First-Order logic (FO)

First-Order logic (FO)

First-Order logic (FO)

FO = First-Order logic

Vocabulary	<u>Relational symbols</u>:	$\Sigma = \{R, S, T, \ldots\}$	(aka <u>signature</u>)
	<u>Variables</u>:	$x, y, \ldots, x_1, x_2, \ldots$	
	<u>Quantifiers</u>:	$\exists, \forall$	
	Boolean connectives:	$\vee, \wedge, \neg, \rightarrow, \leftrightarrow$	

FO = First-Order logic

Vocabulary	Relational symbols:	$\Sigma = \{R, S, T, ...\}$	(aka signature)
	Variables:	$x, y, ..., x_1, x_2, ...$	
	Quantifiers:	$\exists, \forall$	
	Boolean connectives:	$\vee, \wedge, \neg, \rightarrow, \leftrightarrow$	

Syntax $\quad \phi : \quad R(x_1,\dots,x_k) \mid \dots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\exists x\, \phi \mid \forall x\, \phi \mid \dots$

FO = First-Order logic

Vocabulary

Relational symbols:	$\Sigma = \{R, S, T, \dots\}$	(aka signature)
Variables:	$x, y, \dots, x_1, x_2, \dots$	
Quantifiers:	$\exists, \forall$	
Boolean connectives:	$\vee, \wedge, \neg, \rightarrow, \leftrightarrow$	

Syntax

$\phi : \quad R(x_1,\dots,x_k) \mid \dots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\quad\quad \exists x\, \phi \mid \forall x\, \phi \mid \dots$

Semantics

Now a model consists of a universe U^M

+ some mappings $R \mapsto R^M \subseteq U^M \times \dots \times U^M$

$x \mapsto x^M \in U^M$

FO = First-Order logic

Vocabulary

- Relational symbols: $\Sigma = \{R, S, T, \ldots\}$ (aka signature)
- Variables: $x, y, \ldots, x_1, x_2, \ldots$
- Quantifiers: $\exists, \forall$
- Boolean connectives: $\vee, \wedge, \neg, \rightarrow, \leftrightarrow$

Syntax

$$\phi : \quad R(x_1,\ldots,x_k) \;|\; \ldots \;|\; \phi \vee \phi \;|\; \phi \wedge \phi \;|\; \neg\phi \;|\; \phi \rightarrow \phi \;|\; \phi \leftrightarrow \phi$$
$$\exists x\, \phi \;|\; \forall x\, \phi \;|\; \ldots$$

Semantics

Now a model consists of a universe U^M

+ some mappings $R \mapsto R^M \subseteq U^M \times \ldots \times U^M$

$x \mapsto x^M \in U^M$

$M \models \phi_1 \vee \phi_2$ iff $M \models \phi_1$ or $M \models \phi_2$

…

$M \models R(x_1,\ldots,x_k)$ iff $(x_1^M,\ldots,x_k^M) \in R^M$

$M \models \exists x\, \phi$ iff $M[x:=u] \models \phi$ for *some* $u \in U^M$

$M \models \forall x\, \phi$ iff $M[x:=u] \models \phi$ for *every* $u \in U^M$

Examples

Syntax $\phi : \quad R(x_1,\ldots,x_k) \mid \ldots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \to \phi \mid \phi \leftrightarrow \phi$

$\exists x\ \phi \mid \forall x\ \phi \mid \ldots$

"All humans are mortal. Socrates is human. So Socrates is mortal."

$$\phi(y) = ((\forall x\ A(x) \to B(x))\ \&\ A(y)) \to B(y)$$

Examples

Syntax $\quad \phi : \quad R(x_1,\ldots,x_k) \mid \ldots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\quad \exists x\, \phi \mid \forall x\, \phi \mid \ldots$

"All humans are mortal. Socrates is human. So Socrates is mortal."

$$\phi(y) = ((\forall x\, A(x) \rightarrow B(x)) \,\&\, A(y)) \rightarrow B(y)$$

M : $\quad U^M = \{\text{Socrates, Plato, Cyclop, Jupiter}\}$

$\quad A^M = \{\text{Socrates, Plato}\}$

$\quad B^M = \{\text{Socrates, Plato, Cyclop}\}$

$\quad y^M = \text{Socrates}$

Examples

Syntax $\phi : \quad R(x_1,\ldots,x_k) \;|\; \ldots \;|\; \phi \vee \phi \;|\; \phi \wedge \phi \;|\; \neg\phi \;|\; \phi \to \phi \;|\; \phi \leftrightarrow \phi$

$\exists x\, \phi \;|\; \forall x\, \phi \;|\; \ldots$

"There is a node in the graph that is isolated from all other nodes."

$$\phi = \exists x\, \forall y\, \neg(x=y) \to \neg E(x,y)$$

Examples

Syntax $\phi : \quad R(x_1,\dots,x_k) \mid \dots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\exists x\, \phi \mid \forall x\, \phi \mid \dots$

"There is a node in the graph that is isolated from all other nodes."

$$\phi = \exists x\, \forall y\, \neg(x=y) \rightarrow \neg E(x,y)$$

M : U^M = {nodes of a graph}
E^M = {edges of a graph}

Examples

Syntax $\phi : \quad R(x_1,\ldots,x_k) \;|\; \ldots \;|\; \phi \lor \phi \;|\; \phi \land \phi \;|\; \neg\phi \;|\; \phi \to \phi \;|\; \phi \leftrightarrow \phi$

$\exists x\, \phi \;|\; \forall x\, \phi \;|\; \ldots$

Examples

Syntax ϕ : $R(x_1,\ldots,x_k)$ | … | $\phi \vee \phi$ | $\phi \wedge \phi$ | $\neg\phi$ | $\phi \rightarrow \phi$ | $\phi \leftrightarrow \phi$ |
$\exists x\ \phi$ | $\forall x\ \phi$ | …

"There's a man such that when he runs, everybody runs."

$$\phi = \exists x\ R(x) \rightarrow \forall y\ R(y)$$

Examples

Syntax $\phi : \quad R(x_1,\ldots,x_k) \mid \ldots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\exists x\, \phi \mid \forall x\, \phi \mid \ldots$

"There's a man such that when he runs, everybody runs."

$$\phi = \exists x\ R(x) \rightarrow \forall y\, R(y)$$

M : $U^M = \{\text{Ben, Han, Leia, Luke}\}$

$R^M = \{\text{Ben, Han}\}$

Examples

Syntax $\quad \phi : \quad R(x_1,\ldots,x_k) \mid \ldots \mid \phi \vee \phi \mid \phi \wedge \phi \mid \neg\phi \mid \phi \rightarrow \phi \mid \phi \leftrightarrow \phi$

$\qquad\qquad \exists x\, \phi \mid \forall x\, \phi \mid \ldots$

"There's a man such that when he runs, everybody runs."

$$\phi = \exists x\; R(x) \rightarrow \forall y\, R(y)$$

$M : \quad U^M = \{\text{Ben, Han, Leia, Luke}\}$

$\qquad R^M = \{\text{Ben, Han}\}$

$M' : \quad U^{M'} = \{\text{Ben, Han, Leia, Luke}\}$

$\qquad R^{M'} = \{\text{Ben, Han, Leia, Luke}\}$

Examples

- "R is a function" $\phi = \forall x\, \exists y\; R(x,y) \;\wedge\; \forall z\, R(x,z) \rightarrow y=z$

  in this case, one can use the shorthand
  "R(x)=…" for $\exists y\, R(x,y) \;\wedge\; \forall z\, R(x,z) \rightarrow z=\ldots$

Examples

- "R is a function" $\phi = \forall x\, \exists y\ R(x,y)\ \wedge\ \forall z\, R(x,z) \rightarrow y=z$

  in this case, one can use the shorthand
  "R(x)=..." for $\exists y\, R(x,y)\ \wedge\ \forall z\, R(x,z) \rightarrow z=\ldots$

- "+ is commutative" $\phi = \forall x\, \forall y\ \ x+y = y+x$

  note: + is a ternary relational symbol, so "x+y=z" is shorthand for "+(x,y,z)"

Examples

- "R is a function" $\phi = \forall x\ \exists y\ \ R(x,y)\ \wedge\ \forall z\ R(x,z) \rightarrow y=z$

  in this case, one can use the shorthand
  "$R(x)=\ldots$" for $\exists y\ R(x,y)\ \wedge\ \forall z\ R(x,z) \rightarrow z=\ldots$

- "+ is commutative" $\phi = \forall x\ \forall y\ \ x+y = y+x$

  note: + is a ternary relational symbol, so "x+y=z" is shorthand for "+(x,y,z)"

- "+ admits *zero* and *inverses*" $\phi = \exists x_0\ \ \forall y\ \ x_0+y = y\ \wedge\ \forall y\ \exists z\ \ y+z = x_0$

Exercices

- "f is continuous" $\phi = \forall x\ \forall \varepsilon\ \exists \delta\ \forall y\ \ ||x\text{-}y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$
- "f is uniformly continuous" $\phi = \forall \varepsilon\ \exists \delta\ \forall x\ \forall y\ \ ||x\text{-}y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$

Exercices

- "f is continuous" $\phi = \forall x\ \forall \varepsilon\ \exists \delta\ \forall y\ \ ||x\text{-}y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$

- "f is uniformly continuous" $\phi = \forall \varepsilon\ \exists \delta\ \forall x\ \forall y\ \ ||x\text{-}y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$

What is an appropriate signature for the above formulas?

Exercices

- "f is continuous" $\phi = \forall x\ \forall \varepsilon\ \exists \delta\ \forall y\ \ ||x-y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$

- "f is uniformly continuous" $\phi = \forall \varepsilon\ \exists \delta\ \forall x\ \forall y\ \ ||x-y|| < \delta \rightarrow ||f(x) - f(y)|| < \varepsilon$

What is an appropriate <u>signature</u> for the above formulas?

Are the formulas equivalent? Is one a consequence of another? Can you prove it?

(hint: $\exists x\ \forall y\ \alpha \rightarrow \forall y\ \exists x\ \alpha$ *assuming universe is non-empty*)

Exercices

Choose appropriate universes and signatures, and define these properties in FO:

1. "There are infinitely many Prime numbers" $\phi = \ldots$

2. "In the tree, z is the least common ancestor of x and y" $\phi(x,y,z) = \ldots$

3. "Polynomial *p* evaluates to y on x" (for fixed *p*) $\phi_p(x,y) = \ldots$

4. "The graph is strongly connected" $\phi = \ldots$

5. "In the infinite sequence of *a*'s and *b*'s, every *a* is followed by *b*" $\phi = \ldots$

Normal forms

Prenex [+CNF/DNF] as for QBF, i.e. $\phi = Qx_1 \ldots Qx_n \ \alpha(x_1,\ldots,x_n)$

NNF (Negation Normal Form)

$\phi : \quad \exists x\, \phi \ \mid \ \forall x\, \phi \ \mid \ \phi \vee \phi \ \mid \ \phi \wedge \phi \ \mid \ \alpha$

$\alpha : \quad R(x_1,\ldots,x_k) \ \mid \ \neg R(x_1,\ldots,x_k)$

Normal forms

Prenex [+CNF/DNF] as for QBF, i.e. $\phi = Qx_1 \dots Qx_n \ \alpha(x_1,\dots,x_n)$

NNF (Negation Normal Form)

$$\phi : \quad \exists x\, \phi \ \mid\ \forall x\, \phi \ \mid\ \phi \vee \phi \ \mid\ \phi \wedge \phi \ \mid\ \alpha$$
$$\alpha : \quad R(x_1,\dots,x_k) \ \mid\ \neg R(x_1,\dots,x_k)$$

Lemma Given ϕ ($\leftrightarrow$-free), one can compute in polynomial time an *equivalent* formula ϕ^* in NNF

Proof As for propositional logic, push negations inside:

$$\neg\forall\phi \rightsquigarrow \exists\neg\phi$$
$$\neg\exists\phi \rightsquigarrow \forall\neg\phi$$
$$\neg(\phi_1 \wedge \phi_2) \rightsquigarrow \neg\phi_1 \vee \neg\phi_2$$
$$\neg(\phi_1 \vee \phi_2) \rightsquigarrow \neg\phi_1 \wedge \neg\phi_2$$

Algorithms

Model-checking problem

input: formula ϕ + *finite* model M
output: yes iff $M \models \phi$

Satisfiability problem

input: formula ϕ
output: yes iff $M \models \phi$ for *some* M

(recall: ϕ valid iff $\neg\phi$ is not satisfiable
ϕ, ϕ' equivalent iff $\phi \leftrightarrow \phi'$ is valid)

Algorithms

🎉 **PSPACE** 🎉

Model-checking problem

input: formula ϕ + *finite* model M
output: yes iff $M \vDash \phi$

💀 **UNDECIDABLE** 💀

Satisfiability problem

input: formula ϕ
output: yes iff $M \vDash \phi$ for *some* M

(recall: ϕ valid iff $\neg\phi$ is not satisfiable
ϕ, ϕ' equivalent iff $\phi \leftrightarrow \phi'$ is valid)

Algorithms — model-checking

```
Model-check(φ, M)
    if φ = R(x₁,…,xₖ) then
        if (x₁ᴹ,…,xₖᴹ) ∈ Rᴹ then
            return true
        else
            return false
    else if φ = φ₁ ∨ φ₂ then
        return Model-check(φ₁, M) OR
               Model-check(φ₂, M)
    else if …
    …
    else if φ = ∃x φ' then
        for u ∈ Uᴹ do
            if Model-check(φ', M[x:=u]) then
                return true
        return false
    else if φ = ∀x φ' then
        for u ∈ Uᴹ do
            if NOT Model-check(φ', M[x:=u]) then
                return false
        return true
```

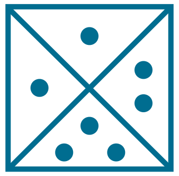
Algorithms — satisfiability

Theorem [Trakhtenbrot '50] Satisfiability of FO is undecidable

Algorithms — satisfiability

Theorem [Trakhtenbrot '50] Satisfiability of FO is undecidable

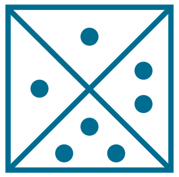
Proof by reduction from Domino (aka Tiling) problem...



Algorithms — satisfiability

Theorem [Trakhtenbrot '50] Satisfiability of FO is undecidable

Proof by reduction from Domino (aka Tiling) problem...



