Complexity Theory

Polynomial Space

Daniel Borchmann, Markus Krötzsch

Computational Logic

2015-12-01

Review

Polynomial Space

The Class PSpace

We defined PSpace as:

$$\text{PSpace} = \bigcup_{d\geq 1} \text{DSpace}(n^d)$$

and we observed that

$$\text{P} \subseteq \text{NP} \subseteq \text{PSpace} = \text{NPSpace} \subseteq \text{ExpTime}.$$

We can also define a corresponding notion of PSpace-hardness:

Definition 11.1

- A language $\mathcal{H}$ is PSpace-hard, if $\mathcal{L} \leq_p \mathcal{H}$ for every language $\mathcal{L} \in \text{PSpace}$.
- A language $\mathcal{C}$ is PSpace-complete, if $\mathcal{C}$ is PSpace-hard and $\mathcal{C} \in \text{PSpace}$.

Quantified Boolean Formulae (QBF)

A QBF is a formula of the following form:

$$Q_1 X_1.Q_2 X_2.\cdots Q_\ell X_\ell.\varphi[X_1,\ldots,X_\ell]$$

where $Q_i \in \{\exists,\forall\}$ are quantifiers, X_i are propositional logic variables, and φ is a propositional logic formula with variables $X_1,\ldots,X_\ell$ and constants $\top$ (true) and $\bot$ (false)

Semantics:

- Propositional formulae without variables (only constants $\top$ and $\bot$) are evaluated as usual
- $\exists X.\varphi[X]$ is true if either $\varphi[X/\top]$ or $\varphi[X/\bot]$ are true
- $\forall X.\varphi[X]$ is true if both $\varphi[X/\top]$ and $\varphi[X/\bot]$ are true

(where $\varphi[X/\top]$ is "φ with X replaced by $\top$, and similar for $\bot$)

Deciding QBF Validity

TRUE QBF

Input: A quantified Boolean formula φ.

Problem: Is φ true (valid)?

Observation

We can assume that the quantified formula is in CNF or 3-CNF (same transformations possible as for propositional logic formulae)

Deciding QBF Validity

TRUE QBF

Input: A quantified Boolean formula φ.

Problem: Is φ true (valid)?

Observation

We can assume that the quantified formula is in CNF or 3-CNF (same transformations possible as for propositional logic formulae)

Consider a propositional logic formula φ with variables $X_1, \ldots, X_\ell$:

Example 11.2

The QBF $\exists X_1. \cdots \exists X_\ell.\varphi$ is true if and only if φ is satisfiable.

Example 11.3

The QBF $\forall X_1. \cdots \forall X_\ell.\varphi$ is true if and only if φ is a tautology.

The Power of QBF

Theorem 11.4

TRUE QBF *is* PSPACE*-complete.*

Proof.

- TRUE QBF $\in$ PSPACE:
  Give an algorithm that runs in polynomial space.
- TRUE QBF is PSPACE-hard:
  Proof by reduction from the word problem for polynomially space-bounded TMs.

Solving True QBF in PSpace

```
01 TrueQBF(φ) {
02   if φ has no quantifiers :
03     return "evaluation of φ"
04   else if φ = ∃X.ψ :
05     return (TrueQBF(ψ[X/⊤]) OR TrueQBF(ψ[X/⊥]))
06   else if φ = ∀X.ψ :
07     return (TrueQBF(ψ[X/⊤]) AND TrueQBF(ψ[X/⊥]))
08 }
```

- Evaluation in line 03 can be done in polynomial space
- Recursions in lines 05 and 07 can be executed one after the other, reusing space
- Maximum depth of recursion = number of variables (linear)
- Store one variable assignment per recursive call

$\rightsquigarrow$ polynomial space algorithm

PSPACE-Hardness of TRUE QBF

Express TM computation in logic, similar to Cook-Levin

Given:

- a polynomial p
- a p-space bounded 1-tape NTM $\mathcal{M} = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}})$
- a word w

Intended reduction

Define a QBF $\varphi_{p,\mathcal{M},w}$ such that
$\varphi_{p,\mathcal{M},w}$ is true if and only if $\mathcal{M}$ accepts w in space $p(|w|)$.

