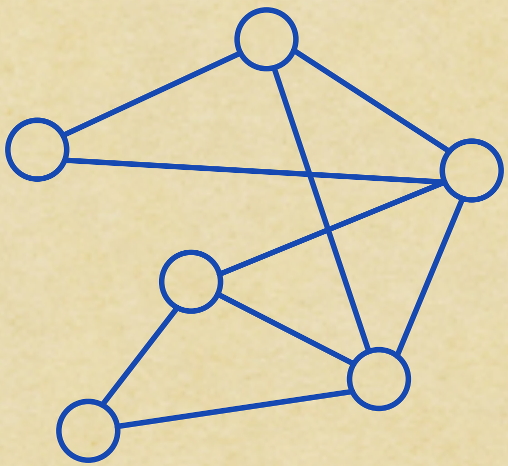
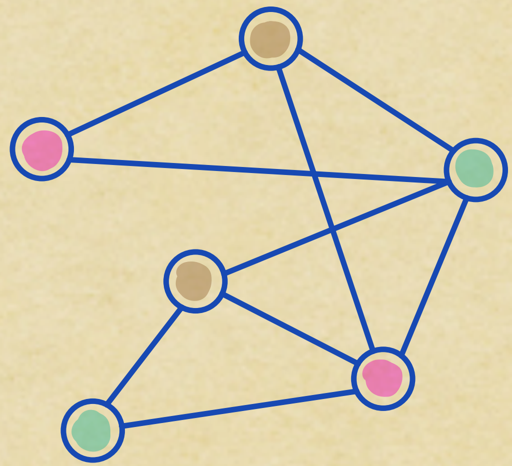
Proof Complexity Meets Finite Model Theory

Joanna Fijalkow
CNRS, University of Bordeaux

CAALM 2025
Villetaneuse, 3 June 2025

Is the graph G 3-colorable?





How complex is ...

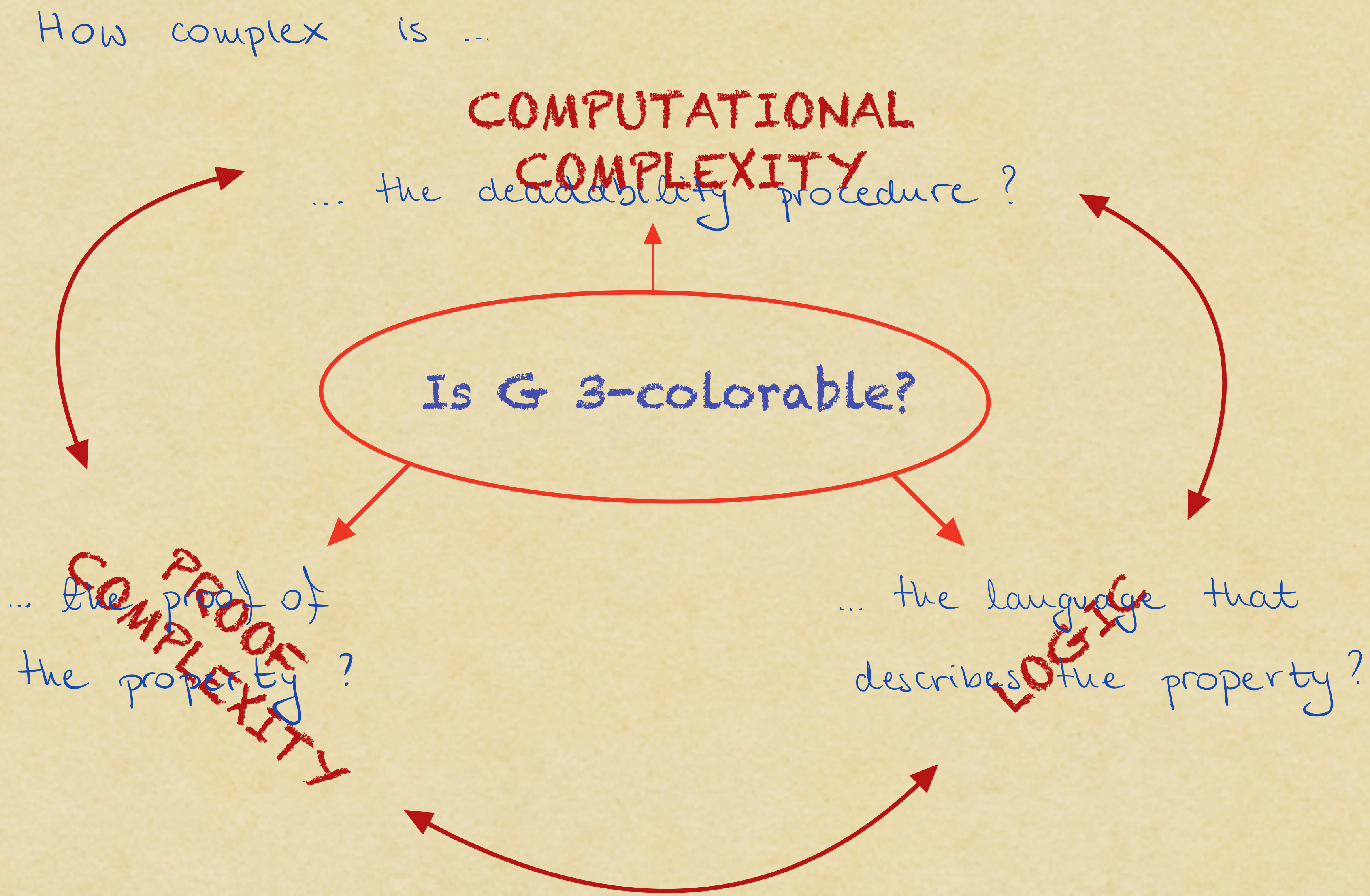
... the decidability procedure ?

Is G 3-colorable?

... the proof of the property ?

... the language that describes the property ?

(Inspired by Antonina Kolokolova.)



OUTLINE

- introduction
- pebble games
- expressibility of proof search
- trade-offs

PROPOSITIONAL FORMULAS

variable — negated variable — literals

$$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_3)$$

clause (disjunction of literals)

CNF - Conjunctive Normal Form

conjunction of clauses

PROOF SYSTEM (Cook & Reckhow '79)

YOU: give me a proportional formula F

ME: give you a candidate proof π of $F \in \text{UNSAT}$

YOU: check in time polynomial in the size of (π, F) that π indeed certifies that $F \in \text{UNSAT}$

