Right linear lattices:

An equational theory of alternating parity automata

GT Scalp '24

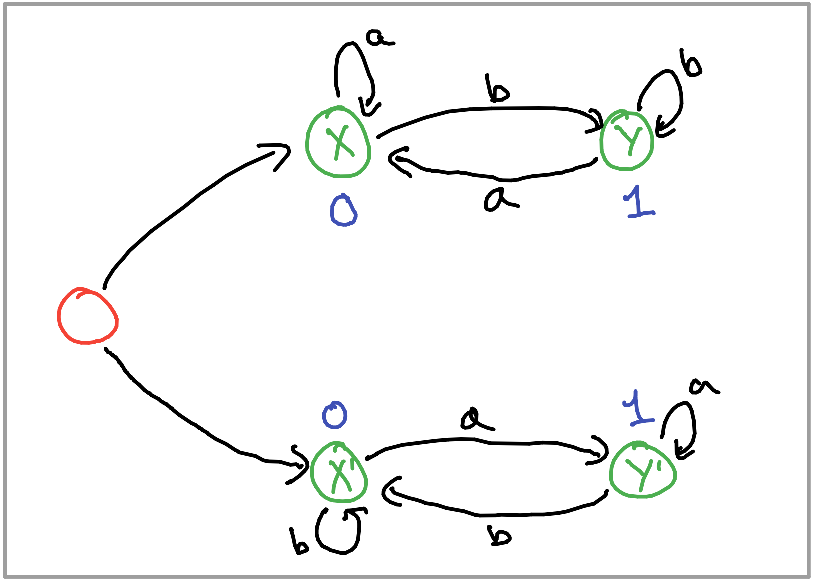
18 November 2024

Anupam Das

University of Birmingham

j.w.i.p.w.
Abhishek De

ALTERNATING PARITY AUTOMATA (APAs) OVER ω-WORDS



Accepts ω-words over $\{a, b\}$ with ∞ a's and ∞ b's.

REASONING ABOUT APAs

Right-Linear Lattice (RLL) Expressions

$$
\boxed{\begin{array}{rl} e, f, \ldots ::= & X \mid ae \mid 0 \mid e+f \mid \mu X e \\ & \mid \top \mid e \cap f \mid \nu X e \end{array}}
$$

dual

no general products, unlike reg. exprs.

We construe RLL-expressions as a notation for APAs.

Right-Linear Lattice (RLL) Expressions

$$e, f, \ldots ::= X \mid ae \mid 0 \mid e+f \mid \mu X e$$
$$\mid \top \mid e \cap f \mid \nu X e$$

dual

no general products, unlike reg. exprs.

We construe RLL-expressions as a notation for APAs.

Semantics

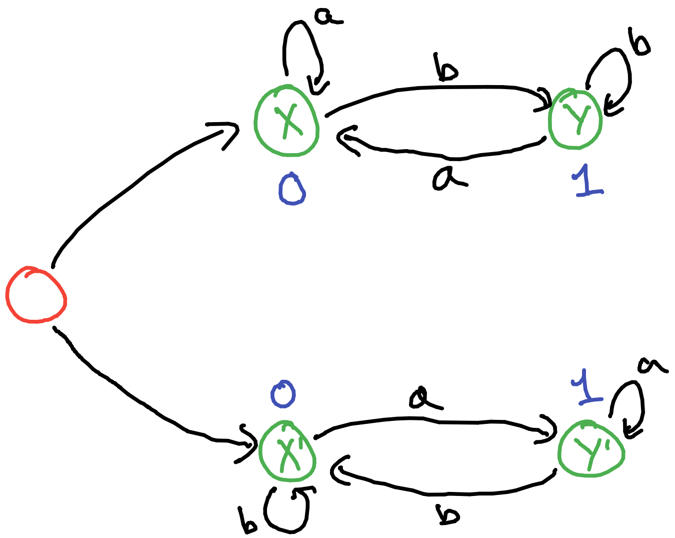
$\mathcal{L}(e) \subseteq \mathcal{A}^\omega$ by $\mathcal{L}(ae) := \{aw : w \in \mathcal{L}(e)\}$ and:

$\mathcal{L}(0) := \emptyset$ $\qquad$ $\mathcal{L}(\top) := \mathcal{A}^\omega$

$\mathcal{L}(e+f) := \mathcal{L}(e) \cup \mathcal{L}(f)$ $\qquad$ $\mathcal{L}(e \cap f) := \mathcal{L}(e) \cap \mathcal{L}(f)$

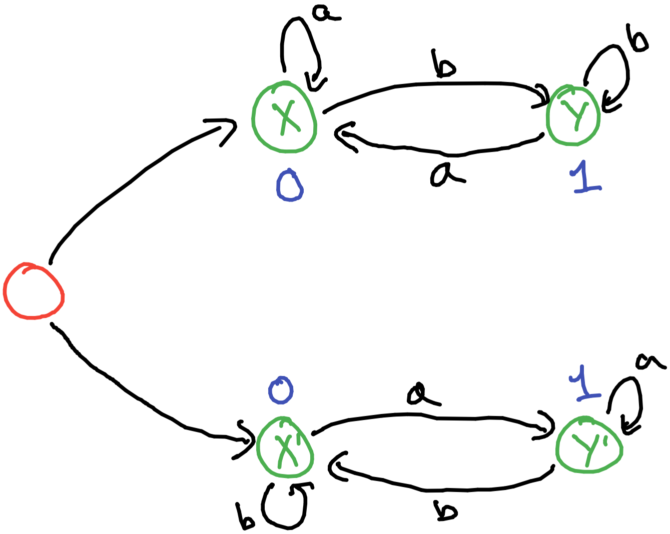
$\mathcal{L}(\mu X e(X)) := \mathrm{LFP}[A \mapsto \mathcal{L}(e(A))]$ $\qquad$ $\mathcal{L}(\nu X e(X)) := \mathrm{GFP}[A \mapsto \mathcal{L}(e(A))]$

EXAMPLE



$$\nu X \mu Y (aX + bY) \cap \nu X' \mu Y' (aY' + bX')$$

EXAMPLE



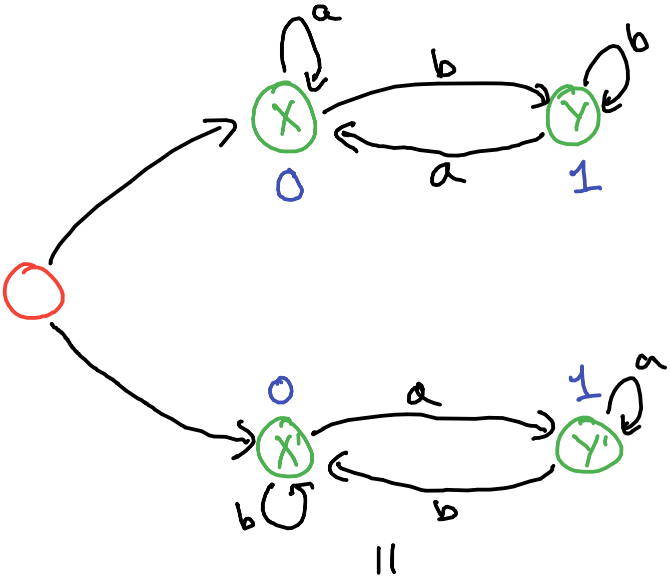
$$\boxed{\nu X \mu Y(aX + bY) \cap \nu X' \mu Y'(aY' + bX')}$$

Evaluation games

Position	Player	Available moves
(aw, ae)	$\exists$	(w, e)
(aw, be) with $a \neq b$	$\exists$	
$(w, e + f)$	$\exists$	(w, e), (w, f)
$(w, e \cap f)$	$\forall$	(w, e), (w, f)
$(w, \mu X e(X))$	-	$(w, e(\mu X e(X)))$
$(w, \nu X e(X))$	-	$(w, e(\nu X e(X)))$

- $\exists$ wins if smallest inf. occ. fmla. is ν.
- $\exists$ has win strat from $(w,e) \Leftrightarrow w \in \mathcal{L}(e)$