Note

We show the reduction for NTMs, which is more than needed, but makes little difference in logic and allows us to reuse our previous formulae from Cook-Levin

Review: Encoding Configurations

Use propositional variables for describing configurations:

Q_q for each $q \in Q$ means "$\mathcal{M}$ is in state $q \in Q$"

P_i for each $0 \leq i < p(n)$ means "the head is at Position i"

$S_{a,i}$ for each $a \in \Gamma$ and $0 \leq i < p(n)$ means "tape cell i contains Symbol a"

Represent configuration $(q, p, a_0 \ldots a_{p(n)})$

by assigning truth values to variables from the set

$$\overline{C} := \{Q_q, P_i, S_{a,i} \mid q \in Q, \quad a \in \Gamma, \quad 0 \leq i < p(n)\}$$

using the truth assignment β defined as

$$\beta(Q_s) := \begin{cases} 1 & s = q \\ 0 & s \neq q \end{cases} \qquad \beta(P_i) := \begin{cases} 1 & i = p \\ 0 & i \neq p \end{cases} \qquad \beta(S_{a,i}) := \begin{cases} 1 & a = a_i \\ 0 & a \neq a_i \end{cases}$$

Review: Validating Configurations

We define a formula $\textsc{Conf}(\overline{C})$ for a set of configuration variables

$$\overline{C} = \{Q_q, P_i, S_{a,i} \mid q \in Q, \quad a \in \Gamma, \quad 0 \leq i < p(n)\}$$

as follows:

$\textsc{Conf}(\overline{C}) :=$ "the assignment is a valid configuration":

$$\bigvee_{q \in Q} \Big(Q_q \wedge \bigwedge_{q' \neq q} \neg Q_{q'} \Big)$$ "TM in exactly one state $q \in Q$"

$$\wedge \bigvee_{p < p(n)} \Big(P_p \wedge \bigwedge_{p' \neq p} \neg P_{p'} \Big)$$ "head in exactly one position $p < p(n)$"

$$\wedge \bigwedge_{0 \leq i < p(n)} \bigvee_{a \in \Gamma} \Big(S_{a,i} \wedge \bigwedge_{b \neq a \in \Gamma} \neg S_{b,i} \Big)$$ "exactly one $a \in \Gamma$ in each cell"

Review: Validating Configurations

For an assignment β defined on variables in $\overline{C}$ define

$$\mathrm{conf}(\overline{C},\beta) := \left\{ (q,p,w_0 \dots w_{p(n)}) \mid \begin{array}{l} \beta(Q_q) = 1, \\ \beta(P_p) = 1, \\ \beta(S_{w_i,i}) = 1 \text{ for all } 0 \leq i < p(n) \end{array} \right\}$$

Note: β may be defined on other variables besides those in $\overline{C}$.

Lemma 11.5

If β satisfies $\textsc{Conf}(\overline{C})$ then $|\mathrm{conf}(\overline{C},\beta)| = 1$.
We can therefore write $\mathrm{conf}(\overline{C},\beta) = (q,p,w)$ to simplify notation.

Observations:

- $\mathrm{conf}(\overline{C},\beta)$ is a potential configuration of $\mathcal{M}$, but it may not be reachable from the start configuration of $\mathcal{M}$ on input w.
- Conversely, every configuration $(q,p,w_1 \dots w_{p(n)})$ induces a satisfying assignment β or which $\mathrm{conf}(\overline{C},\beta) = (q,p,w_1 \dots w_{p(n)})$.