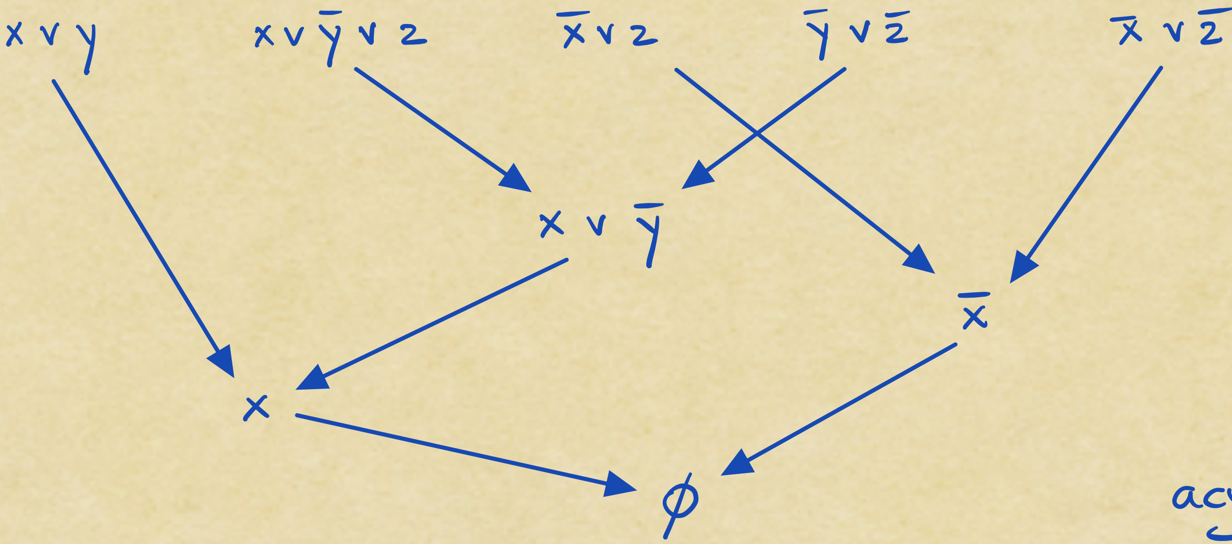
Proof of unsatisfiability = refutation

RESOLUTION RULE

$$\frac{B \vee x \qquad C \vee \bar{x}}{B \vee C}$$

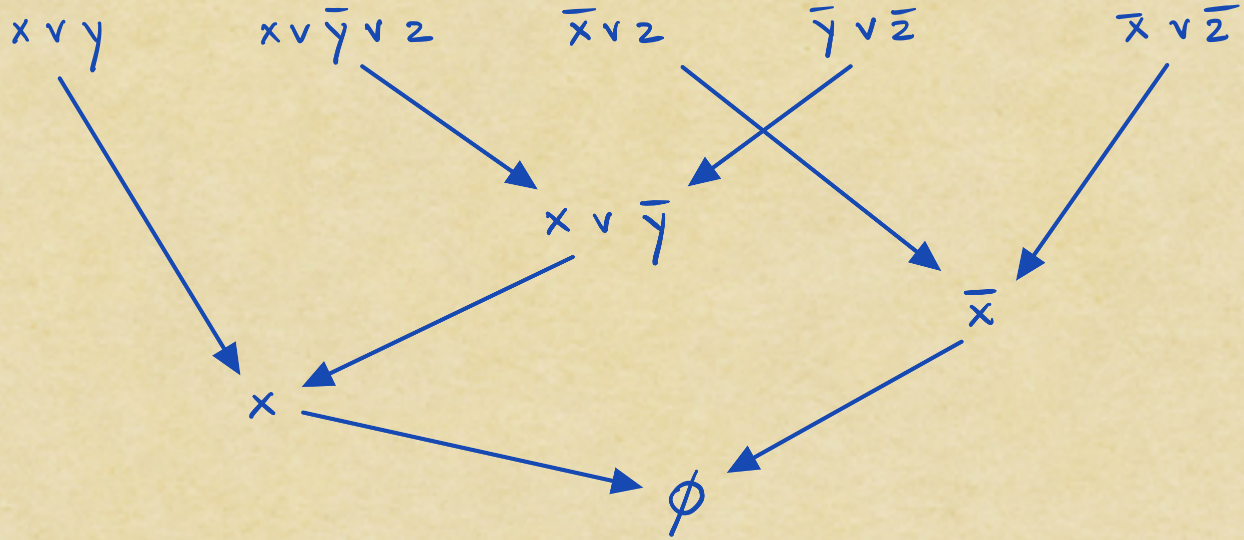
resolvent → $B \vee C$

$$(x \vee y) \wedge (x \vee \bar{y} \vee z) \wedge (\bar{x} \vee z) \wedge (\bar{y} \vee \bar{z}) \wedge (\bar{x} \vee \bar{z})$$



directed acyclic graph

COMPLEXITY MEASURES



size = number of nodes (9)

width = max clause size (3)

depth = max path length (3)

MOTIVATIONS

- rule out large families of P-time algorithms for problems in NP by studying lower bounds for specific proof systems

- translate upper bounds to efficient algorithms

- model methods of reasoning used by SAT solvers, prove upper and lower bounds for these systems

Finite model theory is the study of the expressive power of logic on finite structures.

MOTIVATIONS

- database theory
- verification
- automata theory

COMPLEXITY MEASURES

number of variables

quantifier depth = max nesting of quantifiers

EXAMPLE:

exists a directed path of length 4

$$\exists x \exists y \, (E(x,y) \wedge \exists x \, (E(y,x) \wedge \exists y \, (E(x,y) \wedge \exists x \, E(y,x))))$$

THEOREM (Atserias & Dalmau '08)

Let F be a k-CNF. F has a resolution refutation of width k iff Spoiler wins the existential $(k+1)$-pebble game on $M(F)$ and $\mathbb{T}_k$.

THEOREM (Ben-Sasson & Wigderson '01)

Let F be a 3-CNF. If every resolution refutation of F requires width k, then every resolution refutation of F requires size $2^{\Omega(k^2/n)}$, where n is the number of variables.

(finite relational) structure $\mathbb{A} = (A; R_1, \dots, R_n)$, with $R_1 \subseteq A^{k_1}$, …, $R_n \subseteq A^{k_n}$

(finite) universe → A

EXAMPLE: directed graph $G = (V; E)$, $E \subseteq V^2$

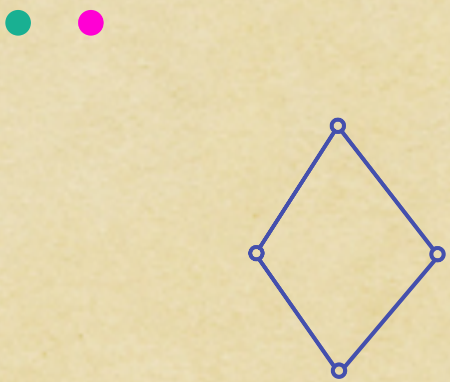
$\mathbb{A} = (A; R_1^{\mathbb{A}}, \dots, R_n^{\mathbb{A}})$ $\qquad$ $\mathbb{B} = (B; R_1^{\mathbb{B}}, \dots, R_n^{\mathbb{B}})$

homomorphism $\quad f: A \to B \qquad f(R_i^{\mathbb{A}}) \subseteq R_i^{\mathbb{B}}$

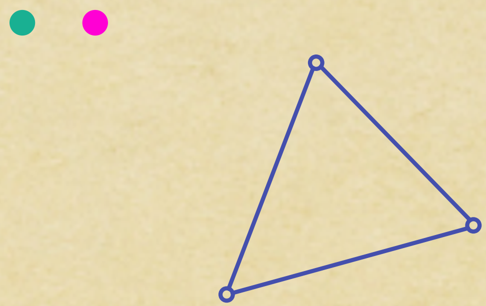
EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler



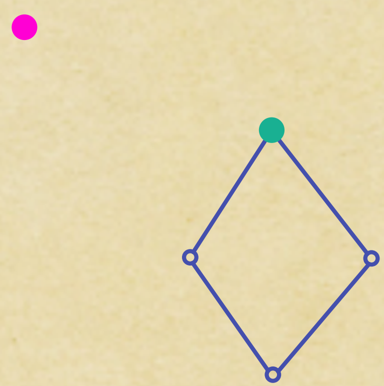
Duplicator



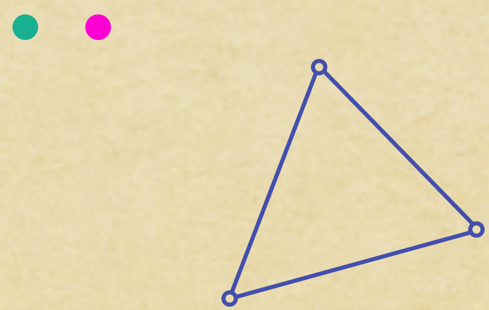
EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler



Duplicator



EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler | Duplicator

EXISTENITAL k-PEBBLE GAME

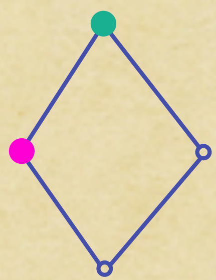
$k = 2$

Spoiler Duplicator

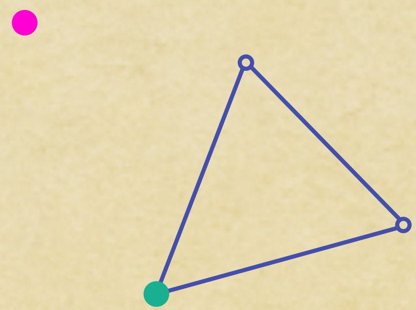
EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler



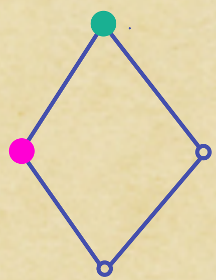
Duplicator



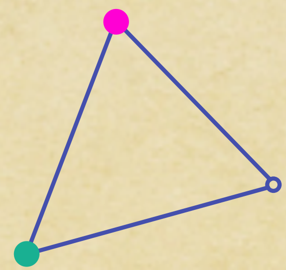
EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler



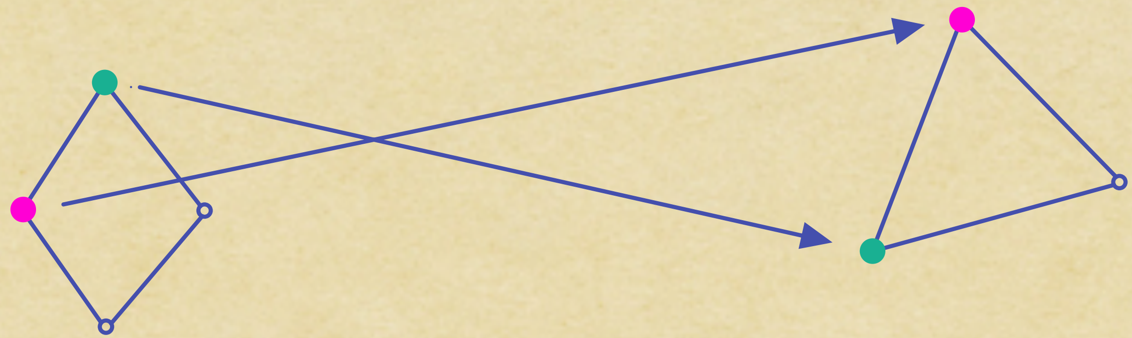
Duplicator



EXISTENITAL k-PEBBLE GAME

k = 2

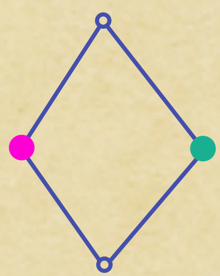
Spoiler Duplicator



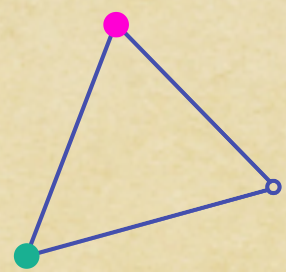
EXISTENITAL K-PEBBLE GAME

$k = 2$

Spoiler



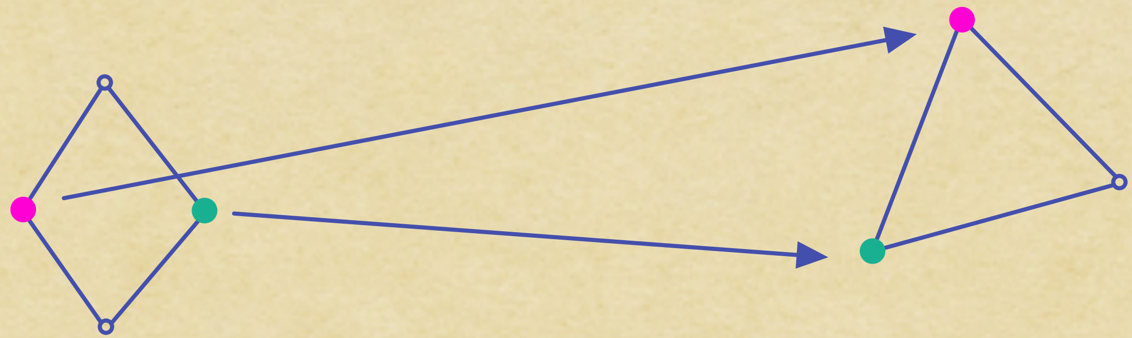
Duplicator



EXISTENITAL k-PEBBLE GAME

$k = 2$

Spoiler — Duplicator



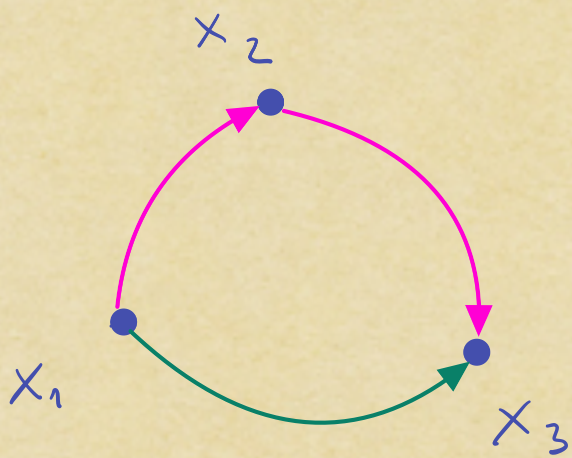
THEOREM (Kolaitis & Vardi '90)

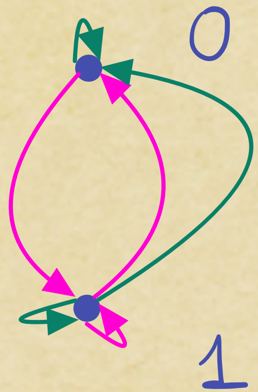
Duplicator has a winning strategy in the existential k-pebble game on $\mathbb{A}$ and $\mathbb{B}$ iff every sentence of the existential positive k-variable fragment of FO satisfied by $\mathbb{A}$ is also satisfied by $\mathbb{B}$.