EXAMPLE



$$\nu X \mu Y (aX + bY) \cap \nu X' \mu Y' (aY' + bX')$$

Evaluation games

Position	Player	Available moves
(aw, ae)	$\exists$	(w, e)
(aw, be) with $a \neq b$	$\exists$	
$(w, e+f)$	$\exists$	(w,e), (w,f)
$(w, e \cap f)$	$\forall$	(w,e), (w,f)
$(w, \mu X e(X))$	-	$(w, e(\mu X e(X)))$
$(w, \nu X e(X))$	-	$(w, e(\nu X e(X)))$

- $\exists$ wins if smallest inf. oc. fmla. is ν.
- $\exists$ has win strat from $(w,e) \iff w \in \mathcal{L}(e)$

QUESTION: How to axiomatise the RLL theory of $\mathcal{L}$?

Some RLL-principles of $\mathcal{L}$ – an attempted axiomatisation

(1) $(0, \top, +, \cap)$ forms a bounded distributive lattice

(2) Each $a \in \mathcal{A}$ is a lower-bounded lattice homomorphism:

$$\boxed{a0 = 0 \qquad a(e+f) = ae + af \qquad a(e \cap f) = ae \cap af}$$

(3) The ranges of $a \in \mathcal{A}$ partition the domain:

$$\boxed{ae \cap bf = 0 \ (a \neq b) \qquad \sum_{a \in \mathcal{A}} a\top = \top}$$

Some RLL-principles of $\mathcal{L}$ – an attempted axiomatisation

(1) $(0, \top, +, \cap)$ forms a bounded distributive lattice

(2) Each $a \in \mathcal{A}$ is a lower-bounded lattice homomorphism:

$$a0 = 0 \qquad a(e+f) = ae + af \qquad a(e \cap f) = ae \cap af$$

(3) The ranges of $a \in \mathcal{A}$ partition the domain:

$$ae \cap bf = 0 \ (a \neq b) \qquad \sum_{a \in \mathcal{A}} a\top = \top$$

(4) $\mu X e(X)$ is the least prefixed point of $X \mapsto e(X)$:

$$e(\mu X e(X)) \leq \mu X e(X) \qquad e(f) \leq f \implies \mu X e(X) \leq f$$

(5) $\nu X e(X)$ is the greatest postfixed point of $X \mapsto e(X)$:

$$\nu X e(X) \leq e(\nu X e(X)) \qquad f \leq e(f) \implies f \leq \nu X e(X)$$

Main Results

- Cyclic system induced by (1) - (5) is sound & complete for $\mathcal{L}$.
- (1) - (5) is incomplete for $\mathcal{L}$!
- A natural axiomatisation extending (1) - (5) is sound & complete for $\mathcal{L}$.

A CYCLIC SYSTEM: CRLL

System $\widehat{\text{LRLL}}$

$\mathcal{A}$ rules:

$$\text{p-}l\ \frac{}{ae, bf \to}\ a \neq b \qquad \mathsf{h}_a\ \frac{\Gamma \to \Delta}{a\Gamma \to a\Delta}\ \Gamma \neq \varnothing \qquad \text{p-}r\ \frac{\{\to \Gamma_a\}_{a\in\mathcal{A}}}{\to \{a\Gamma_a\}_{a\in\mathcal{A}}}$$

(2) - (3)

Identity and Structural rules:

$$\mathsf{id}\ \frac{}{e \to e} \qquad \text{w-}l\ \frac{\Gamma \to \Delta}{\Gamma, e \to \Delta} \qquad \text{w-}r\ \frac{\Gamma \to \Delta}{\Gamma \to \Delta, e}$$

Left logical rules:

$$+\text{-}l\ \frac{\Gamma, e \to \Delta \quad f \to \Delta}{\Gamma, e + f \to \Delta} \qquad \cap\text{-}l\ \frac{\Gamma, e, f \to \Delta}{\Gamma, e \cap f \to \Delta}$$

$$\mu\text{-}l\ \frac{\Gamma, e(\mu X e(X)) \to \Delta}{\Gamma, \mu X e(X) \to \Delta} \qquad \nu\text{-}l\ \frac{\Gamma, e(\nu X e(X)) \to \Delta}{\Gamma, \nu X e(X) \to \Delta}$$