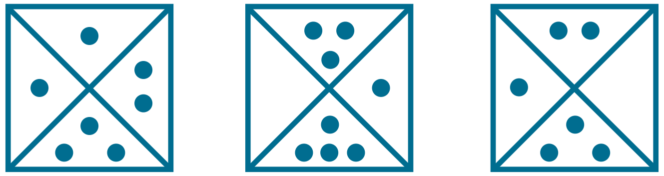
Reduction from P to P': Algorithm A that solves P by using an oracle that returns solutions to P'

(think of "P easier than P'")

e.g. many-one reduction: for all x P(x) iff P'(A(x))

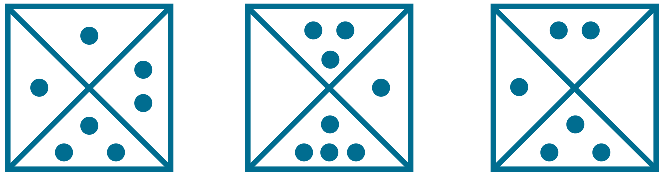
The (undecidable) Domino problem

Domino

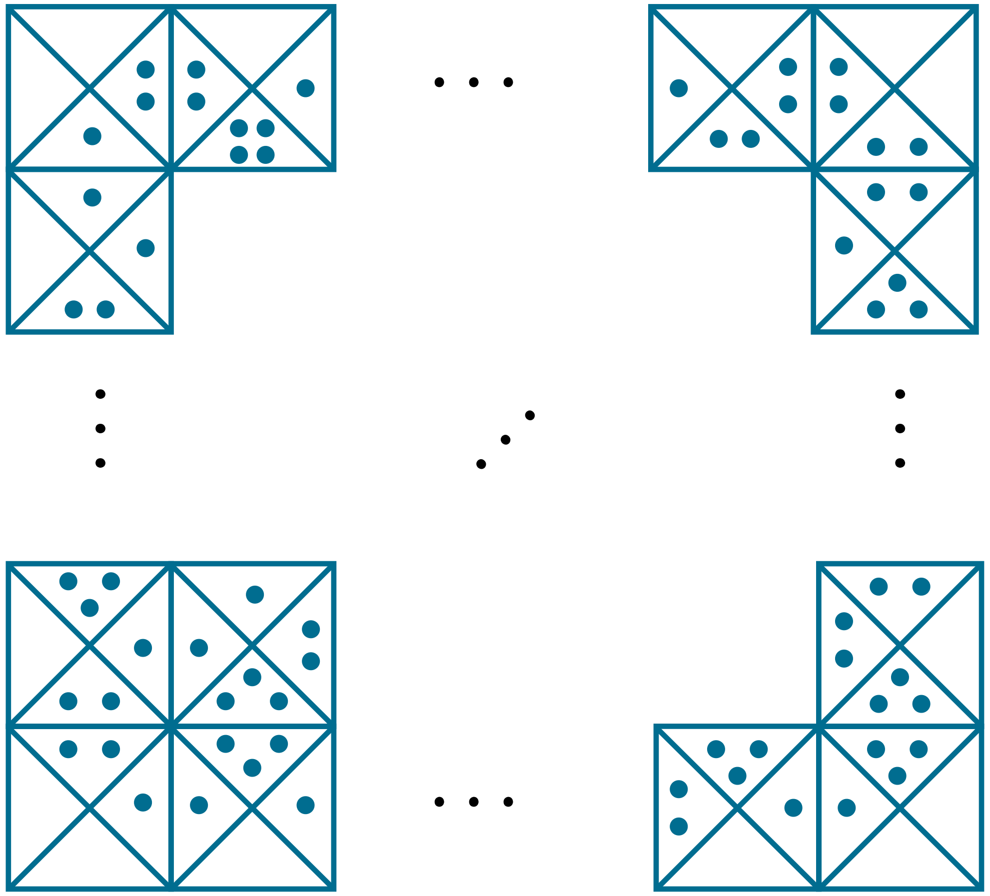
Input: 4-sided dominos: 

The (undecidable) Domino problem

Domino

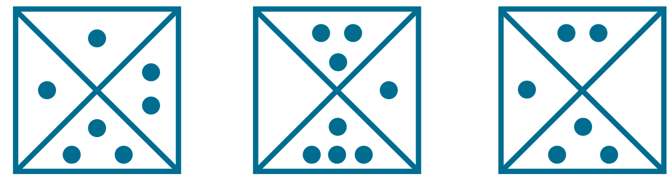
Input: 4-sided dominos: 

Output: Is it possible to form a white-bordered rectangle? (of any size)

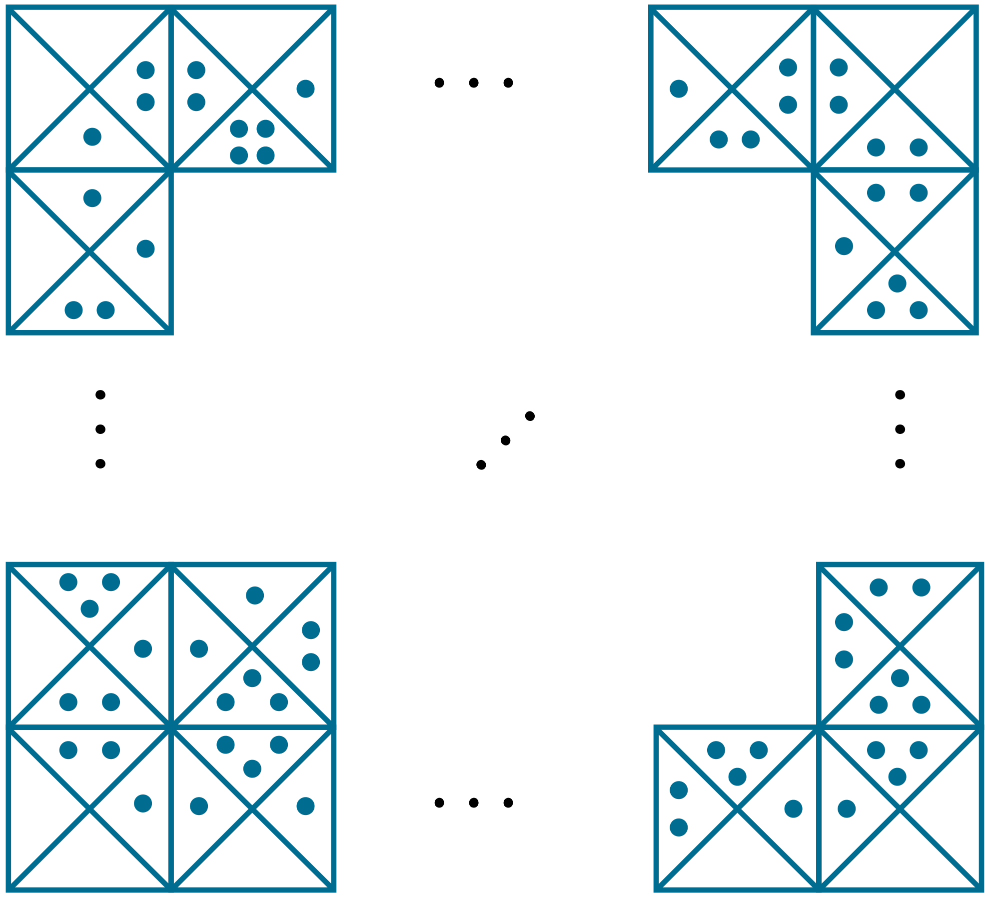


The (undecidable) Domino problem

Domino

Input: 4-sided dominos: 

Output: Is it possible to form a white-bordered rectangle? (of any size)

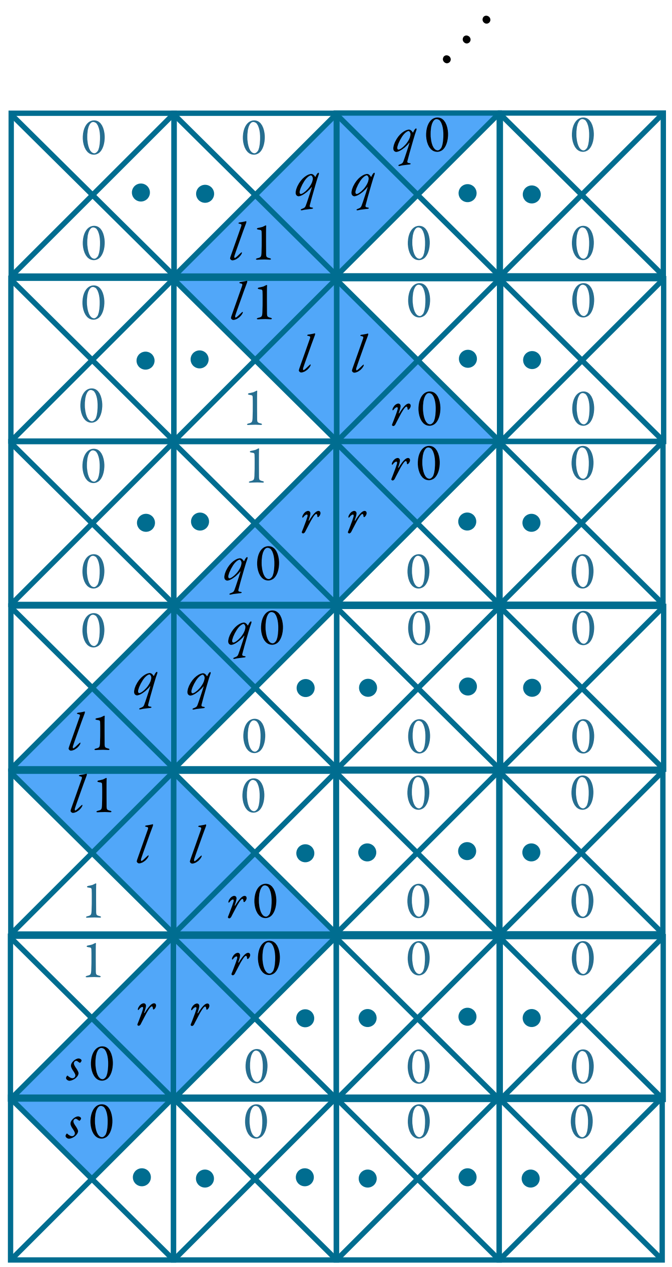


Rules: sides must match,
you can't rotate the dominos, but you can 'clone' them.

The (undecidable) Domino problem

Domino - Why is it undecidable?

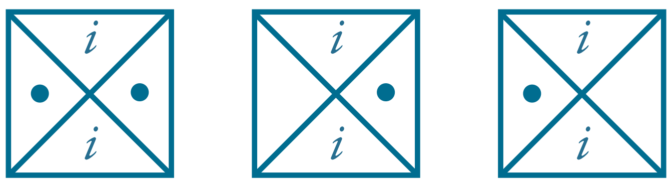
It can encode *halting* computations of Turing machines:



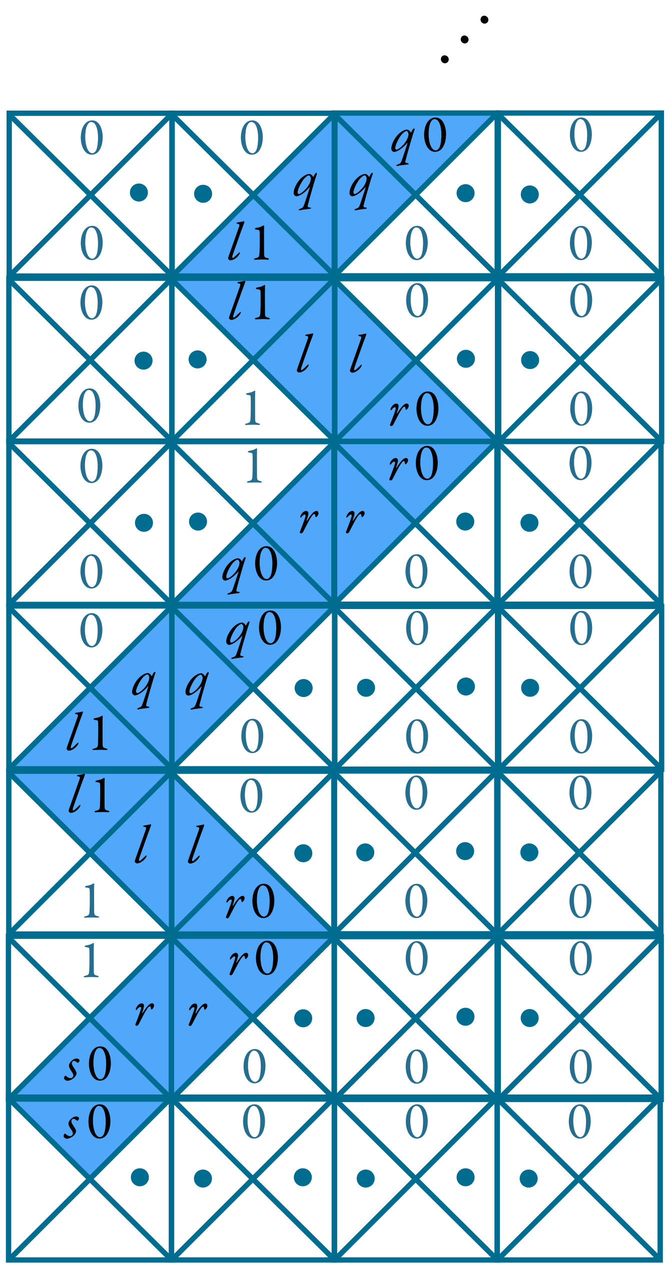
The (undecidable) Domino problem

Domino - Why is it undecidable?

It can encode *halting* computations of Turing machines:



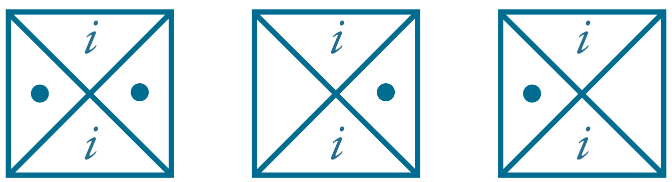
(head is elsewhere, symbol is not modified)



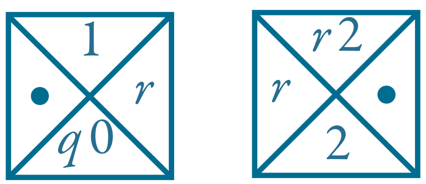
The (undecidable) Domino problem

Domino - Why is it undecidable?

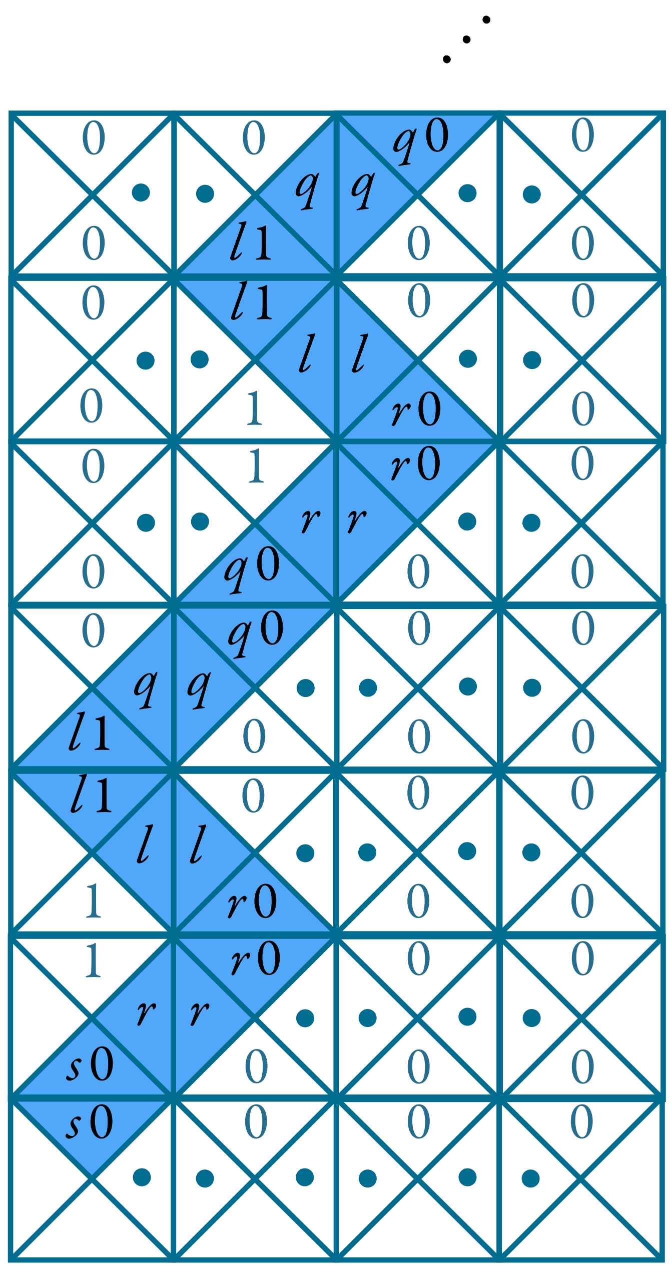
It can encode *halting* computations of Turing machines:



(head is elsewhere,
symbol is not modified)



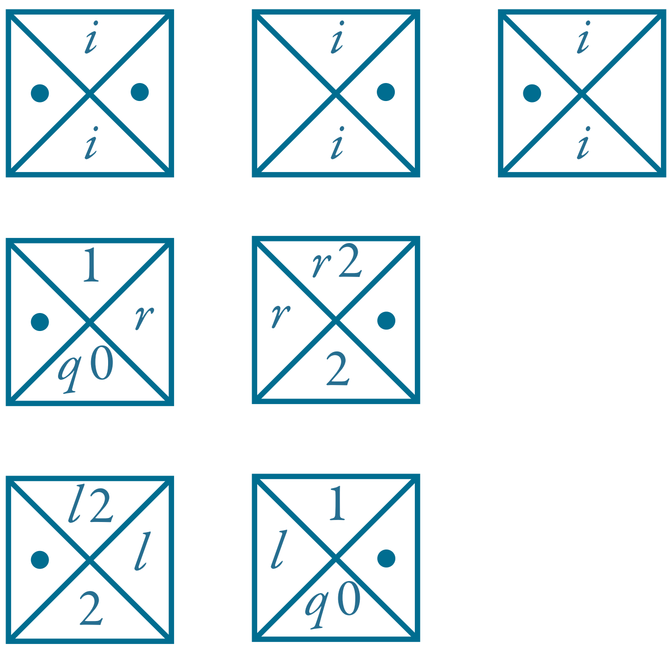
(head is here, symbol is
rewritten, head moves right)



The (undecidable) Domino problem

Domino - Why is it undecidable?