THEOREM (Atserias & Dalmau '08)

Let F be a k-CNF. F has a resolution refutation of width k iff Spoiler wins the existential $(k+1)$-pebble game on $M(F)$ and $\mathbb{T}_k$.

$$(x_1 \vee x_2) \wedge (x_2 \vee x_3) \wedge (x_1 \vee \bar{x}_3)$$

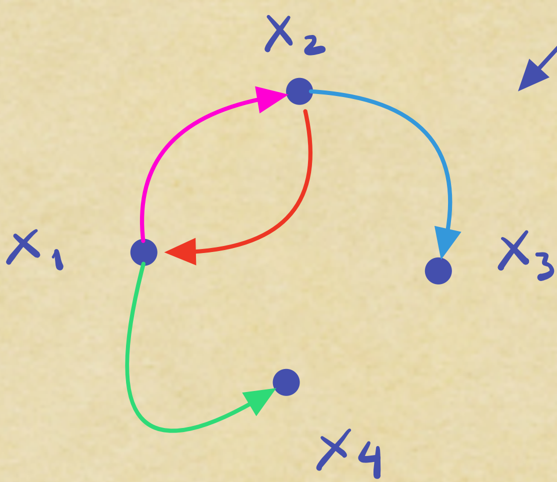




$$R_{00} = \{0,1\}^2 \setminus \{(0,0)\}$$

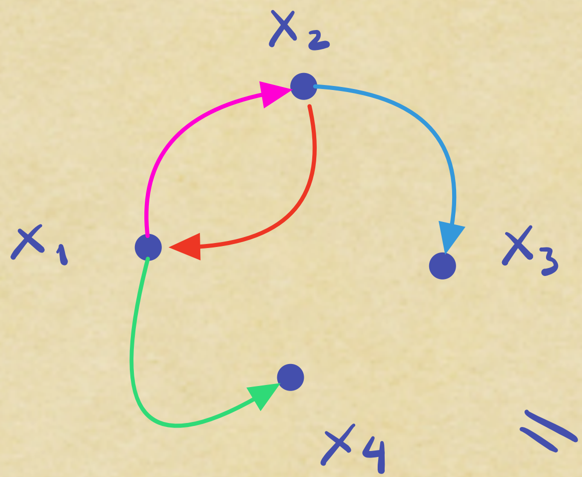
$$R_{01} = \{0,1\}^2 \setminus \{(0,1)\}$$

$$(x_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge (x_1 \vee \bar{x}_4) \wedge (\bar{x}_2 \vee \bar{x}_1)$$



$$(\{0,1\};\ R_{00}, R_{10}, R_{01}, R_{11}) = \Pi_2$$

$F: \quad (x_1 \lor x_2) \land (\bar{x}_2 \lor x_3) \land (x_1 \lor \bar{x}_4) \land (\bar{x}_2 \lor \bar{x}_1)$



$= M(F)$

$(\{0,1\};\ R_{00}, R_{10}, R_{01}, R_{11}) = \Pi_2$

Π_k defined similarly for k-CNF

THEOREM (Atserias & Dalmau '08)

Let F be a k-CNF. F has a resolution refutation of width k iff Spoiler wins the existential $(k+1)$-pebble game on $M(F)$ and $\mathbb{T}_k$.

- allowed to rederive all previously known width lower bounds
- complexity of resolution width problem (Berkholz '12)
- PC space & resolution width (Galesi, Thapen, Kołodziejczyk '19)

EXPRESSIBILITY OF PROOF SEARCH

width-k resolution → $\exists FP^{O(k)}$

degree-k Sherali-Adams → $FPC^{O(k)}$

degree-k Sum-of-Squares → $C^{O(k)}_{\infty\omega}$

Atserias & Dalmau '08
Grädel et al. '19

Atserias & F. '18

Anderson et al. '15

SEMIALGEBRAIC PROOF SYSTEMS

(equation ≈ pair of inequalities)

$q_1 \geq 0 \;,\; q_2 \geq 0 \;, \dots ,\; q_k \geq 0$

sum of squares of polynomials

SOS refutation : $\sum_j p_j s_j = -1$

$$\cap$$

$$\{ q_1, \dots, q_k, 1, x_i, 1-x_i, x_i^2 - x_i, x_i - x_i^2 \}$$

$$\cup$$

SA refutation : $\sum_j p_j m_j = -1$

extended monomials : $c \prod x_i \prod (1 - x_j)$, $c \geq 0$

$$-x^2 - y - 2 \geq 0$$

$$x - y^2 + 3 \geq 0$$

sum of squares of polynomials

$$6\left(-x^2 - y - 2\right) + 2\left(x - y^2 + 3\right) + \frac{1}{3} + 2\left(y + \frac{3}{2}\right)^2 + 6\left(x - \frac{1}{6}\right)^2$$

$$\parallel$$

$$-1$$

SOUND AND COMPLETE

$q_1 \geq 0, \dots, q_k \geq 0$ has no 0/1 solution

$\Updownarrow$

there is a SA refutation

$\Updownarrow$

there is a SOS refutation

POLYNOMIAL EQUATIONS ENCODING

$x \vee \bar{y} \vee z \longrightarrow (1-x)\,y\,(1-z) = 0$

the same satisfying 0/1 assignments
(anything but $x \mapsto 0, y \mapsto 1, z \mapsto 0$)

CNF $\longrightarrow$ system of polynomial equations

UNSAT iff no 0/1 solutions

POLYNOMIAL INEQUALITIES ENCODING

$x \vee \bar{y} \vee z \longrightarrow x + (1-y) + z - 1 \geq 0$

the same satisfying 0/1 assignments
(anything but $x \mapsto 0, y \mapsto 1, z \mapsto 0$)

CNF $\longrightarrow$ system of polynomial inequalities

UNSAT iff no 0/1 solutions

COMPLEXITY MEASURES

$$\{ q_1, \dots, q_k, 1, x_i, 1 - x_i, x_i^2 - x_i, x_i - x_i^2 \}$$

$$\cup$$

$$\sum_j p_j m_j = -1$$

extended monomials: $c \prod x_i \prod (1 - x_j)$, $\quad c \geq 0$

<u>degree</u> = max degree of $p_j m_j$

<u>size</u> = bit-complexity

<u>monomial-size</u> = number of monomials

DEGREE d SHERALI-ADAMS

$$\{q_1, \dots, q_k, 1, x_i, 1-x_i, x_i^2 - x_i, x_i - x_i^2\}$$

$$\sum_i p_j m_j = -1 \qquad \deg(p_j m_j) \le d$$

$$c \prod x_i \prod (1-x_i) \qquad c \ge 0$$

deciding whether degree-d SA refutation exists

$\leq$

deciding feasibility of a LP

DEGREE - d SUM - OF - SQUARES

deciding whether degree-d SOS refutation exists

$\Updownarrow$

deciding feasibility of a SDP

Semidefinite program :