Right logical rules:

$$+\text{-}r\ \frac{\Gamma \to \Delta, e, f}{\Gamma \to \Delta, e + f} \qquad \cap\text{-}r\ \frac{\Gamma \to \Delta, e \quad \Gamma \to \Delta, f}{\Gamma \to \Delta, e \cap f}$$

$$\mu\text{-}r\ \frac{\Gamma \to \Delta, e(\mu X e(X))}{\Gamma \to \Delta, \mu X e(X)} \qquad \nu\text{-}r\ \frac{\Gamma \to \Delta, e(\nu X e(X))}{\Gamma \to \Delta, \nu X e(X)}$$

Sequents: $\Gamma \to \Delta$

sets of expressions

read: $\bigcap \Gamma \leq \sum \Delta$

fixed point unfoldings cf. (4)-(5)

CYCLIC PROOFS

- <u>Preproofs</u> are coinductively generated from system.
- ... <u>regular</u> (or <u>cyclic</u>) if only finitely many distinct subpreproofs.

CYCLIC PROOFS

- Preproofs are coinductively generated from system.
- ... regular (or cyclic) if only finitely many distinct subpreproofs.

- A preproof is progressing if every infinite branch has a formula 'trace' with smallest inf. often principal fmla. μ on LHS or ν on RHS.

- A cyclic proof is a regular progressing preproof.

CYCLIC PROOFS

- <u>Preproofs</u> are coinductively generated from system.
- ... <u>regular</u> (or <u>cyclic</u>) if only finitely many distinct subpreproofs.

- A preproof is <u>progressing</u> if every infinite branch has a formula 'trace' with smallest inf. often principal fmla. μ on LHS or ν on RHS.

- A <u>cyclic proof</u> is a regular progressing preproof.

$$\boxed{\mathrm{CRLL} := \text{theory of cyclic proofs of } \widehat{\mathrm{LRLL}}.}$$

Example (every word has $<\infty$ a's or ∞ a's)

$$
\begin{prooftree}
\AxiomC{$\vdots$}
\UnaryInfC{$(a+b)^\omega \longrightarrow f_a, i_a$}
\RightLabel{$\bullet$}
\LeftLabel{k_a}
\UnaryInfC{$a(a+b)^\omega \longrightarrow af_a, ai_a$}
\LeftLabel{w-r}
\UnaryInfC{$a(a+b)^\omega \longrightarrow \Gamma$}
\AxiomC{$\vdots$}
\RightLabel{$\circ$}
\UnaryInfC{$(a+b)^\omega \longrightarrow af_a, bf_a, b^\omega, i'_a$}
\LeftLabel{μ-r,$+$-r}
\UnaryInfC{$(a+b)^\omega \longrightarrow f_a, b^\omega, i'_a$}
\LeftLabel{k_b}
\UnaryInfC{$b(a+b)^\omega \longrightarrow bf_a, bb^\omega, bi'_a$}
\LeftLabel{w-r}
\UnaryInfC{$b(a+b)^\omega \longrightarrow \Gamma$}
\LeftLabel{$+_l$}
\BinaryInfC{$a(a+b)^\omega + b(a+b)^\omega \longrightarrow \Gamma$}
\LeftLabel{$+$-r}
\UnaryInfC{$a(a+b)^\omega + b(a+b)^\omega \longrightarrow af_a, bf_a, bb^\omega, bi'_a + ai_a$}
\LeftLabel{ν-r,μ-r}
\RightLabel{$\circ$}
\UnaryInfC{$(a+b)^\omega \longrightarrow af_a, bf_a, b^\omega, i'_a$}
\LeftLabel{$+$-r}
\UnaryInfC{$(a+b)^\omega \longrightarrow af_a + bf_a + b^\omega, i'_a$}
\LeftLabel{μ-r,ν-r}
\RightLabel{$\bullet$}
\UnaryInfC{$(a+b)^\omega \longrightarrow f_a, i_a$}
\LeftLabel{$+$-r}
\UnaryInfC{$(a+b)^\omega \longrightarrow f_a + i_a$}
\end{prooftree}
$$