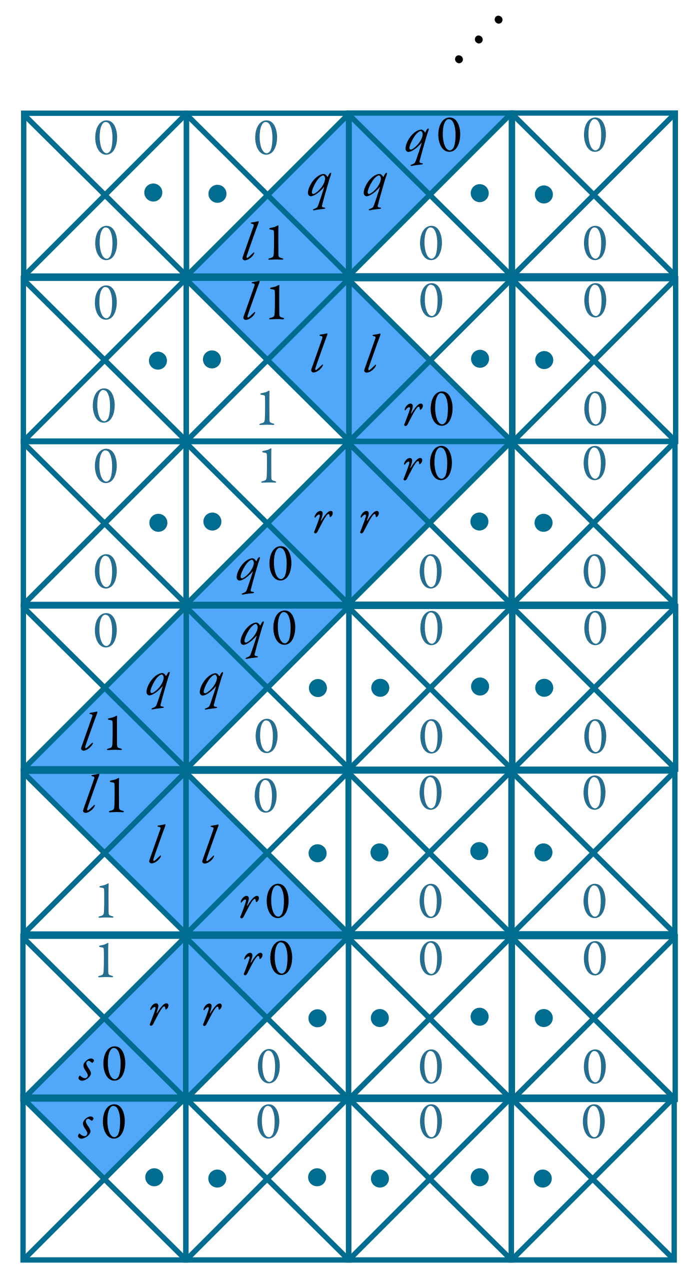
It can encode *halting* computations of Turing machines:



(head is elsewhere, symbol is not modified)

(head is here, symbol is rewritten, head moves right)

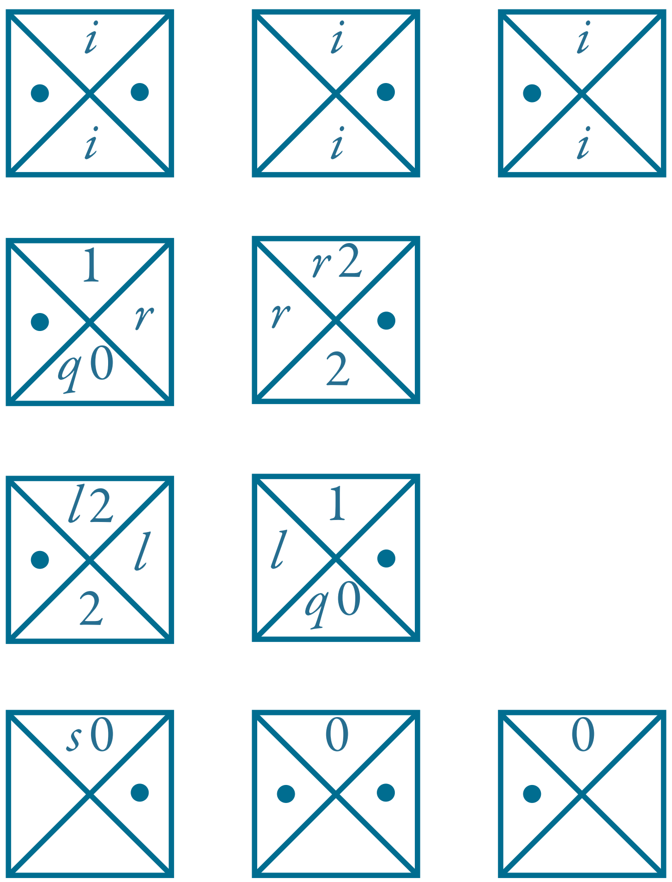
(head is here, symbol is rewritten, head moves left)



The (undecidable) Domino problem

Domino - Why is it undecidable?

It can encode *halting* computations of Turing machines:

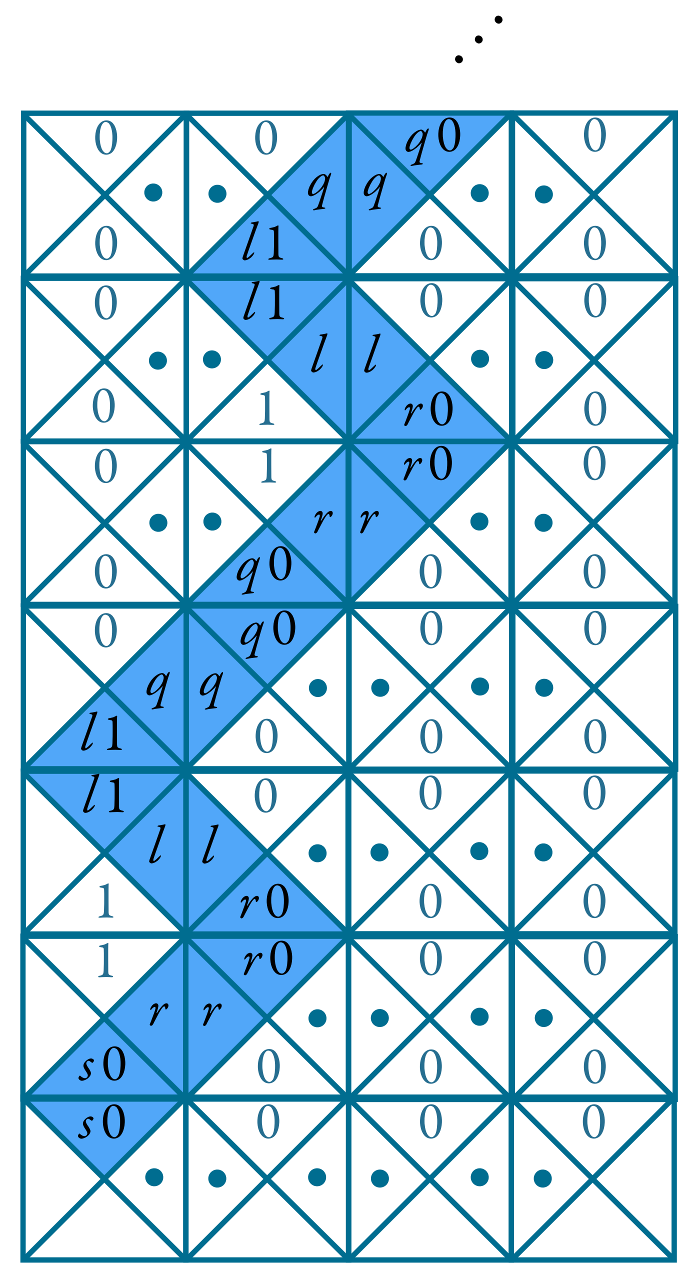


(head is elsewhere, symbol is not modified)

(head is here, symbol is rewritten, head moves right)

(head is here, symbol is rewritten, head moves left)

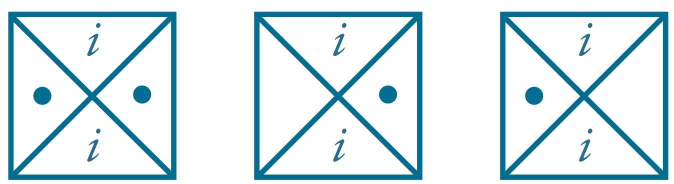
(initial configuration)



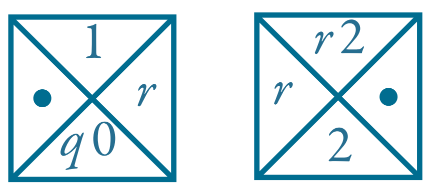
The (undecidable) Domino problem

Domino - Why is it undecidable?

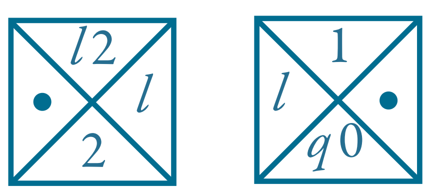
It can encode *halting* computations of Turing machines:



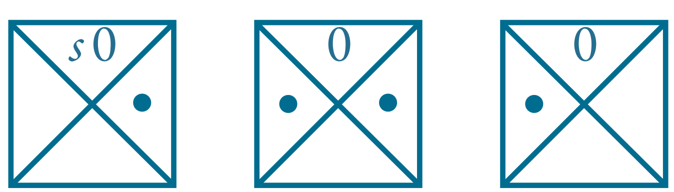
(head is elsewhere, symbol is not modified)



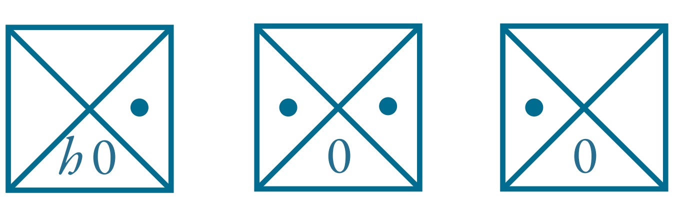
(head is here, symbol is rewritten, head moves right)



(head is here, symbol is rewritten, head moves left)

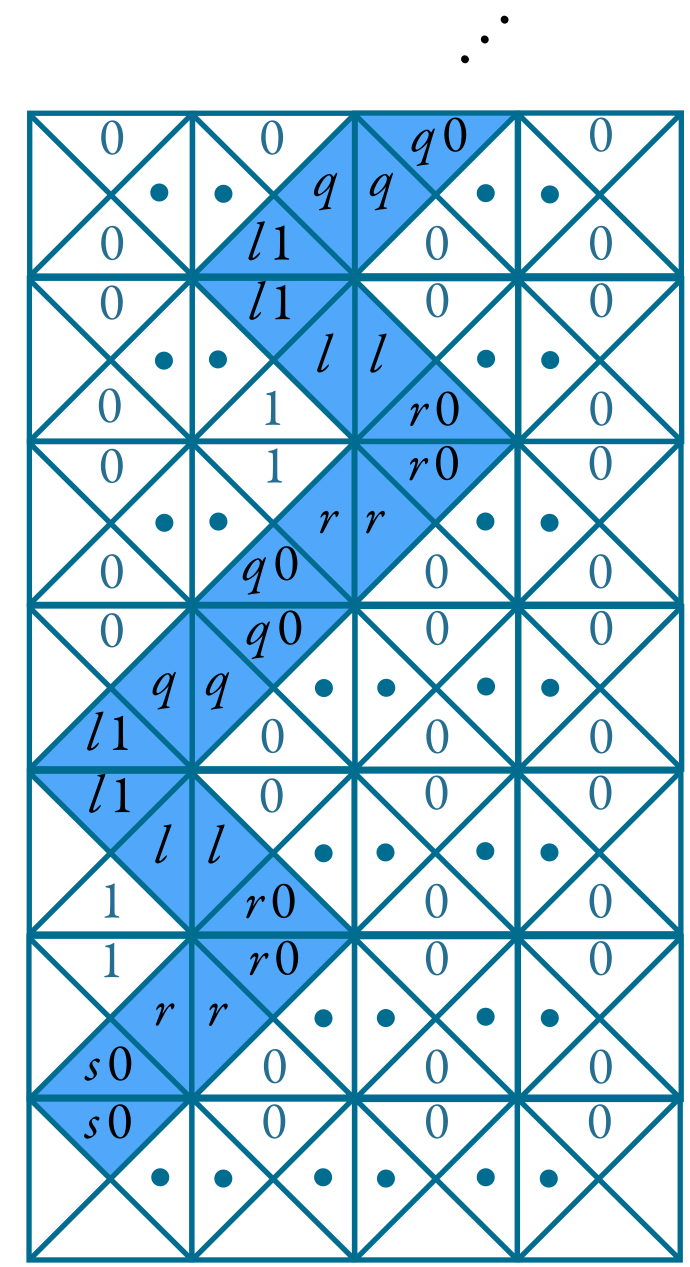


(initial configuration)



(halting configuration)

. . .

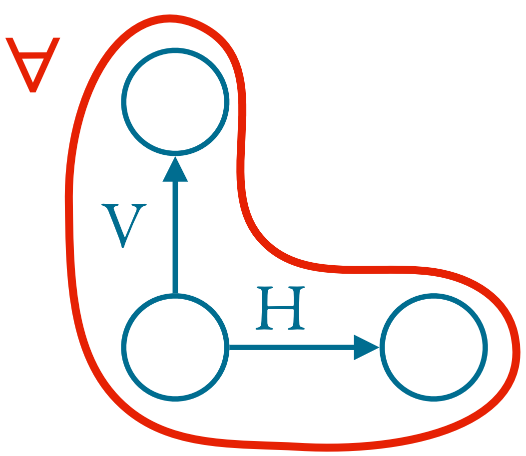


Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that…

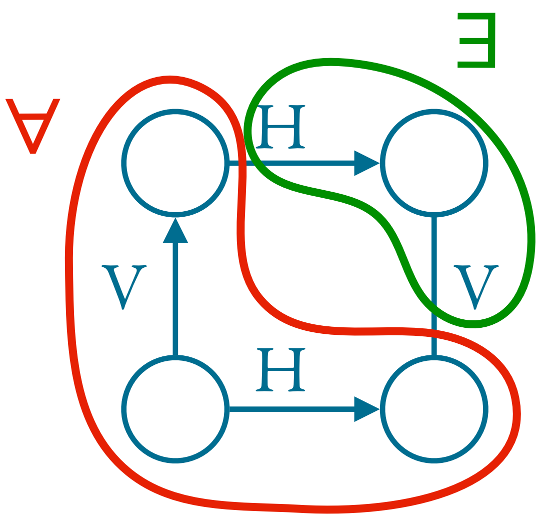
Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that…