$$X \succcurlyeq 0$$

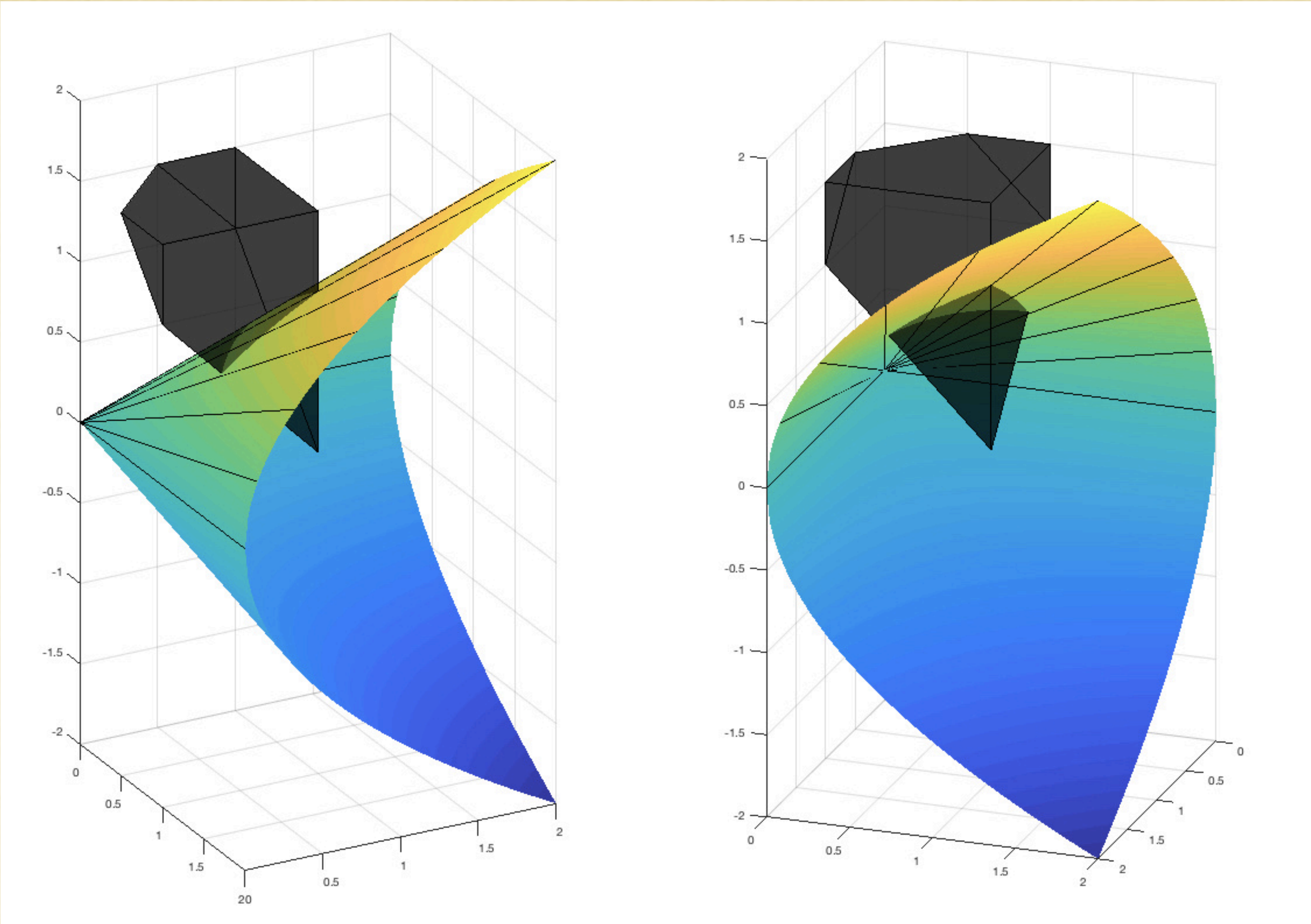
$$AX \leq b$$

X - symmetric

$z^T X z \geq 0 \quad \forall z$

$\Updownarrow$

$X = Y^T Y$



THEOREM (Anderson & Dawar & Holm '15)

Feasibility of LPs is expressible in FPC.

THEOREM (Atserias & F. '19)

Feasibility of SDPs is expressible in $C^{\omega}_{\infty\omega}$.

PROOF SEARCH FOR DEGREE d SOS

T - system of polynomial inequalities

encoding of SDP

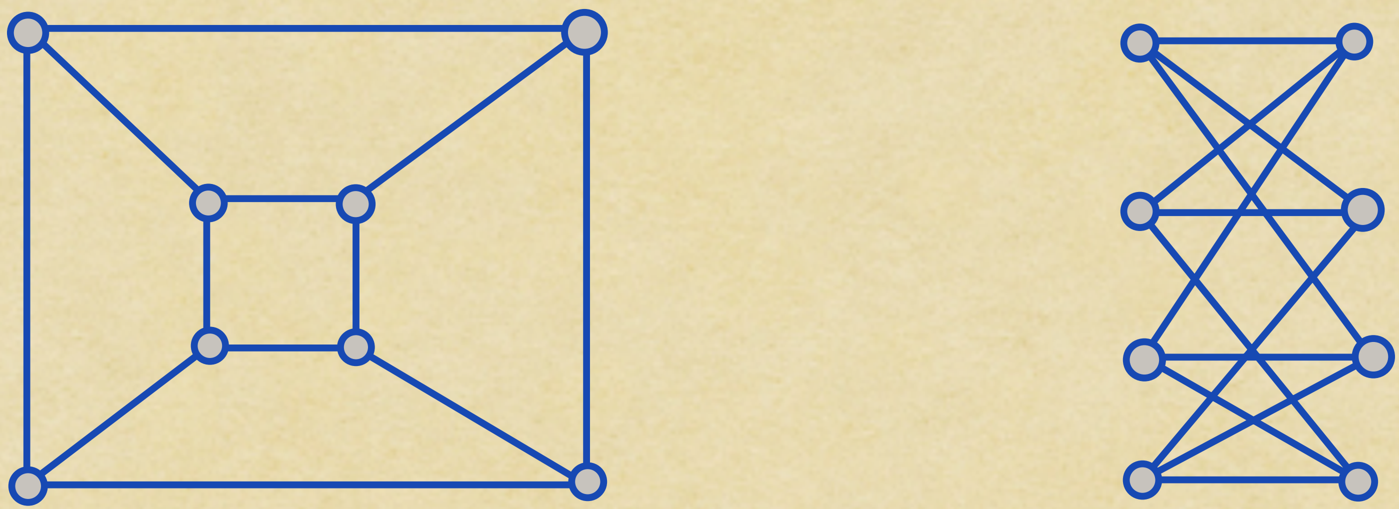
$$\Pi \xrightarrow{\ \psi_d\ } \mathbb{P}_T \xrightarrow{\ \varphi\ } 0/1$$

$C^{O(d)}_{\infty\omega}$ interpretation (→ ψ_d)

$C^{c}_{\infty\omega}$ formula for SDP feasibility (→ φ)

$$\varphi(\psi_d) \longleftarrow C^{O(d)}_{\infty\omega}$$ formula for proof search

GRAPH ISOMORPHISM PROBLEM



ISO (G, H) :

$$\sum_{w \in V(H)} x_{vw} - 1 = 0 \qquad \forall \ v \in V(G)$$

$$\sum_{v \in V(G)} x_{vw} - 1 = 0 \qquad \forall \ w \in V(H)$$

$$x_{vw} \, x_{v'w'} = 0 \qquad (v,v') \in E(G) \, , \, (w,w') \notin E(H)$$

$$x_{vw} \, x_{v'w'} = 0 \qquad (v,v') \notin E(G) \, , \, (w,w') \in E(H)$$

ISO (G, H) has a 0/1 solution

$\Updownarrow$

G and H are isomorphic

ISO (G, H) has a degree d SA refutation

$\Downarrow$ (Berkholz & Grohe '15)

ISO (G, H) has a degree d PC refutation

$\Downarrow$ (Berkholz '18)

ISO (G, H) has a degree 2d SOS refutation

$\Downarrow$ (Atserias & F. '19)

ISO (G, H) has a degree cd SA refutation

THEOREM (Cai & Fürer & Immerman '92)

There is a family of pairs of non-isomorphic 3-regular graphs (G_n, H_n) with $O(n)$ vertices such that $G_n \equiv^n H_n$.