Key

$i_a := \nu X \mu Y (bY + aX)$

$f_a := \mu X (aX + bY + b^\omega)$

$b^\omega := \nu X\, bX$

$(a+b)^\omega := \nu X (aX + bX)$

$i'_a := \mu Y (bY + a i_a)$

$\Gamma := af_a, bf_a, bb^\omega, bi'_a, ai_a$

Example (every word has $<\infty$ a's or ∞ a's)

$$\vdots$$

$$(a+b)^\omega \longrightarrow f_a, i_a \quad \bullet$$

k_a

$$a(a+b)^\omega \longrightarrow af_a, ai_a$$

w-r

$$a(a+b)^\omega \longrightarrow \Gamma$$

$$\vdots$$

$$(a+b)^\omega \longrightarrow af_a, bf_a, b^\omega, i'_a \quad \circ$$

μ-r,$+$-r

$$(a+b)^\omega \longrightarrow f_a, b^\omega, i_a$$

k_b

$$b(a+b)^\omega \longrightarrow bf_a, bb^\omega, bi'_a$$

w-r

$$b(a+b)^\omega \longrightarrow \Gamma$$

$+_l$

$$a(a+b)^\omega + b(a+b)^\omega \longrightarrow \Gamma$$

$+$-r

$$a(a+b)^\omega + b(a+b)^\omega \longrightarrow af_a, bf_a, bb^\omega, bi'_a, ai_a \quad \circ$$

ν-r,μ-r

$$(a+b)^\omega \longrightarrow af_a, bf_a, b^\omega, i_a$$

$+$-r

$$(a+b)^\omega \longrightarrow af_a + bf_a + b^\omega, i'_a \quad \bullet$$

μ-r,ν-r

$$(a+b)^\omega \longrightarrow f_a, i_a$$

$+$-r

$$(a+b)^\omega \longrightarrow f_a + i_a$$

"progress points"

Key

$i_a := \nu X \mu Y (bY + aX)$

$f_a := \mu X (aX + bY + b^\omega)$

$b^\omega := \nu X\, bX$

$(a+b)^\omega := \nu X (aX + bX)$

$i'_a := \mu Y (bY + ai_a)$

$\Gamma := af_a, bf_a, bb^\omega, bi'_a, ai_a$

SOUNDNESS

THEOREM. $\mathrm{CRLL} \vdash e \to f \implies \mathcal{L}(e) \subseteq \mathcal{L}(f)$

SOUNDNESS

THEOREM. $CRLL \vdash e \to f \implies \mathcal{L}(e) \subseteq \mathcal{L}(f)$

LEMMA: The evaluation game for RLL-expressions over $\mathcal{L}$ is positionally determined.

Soundness

Theorem. $CRLL \vdash e \to f \implies \mathcal{L}(e) \subseteq \mathcal{L}(f)$

Lemma: The evaluation game for RLL-expressions over $\mathcal{L}$ is positionally determined.

Proof of soundness

- suppose $w \in \mathcal{L}(e) \setminus \mathcal{L}(f)$ and let ε, α be appropriate $\exists, \forall$ winning strategies from $(w, e), (w, f)$ in evaluation game.
- (ε, α) induces a unique branch $B = (\Gamma_i \to \Delta_i)_{i<\omega}$ satisfying $w_i \in \mathcal{L}(\Gamma_i) \setminus \mathcal{L}(\Delta_i)$ for some w_i.
- B cannot be progressing, by assumption that ε, α are winning.

Completeness

Proof search game:

- Prover (P) chooses inference steps;
- Denier (D) chooses premisses

P wins if branch constructed has a progressing trace.

COMPLETENESS

Proof search game:

- Prover (P) chooses inference steps;
- Denier (D) chooses premisses

P wins if branch constructed has a progressing trace.

- Proof search game is finite memory determined. Büchi-Landweber
- Finite memory P-winning-strategies $\approx$ cyclic proofs.

Completeness

Proof search game:

- Prover (P) chooses inference steps;
- Denier (D) chooses premisses

P wins if branch constructed has a progressing trace.

