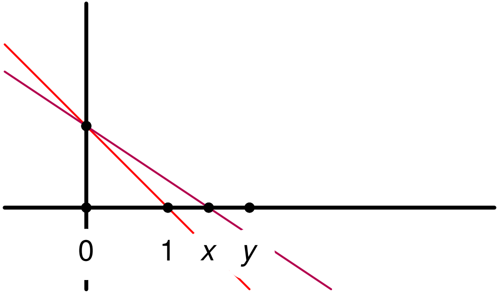


Multiplication

Von Staudt constructions

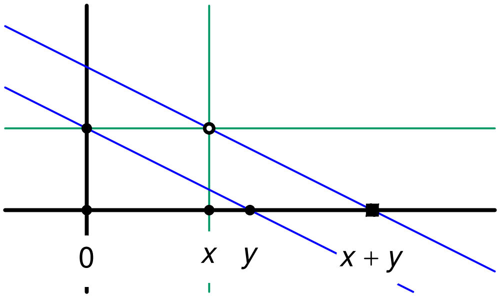


Addition

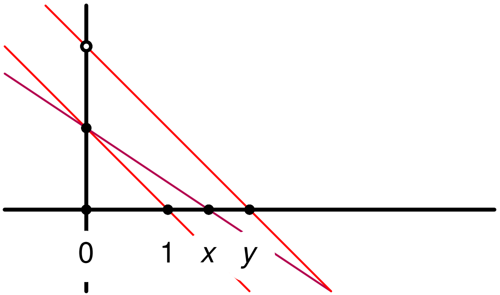


Multiplication

Von Staudt constructions

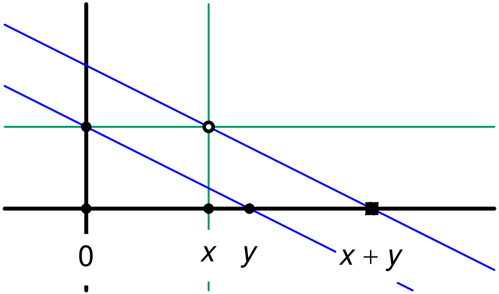


Addition

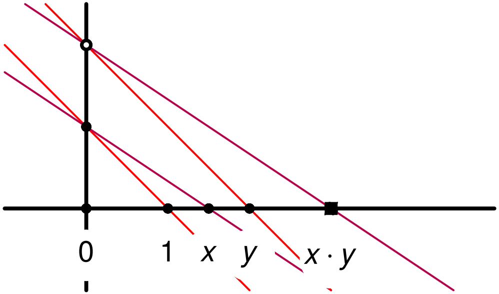


Multiplication

Von Staudt constructions

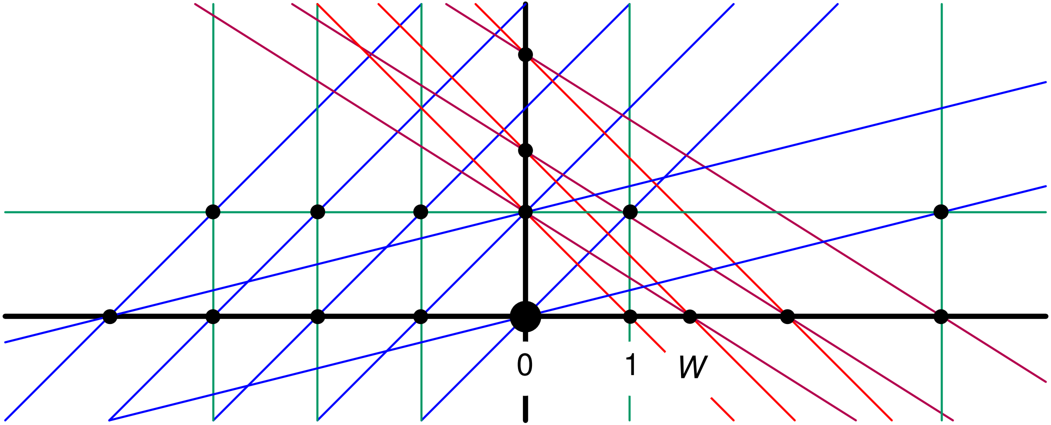


Addition

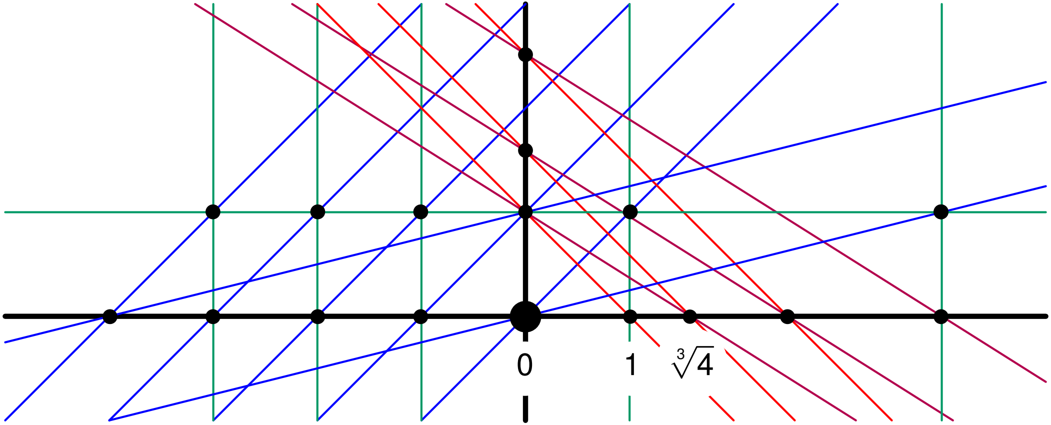


Multiplication

Where is Waldo?



Where is Waldo? On the cube root of 4!



$\exists\mathbb{R}$-complete problems

- PLR is $\exists\mathbb{R}$-complete.

$\exists\mathbb{R}$-complete problems

- PLR is $\exists\mathbb{R}$-complete.
- Solving systems consisting only of equations of the form $x = 0$, $x = 1$ or $\langle p, \ell \rangle = ax + by + cz = 0$ is $\exists\mathbb{R}$-complete.

$\exists\mathbb{R}$-complete problems

- PLR is $\exists\mathbb{R}$-complete.
- Solving systems consisting only of equations of the form $x = 0$, $x = 1$ or $\langle p, \ell \rangle = ax + by + cz = 0$ is $\exists\mathbb{R}$-complete.
- Solving systems consisting only of equations of the form $x = 0$, $x = 1$ or

$$\langle p, q \times r \rangle = \det \begin{pmatrix} p_x & q_x & r_x \\ p_y & q_y & r_y \\ p_z & q_z & r_z \end{pmatrix} = 0$$

  is $\exists\mathbb{R}$-complete. → matroid theory