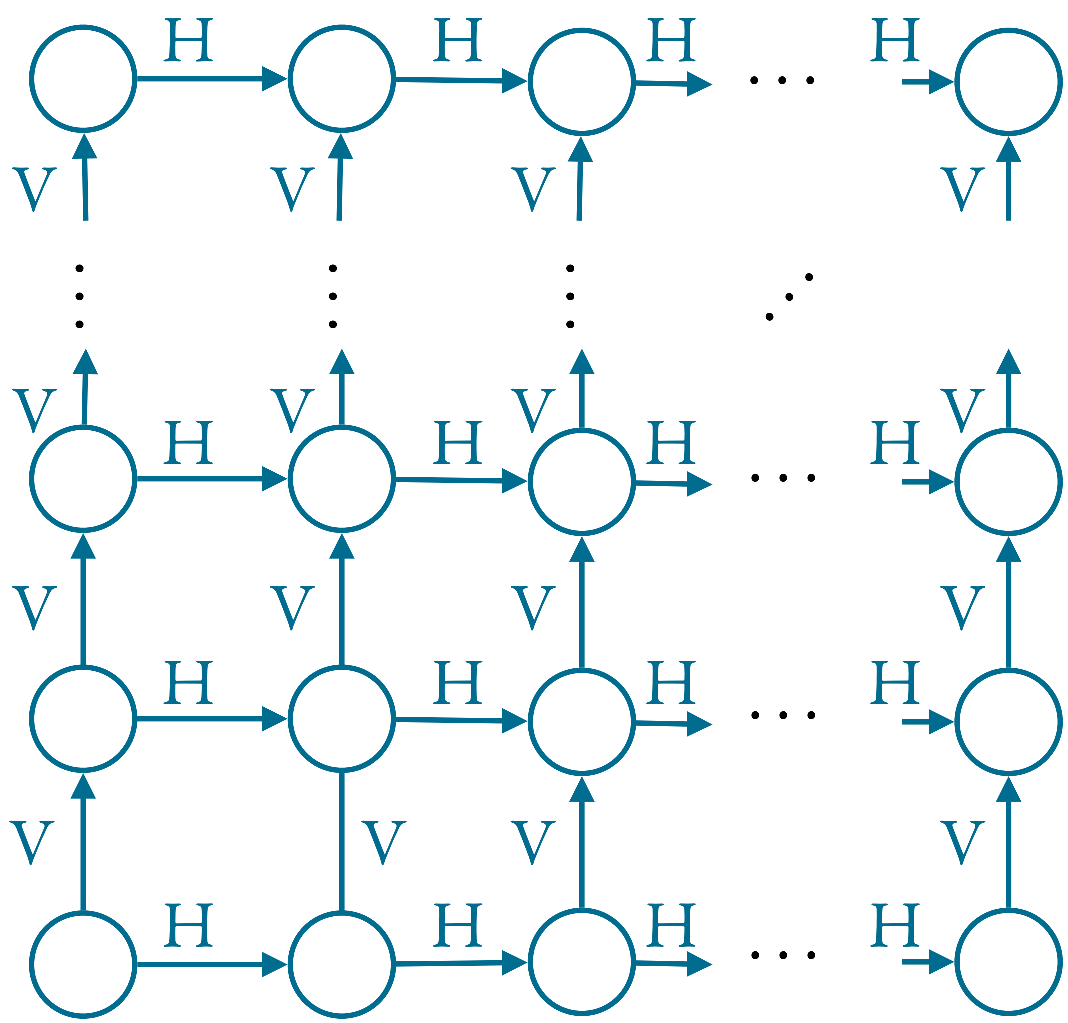
Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that…



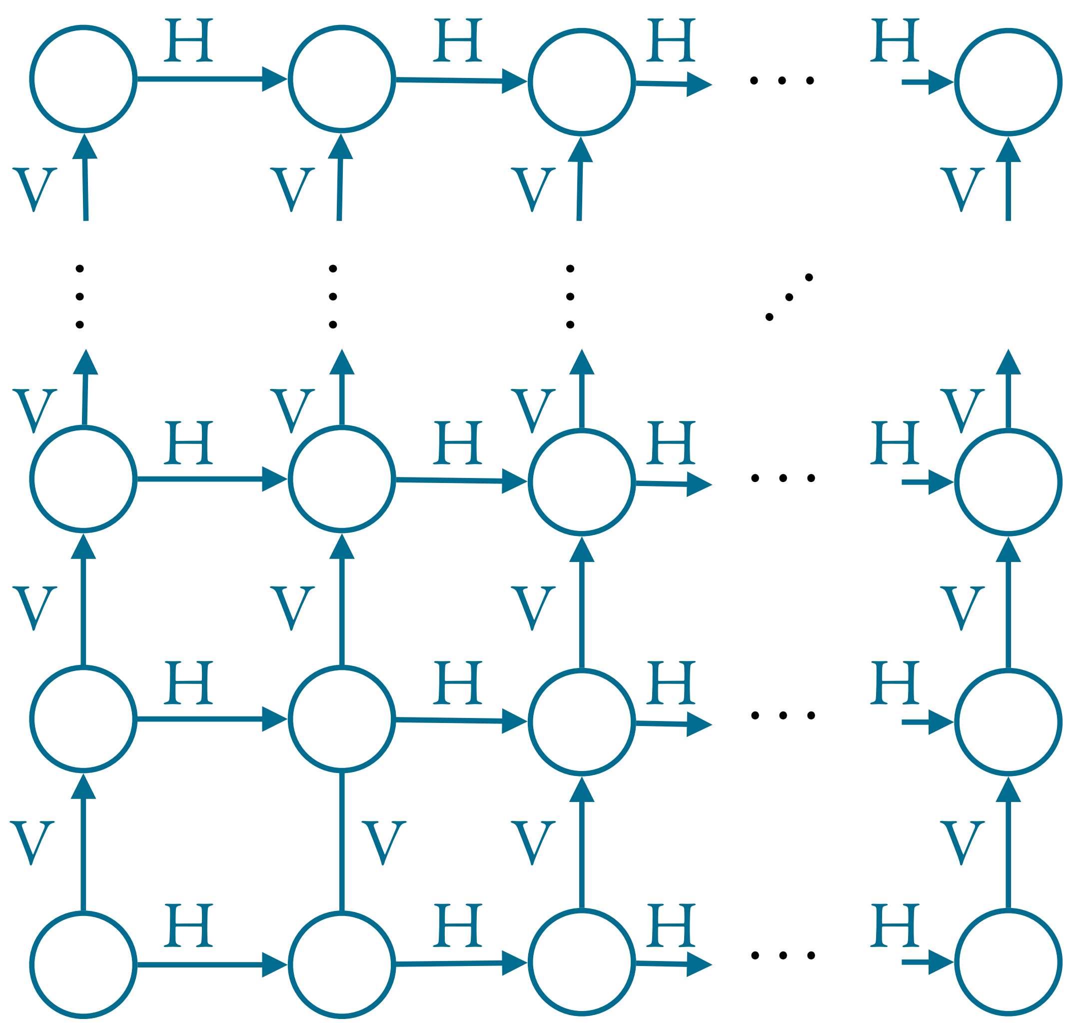
Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that...



Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that…



2. **Assign one domino to each node:**

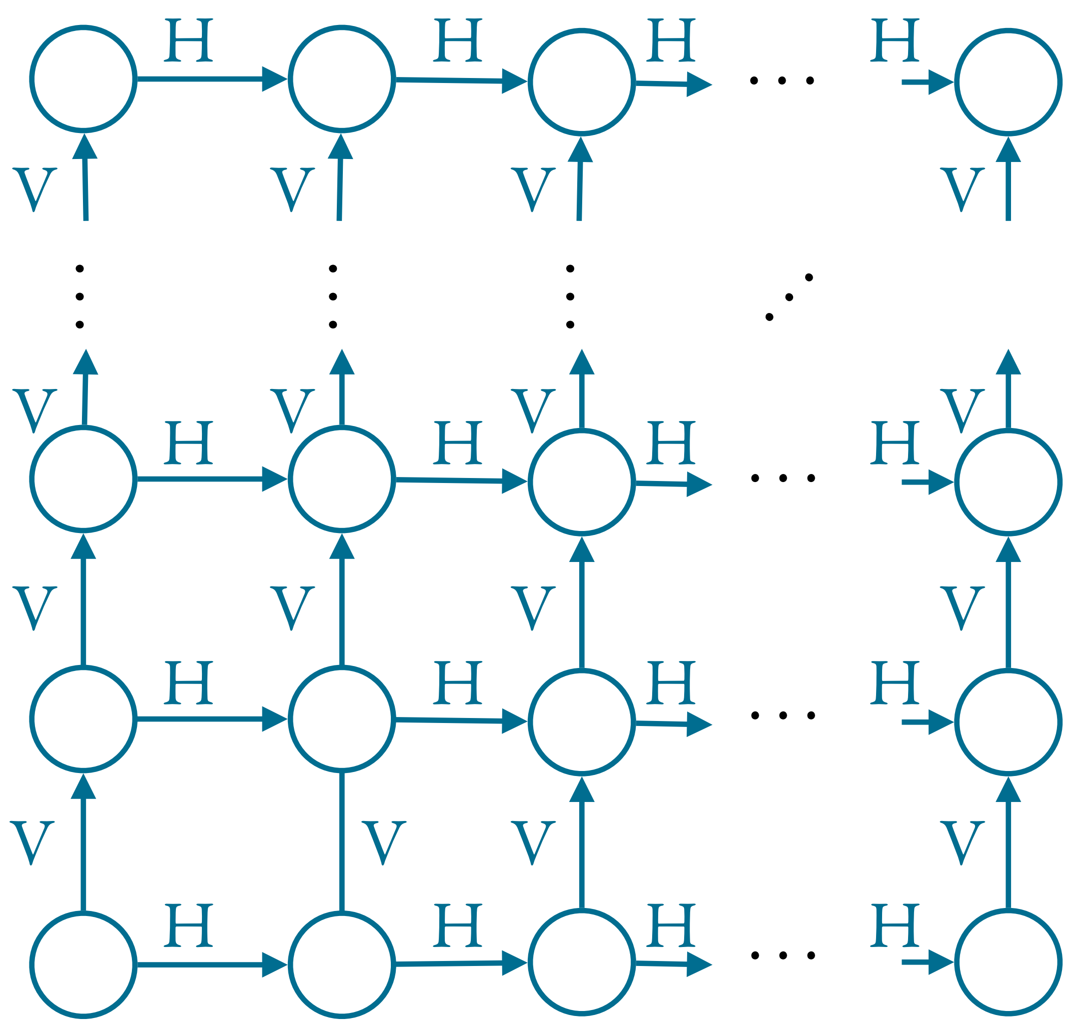
a unary relation

$$\mathbf{D}_{\boxtimes}(\mathbf{x})$$

for each domino $\boxtimes$

Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that…



2. **Assign one domino to each node:**

a unary relation

$$D_{\boxtimes}(x)$$

for each domino $\boxtimes$

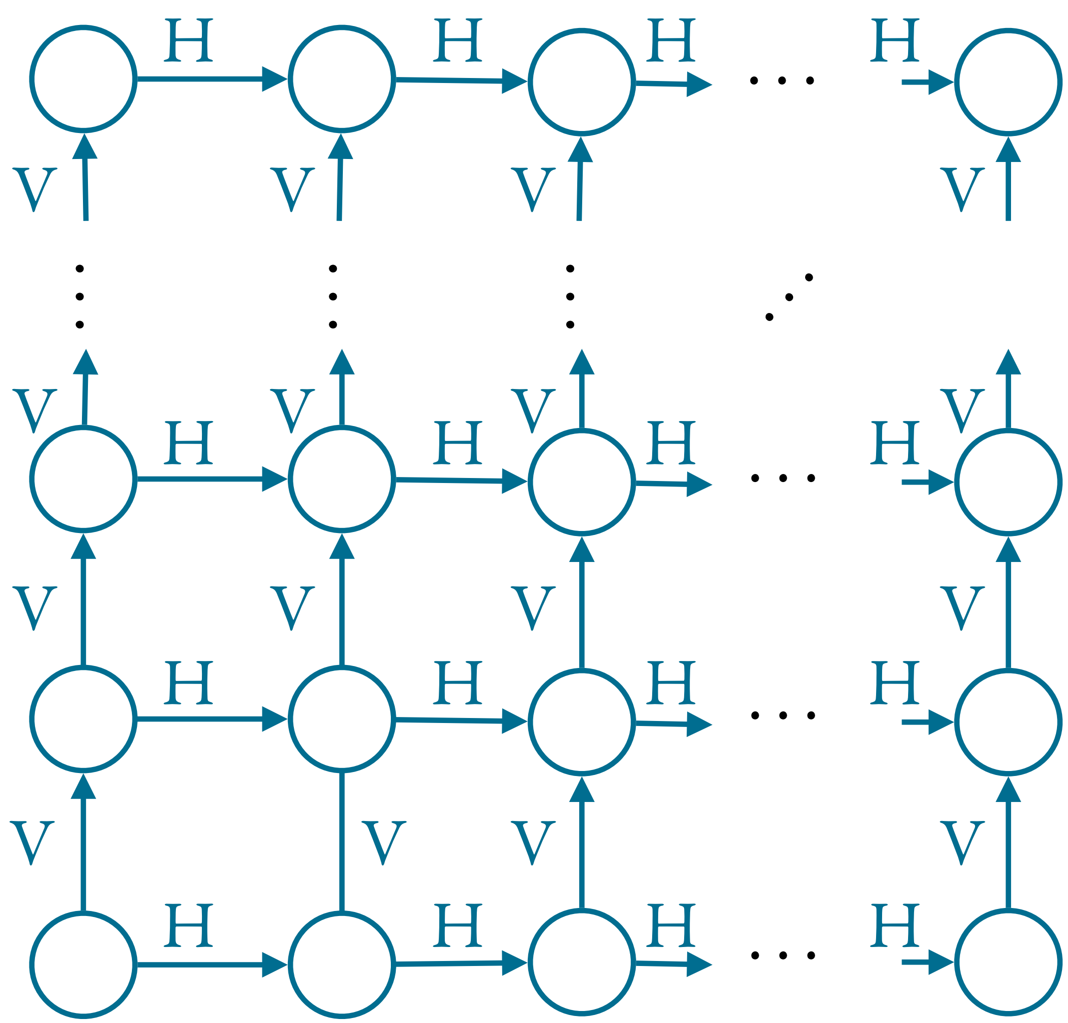
3. **Match the sides** $\forall x\ \forall y$

if $H(x,y)$, then $D_a(x) \wedge D_b(y)$

for some dominos **a,b** that 'match' horizontally (Idem vertically)

Domino reduces to Sat-FO (domino has a solution iff ϕ satisfiable)

1. **There is a grid:** H(,) and V(,) are relations representing bijections such that...



2. **Assign one domino to each node:**

a unary relation

$$D_{\boxtimes}(x)$$

for each domino $\boxtimes$

3. **Match the sides** $\forall x \, \forall y$

if $H(x,y)$, then $D_a(x) \wedge D_b(y)$

for some dominos **a,b** that 'match' horizontally (Idem vertically)

4. **Borders are white.**

Recap + quiz

- <u>Model-checking</u> for FO (does $M \models \phi$?) is **PSPACE**-complete
- <u>Satisfiability</u> for FO (does $M \models \phi$ for some M?) is **undecidable**

Recap + quiz

- Model-checking for FO (does $M \vDash \phi$?) is **PSPACE**-complete
- Satisfiability for FO (does $M \vDash \phi$ for some M?) is **undecidable**

What about

- Validity for FO? (Problem def.: does $M \vDash \phi$ for every M?)
- Equivalence for FO? (Problem def.: is it true that, for every M, $M \vDash \phi$ iff $M \vDash \phi'$?)

Recap + quiz

- Model-checking for FO (does $M \vDash \phi$?) is **PSPACE**-complete

- Satisfiability for FO (does $M \vDash \phi$ for some M?) is **undecidable**

What about

- Validity for FO? (Problem def.: does $M \vDash \phi$ for every M?)
- Equivalence for FO? (Problem def.: is it true that, for every M,
  $M \vDash \phi$ iff $M \vDash \phi'$?)

Can you recall the complexity of analogous problems for

- Propositional logic?
- QBF?

