Quasipolynomial Computation of Nested Fixpoints

Daniel Hausmann and Lutz Schröder, University Erlangen-Nuremberg

Gothenburg, Formal Methods Seminar – February 25 2021

Why Nested Fixpoints?

- Applications of parity games:
  - Model checking for the modal μ-calculus
  - Satisfiability checking for the modal μ-calculus
  - Synthesis for linear-time logics (e.g. LTL)

- Recent breakthrough result: solving parity games is in QP

Why Nested Fixpoints?

- Applications of parity games:
  - Model checking for the modal μ-calculus
  - Satisfiability checking for the modal μ-calculus
  - Synthesis for linear-time logics (e.g. LTL)

- Recent breakthrough result: solving parity games is in QP

- Winning regions of parity games are specific nested fixpoints

Why Nested Fixpoints?

- Applications of parity games:
  - Model checking for the modal μ-calculus
  - Satisfiability checking for the modal μ-calculus
  - Synthesis for linear-time logics (e.g. LTL)
- Recent breakthrough result: solving parity games is in QP
- Winning regions of parity games are specific nested fixpoints
- Idea: Use QP parity game solving algorithm to compute general nested fixpoints, obtain same results for more general games / logics.

Why Nested Fixpoints?

- Applications of parity games:
  - Model checking for the modal μ-calculus
  - Satisfiability checking for the modal μ-calculus
  - Synthesis for linear-time logics (e.g. LTL)

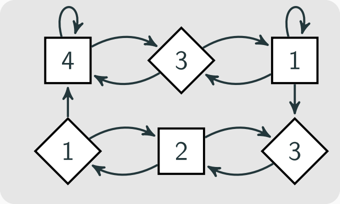
- Recent breakthrough result: solving parity games is in QP
- Winning regions of parity games are specific nested fixpoints
- Idea: Use QP parity game solving algorithm to compute general nested fixpoints, obtain same results for more general games / logics.

We show:

- Nested fixpoints stabilize after quasipolynomially many iterations.

Motivation: Parity Games

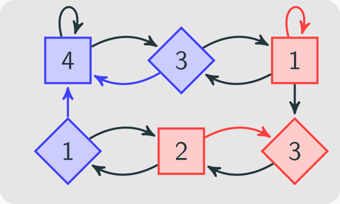
Parity games: $(V = V_\diamond \mathbin{\dot\cup} V_\Box, E \subseteq V \times V, \Omega : V \to [k])$, $[k] = \{0, \dots, k\}$



- $\diamond$-strategy: $s : V^* V_\diamond \to V$ such that $s(\bar{v}v) \in E(v)$
- $\diamond$ wins $v \in V$ iff there is $\diamond$-strategy with which all v-plays are even

Motivation: Parity Games

Parity games: $(V = V_\Diamond \cup V_\Box, E \subseteq V \times V, \Omega : V \to [k])$, $[k] = \{0, \dots, k\}$



- history-free $\Diamond$-strategy: $s : V_\Diamond \to V$ such that $s(v) \in E(v)$
- $\Diamond$ wins $v \in V$ iff there is $\Diamond$-strategy with which all v-plays are even

Central result: parity games are history-free determined.

Observation: $\mathrm{win}_\Diamond$ (and $\mathrm{win}_\Box$) can be specified by μ-calculus formula.

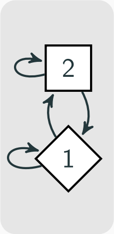
Motivation: Reducing Parity Games to Safety Games

Idea: Use deterministic Büchi automaton $A = (Q, [k], \delta, F)$ accepting exactly the even priority sequences in $G = (V, E, \Omega : V \to [k])$.

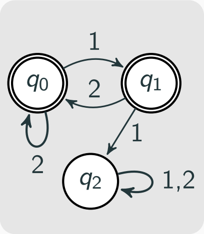
Parity game G is equivalent to safety game $G \bowtie A = (V \times Q, E \bowtie \delta, F \circ \pi_2)$,

$$(E \bowtie \delta)(v, q) = \{(w, \delta(q, \Omega(v)) \mid w \in E(v)\}$$

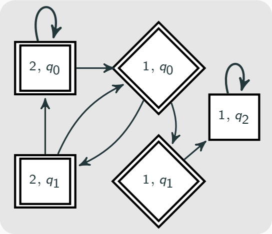
G :



A :



$G \bowtie A$:



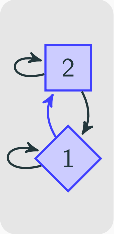
Motivation: Reducing Parity Games to Safety Games

Idea: Use deterministic Büchi automaton $A = (Q, [k], \delta, F)$ accepting exactly the even priority sequences in $G = (V, E, \Omega : V \to [k])$.