- Proof search game is finite memory determined.
- Finite memory P-winning-strategies $\approx$ cyclic proofs.

Büchi-Landweber

Theorem. $\mathcal{L}(e) \subseteq \mathcal{L}(f) \Rightarrow \mathrm{CRLL} \vdash e \rightarrow f$ (e, f guarded)

- Suppose not. Play D-winning-strat against validity-preserving proof search.
- Play induces a word ω and $\exists$-winning-strat. from (ω, e)
  and $\forall$-winning-strat. from (ω, f)

AXIOMATIC SUBTLETIES

THE PROBLEM OF COMPLETENESS

We want to prove (1) - (5) sound & complete for $\mathcal{L}$

THE PROBLEM OF COMPLETENESS

We want to prove (1)-(5) sound & complete for $\mathcal{L}$.

PROPOSITION. There are e, f and a model $\mathcal{C} \models (1)-(5)$ s.t.:

- $\mathcal{L}(e) = \mathcal{L}(f)$
- $\mathcal{C}(e) \neq \mathcal{C}(f)$

THE PROBLEM OF COMPLETENESS

We want to prove (1)-(5) sound & complete for $\mathcal{L}$.

Proposition. There are e, f and a model $\mathcal{C} \models$ (1)-(5) s.t.:

- $\mathcal{L}(e) = \mathcal{L}(f)$
- $\mathcal{C}(e) \neq \mathcal{C}(f)$

Idea: set $\mathcal{C}$ to be the Cantor topology on $\mathfrak{A}$, and interpret:

- μ as $\bigcup$ approximants
- ν as $\bigcup$ postfixed

Problem: in $\mathcal{C}$, μ and ν are no longer dual.

AN AXIOMATISATION

A <u>Right-Linear Lattice</u> (RLL) is a structure satisfying (1)-(5) and:

$\boxed{\text{(6) whenever } e(-), f(-) \text{ are dual operators, } \mu X e(X) \text{ and } \nu X f(X) \text{ are dual.}}$

An FO axiom!

An Axiomatisation

A <u>Right-Linear Lattice</u> (RLL) is a structure satisfying (1)-(5) and:

(6) whenever $e(-), f(-)$ are dual operators, $\mu X e(X)$ and $\nu X f(X)$ are dual.

An FO axiom!

THEOREM: $\mathrm{RLL} \vdash e \leq f \iff \mathcal{L}(e) \subseteq \mathcal{L}(f)$

AN AXIOMATISATION

A Right-Linear Lattice (RLL) is a structure satisfying (1)-(5) and:

(6) whenever $e(-), f(-)$ are dual operators, $\mu X e(X)$ and $\nu X f(X)$ are dual.

An FO axiom!

THEOREM: $RLL \vdash e \leq f \iff \mathcal{L}(e) \subseteq \mathcal{L}(f)$

- expressions induce a Boolean subalgebra of any RLL:

$$(ae)^c := ae^c + \sum_{b \neq a} bT$$

- exploit this to extract (co)inductive invariants from cyclic proofs.

Conclusions

Conclusions

- We gave a sound & complete cyclic system and axiomatisation for the equational theory of APAs, written as RLL-expressions.
- We developed game-theoretic tools, and applied state-of-the-art techniques in cyclic proof theory.

Conclusions

- We gave a sound & complete cyclic system and axiomatisation for the equational theory of APAs, written as RLL-expressions.
- We developed game-theoretic tools, and applied state-of-the-art techniques in cyclic proof theory.

- Relationship to Santocanale's μ-lattices and Kozen's μ-calculus.
- Can axiomatisation be made quantifier-free?
- Further development of 'Right-Linear' paradigm (cf. Kleene Algebras)

Conclusions

- We gave a sound & complete cyclic system and axiomatisation for the equational theory of APAs, written as RLL-expressions.
- We developed game-theoretic tools, and applied state-of-the-art techniques in cyclic proof theory.

- Relationship to Santocanale's μ-lattices and Kozen's μ-calculus.
- Can axiomatisation be made quantifier-free?
- Further development of 'Right-Linear' paradigm (cf. Kleene Algebras)

THANK YOU!