FO theories

<u>Logical theory of a model</u> M = set of all formulas ϕ that hold on M

FO theories

Logical theory of a model M = set of all formulas ϕ that hold on M

FO[U^M, R^M, S^M, ...] denotes the FO theory of $M = (U^M, R^M, S^M, \ldots)$

FO theories

Logical theory of a model M = set of all formulas ϕ that hold on M

$FO[U^M, R^M, S^M, \ldots]$ denotes the FO theory of $M = (U^M, R^M, S^M, \ldots)$

Example

$FO[\mathbb{N},<] = \{ \exists x\, (x=x),\ \forall x \exists y\, x<y,\ \exists y\, \forall x\, \neg(x<y),\ \forall x \forall y\, x=y \vee x<y \vee y<x,\ \ldots \}$

FO theories

<u>Logical theory of a model</u> M = set of all formulas ϕ that hold on M

$FO[U^M, R^M, S^M, \ldots]$ denotes the FO theory of $M = (U^M, R^M, S^M, \ldots)$

Example

$FO[\mathbb{N},<] = \{\ \exists x\,(x=x),\ \forall x \exists y\ x<y,\ \exists y\ \forall x\ \neg(x<y),\ \forall x \forall y\ x=y \vee x<y \vee y<x,\ \ldots\ \}$

(notation abuse: relation = is often present, but not explicitly listed
any symbol R is often identified with its relation R^M)

Some fancy FO theories

(Skip)

$\mathrm{FO}[\mathbb{N}, +, \cdot\,] \;=\;$ Peano arithmetic

$\mathrm{FO}[\mathbb{R}, +, \cdot\,] \;=\;$ Arithmetic theory of real numbers

$\mathrm{FO}[\mathbb{Z}, +] \;=\;$ Presburger arithmetic

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2] \;=\;$ First-order theory of the unlabelled grid

$\mathrm{FO}[\{0,1\}, =] \;\approx\;$ {Valid QBFs}

$\mathrm{FO}[V_R, E_R] \;=\;$ First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M] \;=\;$ First-order theory of the transition graph of a Turing machine M

Some fancy FO theories (Skip)

$\mathrm{FO}[\mathbb{N}, +, \cdot\,] \;=\;$ Peano arithmetic

$\mathrm{FO}[\mathbb{R}, +, \cdot\,] \;=\;$ Arithmetic theory of real numbers

$\mathrm{FO}[\mathbb{Z}, +] \;=\;$ Presburger arithmetic

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2] \;=\;$ First-order theory of the unlabelled grid

$\mathrm{FO}[\{0,1\}, =] \;\approx\;$ {Valid QBFs}

$\mathrm{FO}[V_R, E_R] \;=\;$ First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M] \;=\;$ First-order theory of the transition graph of a Turing machine M

How do I compare them?

Logical reductions

<u>Reduction</u> from P to P':

Algorithm A that solves P by using an oracle that returns solutions to P'

e.g. for all x P(x) iff P'(A(x))

Logical reductions

Reduction from P to P':

Algorithm A that solves P by using an oracle that returns solutions to P'

e.g. for all x $P(x)$ iff $P'(A(x))$

Take $P = FO[M] = \{\phi \mid M \vDash \phi\}$
$P' = FO[M'] = \{\phi' \mid M' \vDash \phi'\}$

for all ϕ $M \vDash \phi$ iff $M' \vDash A(\phi)$

described by a logical interpretation of M into M'

Logical reductions

Reduction from P to P':

Algorithm A that solves P by using an oracle that returns solutions to P'

e.g. for all x $P(x)$ iff $P'(A(x))$

Take $P = FO[M] = \{\phi \mid M \vDash \phi\}$
$P' = FO[M'] = \{\phi' \mid M' \vDash \phi'\}$

for all ϕ $M \vDash \phi$ iff $M' \vDash A(\phi)$

described by a logical interpretation of M into M'

FO interpretation of M into M': a mapping $\alpha : R \mapsto \alpha_R$ such that

$M[\bar{u}] \vDash R(\bar{x})$ iff $M'[\bar{x} := \bar{u}] \vDash \alpha_R(\bar{x})$

Logical reductions

FO interpretation of M into M': a mapping $\alpha : R \mapsto \alpha_R$ such that

$$M[\bar{u}] \models R(\bar{x}) \text{ iff } M'[\bar{x} := \bar{u}] \models \alpha_R(\bar{x})$$

Logical reductions

FO interpretation of M into M': a mapping $\alpha : R \mapsto \alpha_R$ such that

$$M[\bar{u}] \vDash R(\bar{x}) \text{ iff } M'[\bar{x} := \bar{u}] \vDash \alpha_R(\bar{x})$$

Examples

- interpretation of $M = (\mathbb{N}, \leq)$ into $M' = (\mathbb{N}, +)$

$$\alpha_{\leq}(x, y) = \exists z \; y = x + z$$

Logical reductions

<u>FO interpretation</u> of M into M': a mapping $\alpha : R \mapsto \alpha_R$ such that

$$M[\bar{u}] \models R(\bar{x}) \text{ iff } M'[\bar{x} := \bar{u}] \models \alpha_R(\bar{x})$$

Examples

- interpretation of $M = (\mathbb{N}, \leq)$ into $M' = (\mathbb{N}, +)$

$$\alpha_{\leq}(x, y) = \exists z \ \ y=x+z$$

- interpretation of $M = (\{0,1\}^*, \leq_{\text{inorder}})$ into $M' = (\{0,1\}^*, 0, 1, \cdot)$
  $\approx (\mathbb{Q}, \leq)$

$$\alpha_{\leq_{\text{inorder}}}(x, y) = \exists x', y', z \ \ (x=z\cdot 0\cdot x' \wedge y=z\cdot 1\cdot y') \vee (x=y\cdot 0\cdot x') \vee (y=x\cdot 1\cdot x')$$

Logical reductions

In fact, an FO interpretation of M into M' is more complex (and powerful)

- <u>definitions of relations</u>: $\alpha_R(\bar{x})$ such that $R^M = \{ \bar{u} \mid M'[\bar{x} := \bar{u}] \vDash \alpha_R(\bar{x}) \}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{N},+)$)

Logical reductions

In fact, an FO interpretation of M into M' is more complex (and powerful)

- <u>definitions of relations</u>: $\alpha_R(\bar{x})$ such that $R^M = \{\, \bar{u} \mid M'[\bar{x} := \bar{u}] \vDash \alpha_R(\bar{x}) \,\}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{N},+)$)

- <u>definition of universe</u>: $\alpha_U(x)$ such that $U^M = \{\, u \mid M'[x{:=}u] \vDash \alpha_U(x) \,\}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{Z},\leq,0)$)

Logical reductions

In fact, an FO interpretation of M into M' is more complex (and powerful)

- <u>definitions of relations</u>: $\alpha_R(\bar{x})$ such that $R^M = \{ \bar{u} \mid M'[\bar{x} := \bar{u}] \models \alpha_R(\bar{x}) \}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{N},+)$)

- <u>definition of universe</u>: $\alpha_U(x)$ such that $U^M = \{ u \mid M'[x{:=}u] \models \alpha_U(x) \}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{Z},\leq,0)$)

- <u>k-dimensionality</u>: elements of U^M can be k-*tuples* of elements of $U^{M'}$

  (e.g. to interpret $(\mathbb{C},+,\cdot)$ into $(\mathbb{R},+,\cdot)$)

Logical reductions

In fact, an FO interpretation of M into M' is more complex (and powerful)

- <u>definitions of relations</u>: $\alpha_R(\bar{x})$ such that $R^M = \{\, \bar{u} \mid M'[\bar{x} := \bar{u}] \vDash \alpha_R(\bar{x}) \,\}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{N},+)$)

- <u>definition of universe</u>: $\alpha_U(x)$ such that $U^M = \{\, u \mid M'[x{:=}u] \vDash \alpha_U(x) \,\}$

  (e.g. to interpret $(\mathbb{N},\leq)$ into $(\mathbb{Z},\leq,0)$)

- <u>k-dimensionality</u>: elements of U^M can be k-*tuples* of elements of $U^{M'}$

  (e.g. to interpret $(\mathbb{C},+,\cdot)$ into $(\mathbb{R},+,\cdot)$)

- <u>quotient</u>: $\alpha_=(\bar{x},\bar{y})$ such that $M[\ldots] \vDash (\bar{x}=\bar{y})$ iff $M'[\ldots] \vDash \alpha_=(\bar{x},\bar{y})$

  (e.g. to interpret $(\mathbb{Q},+,\cdot)$ into $(\mathbb{Z},+,\cdot)$)

Logical reductions

Given M' and an FO interpretation $\alpha = (\alpha_U, \alpha_=, \alpha_R, \alpha_S, \ldots)$
the interpreted model is $\alpha(M') = (U^M, R^M, S^M, \ldots)$ where

- $U^M = \{\, [\bar{u}]_{\approx} \mid M'[\bar{x} := \bar{u}] \vDash \alpha_U(\bar{x}) \,\}$
- $\bar{u} \approx \bar{v}$ iff $M'[\bar{x} := \bar{u}, \bar{y} := \bar{v}] \vDash \alpha_=(\bar{x},\bar{y})$
- $R^M = \{\, ([\bar{u}_1]_{\approx}, \ldots, [\bar{u}_k]_{\approx}) \mid M'[\bar{x}_1 := \bar{u}_1, \ldots, \bar{x}_k := \bar{u}k] \vDash \alpha_R(\bar{x}_1, \ldots, \bar{x}_k) \,\}$

  (needs to be well-defined, namely, $\approx$ needs to be a congruence w.r.t. every relation R)
- …

Logical reductions

Given M' and an FO interpretation $\alpha = (\alpha_U, \alpha_=, \alpha_R, \alpha_S, \ldots)$
the interpreted model is $\alpha(M') = (U^M, R^M, S^M, \ldots)$ where

- $U^M = \{\, [\bar{u}]_\approx \mid M'[\bar{x} := \bar{u}] \vDash \alpha_U(\bar{x}) \,\}$
- $\bar{u} \approx \bar{v}$ iff $M'[\bar{x} := \bar{u}, \bar{y} := \bar{v}] \vDash \alpha_=(\bar{x},\bar{y})$
- $R^M = \{\, ([\bar{u}_1]_\approx, \ldots, [\bar{u}_k]_\approx) \mid M'[\bar{x}_1 := \bar{u}_1, \ldots, \bar{x}_k := \bar{u}_k] \vDash \alpha_R(\bar{x}_1, \ldots, \bar{x}_k) \,\}$

  (needs to be well-defined, namely, $\approx$ needs to be a congruence w.r.t. every relation R)
- …

Theorem If $\alpha = (\alpha_U, \alpha_=, \alpha_R, \alpha_S, \ldots)$ is an FO interpretation of M into M' then FO[M] *reduces to* FO[M'], namely, there is an algorithm A_α

for all ϕ $\quad M \vDash \phi$ iff $M' \vDash A_\alpha(\phi)$

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$	$=$	Peano arithmetic
$\mathrm{FO}[\mathbb{R}, +, \cdot\,]$	$=$	Arithmetic theory of real numbers
$\mathrm{FO}[\mathbb{Z}, +]$	$=$	Presburger arithmetic
$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$	$=$	First-order theory of the unlabelled grid
$\mathrm{FO}[\{0,1\}, =]$	$\approx$	{Valid QBFs}
$\mathrm{FO}[V_R, E_R]$	$=$	First-order theory of "random" graph
$\mathrm{FO}[C_M, T_M]$	$=$	First-order theory of the transition graph of a Turing machine M

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$ — Peano arithmetic

Theorem Peano arithmetic is undecidable

(one cannot check whether $(\mathbb{N},+,\cdot\,) \models \phi$ for a given ϕ)

FO[$\mathbb{N}$, +, $\cdot$] — Peano arithmetic

Theorem Peano arithmetic is undecidable

(one cannot check whether $(\mathbb{N},+,\cdot) \models \phi$ for a given ϕ)

Proof by reduction from undecidable Hilbert's 10th problem... [Matiyasevic '70]

Hilbert's 10th

Given a polynomial $p(x,y,z,...)$
tell whether $p(x,y,z,...) = 0$ for *some integers* x, y, z

FO[$\mathbb{N}$, +, $\cdot$] — Peano arithmetic

Theorem Peano arithmetic is undecidable

(one cannot check whether $(\mathbb{N},+,\cdot) \vDash \phi$ for a given ϕ)

Proof by reduction from undecidable Hilbert's 10th problem... [Matiyasevic '70]

Hilbert's 10th

Given a polynomial $p(x,y,z,\ldots)$
tell whether $p(x,y,z,\ldots) = 0$ for *some integers* x, y, z

1. Given polynomial $p(x,y,z,\ldots)$, inductively construct $\phi_p(x,y,z,\ldots,t)$ such that

$$(\mathbb{Z},+,\cdot, x,y,z,\ldots,t) \vDash \phi_p \quad \text{iff} \quad p(x,y,z)=t$$

2. Interpret $(\mathbb{Z},+,\cdot,0)$ into $(\mathbb{N},+,\cdot)$

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$ = Peano arithmetic — 💀 **UNDECIDABLE** 💀 (reduction from H's 10th)

$\mathrm{FO}[\mathbb{R}, +, \cdot\,]$ = Arithmetic theory of real numbers

$\mathrm{FO}[\mathbb{Z}, +]$ = Presburger arithmetic

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$ = First-order theory of the unlabelled grid

$\mathrm{FO}[\{0,1\}, =]$ $\approx$ {Valid QBFs}

$\mathrm{FO}[V_R, E_R]$ = First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M]$ = First-order theory of the transition graph of a Turing machine M

FO[$\mathbb{R}$, +, $\cdot$] — Arithmetic theory of real numbers

Theorem [Tarski '51] Every FO formula ϕ over $(\mathbb{R},+,\cdot)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

FO[$\mathbb{R}$, +, $\cdot$] — Arithmetic theory of real numbers

Theorem [Tarski '51]

Every FO formula ϕ over $(\mathbb{R},+,\cdot)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Corollary

Given ϕ, one can decide whether $(\mathbb{R},+,\cdot) \vDash \phi$

FO[ℝ, +, ·] — Arithmetic theory of real numbers

Theorem [Tarski '51] Every FO formula ϕ over $(\mathbb{R},+,\cdot)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Corollary Given ϕ, one can decide whether $(\mathbb{R},+,\cdot) \models \phi$

Algebraic geometry

Programs verification

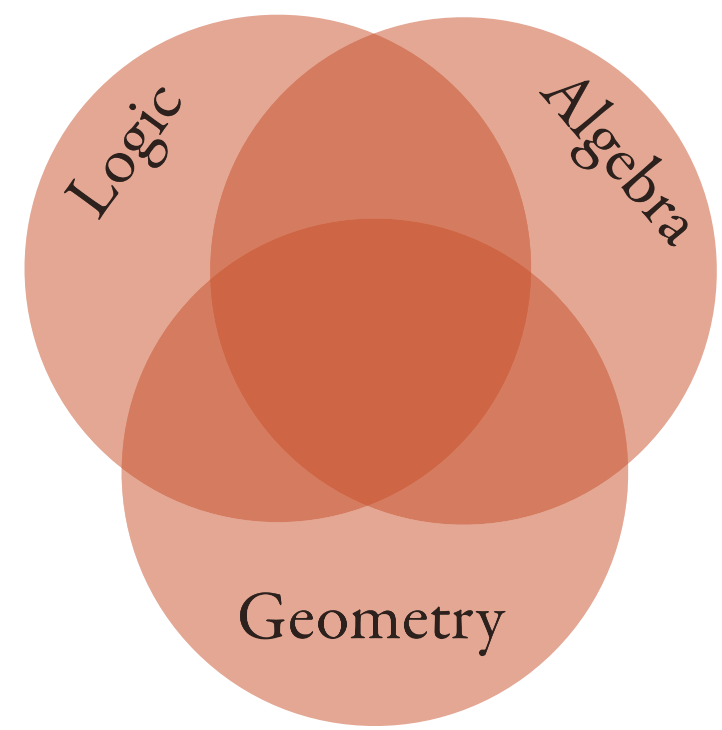
Continuous & discrete dynamical systems

Computer graphics

Robotics

Coding theory & Cryptography

Grammars & Transducers



Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot] \;=\;$ Peano arithmetic

💀 **UNDECIDABLE** 💀
(reduction from H's 10th)

$\mathrm{FO}[\mathbb{R}, +, \cdot] \;=\;$ Arithmetic theory of real numbers

🎉 **DECIDABLE** 🎉
(quantifier elimination)

$\mathrm{FO}[\mathbb{Z}, +] \;=\;$ Presburger arithmetic

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2] \;=\;$ First-order theory of the unlabelled grid

$\mathrm{FO}[\{0,1\}, =] \;\approx\;$ {Valid QBFs}

$\mathrm{FO}[V_R, E_R] \;=\;$ First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M] \;=\;$ First-order theory of the transition graph of a Turing machine M

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Corollary

Given ϕ over $(\mathbb{Z},+)$, one can decide whether $(\mathbb{Z},+) \models \phi$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Corollary

Given ϕ over $(\mathbb{Z},+)$, one can decide whether $(\mathbb{Z},+) \vDash \phi$

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

$\mathrm{FO}[\mathbb{Z}, +]$ — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Corollary Given ϕ over $(\mathbb{Z},+)$, one can decide whether $(\mathbb{Z},+) \vDash \phi$

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \dots Qz\, \alpha(\dots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Corollary

Given ϕ over $(\mathbb{Z},+)$, one can decide whether $(\mathbb{Z},+) \models \phi$

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example $\exists z\, \alpha(x,y,z) \;=\; \exists z\; (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \dots Qz\, \alpha(\dots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example $\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example $\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

$\exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

$$\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(\mathbb{Z},+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots\, Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

$$\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ 2\cdot(2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)\cdot 3$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example $\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$

$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z \neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z \neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29] Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots\, Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\, \alpha(x,y,z) \;=\; \exists z\; (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\; (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\; (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

$$(4\text{-}9)x + (8\text{-}3)y - (14\text{-}12) \leq 0$$

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

$$(\ -5\ )x + (\ 5\ )y - (\ 2\ ) \leq 0$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

temporarily assume formulas are over the reals or the rationals...