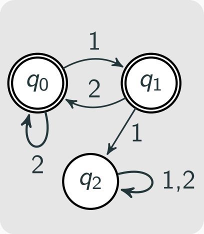
Parity game G is equivalent to safety game $G \bowtie A = (V \times Q, E \bowtie \delta, F \circ \pi_2)$,

$$(E \bowtie \delta)(v, q) = \{(w, \delta(q, \Omega(v)) \mid w \in E(v)\}$$

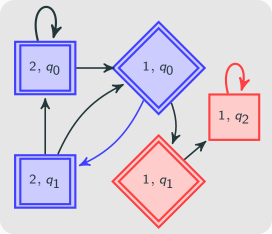
G :



A :



$G \bowtie A$:

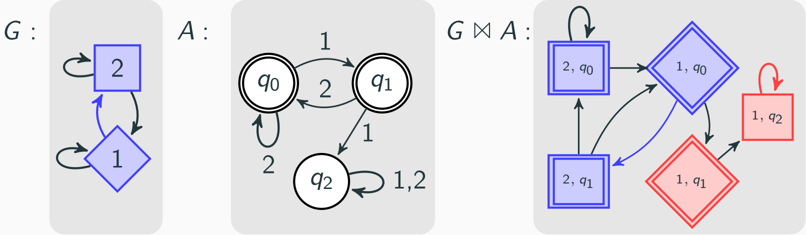


Motivation: Reducing Parity Games to Safety Games

Idea: Use deterministic Büchi automaton $A = (Q, [k], \delta, F)$ accepting exactly the even priority sequences in $G = (V, E, \Omega : V \to [k])$.

Parity game G is equivalent to safety game $G \bowtie A = (V \times Q, E \bowtie \delta, F \circ \pi_2)$,

$$(E \bowtie \delta)(v, q) = \{(w, \delta(q, \Omega(v)) \mid w \in E(v)\}$$



Size of suitable automaton A?

- Immediate: $|Q| \in \mathcal{O}(|V|^{\frac{k}{2}})$
- Calude et al., 2017: $|Q| \in \mathcal{O}(|V|^{\log k})$, $|Q| \in \mathcal{O}(|V|^4)$ if $k \leq \log |V|$

Finite Lattices

Finite lattice: $(L, \sqsubseteq)$, $L \neq \emptyset$ finite set, $\sqsubseteq$ partial order on L s.t. join $\bigsqcup X$ and meet $\bigsqcap X$ exist for all $X \subseteq L$.

Basis of L: $B_L \subseteq L$ s.t. $l = \bigsqcup\{b \in B_L \mid b \sqsubseteq l\}$ for all $l \in L$.

Examples

- For finite set V, powerset lattice $(\mathcal{P}(V), \subseteq)$ is finite lattice with join $\bigcup U$, meet $\bigcap U$ for $U \in \mathcal{P}(V)$; V is a basis.
- For finite set V and number n, $(n^V, \sqsubseteq)$ is finite lattice, where $n^V = \{f : V \to [n-1]\}$, $f \sqsubseteq g$ iff for all $v \in V$, $f(v) \leq g(v)$.

Fix a finite lattice L and basis B_L.

Systems of Fixpoint Equations

Function $f : L^{k+1} \to L$ is monotone if for all $U_i \sqsubseteq V_i$, $0 \leq i \leq k$,

$$f(U_0, \dots, U_k) \sqsubseteq f(V_0, \dots, V_k)$$

Extremal fixpoints, systems of fixpoint equations

Let $f : L \to L$ and $f_i : L^{k+1} \to L$, $0 \leq i \leq k$ be monotone functions.

$$\mathsf{LFP}\, f = \bigsqcap \{Z \sqsubseteq U \mid f(Z) \sqsubseteq Z\} \qquad \mathsf{GFP}\, f = \bigsqcup \{Z \sqsubseteq U \mid Z \sqsubseteq f(Z)\}$$

System of fixpoint equations:

$$X_i =_{\eta_i} f_i(X_0, \dots, X_k) \qquad\qquad 0 \leq i \leq k, \eta_i \in \{\mathsf{LFP}, \mathsf{GFP}\}$$

Semantics of Fixpoint Equation Systems

Fix equation system $\mathbb{E}$ of $k+1$ equations $X_i =_{\eta_i} f_i(X_0, \dots, X_k)$.