Review: Transitions Between Configurations

Consider the following formula $\textsc{Next}(\overline{C}, \overline{C}')$ defined as

$$\textsc{Conf}(\overline{C}) \wedge \textsc{Conf}(\overline{C}') \wedge \textsc{NoChange}(\overline{C}, \overline{C}') \wedge \textsc{Change}(\overline{C}, \overline{C}').$$

$$\textsc{NoChange} := \bigvee_{0 \leq p < p(n)} \Big(P_p \wedge \bigwedge_{i \neq p, a \in \Gamma} \big(S_{a,i} \to S'_{a,i} \big) \Big)$$

$$\textsc{Change} := \bigvee_{0 \leq p < p(n)} \Big(P_p \wedge \bigvee_{\substack{q \in Q \\ a \in \Gamma}} \big(Q_q \wedge S_{a,p} \wedge \bigvee_{(q',b,D) \in \delta(q,a)} (Q'_{q'} \wedge S'_{b,p} \wedge P'_{D(p)}) \big) \Big)$$

where $D(p)$ is the position reached by moving in direction D from p.

Lemma 11.6

For any assignment β defined on $\overline{C} \cup \overline{C}'$:

β *satisfies* $\textsc{Next}(\overline{C}, \overline{C}')$ *if and only if* $\mathrm{conf}(\overline{C}, \beta) \vdash_{\mathcal{M}} \mathrm{conf}(\overline{C}', \beta)$

Review: Start and End

Defined so far:

- $\textsc{Conf}(\overline{C})$: $\overline{C}$ describes a potential configuration
- $\textsc{Next}(\overline{C}, \overline{C}')$: $\text{conf}(\overline{C},\beta) \vdash_{\mathcal{M}} \text{conf}(\overline{C}',\beta)$

Start configuration: Let $w = w_0 \cdots w_{n-1} \in \Sigma^*$ be the input word

$$\textsc{Start}_{\mathcal{M},w}(\overline{C}) := \textsc{Conf}(\overline{C}) \wedge Q_{q_0} \wedge P_0 \wedge \bigwedge_{i=0}^{n-1} S_{w_i,i} \wedge \bigwedge_{i=n}^{p(n)-1} S_{\square,i}$$

Then an assignment β satisfies $\textsc{Start}_{\mathcal{M},w}(\overline{C})$ if and only if $\overline{C}$ represents the start configuration of $\mathcal{M}$ on input w.

Accepting stop configuration:

$$\textsc{Acc-Conf}(\overline{C}) := \textsc{Conf}(\overline{C}) \wedge Q_{q_{\text{accept}}}$$

Then an assignment β satisfies $\textsc{Acc-Conf}(\overline{C})$ if and only if $\overline{C}$ represents an accepting configuration of $\mathcal{M}$.

Simulating Polynomial Space Computations

For Cook-Levin, we used one set of configuration variables for every computating step: polynomially time $\leadsto$ polynomially many variables

Problem: For polynomial space, we have $2^{O(p(n))}$ possible steps ...

Simulating Polynomial Space Computations

For Cook-Levin, we used one set of configuration variables for every computating step: polynomially time $\leadsto$ polynomially many variables

Problem: For polynomial space, we have $2^{O(p(n))}$ possible steps . . .

What would Savitch do?

Simulating Polynomial Space Computations

For Cook-Levin, we used one set of configuration variables for every computating step: polynomially time $\rightsquigarrow$ polynomially many variables

Problem: For polynomial space, we have $2^{O(p(n))}$ possible steps ...

What would Savitch do?

Define a formula $\textsc{CanYield}_i(\overline{C}_1, \overline{C}_2)$ to state that $\overline{C}_2$ is reachable from $\overline{C}_1$ in at most 2^i steps:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

Simulating Polynomial Space Computations

For Cook-Levin, we used one set of configuration variables for every computating step: polynomially time $\leadsto$ polynomially many variables

Problem: For polynomial space, we have $2^{O(p(n))}$ possible steps ...

What would Savitch do?

Define a formula $\textsc{CanYield}_i(\overline{C}_1, \overline{C}_2)$ to state that $\overline{C}_2$ is reachable from $\overline{C}_1$ in at most 2^i steps:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

But what is $\overline{C}_1 = \overline{C}_2$ supposed to mean here?

Simulating Polynomial Space Computations

For Cook-Levin, we used one set of configuration variables for every computating step: polynomially time $\rightsquigarrow$ polynomially many variables

Problem: For polynomial space, we have $2^{O(p(n))}$ possible steps ...