$\exists\mathbb{R}$-complete problems

- PLR is $\exists\mathbb{R}$-complete.
- Solving systems consisting only of equations of the form $x = 0$, $x = 1$ or $\langle p, \ell \rangle = ax + by + cz = 0$ is $\exists\mathbb{R}$-complete.
- Solving systems consisting only of equations of the form $x = 0$, $x = 1$ or

$$\langle p, q \times r \rangle = \det \begin{pmatrix} p_x & q_x & r_x \\ p_y & q_y & r_y \\ p_z & q_z & r_z \end{pmatrix} = 0$$

  is $\exists\mathbb{R}$-complete. $\rightarrow$ matroid theory
- Other examples, see Miltzow and Schmiermann (2021).

Conditional independence $[X \perp\!\!\!\perp Y \mid Z]$

"When does knowing Z make X irrelevant for Y?"

Conditional independence $[X \perp\!\!\!\perp Y \mid Z]$

"When does knowing Z make X irrelevant for Y?"

Example: Two independent fair coins c_1 and c_2 are wired to a bell b which rings if and only if $c_1 = c_2$.

Conditional independence $[X \perp\!\!\!\perp Y \mid Z]$

"When does knowing Z make X irrelevant for Y?"

Example: Two independent fair coins c_1 and c_2 are wired to a bell b which rings if and only if $c_1 = c_2$.

- $c_1 \perp\!\!\!\perp c_2$

Conditional independence $[X \perp\!\!\!\perp Y \mid Z]$

"When does knowing Z make X irrelevant for Y?"

Example: Two independent fair coins c_1 and c_2 are wired to a bell b which rings if and only if $c_1 = c_2$.