Semantics of fixpoint equation systems

For valuation $\sigma : [k] \rightharpoonup L$, put $[\![X_i]\!]^\sigma = \eta_i\, f_i^\sigma$ where, for $A \in L$,

$$f_i^\sigma(A) = f_i([\![X_0]\!]^{\sigma[A/i]}, \dots, [\![X_{i-1}]\!]^{\sigma[A/i]}, A, \sigma(i+1), \dots, \sigma(k))$$

Solution for variable X_k in $\mathbb{E}$: $[\![X_k]\!]_{\mathbb{E}} = [\![X_k]\!]^{\epsilon}$, where $\mathrm{dom}(\epsilon) = \emptyset$.

Example: Parity Games

For parity game $(V, E, \Omega : V \to [k])$, use lattice $L = \mathcal{P}(V)$ and define

$$\mathrm{force}(U) = \{v \in V_\Diamond \mid E(v) \cap U \neq \emptyset\} \cup \{v \in V_\Box \mid E(v) \subseteq U\}$$

$$f_{\mathsf{PG}}(X_0, \ldots, X_k) = \bigcup_{0 \le i \le k} (\{v \in V \mid \Omega(v) = i\} \cap \mathrm{force}(X_i))$$

Define equation system: $\eta_i = \mathsf{LFP}$ if i odd, $\eta_i = \mathsf{GFP}$ otherwise and

$$X_0 =_{\mathsf{GFP}} f_{\mathsf{PG}}(X_0, \ldots, X_k) \qquad\qquad X_i =_{\eta_i} X_{i-1} \text{ for } i > 0,$$

Theorem (e.g. [Dawar, Grädel, 2008])

$$\mathrm{win}_\Diamond = [\![X_k]\!]_{f_{\mathsf{PG}}}$$

History-freeness for Equation Systems

Even k-graph: $G = (W, \delta \subseteq W \times [k] \times W)$ s.t. all δ-paths are even

Definition: History-free witnesses

Even k-graph (V, S) s.t. $V = B_L \times [k]$ and for all $(u, j) \in V$,

$$u \sqsubseteq f_j(S_0(u, j), \ldots, S_k(u, j))$$

where $S_i(u, j) = \bigsqcup\{(w, i) \mid ((u, j), i, (w, i)) \in S\}$

Note: $|V| \in \mathcal{O}(|B_L| \cdot (k + 1))$

Lemma

There is history-free witness s.t. $(u, j) \in V$ if and only if $u \sqsubseteq [\![X_j]\!]_{\mathbb{E}}$.

Universal Graphs

Definition - Universal Graphs [Colcombet, Fijalkow, 2019]

Homomorphism from $G = (W, \delta)$ to $G' = (W', \delta')$: $h : W \to W'$ s.t.

$$\text{for all } (v, p, w) \in \delta, \text{ we have } (h(v), p, h(w)) \in \delta'.$$

(n, k)-universal graph S: even k-graph s.t. for all even k-graphs G with $|G| \leq n$, there is homomorphism from G to S.

Theorem [Czerwiński et al., 2019]

- There is a deterministic (n, k)-universal graph of size $n^{\log k + \mathcal{O}(1)}$, and of size $\mathcal{O}(n^4)$ if $k \leq \log n$.
- Every (n, k)-universal graph has size at least $n^{\log \frac{k}{\log n} - 1}$.

Solving Equation Systems using Universal Graphs

Fix deterministic $((|B_L|(k+1), k+1)$-universal graph $S = (W, \delta)$.

Definition - Product fixpoint

Define $\mathbb{E} \bowtie S : \mathcal{P}(B_L \times [k] \times W) \to \mathcal{P}(B_L \times [k] \times W)$ by

$$(\mathbb{E} \bowtie S)(Z) = \{(v, p, q) \in B_L \times [k] \times W \mid v \sqsubseteq f_p(Z_0^q, \dots, Z_k^q)\}$$

where

$$Z_i^q = \bigsqcup \{u \in B_L \mid (u, i, \delta(q, i)) \in Z\}.$$

$Y =_{\mathsf{GFP}} (\mathbb{E} \bowtie S)(Y)$ is chained product fixpoint of $\mathbb{E}$ and S.

Theorem

We have $u \sqsubseteq [\![X_i]\!]_{\mathbb{E}}$ if and only if there is $q \in W$ s.t. $(u, i, q) \in [\![Y]\!]_{\mathbb{E} \bowtie S}$.