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

$$-5x + 5y - 2 \leq 0$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

$$\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 \leq -9x + 3y - 12$$

$$-5x + 5y - 2 \leq 0$$

~~temporarily assume formulas are over the reals or the rationals...~~

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\, \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

~~temporarily assume formulas are over the reals or the rationals...~~

$$\exists z\, \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$4x + 8y - 14 + m \leq -9x + 3y - 12$$

$$-5x + 5y - 2 + m \leq 0$$

$FO[\mathbb{Z},+]$ — Presburger arithmetic

Theorem [Presburger '29]

Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an equivalent quantifier-free formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z\neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example

~~temporarily assume formulas are over the reals or the rationals...~~

$$\exists z\ \alpha(x,y,z) \ = \ \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$$

$$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$$

$$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$$

$$6 \mid 4x + 8y - 14 + m \ \wedge\ 4x + 8y - 14 + m \leq -9x + 3y - 12$$

$$6 \mid 4x + 8y - 14 + m \ \wedge\ -5x + 5y - 2 + m \leq 0$$

FO[$\mathbb{Z}$, +] — Presburger arithmetic

Theorem [Presburger '29]
Every FO formula ϕ over $(Z,+,0,1,\leq,|)$ can be effectively transformed into an <u>equivalent quantifier-free</u> formula ϕ^*

Proof idea

Show how to remove an innermost quantifier Qz from $\phi = \ldots Qz\ \alpha(\ldots, z)$

Assume:

- $Qz = \exists z$ (if not, treat $\forall z$ as $\neg\exists z \neg$)
- α is $\vee$-free (if not, commute $\exists$ and $\vee$)

Example $\exists z\ \alpha(x,y,z) = \exists z\ (2x + 4y - 3z \leq 7) \wedge (3x - y + 2z \leq -4)$

$\exists z\ (2x + 4y - 7 \leq 3z) \wedge (2z \leq -3x + y - 4)$

~~temporarily assume formulas are over the reals or the rationals...~~

$\exists z\ (4x + 8y - 14 \leq 6z) \wedge (6z \leq -9x + 3y - 12)$

$$\bigvee_{m=0,\ldots,5}\ 6 \mid 4x + 8y - 14 + m \ \wedge\ 4x + 8y - 14 + m \leq -9x + 3y - 12$$

$$\bigvee_{m=0,\ldots,5}\ 6 \mid 4x + 8y - 14 + m \ \wedge\ -5x + 5y - 2 + m \leq 0$$

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,] = $ Peano arithmetic — 💀 **UNDECIDABLE** 💀 (reduction from H's 10th)

$\mathrm{FO}[\mathbb{R}, +, \cdot\,] = $ Arithmetic theory of real numbers — 🎉 **DECIDABLE** 🎉 (quantifier elimination)

$\mathrm{FO}[\mathbb{Z}, +] = $ Presburger arithmetic — 🎉 **DECIDABLE** 🎉 (quantifier elimination)

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2] = $ First-order theory of the unlabelled grid

$\mathrm{FO}[\{0,1\}, =] \approx$ {Valid QBFs}

$\mathrm{FO}[V_R, E_R] = $ First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M] = $ First-order theory of the transition graph of a Turing machine M

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$ = Peano arithmetic 💀 UNDECIDABLE 💀
(reduction from H's 10th)

$\mathrm{FO}[\mathbb{R}, +, \cdot\,]$ = Arithmetic theory of real numbers 🎉 DECIDABLE 🎉
(quantifier elimination)

$\mathrm{FO}[\mathbb{Z}, +]$ = Presburger arithmetic 🎉 DECIDABLE 🎉
(quantifier elimination)

$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$ = First-order theory of the unlabelled grid 🎉 DECIDABLE 🎉
(interpreted in the former)

$\mathrm{FO}[\{0,1\}, =]$ ≈ {Valid QBFs}

$\mathrm{FO}[V_R, E_R]$ = First-order theory of "random" graph

$\mathrm{FO}[C_M, T_M]$ = First-order theory of the transition graph of a Turing machine M

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot]$	$=$	Peano arithmetic	💀 UNDECIDABLE 💀 (reduction from H's 10th)
$\mathrm{FO}[\mathbb{R}, +, \cdot]$	$=$	Arithmetic theory of real numbers	🎉 DECIDABLE 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{Z}, +]$	$=$	Presburger arithmetic	🎉 DECIDABLE 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$	$=$	First-order theory of the unlabelled grid	🎉 DECIDABLE 🎉 (interpreted in the former)
$\mathrm{FO}[\{0,1\}, =]$	$\approx$	{Valid QBFs}	
$\mathrm{FO}[V_R, E_R]$	$=$	First-order theory of "random" graph	
$\mathrm{FO}[C_M, T_M]$	$=$	First-order theory of the transition graph of a Turing machine M	

FO[{0,1}, =] — The FO theory of Boolean algebra

Lemma Given any QBF ϕ without free variables,
one can construct an FO formula ϕ^* such that

$$\models \phi \quad \text{iff} \quad (\{0,1\}, =) \models \phi^*$$

FO[{0,1}, =] — The FO theory of Boolean algebra

Lemma Given any QBF ϕ without free variables,
one can construct an FO formula ϕ^* such that

$$\models \phi \quad \text{iff} \quad (\{0,1\}, =) \models \phi^*$$

Proof

define $\phi^* = \exists t \; \phi[x \,/\, (x{=}t)]$ (for all bound variables x)

FO[{0,1}, =] — The FO theory of Boolean algebra

Lemma Given any QBF ϕ without free variables,
one can construct an FO formula ϕ^* such that

$$\models \phi \quad \text{iff} \quad (\{0,1\}, =) \models \phi^*$$

Proof

define $\phi^* = \exists t\ \phi[x \,/\, (x=t)]$ (for all bound variables x)

Corollary FO[{0,1}, =] encodes the set of valid QBF formulas

Some fancy FO theories

$FO[\mathbb{N}, +, \cdot]$	$=$	Peano arithmetic	UNDECIDABLE (reduction from H's 10th)
$FO[\mathbb{R}, +, \cdot]$	$=$	Arithmetic theory of real numbers	DECIDABLE (quantifier elimination)
$FO[\mathbb{Z}, +]$	$=$	Presburger arithmetic	DECIDABLE (quantifier elimination)
$FO[\mathbb{N}^2, \leq_1, \leq_2]$	$=$	First-order theory of the unlabelled grid	DECIDABLE (interpreted in the former)
$FO[\{0,1\}, =]$	$\approx$	{Valid QBFs}	EASY
$FO[V_R, E_R]$	$=$	First-order theory of "random" graph	
$FO[C_M, T_M]$	$=$	First-order theory of the transition graph of a Turing machine M	

Some fancy FO theories

$FO[\mathbb{N}, +, \cdot] \;=\;$ Peano arithmetic — **UNDECIDABLE** (reduction from H's 10th)

$FO[\mathbb{R}, +, \cdot] \;=\;$ Arithmetic theory of real numbers — **DECIDABLE** (quantifier elimination)

$FO[\mathbb{Z}, +] \;=\;$ Presburger arithmetic — **DECIDABLE** (quantifier elimination)

$FO[\mathbb{N}^2, \leq_1, \leq_2] \;=\;$ First-order theory of the unlabelled grid — **DECIDABLE** (interpreted in the former)

$FO[\{0,1\}, =] \;\approx\;$ {Valid QBFs} — **EASY**

$FO[V_R, E_R] \;=\;$ First-order theory of "random" graph

$FO[C_M, T_M] \;=\;$ First-order theory of the transition graph of a Turing machine M

FO[V_R, E_R] — The FO theory of the "random" graph

A different perspective and a coarser view on expressiveness...

What percentage of finite graphs verify a given FO sentence?

Probability of a formula

$P_n[\phi] \quad = \quad$ probability that ϕ holds on a <u>random</u> finite graph with n nodes

Probability of a formula

$P_n[\phi]$ = probability that ϕ holds on a random finite graph with n nodes

$$P_\infty[\phi] = \lim_{n \to \infty} P_n[\phi]$$

Probability of a formula

$P_n[\phi]$ = probability that ϕ holds on a random finite graph with n nodes

$$P_\infty[\phi] = \lim_{n \to \infty} P_n[\phi]$$

Example For ϕ = "the graph is complete",

we have $P_n[\phi] = \dfrac{1}{2^{n(n-1)}}$

and hence $P_\infty[\phi] = 0$

Probability of a formula

Theorem (0/1 Law)
[Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> $(P_\infty[\phi] = 1)$
or <u>almost surely false</u> $(P_\infty[\phi] = 0)$

Probability of a formula

Theorem (0/1 Law)
[Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> ($P_\infty[\phi] = 1$)
or <u>almost surely false</u> ($P_\infty[\phi] = 0$)

Examples

- ϕ = "there is a triangle" $P_\infty[\phi] = 1$

Probability of a formula

Theorem (0/1 Law) [Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> ($P_\infty[\phi] = 1$)
or <u>almost surely false</u> ($P_\infty[\phi] = 0$)

Examples

- ϕ = "there is a triangle" $P_\infty[\phi] = 1$
- ϕ = "there no 5-clique" $P_\infty[\phi] = 0$

Probability of a formula

Theorem (0/1 Law)
[Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> ($P_\infty[\phi] = 1$)
or <u>almost surely false</u> ($P_\infty[\phi] = 0$)

Examples

- ϕ = "there is a triangle" $P_\infty[\phi] = 1$
- ϕ = "there no 5-clique" $P_\infty[\phi] = 0$
- ϕ = "even number of edges"
- ϕ = "even number of nodes"

Your turn!

Probability of a formula

Theorem (0/1 Law)
[Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> ($P_\infty[\phi] = 1$)
or <u>almost surely false</u> ($P_\infty[\phi] = 0$)

Examples

- ϕ = "there is a triangle" $P_\infty[\phi] = 1$
- ϕ = "there no 5-clique" $P_\infty[\phi] = 0$
- ϕ = "even number of edges" $P_\infty[\phi] = 1/2$
- ϕ = "even number of nodes" $P_\infty[\phi]$ not even defined

Your turn!

Probability of a formula

Theorem (0/1 Law)
[Glebskii et al. '69, Fagin '76]

Every FO formula ϕ is
either <u>almost surely true</u> $(P_\infty[\phi] = 1)$
or <u>almost surely false</u> $(P_\infty[\phi] = 0)$

Examples

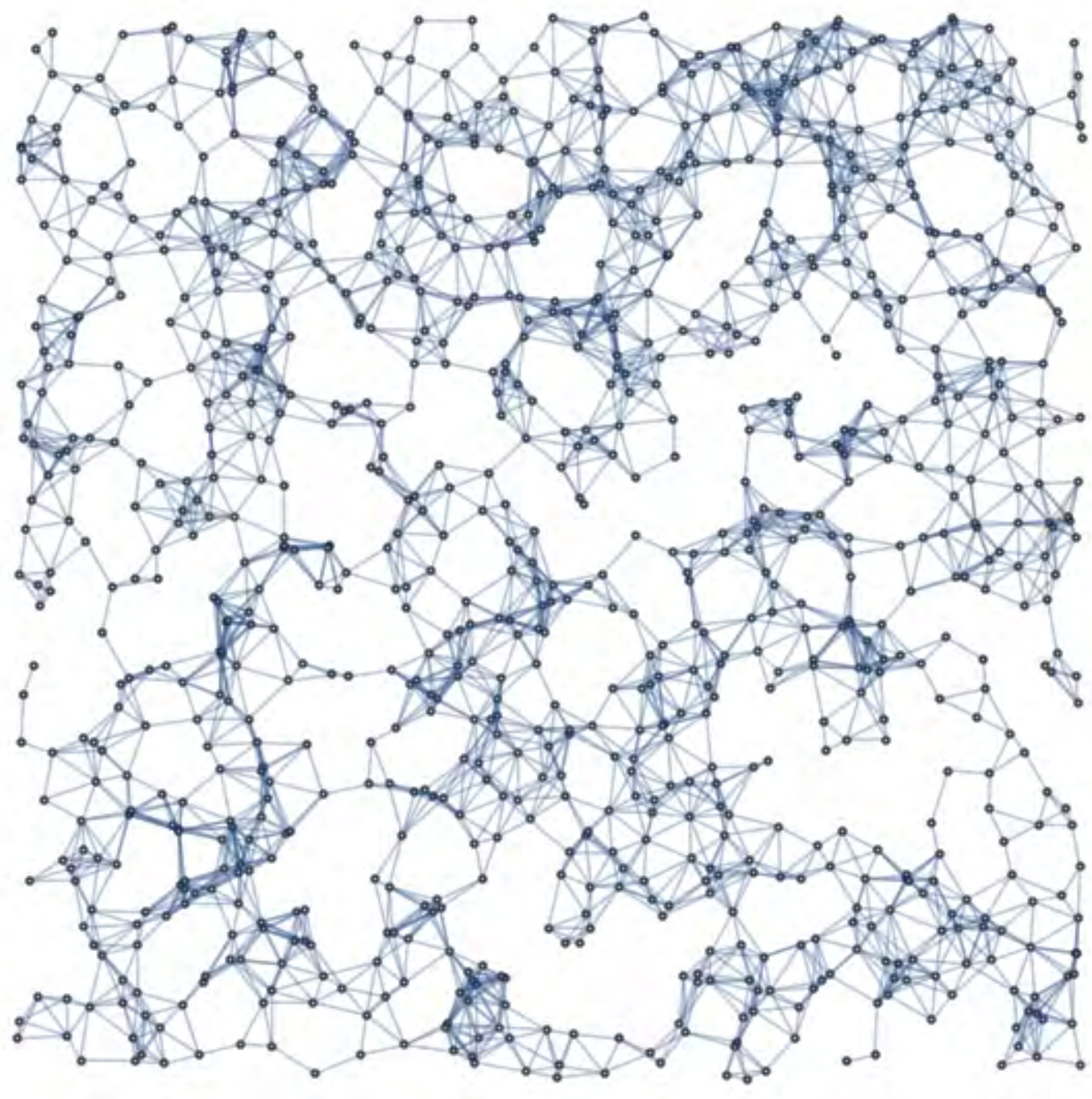
- ϕ = "there is a triangle" $P_\infty[\phi] = 1$
- ϕ = "there no 5-clique" $P_\infty[\phi] = 0$
- ϕ = "even number of edges" $P_\infty[\phi] = 1/2$
- ϕ = "even number of nodes" $P_\infty[\phi]$ not even defined
- ϕ = "more edges than nodes" $P_\infty[\phi] = 1$ (yet not FO-definable...)

Your turn!