↑ satisfy the same sentences of $C^n_{\infty\omega}$

THEOREM (Cai & Fürer & Immerman '92)

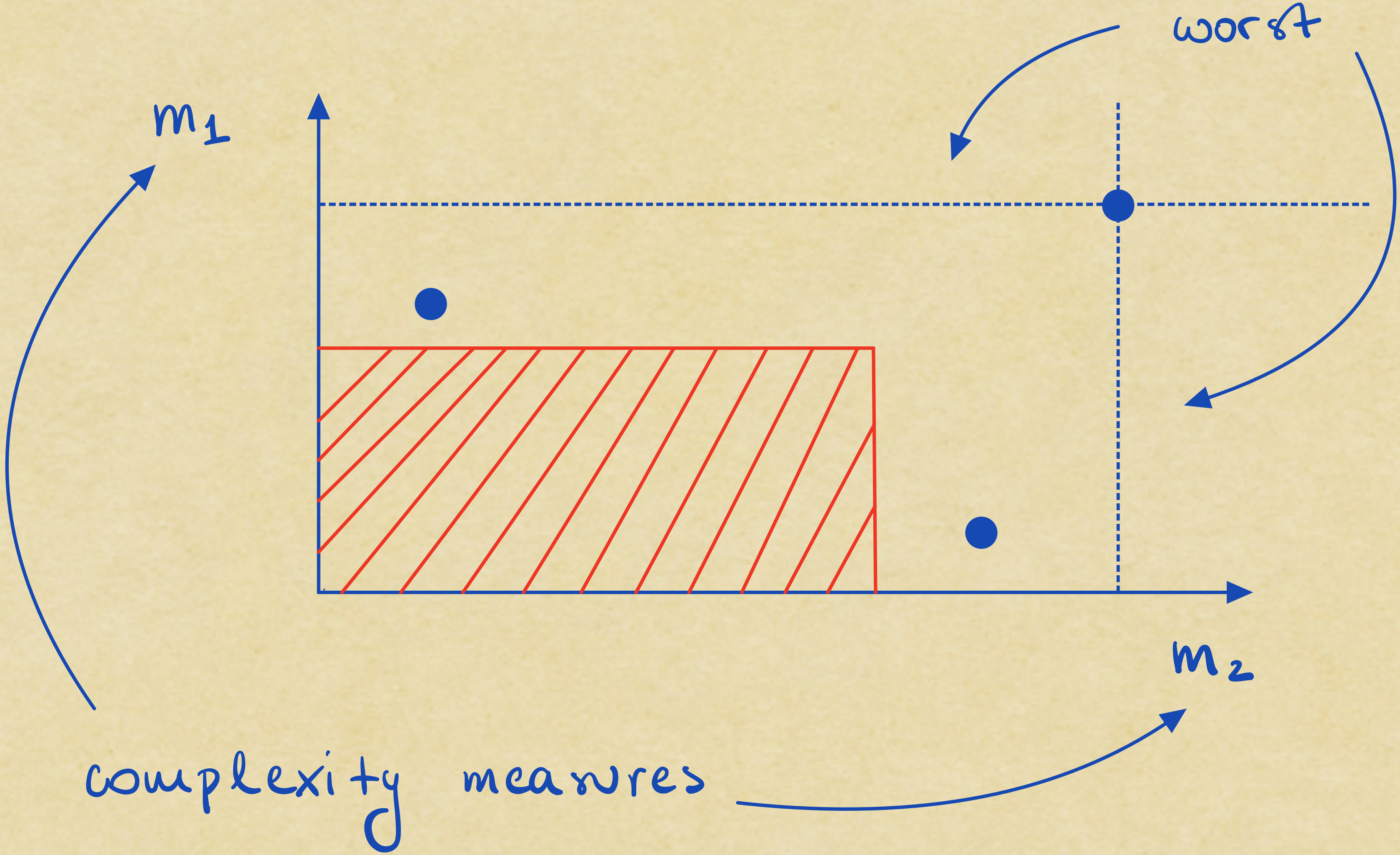
There is a family of pairs of non-isomorphic 3-regular graphs (G_n, H_n) with $O(n)$ vertices such that $G_n \equiv^n H_n$.

THEOREM (O'Donnell et al., Codenotti et al. '14)

$ISO(G,H)$ requires degree $\Omega(n)$ to refute in SOS.

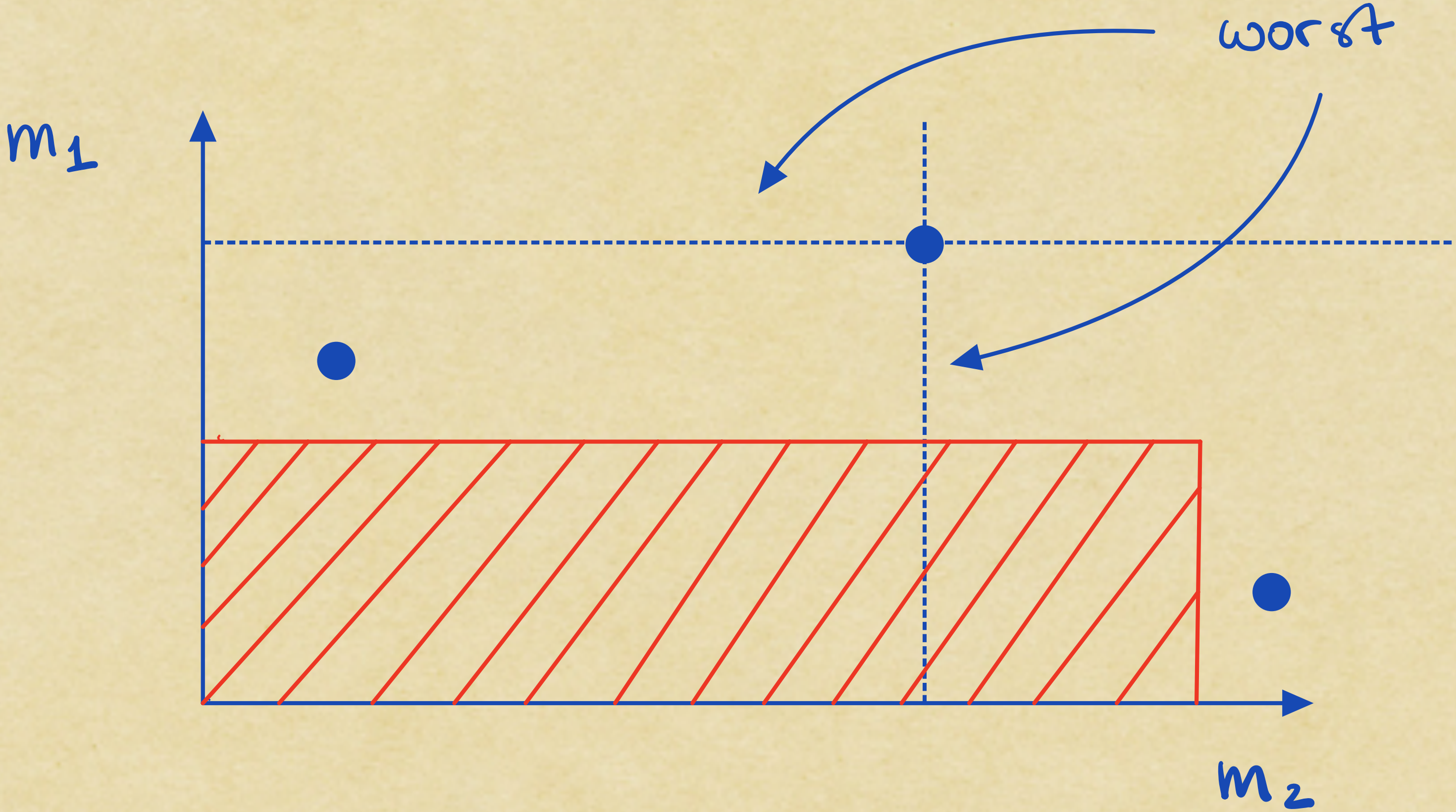
TRADE-OFF RESULTS

(Inspired by Jakob Nordström.)