What would Savitch do?

Define a formula $\textsc{CanYield}_i(\overline{C}_1, \overline{C}_2)$ to state that $\overline{C}_2$ is reachable from $\overline{C}_1$ in at most 2^i steps:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

But what is $\overline{C}_1 = \overline{C}_2$ supposed to mean here? It is short for:

$$\bigwedge_{q \in Q} Q_q^1 \leftrightarrow Q_q^2 \wedge \bigwedge_{0 \leq i < p(n)} P_i^1 \leftrightarrow P_i^2 \wedge \bigwedge_{a \in \Gamma, 0 \leq i < p(n)} S_{a,i}^1 \leftrightarrow S_{a,i}^2$$

Putting Everything Together

We define the formula $\varphi_{p,\mathcal{M},w}$ as follows:

$$\varphi_{p,\mathcal{M},w} := \exists\overline{C}_1.\exists\overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

where we select d to be the least number such that $\mathcal{M}$ has less than $2^{dp(n)}$ configurations in space $p(n)$.

Lemma 11.7

$\varphi_{p,\mathcal{M},w}$ is satisfiable if and only if $\mathcal{M}$ accepts w in space $p(|w|)$.

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Now that's quite interesting . . .

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Now that's quite interesting ...

- With only (non-negated) $\exists$ quantifiers, True QBF coincides with Sat

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \lor \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \land \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \land \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \land \textsc{Acc-Conf}(\overline{C}_2) \land \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Now that's quite interesting . . .

- With only (non-negated) $\exists$ quantifiers, TRUE QBF coincides with SAT
- SAT is in NP

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1,\overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1,\overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1,\overline{C}_2) := \exists\overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1,\overline{C}) \wedge \textsc{CanYield}_i(\overline{C},\overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists\overline{C}_1.\exists\overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1,\overline{C}_2)$$

Now that's quite interesting . . .

- With only (non-negated) $\exists$ quantifiers, True QBF coincides with Sat
- Sat is in NP
- So we showed that the word problem for PSPACE NTMs to be in NP

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Now that's quite interesting . . .

- With only (non-negated) $\exists$ quantifiers, True QBF coincides with Sat
- Sat is in NP
- So we showed that the word problem for PSpace NTMs to be in NP

So we found that $\mathrm{NP} = \mathrm{PSpace}$!

Did we do it?

Note: we used only existential quantifiers when defining $\varphi_{p,\mathcal{M},w}$:

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Now that's quite interesting . . .

- With only (non-negated) $\exists$ quantifiers, True QBF coincides with Sat
- Sat is in NP
- So we showed that the word problem for PSpace NTMs to be in NP

So we found that $\mathrm{NP} = \mathrm{PSpace}$!

Strangely, most textbooks claim that this is not known to be true . . .

Are we up for the next Turing Award, or did we make a mistake?

Size

How big is $\varphi_{p,\mathcal{M},w}$?

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists\overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists\overline{C}_1.\exists\overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Size

How big is $\varphi_{p,\mathcal{M},w}$?

$$\textsc{CanYield}_0(\overline{C}_1, \overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \textsc{Next}(\overline{C}_1, \overline{C}_2)$$

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) := \exists \overline{C}.\textsc{Conf}(\overline{C}) \wedge \textsc{CanYield}_i(\overline{C}_1, \overline{C}) \wedge \textsc{CanYield}_i(\overline{C}, \overline{C}_2)$$

$$\varphi_{p,\mathcal{M},w} := \exists \overline{C}_1.\exists \overline{C}_2.\textsc{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \textsc{Acc-Conf}(\overline{C}_2) \wedge \textsc{CanYield}_{dp(n)}(\overline{C}_1, \overline{C}_2)$$

Size of $\textsc{CanYield}_{i+1}$ is more than twice the size of $\textsc{CanYield}_i$
$\rightsquigarrow$ Size of $\varphi_{p,\mathcal{M},w}$ is in $2^{O(p(n))}$. Oops.