The “random” infinite graph

Every FO formula ϕ is either almost surely true or almost surely false,
and this depends on whether $(V_R, E_R) \vDash \phi$

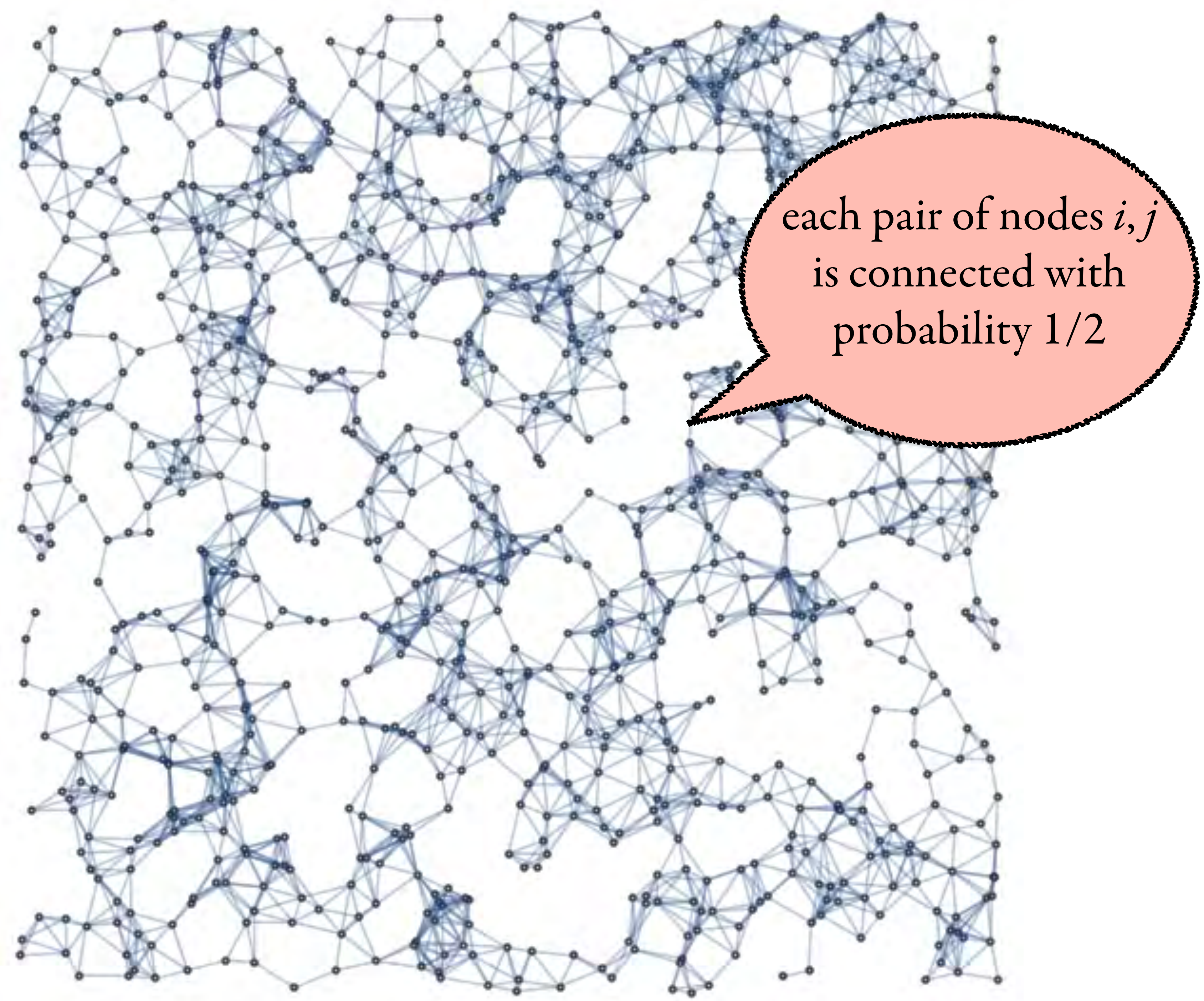
The “random” graph
(V_R, E_R)



The “random” infinite graph

Every FO formula ϕ is either <u>almost surely true</u> or <u>almost surely false</u>, *and this depends on whether* $(V_R, E_R) \vDash \phi$

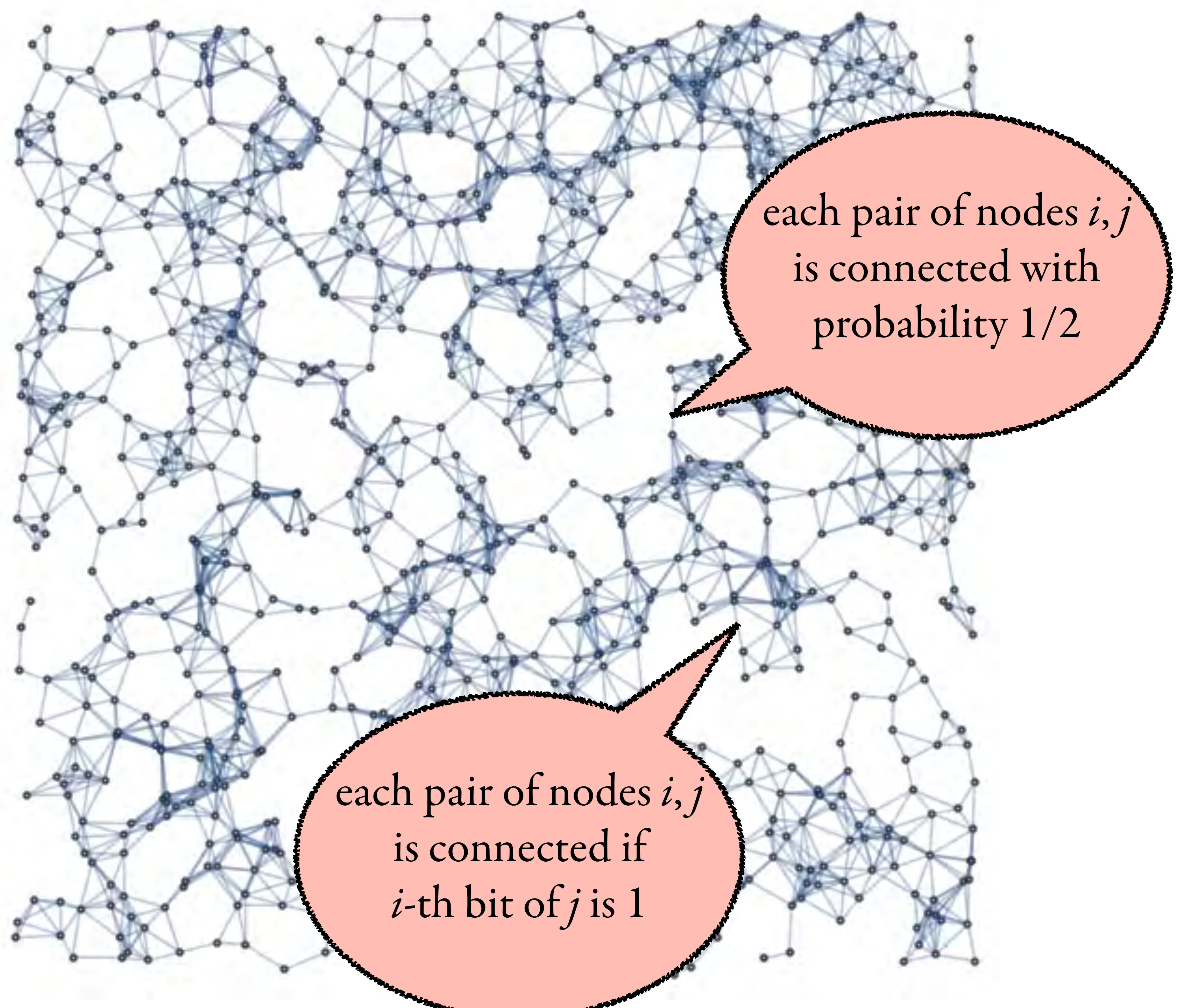
The “random” graph
(V_R, E_R)



The “random” infinite graph

Every FO formula ϕ is either <u>almost surely true</u> or <u>almost surely false</u>, *and this depends on whether* $(V_R, E_R) \vDash \phi$

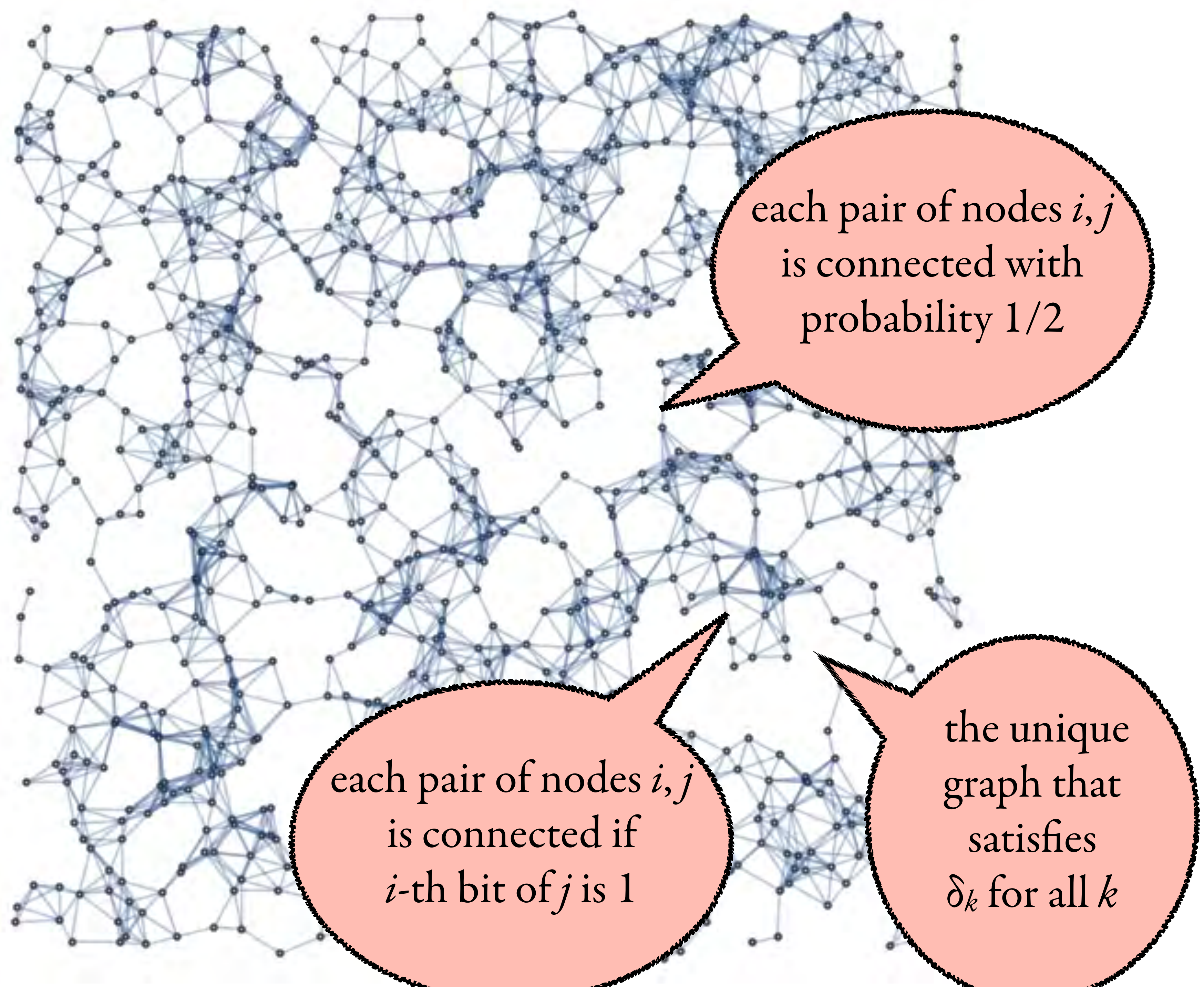
The “random” graph (V_R, E_R)



The “random” infinite graph

Every FO formula ϕ is either <u>almost surely true</u> or <u>almost surely false</u>,
and this depends on whether $(V_R, E_R) \vDash \phi$

The “random” graph
(V_R, E_R)

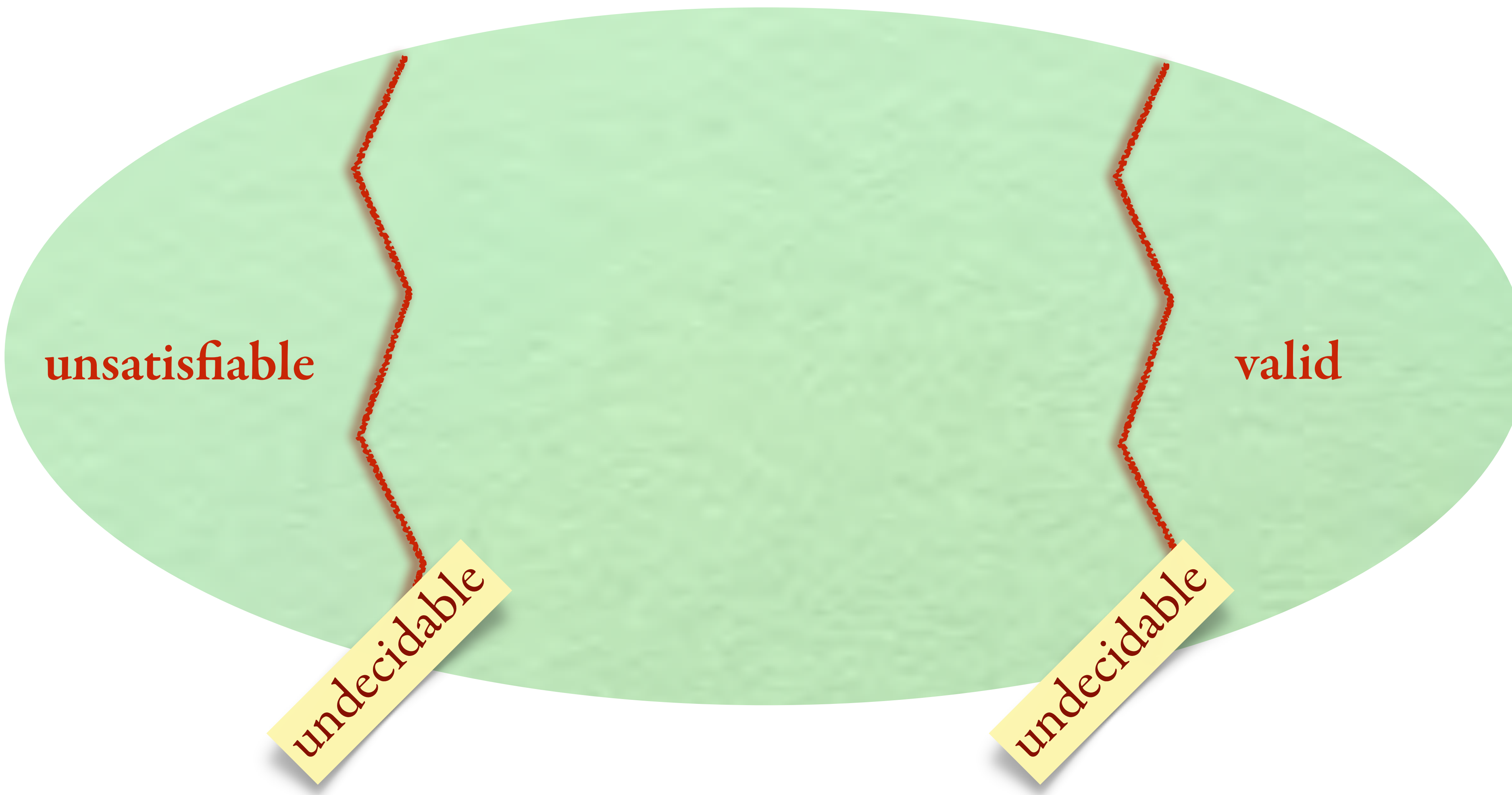


Probability of a formula - application

Theorem [Grandjean '83] One can decide in **PSPACE** whether ϕ is almost surely true on finite graphs