- $c_1 \perp\!\!\!\perp c_2$
- $\neg(c_1 \perp\!\!\!\perp c_2 \mid b) \ldots$

Conditional independence $[X \perp\!\!\!\perp Y \mid Z]$

"When does knowing Z make X irrelevant for Y?"

Example: Two independent fair coins c_1 and c_2 are wired to a bell b which rings if and only if $c_1 = c_2$.

- $c_1 \perp\!\!\!\perp c_2$
- $\neg(c_1 \perp\!\!\!\perp c_2 \mid b)$ ...

Question: When can we conclude from some independences other independences? E.g., is it possible that $c_1 \perp\!\!\!\perp b$?

Gaussian conditional independence

Assume $\xi = (\xi_i : i \in N)$ are jointly Gaussian with covariance matrix $\Sigma \in \mathrm{PD}_N$.

Definition

The polynomial $\Sigma[K] \coloneqq \det \Sigma_{K,K}$ is a *principal minor* of Σ and $\Sigma[ij \mid K] \coloneqq \det \Sigma_{iK,jK}$ is an *almost-principal minor*.

Algebraic statistics proves:

- Σ is PD if and only if $\Sigma[K] > 0$ for all $K \subseteq N$.
- $[\xi_i \perp\!\!\!\perp \xi_j \mid \xi_K]$ holds if and only if $\Sigma[ij \mid K] = 0$.
- $\mathbb{E}[\xi] = \mu$ is irrelevant.

Very special polynomials

$$
\begin{aligned}
\Sigma[\,ij\,|\,\,] &= x_{ij} \\
\Sigma[\,ij\,|\,k\,] &= x_{ij}x_{kk} - x_{ik}x_{jk} \\
\Sigma[\,ij\,|\,kl\,] &= x_{ij}x_{kk}x_{ll} - x_{il}x_{jl}x_{kk} + x_{il}x_{jk}x_{kl} + x_{ik}x_{jl}x_{kl} - x_{ij}x_{kl}^2 - x_{ik}x_{jk}x_{ll} \\
\Sigma[\,ij\,|\,klm\,] &= x_{ij}x_{kk}x_{ll}x_{mm} + x_{im}x_{jm}x_{kl}^2 - x_{im}x_{jl}x_{kl}x_{km} - x_{il}x_{jm}x_{kl}x_{km} + \\
&\quad x_{il}x_{jl}x_{km}^2 - x_{im}x_{jm}x_{kk}x_{ll} + x_{im}x_{jk}x_{km}x_{ll} + x_{ik}x_{jm}x_{km}x_{ll} - \\
&\quad x_{ij}x_{km}^2x_{ll} + x_{im}x_{jl}x_{kk}x_{lm} + x_{il}x_{jm}x_{kk}x_{lm} - x_{im}x_{jk}x_{kl}x_{lm} - \\
&\quad x_{ik}x_{jm}x_{kl}x_{lm} - x_{il}x_{jk}x_{km}x_{lm} - x_{ik}x_{jl}x_{km}x_{lm} + 2x_{ij}x_{kl}x_{km}x_{lm} + \\
&\quad x_{ik}x_{jk}x_{lm}^2 - x_{ij}x_{kk}x_{lm}^2 - x_{il}x_{jl}x_{kk}x_{mm} + x_{il}x_{jk}x_{kl}x_{mm} + \\
&\quad x_{ik}x_{jl}x_{kl}x_{mm} - x_{ij}x_{kl}^2x_{mm} - x_{ik}x_{jk}x_{ll}x_{mm} \\
&\vdots
\end{aligned}
$$

Gaussian CI models

Definition

A *CI constraint* is a CI statement $[\xi_i \perp\!\!\!\perp \xi_j \mid \xi_K]$ or its negation $\neg[\xi_i \perp\!\!\!\perp \xi_j \mid \xi_K]$.
The *model* of a set of CI constraints is the set of all PD matrices which satisfy them.

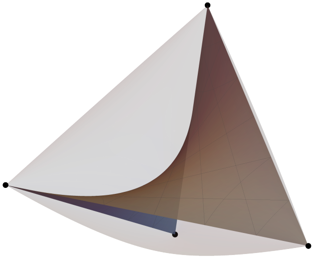


Figure: Model of $\Sigma[12 \mid 3] = a - bc = 0$ in the space of 3×3 correlation matrices.