Size

How big is $\varphi_{p,\mathcal{M},w}$?

$$\text{CanYield}_0(\overline{C}_1,\overline{C}_2) := (\overline{C}_1 = \overline{C}_2) \vee \text{Next}(\overline{C}_1,\overline{C}_2)$$
$$\text{CanYield}_{i+1}(\overline{C}_1,\overline{C}_2) := \exists\overline{C}.\text{Conf}(\overline{C}) \wedge \text{CanYield}_i(\overline{C}_1,\overline{C}) \wedge \text{CanYield}_i(\overline{C},\overline{C}_2)$$
$$\varphi_{p,\mathcal{M},w} := \exists\overline{C}_1.\exists\overline{C}_2.\text{Start}_{\mathcal{M},w}(\overline{C}_1) \wedge \text{Acc-Conf}(\overline{C}_2) \wedge \text{CanYield}_{dp(n)}(\overline{C}_1,\overline{C}_2)$$

Size of CanYield_{i+1} is more than twice the size of CanYield_i
$\rightsquigarrow$ Size of $\varphi_{p,\mathcal{M},w}$ is in $2^{O(p(n))}$. Oops.

A correct reduction: We redefine CanYield by setting

$$\text{CanYield}_{i+1}(\overline{C}_1,\overline{C}_2) :=$$
$$\exists\overline{C}.\text{Conf}(\overline{C}) \wedge$$
$$\forall\overline{Z}_1.\forall\overline{Z}_2.\big(((\overline{Z}_1 = \overline{C}_1 \wedge \overline{Z}_2 = \overline{C}) \vee (\overline{Z}_1 = \overline{C} \wedge \overline{Z}_2 = \overline{C}_2)) \rightarrow \text{CanYield}_i(\overline{Z}_1,\overline{Z}_2)\big)$$

Size

Let's analyse the size more carefully this time:

$$\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2) :=$$
$$\exists \overline{C}.\textsc{Conf}(\overline{C}) \land$$
$$\forall \overline{Z}_1.\forall \overline{Z}_2.\Big(((\overline{Z}_1 = \overline{C}_1 \land \overline{Z}_2 = \overline{C}) \lor (\overline{Z}_1 = \overline{C} \land \overline{Z}_2 = \overline{C}_2)) \to \textsc{CanYield}_i(\overline{Z}_1, \overline{Z}_2)\Big)$$

- $\textsc{CanYield}_{i+1}(\overline{C}_1, \overline{C}_2)$ extends $\textsc{CanYield}_i(\overline{C}_1, \overline{C}_2)$ by parts that are linear in the size of configurations $\leadsto$ growth in $O(p(n))$
- Maximum index i used in $\varphi_{p,\mathcal{M},w}$ is $dp(n)$, that is in $O(p(n))$
- Therefore: $\varphi_{p,\mathcal{M},w}$ has size $O(p^2(n))$ – and thus can be computed in polynomial time

Exercise:

Why can we just use $dp(n)$ in the reduction? Don't we have to compute it somehow? Maybe even in polynomial time?

The Power of QBF

Theorem 11.4

TRUE QBF *is* PSPACE*-complete.*

Proof.

- TRUE QBF $\in$ PSPACE:
  Give an algorithm that runs in polynomial space.
- TRUE QBF is PSPACE-hard:
  Proof by reduction from the word problem for polynomially space-bounded TMs.

□

A More Common Logical Problem in PSPACE

Recall standard first-order logic:

- Instead of propositional variables, we have atoms (predicates with constants and variables)
- Instead of propositional evaluations we have first-order structures (or interpretations)
- First-order quantifiers can be used on variables
- Sentences are formulae where all variables are quantified
- A sentence can be satisfied or not by a given first-order structure

A More Common Logical Problem in PSPACE

Recall standard first-order logic:

- Instead of propositional variables, we have atoms (predicates with constants and variables)
- Instead of propositional evaluations we have first-order structures (or interpretations)
- First-order quantifiers can be used on variables
- Sentences are formulae where all variables are quantified
- A sentence can be satisfied or not by a given first-order structure

FOL MODEL CHECKING

Input: A first-orer sentence φ and a finite first-order structure $\mathcal{I}$.