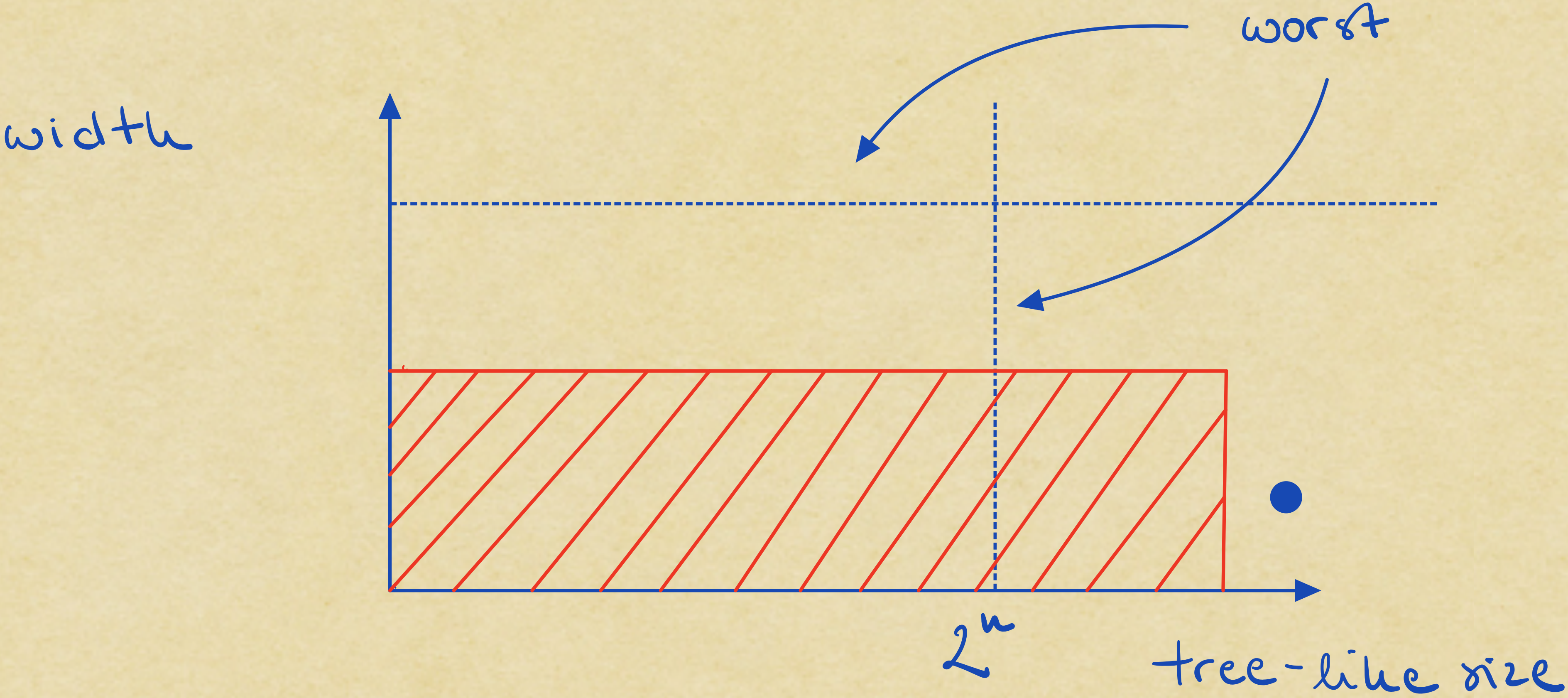


impossible to optimise both

SUPERCRITICAL TRADE-OFF

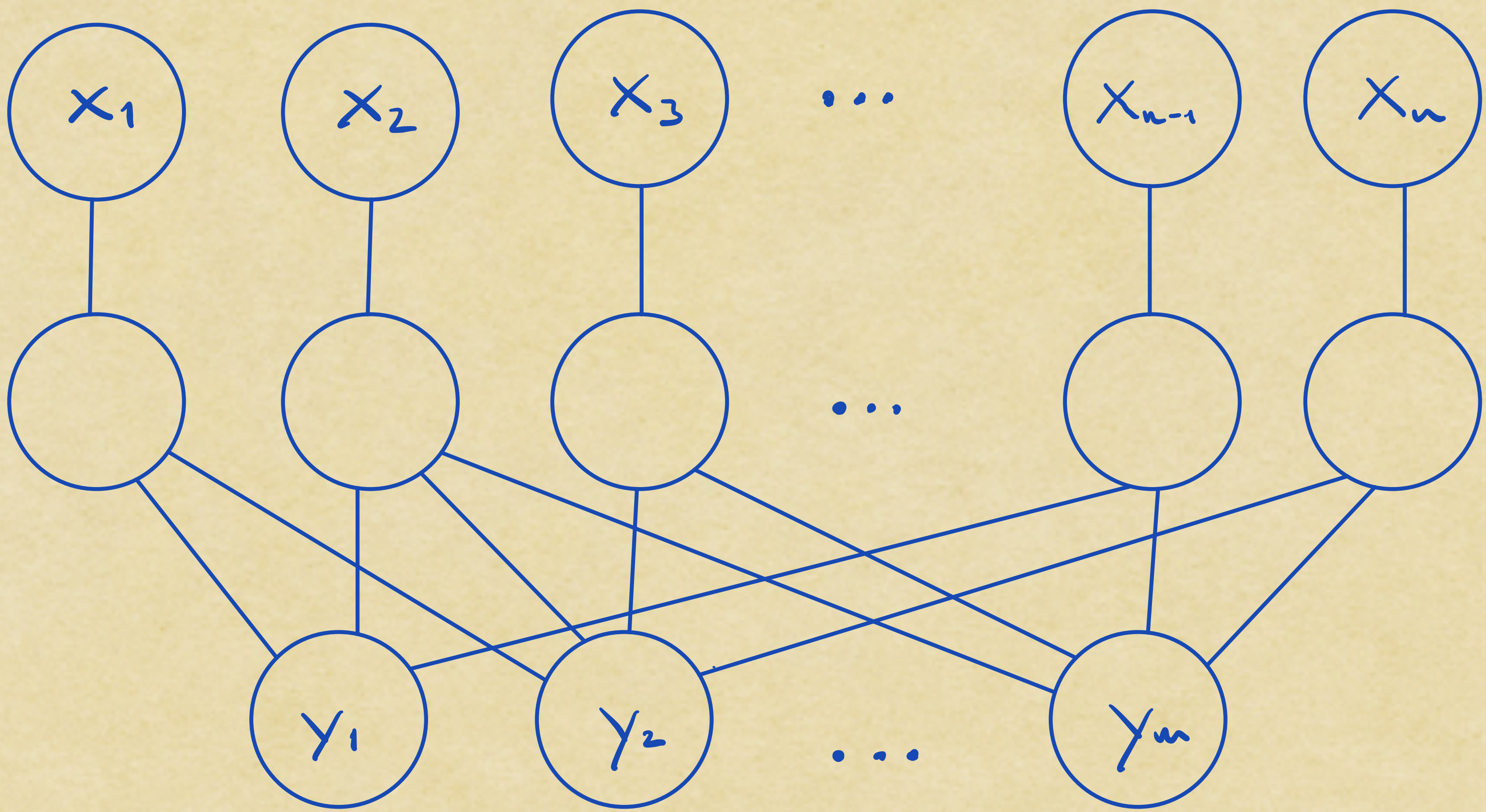


TREE-LIKE RESOLUTION

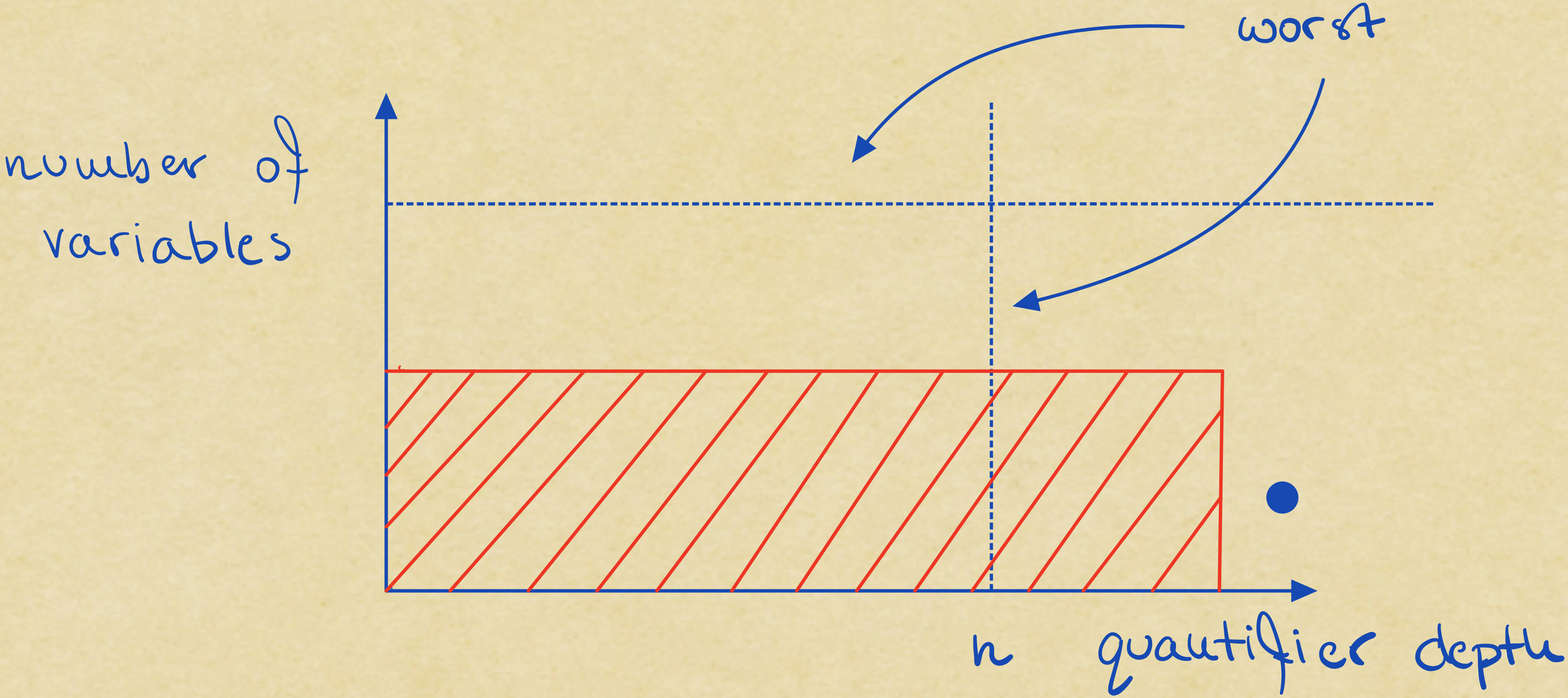


Razborov '16

HARDNESS CONDENSATION

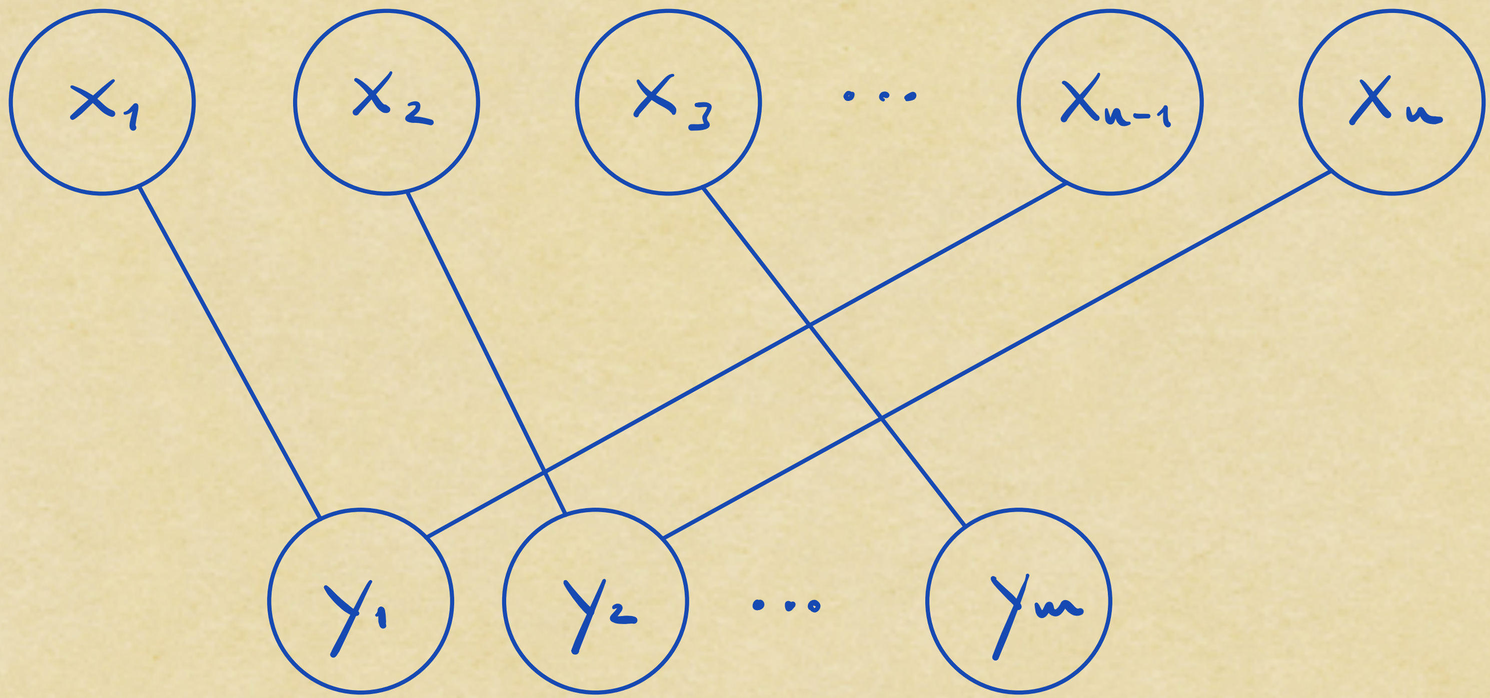


FO (WITH COUNTING QUANTIFIERS)



Berkholz & Nordström '16

VARIABLE COMPRESSION



Grohe, Lichter, Neuen, Schweitzer '23

STRENGTHENING THE COMPRESSION

de Rezende, Fleming, Janett, Nordström, Pang '25

- width vs depth for resolution
- size vs depth for resolution
- size vs depth for cutting planes
- size vs depth for monotone circuits
- number of variables vs quantifier depth for FO (with counting quantifiers)

Thank you!