Models and inference

Inference problem for Gaussian conditional independence `GCI`

Given a clause $\bigwedge \mathcal{P} \Rightarrow \bigvee \mathcal{Q}$, where $\mathcal{P}$ and $\mathcal{Q}$ are sets of CI statements over N, decide if it is valid for all N-variate Gaussians.

$$\bigwedge \mathcal{P} \Rightarrow \bigvee \mathcal{Q}$$

Models and inference

Inference problem for Gaussian conditional independence GCI

Given a clause $\bigwedge \mathcal{P} \Rightarrow \bigvee \mathcal{Q}$, where $\mathcal{P}$ and $\mathcal{Q}$ are sets of CI statements over N, decide if it is valid for all N-variate Gaussians.

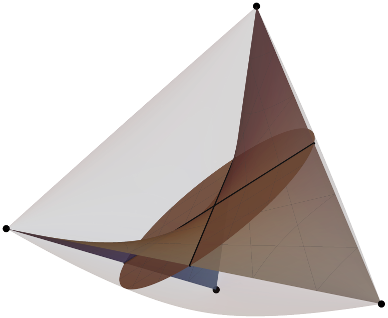
$$\bigwedge \mathcal{P} \Rightarrow \bigvee \mathcal{Q} \text{ is not valid} \iff \mathcal{M}(\mathcal{P} \cup \neg\mathcal{Q}) \text{ has a point}$$

Example of CI inference

$$\Sigma = \begin{pmatrix} 1 & a & b \\ a & 1 & c \\ b & c & 1 \end{pmatrix}$$

- If $\Sigma[12\,|\,] = a$ and $\Sigma[12\,|\,3] = a - bc$ vanish, then $bc = \Sigma[13\,|\,] \cdot \Sigma[23\,|\,]$ must vanish:

$$[12\,|\,] \wedge [12\,|\,3] \;\Rightarrow\; [13\,|\,] \vee [23\,|\,].$$



Completeness result for GCI

The GCI problem is as hard as it could possibly be:

Theorem

GCI *is* $\forall\mathbb{R}$*-complete where* $\forall\mathbb{R}$ *abbreviates co-*$\exists\mathbb{R}$*.*

Completeness result for GCI

The GCI problem is as hard as it could possibly be:

Theorem

GCI *is* $\forall\mathbb{R}$*-complete where* $\forall\mathbb{R}$ *abbreviates co-*$\exists\mathbb{R}$*.*

Proof.

Both parts require care!

Completeness result for `GCI`

The `GCI` problem is as hard as it could possibly be:

Theorem

`GCI` *is* $\forall\mathbb{R}$*-complete where* $\forall\mathbb{R}$ *abbreviates co-*$\exists\mathbb{R}$*.*

Proof.

Both parts require care!

- To show containment in $\forall\mathbb{R}$, we have to show that an $n \times n$ determinant of a symmetric matrix can be computed by a polynomially-sized polynomial system.

Completeness result for `GCI`

The `GCI` problem is as hard as it could possibly be:

Theorem

`GCI` *is* $\forall\mathbb{R}$*-complete where* $\forall\mathbb{R}$ *abbreviates co-*$\exists\mathbb{R}$*.*

Proof.

Both parts require care!

- To show containment in $\forall\mathbb{R}$, we have to show that an $n \times n$ determinant of a symmetric matrix can be computed by a polynomially-sized polynomial system.
- The hardness proof is more interesting! We express $\langle p, \ell \rangle$ using $\Sigma[ij \mid K]$.