Problem: Is φ satisfied by $\mathcal{I}$?

First-Order Logic is PSpace-complete

Theorem 11.8

FOL Model Checking *is* PSpace*-complete.*

Proof.

- FOL Model Checking $\in$ PSpace:
  Give algorithm that runs in polynomial space.
- FOL Model Checking is PSpace-hard:
  Proof by reduction True QBF $\leq_p$ FOL Model Checking.

Checking FOL Models in Polynomial Space (Sketch)

```
Eval(φ, I) {
  switch (φ) :
    case p(c_1, ..., c_n) :  return ⟨c_1, ..., c_n⟩ ∈ p^I
    case ¬ψ :  return NOT Eval(ψ, I)
    case ψ_1 ∧ ψ_2 :  return Eval(ψ_1, I) AND Eval(ψ_2, I)
    case ∃x.ψ :
      for c ∈ Δ^I :
        if Eval(ψ[x ↦ c], I) :  return TRUE
      // eventually, if no success:
      return FALSE
}
```

- We can assume φ only uses $\neg$, $\wedge$ and $\exists$ (easy to get)
- We use $\Delta^{\mathcal{I}}$ to denote the (finite!) domain of $\mathcal{I}$
- We allow domain elements to be used like constants in the formula

Hardness of FOL Model Checking

Given: a QBF $\varphi = \mathsf{Q}_1 X_1 . \cdots \mathsf{Q}_\ell X_\ell . \psi$

FOL Model Checking Problem:

- Interpretation domain $\Delta^{\mathcal{I}} := \{0, 1\}$
- Single predicate symbol true with interpretation $\mathrm{true}^{\mathcal{I}} = \{\langle 1 \rangle\}$
- FOL formula φ' is obtained by replacing variables in input QBF with corresponding first-order expressions:

$$\mathsf{Q}_1 x_1 . \cdots \mathsf{Q}_\ell x_\ell . \psi[X_1 \mapsto \mathrm{true}(x_1), \ldots, X_\ell \mapsto \mathrm{true}(x_\ell)]$$

Lemma 11.9

$\langle \mathcal{I}, \varphi' \rangle \in$ FOL Model Checking *if and only if* $\varphi \in$ True QBF.

First-Order Logic is PSPACE-complete

Theorem 11.8

FOL MODEL CHECKING *is* PSPACE*-complete.*

Proof.

- FOL MODEL CHECKING $\in$ PSPACE:
  Give algorithm that runs in polynomial space.
- FOL MODEL CHECKING is PSPACE-hard:
  Proof by reduction TRUE QBF $\leq_p$ FOL MODEL CHECKING.

□

FOL MODEL CHECKING: Practical Significance

Why is FOL MODEL CHECKING a relevant problem?

FOL Model Checking: Practical Significance

Why is FOL Model Checking a relevant problem?

Correspondence with database query answering:

- Finite first-order interpretation = database
- First-order logic formula = database query
- Satisfying assignments (for non-sentences) = query results

Known correspondence:

As a query language, FOL has the same expressive power as (basic) SQL (relational algebra).

Corollary 11.10

Answering SQL queries over a given database is $\mathrm{PS{\scriptsize PACE}}$*-complete.*

Games

Games as Computational Problems

Many single-player games relate to NP-complete problems:

- Sudoku
- Minesweeper
- Tetris
- ...

Decision problem: Is there a solution?

(For Tetris: is it possible to clear all blocks?)

What about two-player games?

Games as Computational Problems

Many single-player games relate to NP-complete problems:

- Sudoku
- Minesweeper
- Tetris
- ...

Decision problem: Is there a solution?

(For Tetris: is it possible to clear all blocks?)

What about two-player games?

- Two players take moves in turns
- The players have different goals
- The game ends if a player wins

Decision problem: Does Player 1 have a winnings strategy?

In other words: can Player 1 enforce winning, whatever Player 2 does?

Coming Up Next

- How hard is it to determine if there is a winning strategy?
- Which games should we study?

To be continued . . .