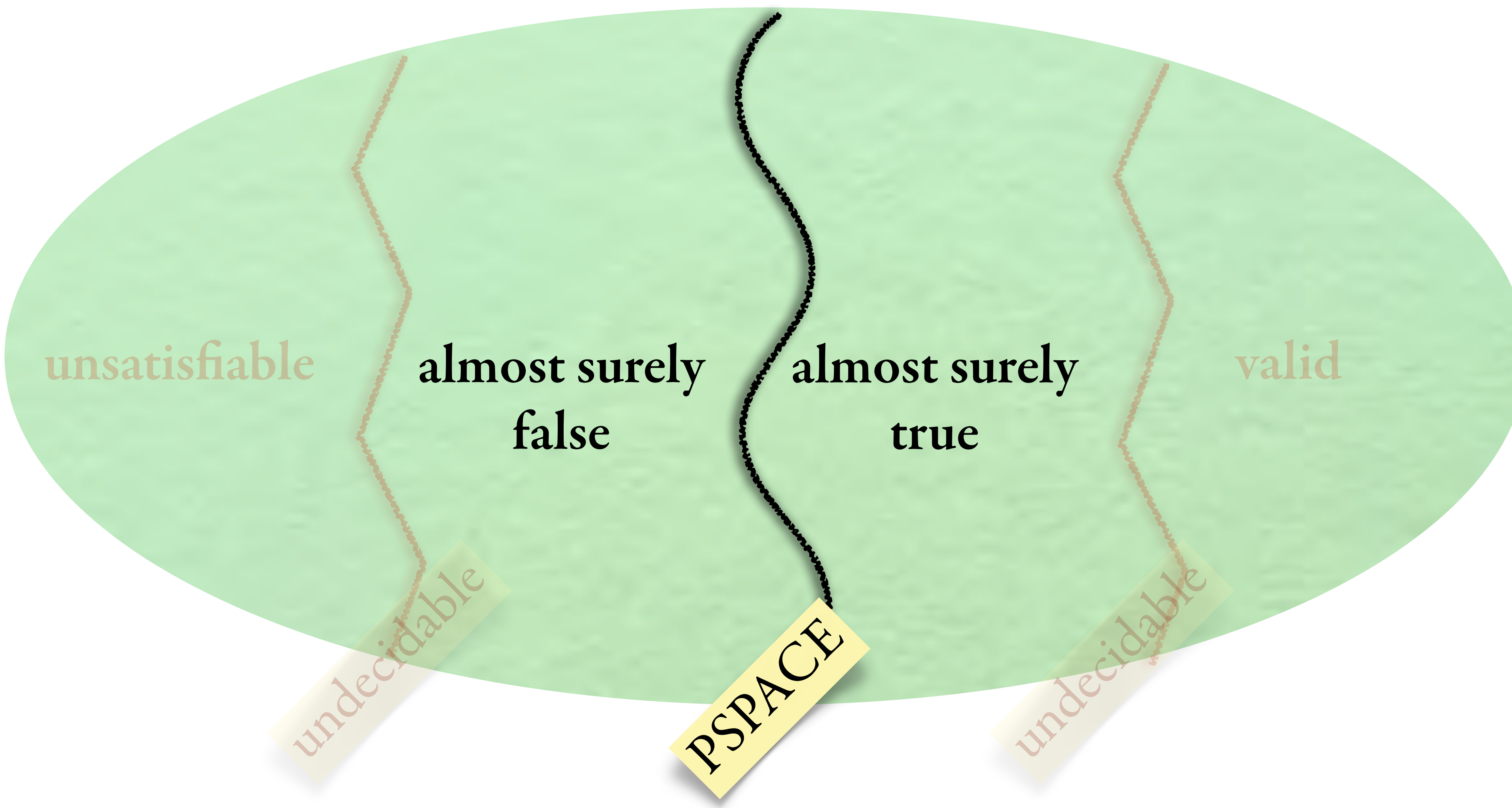
Probability of a formula - application

Theorem [Grandjean '83] One can decide in **PSPACE** whether ϕ is almost surely true on finite graphs



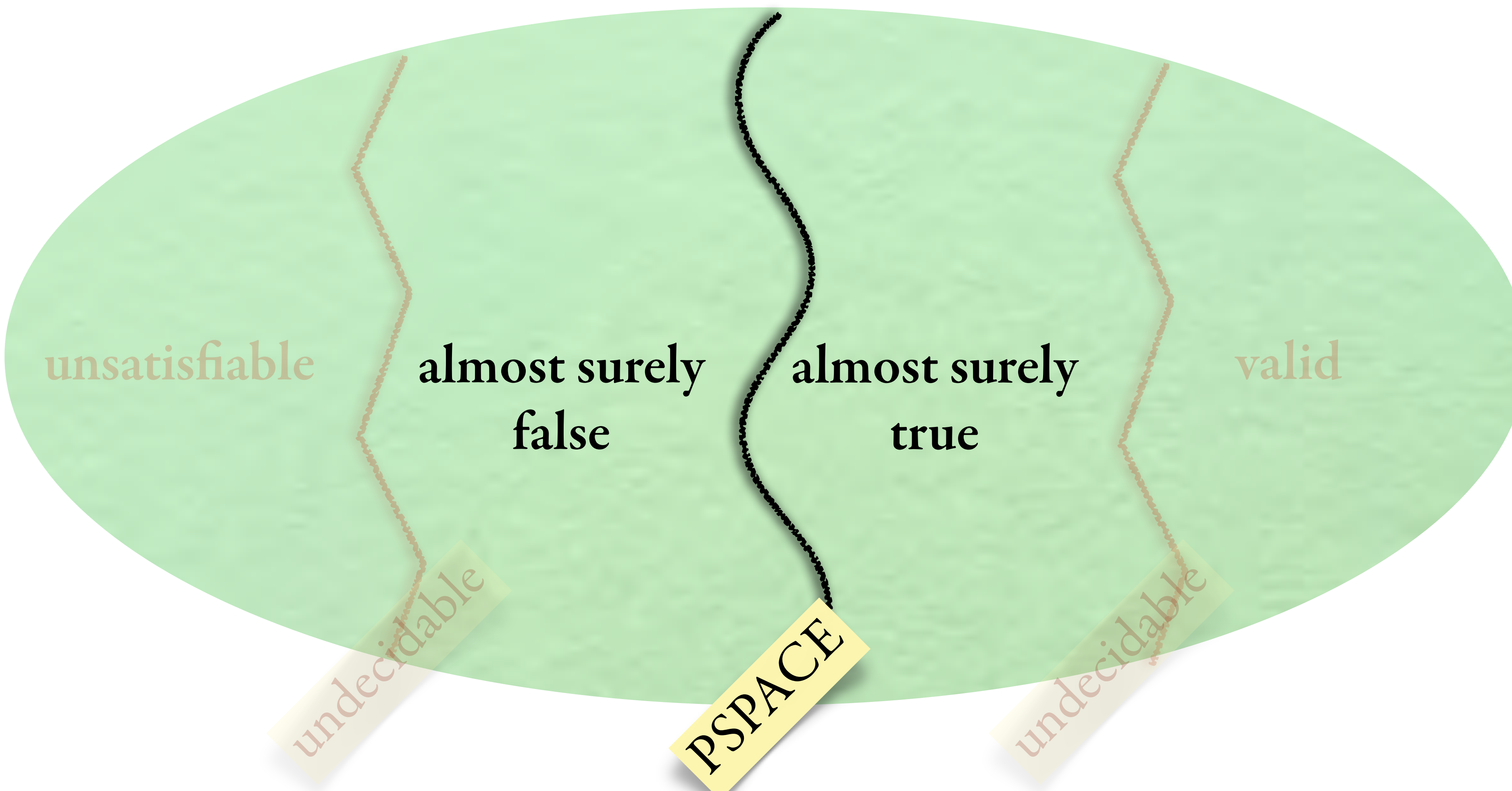
Probability of a formula - application

Theorem [Grandjean '83] One can decide in **PSPACE** whether ϕ is almost surely true on finite graphs



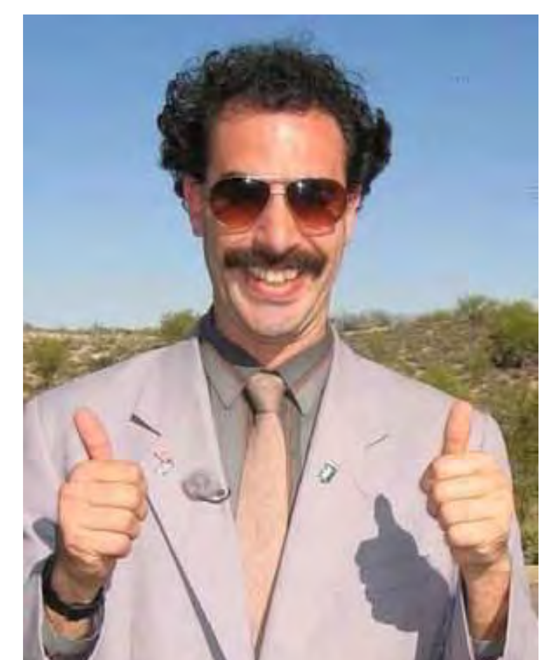
Probability of a formula - application

Theorem [Grandjean '83] One can decide in **PSPACE** whether ϕ is almost surely true on finite graphs



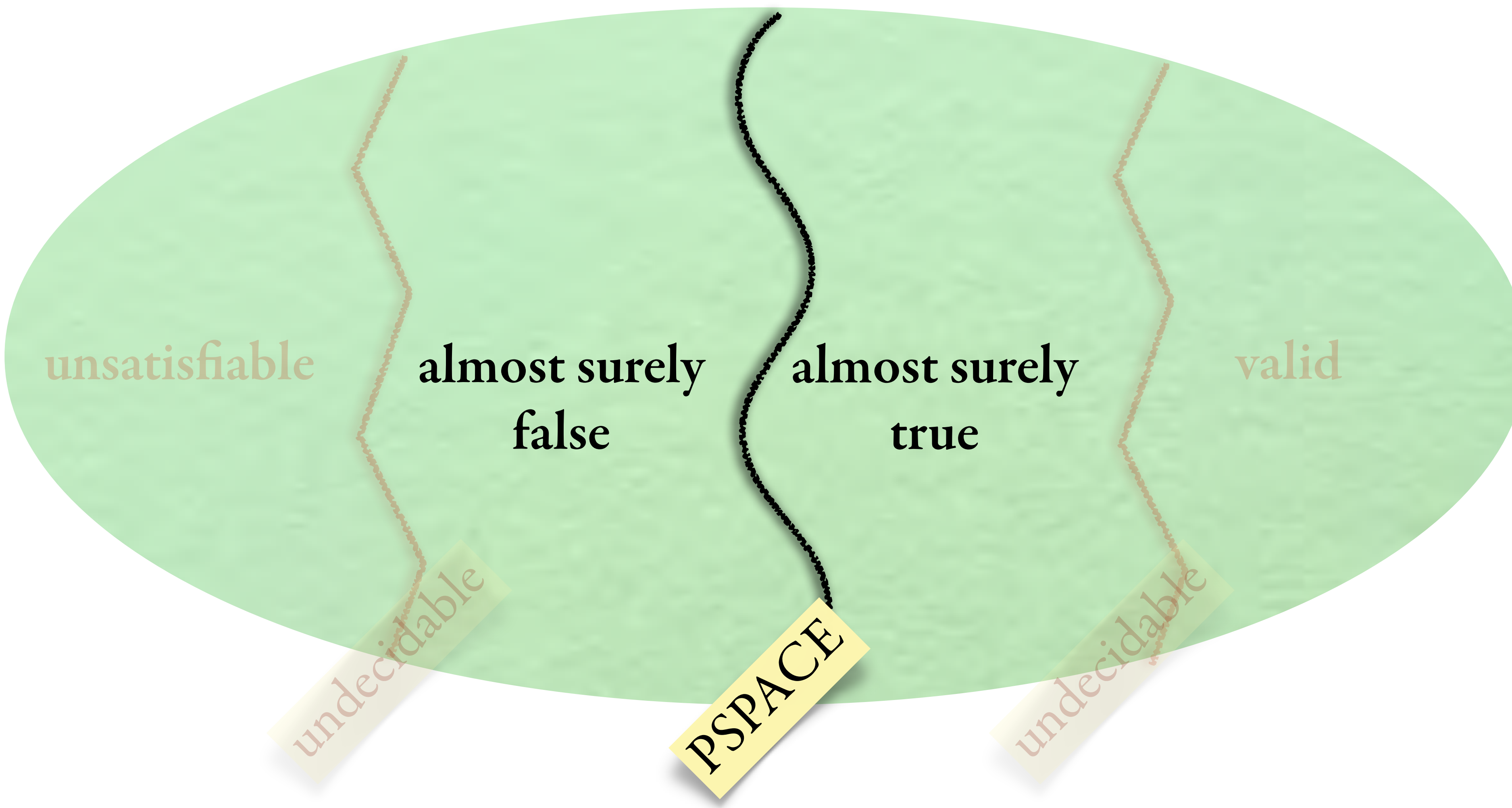
Model-checking on large graphs/databases

Don't bother checking the formula,
either it's *almost surely true* or *almost surely false*!



Probability of a formula - application

Theorem [Grandjean '83] One can decide in **PSPACE** whether ϕ is almost surely true on finite graphs

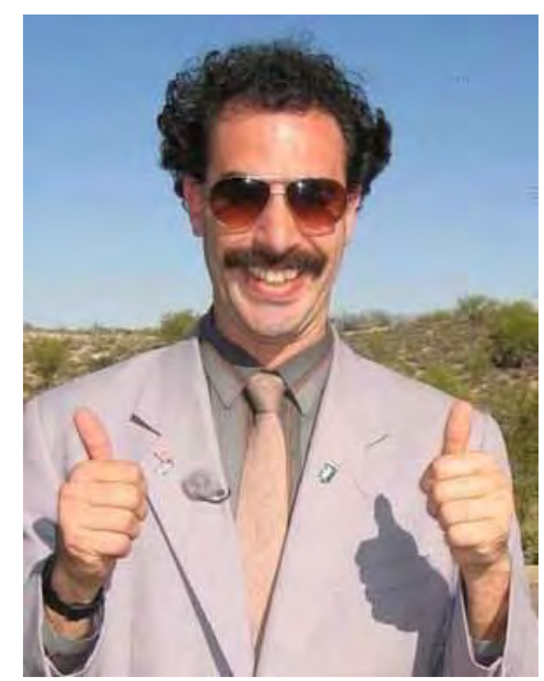


Disclaimer:

0/1 Law only applies applies to unconstrained graphs

Model-checking on large graphs/databases

Don't bother checking the formula,
either it's *almost surely true* or *almost surely false*!



Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$	=	Peano arithmetic	💀 **UNDECIDABLE** 💀 (reduction from H's 10th)
$\mathrm{FO}[\mathbb{R}, +, \cdot\,]$	=	Arithmetic theory of real numbers	🎉 **DECIDABLE** 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{Z}, +]$	=	Presburger arithmetic	🎉 **DECIDABLE** 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$	=	First-order theory of the unlabelled grid	🎉 **DECIDABLE** 🎉 (interpreted in the former)
$\mathrm{FO}[\{0,1\}, =]$	$\approx$	{Valid QBFs}	**EASY**
$\mathrm{FO}[V_R, E_R]$	=	First-order theory of "random" graph	🎉 **DECIDABLE** 🎉 (0/1 Law)
$\mathrm{FO}[C_M, T_M]$	=	First-order theory of the transition graph of a Turing machine M	

Some fancy FO theories

$\mathrm{FO}[\mathbb{N}, +, \cdot\,]$	$=$	Peano arithmetic	💀 **UNDECIDABLE** 💀 (reduction from H's 10th)
$\mathrm{FO}[\mathbb{R}, +, \cdot\,]$	$=$	Arithmetic theory of real numbers	🎉 **DECIDABLE** 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{Z}, +]$	$=$	Presburger arithmetic	🎉 **DECIDABLE** 🎉 (quantifier elimination)
$\mathrm{FO}[\mathbb{N}^2, \leq_1, \leq_2]$	$=$	First-order theory of the unlabelled grid	🎉 **DECIDABLE** 🎉 (interpreted in the former)
$\mathrm{FO}[\{0,1\}, =]$	$\approx$	{Valid QBFs}	**EASY**
$\mathrm{FO}[V_R, E_R]$	$=$	First-order theory of "random" graph	🎉 **DECIDABLE** 🎉 (0/1 Law)
$\mathrm{FO}[C_M, T_M]$	$=$	First-order theory of the transition graph of a Turing machine M	🎉 **DECIDABLE** 🎉 (automatic structure)

Things to remember

Things to remember

- FO is cool and quite expressive
- Model-checking is decidable (in **PSPACE**) when the universe is finite
  Satisfiability, validity, equivalence are all undecidable (reduction from Domino)
- For infinite universes, one can fix a model and study its FO theory
  Some FO theories are decidable, some are not
- Some FO theories can be reduced to others via FO interpretations