A Progress Measure Algorithm

Fix total simulation order $\leq$ on W, least node w.r.t. $\leq$: $q_{\min}$

Measure: $\mu\colon B_L \times [k] \to W \cup \{\star\}$; define function Lift on measures:

$$(\mathrm{Lift}(\mu))(v,p) = \min\{q \in W \mid v \sqsubseteq f_p(U_0^{\mu,q}, \dots, U_k^{\mu,q})\}$$

where $\min(\emptyset) = \star$ and

$$U_i^{\mu,q} = \bigsqcup\{u \in B_L \mid \mu(u,i) \leq \delta(q,i)\},$$

Lifting algorithm

1. Initialize $\mu(v,p) = q_{\min}$ for all $(v,p) \in B_L \times [k]$.
2. If $\mathrm{Lift}(\mu) \neq \mu$, then put $\mu := \mathrm{Lift}(\mu)$ and go to 2. Otherwise go to 3.
3. Return $\mathbb{B} = \{(v,p) \in B_L \times [k] \mid \mu(v,p) \neq \star\}$.

Theorem

We have $(v,p) \in \mathbb{B}$ if and only if $v \sqsubseteq [\![X_p]\!]_{\mathbb{E}}$.

Recent Results on the Coalgebraic μ-Calculus

Coalgebraic μ-calculus [Cirstea, Kupke, Pattinson 2011]:
Generic fixpoint logic framework, subsuming e.g. graded, probabilistic and alternating-time μ-calculi

Recent Results on the Coalgebraic μ-Calculus

Coalgebraic μ-calculus [Cirstea, Kupke, Pattinson 2011]:
Generic fixpoint logic framework, subsuming e.g. graded, probabilistic and alternating-time μ-calculi

- Reduction of model checking [H., Schröder, CONCUR 2019] for the coalgebraic μ-calculus to solving fixpoint equation systems.

Corollary

Model checking for coalgebraic μ-calculi is in QP.

Recent Results on the Coalgebraic μ-Calculus

Coalgebraic μ-calculus [Cirstea, Kupke, Pattinson 2011]:
Generic fixpoint logic framework, subsuming e.g. graded, probabilistic and alternating-time μ-calculi

- Reduction of model checking [H., Schröder, CONCUR 2019] for the coalgebraic μ-calculus to solving fixpoint equation systems.

Corollary

Model checking for coalgebraic μ-calculi is in QP.

- Reduction of satisfiability checking [H., Schröder, FoSSaCS 2019] for the coalgebraic μ-calculus to solving fixpoint equation systems.

Corollary

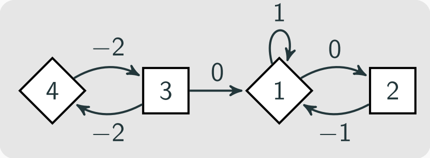
Satisfiability checking for coalgebraic μ-calculi can be done in time $\mathcal{O}(2^{nk \log n})$ (down from $\mathcal{O}(2^{n^2 k^2 \log n})$).

More Examples, Many-valued Games and Logics

- Finite latticed μ-calculus [Bruns, Godefroid, 2004], latticed parity games [Kupferman, Lustig, 2007]
- Games / logics with combined parity and quantitative objective:
  - Energy parity games [Chatterjee, Doyen, 2012], energy μ-calculus [Amram, Maoz, Pistiner, Ringert, 2020]
  - Mean-payoff parity games; recover [Daviaud, Jurdzinski, Lazic, 2018]

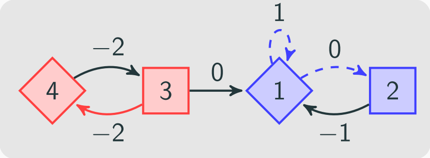
Example, Energy Parity Games

Energy parity game: (V, E, Ω, w), $w : E \to \mathbb{Z}$; player $\diamond$ wins even plays with starting credit c if energy value always remains non-negative.



Example, Energy Parity Games

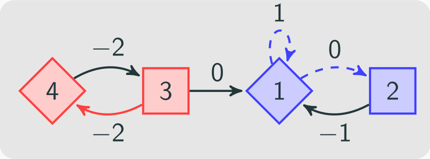
Energy parity game: (V, E, Ω, w), $w : E \to \mathbb{Z}$; player $\diamond$ wins even plays with starting credit c if energy value always remains non-negative.



- History-dependent $\diamond$-strategies: $s(1) = 1$, $s(1, 1) = 2$
- [Chatterjee, Doyen, 2012]: bound on history $c = |V| \cdot k \cdot W$

Example, Energy Parity Games

Energy parity game: (V, E, Ω, w), $w : E \to \mathbb{Z}$; player $\Diamond$ wins even plays with starting credit c if energy value always remains non-negative.