Condensed almost-principal minor

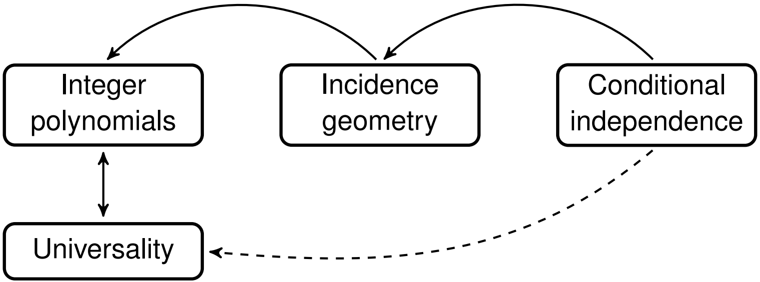
Suppose $x_{xx} = x_{yy} = x_{zz} = 1$ (in a correlation matrix) and $x_{xy} = x_{xz} = x_{yz} = 0$:

$$
\begin{aligned}
\Sigma[ij \mid] &= x_{ij} \\
\Sigma[ij \mid xyz] &= x_{ij} x_{xx} x_{yy} x_{zz} + x_{iz} x_{jz} \underline{x_{xy}^2} - x_{iz} x_{jy} \underline{x_{xy} x_{xz}} - x_{iy} x_{jz} \underline{x_{xy} x_{xz}} + x_{iy} x_{jy} \underline{x_{xz}^2} \\
&\quad - x_{iz} x_{jz} x_{xx} x_{yy} + x_{iz} x_{jx} \underline{x_{xz}} x_{yy} + x_{ix} x_{jz} \underline{x_{xz}} x_{yy} - x_{ij} \underline{x_{xz}^2} x_{yy} \\
&\quad + x_{iz} x_{jy} x_{xx} \underline{x_{yz}} + x_{iy} x_{jz} x_{xx} \underline{x_{yz}} - x_{iz} x_{jx} \underline{x_{xy} x_{yz}} - x_{ix} x_{jz} \underline{x_{xy} x_{yz}} \\
&\quad - x_{iy} x_{jx} \underline{x_{xz} x_{yz}} - x_{ix} x_{jy} \underline{x_{xz} x_{yz}} + 2 x_{ij} \underline{x_{xy} x_{xz} x_{yz}} + x_{ix} x_{jx} \underline{x_{yz}^2} \\
&\quad - x_{ij} x_{xx} \underline{x_{yz}^2} - x_{iy} x_{jy} x_{xx} x_{zz} + x_{iy} x_{jx} \underline{x_{xy}} x_{zz} + x_{ix} x_{jy} \underline{x_{xy}} x_{zz} \\
&\quad - x_{ij} \underline{x_{xy}^2} x_{zz} - x_{ix} x_{jx} x_{yy} x_{zz} \\
&= x_{ij} - \sum_{k=x,y,z} x_{ik} x_{jk} \quad = \quad x_{ij} - \langle p, \ell \rangle .
\end{aligned}
$$

Incidence geometry as conditional independence

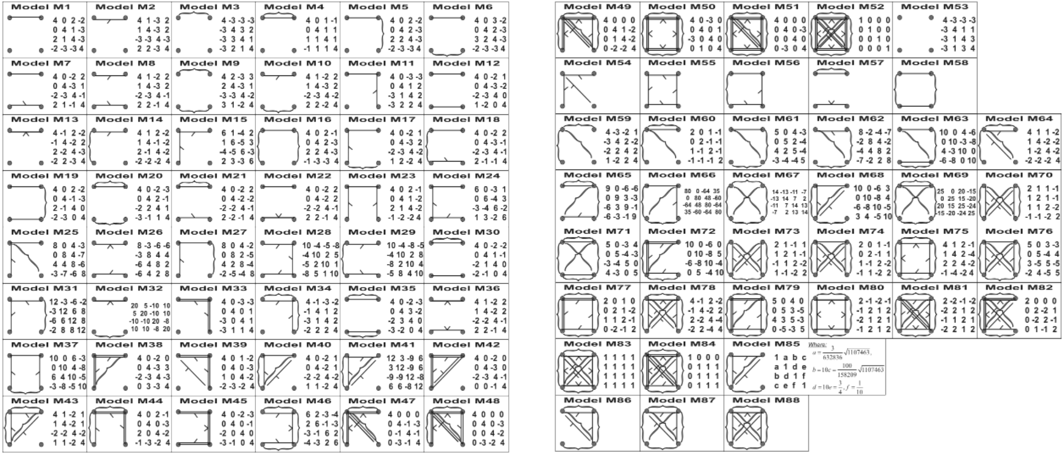
$$
\begin{array}{c}
\\ \mathrm{p}_1 \\ \vdots \\ \mathrm{p}_n \\ \mathrm{l}_1 \\ \vdots \\ \mathrm{l}_m \\ \mathrm{x} \\ \mathrm{y} \\ \mathrm{z}
\end{array}
\begin{array}{c}
\begin{array}{ccc|ccc|ccc}
\mathrm{p}_1 & \cdots & \mathrm{p}_n & \mathrm{l}_1 & \cdots & \mathrm{l}_m & \mathrm{x} & \mathrm{y} & \mathrm{z}
\end{array} \\
\left(\begin{array}{ccc|ccc|ccc}
p_1^* & & \langle p, p' \rangle & & & & p_1^x & p_1^y & p_1^z \\
 & \ddots & & & \langle p, \ell \rangle & & & \vdots & \\
\langle p', p \rangle & & p_n^* & & & & p_n^x & p_n^y & p_n^z \\
\hline
 & & & \ell_1^* & & \langle \ell, \ell' \rangle & \ell_1^x & \ell_1^y & \ell_1^z \\
 & \langle \ell, p \rangle & & & \ddots & & & \vdots & \\
 & & & \langle \ell', \ell \rangle & & \ell_m^* & \ell_m^x & \ell_m^y & \ell_m^z \\
\hline
p_1^x & & p_n^x & \ell_1^x & & \ell_m^x & 1 & 0 & 0 \\
p_1^y & \cdots & p_n^y & \ell_1^y & \cdots & \ell_m^y & 0 & 1 & 0 \\
p_1^z & & p_n^z & \ell_1^z & & \ell_m^z & 0 & 0 & 1
\end{array}\right)
\end{array}
$$