- History-dependent $\Diamond$-strategies: $s(1) = 1$, $s(1,1) = 2$
- [Chatterjee, Doyen, 2012]: bound on history $c = |V| \cdot k \cdot W$

Equation system over lattice $L = c^V$ with elements $g : V \to \{0, \dots, c\}$

Function $f_{\mathsf{EPG}} : L^{k+1} \to L$ is formula of energy μ-calculus.

Theorem [Amram, Maoz, Pistiner, Ringert, 2020]

Player $\Diamond$ wins v with initial credit c if and only if $([\![X_k]\!]_{f_{\mathsf{EPG}}})(v) = c$.

Results: Overview

Unifying progress measure algorithm leads to novel complexity results:

setting	game solving	model checking	satisfiability checking
coalgebraic	QP	QP	$2^{\mathcal{O}(nk \log n)}$
latticed	QP	QP	?
energy	pseudo-QP	QP in c	?
mean pay-off	pseudo-QP	?	?

Conclusion

Results:

- Quasipolynomial solving of fixpoint equations by universal graphs
- Highly general quasipolynomial progress measure algorithm for
  - Energy parity games, model checking energy μ-calculus
  - Latticed parity games, model checking finite latticed μ-calculi
  - Coalgebraic parity games, model checking / satisfiability checking for coalgebraic μ-calculus

Future work:

- Cover more variants of games (e.g. stochastic setting)
- Does this work for all games with finite-history strategies?

G. Amram, S. Maoz, O. Pistiner, and J. O. Ringert.
Energy mu-calculus: Symbolic fixed-point algorithms for omega-regular energy games.
CoRR, abs/2005.00641, 2020.

G. Bruns and P. Godefroid.
Model checking with multi-valued logics.
In *Automata, Languages and Programming, ICALP 2004*, volume 3142 of *LNCS*, pages 281–293. Springer, 2004.

C. S. Calude, S. Jain, B. Khoussainov, W. Li, and F. Stephan.
Deciding parity games in quasipolynomial time.
In *Theory of Computing, STOC 2017*, pages 252–263. ACM, 2017.

References ii

K. Chatterjee and L. Doyen.
Energy parity games.
Theor. Comput. Sci., 458:49–60, 2012.

C. Cîrstea, C. Kupke, and D. Pattinson.
EXPTIME tableaux for the coalgebraic μ-calculus.
Log. Meth. Comput. Sci., 7, 2011.

T. Colcombet and N. Fijalkow.
Universal graphs and good for games automata: New tools for infinite duration games.
In *Foundations of Software Science and Computation Structures, FOSSACS 2019*, volume 11425 of *LNCS*, pages 1–26. Springer, 2019.

W. Czerwinski, L. Daviaud, N. Fijalkow, M. Jurdzinski, R. Lazic, and P. Parys.
Universal trees grow inside separating automata: Quasi-polynomial lower bounds for parity games.
In *Symposium on Discrete Algorithms, SODA 2019*, pages 2333–2349. SIAM, 2019.

A. Dawar and E. Grädel.
The descriptive complexity of parity games.
In *Computer Science Logic, CSL 2008*, volume 5213 of *LNCS*, pages 354–368. Springer, 2008.

References iv

D. Hausmann and L. Schröder.
Game-based local model checking for the coalgebraic μ-calculus.
In *Concurrency Theory, CONCUR 2019*, volume 140 of *LIPIcs*, pages 35:1–35:16. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019.

D. Hausmann and L. Schröder.
Optimal satisfiability checking for arithmetic μ-calculi.
In *Foundations of Software Science and Computation Structures, FOSSACS 2019*, volume 11425 of *LNCS*, pages 277–294. Springer, 2019.

References v

O. Kupferman and Y. Lustig.
Latticed simulation relations and games.
In *Automated Technology for Verification and Analysis, ATVA 2007*, volume 4762 of *LNCS*, pages 316–330. Springer, 2007.

A Tool: Fixpoint Parity Games (Venema, Baldan et al.)

Fixpoint parity game for equation system $\mathbb{E}$

Parity game (V, E, Ω), nodes: $V = (B_L \times [k]) \cup L^{k+1}$

node	priority	owner	moves to
$(u, j) \in B_L \times [k]$	$\mathsf{ad}(j)$	$\Diamond$	$\{\mathbf{U} \in L^k \mid u \sqsubseteq f_j(\mathbf{U})\}$
$\mathbf{U}$	0	$\Box$	$\{(v, i) \mid v \in U_i\}$

where $\mathbf{U} = (U_0, \ldots, U_k) \in L^{k+1}$

Theorem [König et al. 2019]

Eloise wins node (u, i) if and only if $u \in [\![X_i]\!]_{\mathbb{E}}$.

Problem: exponential size

- still useful, e.g. for showing *history-freeness* for equation systems.