Universality theorems



More than computational complexity travels along those arcs!

Certification of consistency



Petr Šimeček. "Gaussian representation of independence models over four random variables".
In: *COMPSTAT conference*. 2006

Consistency certification is hard

Šimeček's Question (2006)

Does every non-empty Gaussian CI model contain a rational point?

Or: can every wrong inference rule be refuted over $\mathbb{Q}$?

Consistency certification is hard

Šimeček's Question (2006)

Does every non-empty Gaussian CI model contain a rational point?

Or: can every wrong inference rule be refuted over $\mathbb{Q}$?

Model M85

$$\begin{matrix} 1 & a & b & c \\ a & 1 & d & e \\ b & d & 1 & f \\ c & e & f & 1 \end{matrix}$$

Where:

$$a = \frac{3}{632836}\sqrt{1107463},$$

$$b = 10c = \frac{100}{158209}\sqrt{1107463}$$

$$d = 10e = \frac{3}{4}, f = \frac{1}{10}$$

$$\begin{pmatrix} 1 & -1/17 & -49/51 & -7/17 \\ -1/17 & 1 & 1/3 & 1/7 \\ -49/51 & 1/3 & 1 & 3/7 \\ -7/17 & 1/7 & 3/7 & 1 \end{pmatrix}$$

Consistency certification is hard

Šimeček's Question (2006)

Does every non-empty Gaussian CI model contain a rational point?

Or: can every wrong inference rule be refuted over $\mathbb{Q}$?

Theorem

For every finite real extension $\mathbb{K}$ of $\mathbb{Q}$ there exists a CI model $\mathcal{M}$ such that $\mathcal{M} \cap \mathrm{PD}_N(\mathbb{K}) \neq \varnothing$ but $\mathcal{M} \cap \mathrm{PD}_N(\mathbb{L}) = \varnothing$ for all proper subfields $\mathbb{L} \subsetneq \mathbb{K}$.

References

- Tobias Boege. “The Gaussian conditional independence inference problem”. PhD thesis. OvGU Magdeburg, 2022.
- Jürgen Bokowski and Bernd Sturmfels. *Computational synthetic geometry*. Vol. 1355. Lecture Notes in Mathematics. Springer, 1989.
- Tillmann Miltzow and Reinier F. Schmiermann. *On Classifying Continuous Constraint Satisfaction Problems*. 2021. DOI: 10.48550/ARXIV.2106.02397. URL: https://arxiv.org/abs/2106.02397.
- Jürgen Richter-Gebert. *Perspectives on projective geometry. A guided tour through real and complex geometry*. Springer, 2011, pp. xxii + 571.
- Petr Šimeček. “Gaussian representation of independence models over four random variables”. In: *COMPSTAT conference*. 2006.