Algebraic Reasoning of Quantum Programs via Non-Idempotent Kleene Algebra

Yuxiang Peng, Mingsheng Ying, Xiaodi Wu

06/16/2022

Classical While-Program Equivalences

- A classical compiler rule: *loop unrolling*.

$\textsc{Unrolling1} \equiv$

$\textbf{while} \quad q > 0 \quad \textbf{do}$

$\quad P$

$\textbf{done}.$

$\textsc{Unrolling2} \equiv$

$\textbf{while} \quad q > 0 \quad \textbf{do}$

$\quad P;$

$\quad \textbf{if} \quad q > 0 \quad \textbf{then}\ P$

$\textbf{done}.$

- Equivalent classical programs.

Quantum While-Programs Equivalences

- What if quantum programs?

$M[q]=0;\ P;$
$\cdots\cdots$
$M[q]=0;\ P;$
$M[q]=1$

$\textsc{Unrolling1} \equiv$

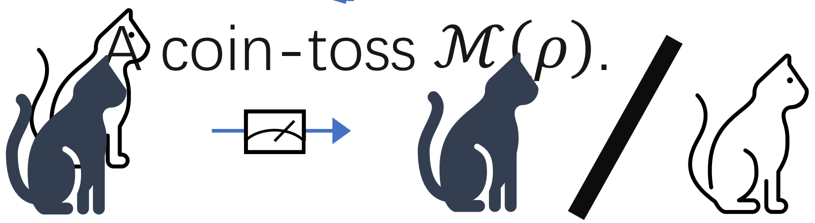
while $M[q] = 0$ **do**
  P
done.

$\textsc{Unrolling2} \equiv$

while $M[q] = 0$ **do**
  $P;$
  if $M[q] = 0$ **then** P
done.

$M[q]=0;P;$
$M[q]=1;$
$M[q]=0;P;$
$M[q]=1;$

A coin-toss $\mathcal{M}(\rho)$.



- Features:
  - Measurements change states.
  - Intrinsic non-deterministic nature.
- They are equivalent if M is *projective*. ($\mathcal{M}_i\mathcal{M}_j = \delta_{ij}\mathcal{M}_i$)

KAT-like Algebraic Reasoning

- Kleene Algebra with Tests: "Regular expressions" ⇔ programs:

UNROLLING1 ≡
while $M[q] = 0$ **do**
  P
done.

UNROLLING2 ≡
while $M[q] = 0$ **do**
  P;
  if $M[q] = 0$ **then** P
done.

$$(m_0 p)^* m_1 \stackrel{?}{=} (m_0 p(m_0 p + m_1 \cdot 1))^* m_1$$

- What are the axioms? Are they *sound and complete*?

Algebraic Reasoning via NKA

- Non-idempotent Kleene Algebra (NKA)

$$
\begin{aligned}
&(m_0 p(m_0 p + m_1 \cdot 1))^* m_1 \\
=\ &(m_0 p m_0 p + m_0 p m_1)^* m_1 \\
=\ &\cdots\cdots \\
=\ &(m_0 p)^* m_1
\end{aligned}
$$

Premises

$m_i m_j = \delta_{ij} m_i$

Axioms of NKA

Semiring Laws

$p + (q + r) = (p + q) + r;$

$p + q = q + p;$

$p + 0 = p;$

$p(qr) = (pq)r;$

$1p = p1 = p;$

$0p = p0 = 0;$

$p(q + r) = pq + pr;$

$(p + q)r = pr + qr;$

Star Laws

$1 + pp^* \leq p^*;$

$q + pr \leq r \rightarrow p^* q \leq r;$

$q + rp \leq r \rightarrow qp^* \leq r;$

Partial Order Laws

$p \leq p;$

$p \leq q \wedge q \leq p \rightarrow p = q;$

$p \leq q \wedge q \leq r \rightarrow p \leq r;$

$p \leq q \wedge r \leq s \rightarrow p + r \leq q + s;$

$p \leq q \wedge r \leq s \rightarrow pr \leq qs;$

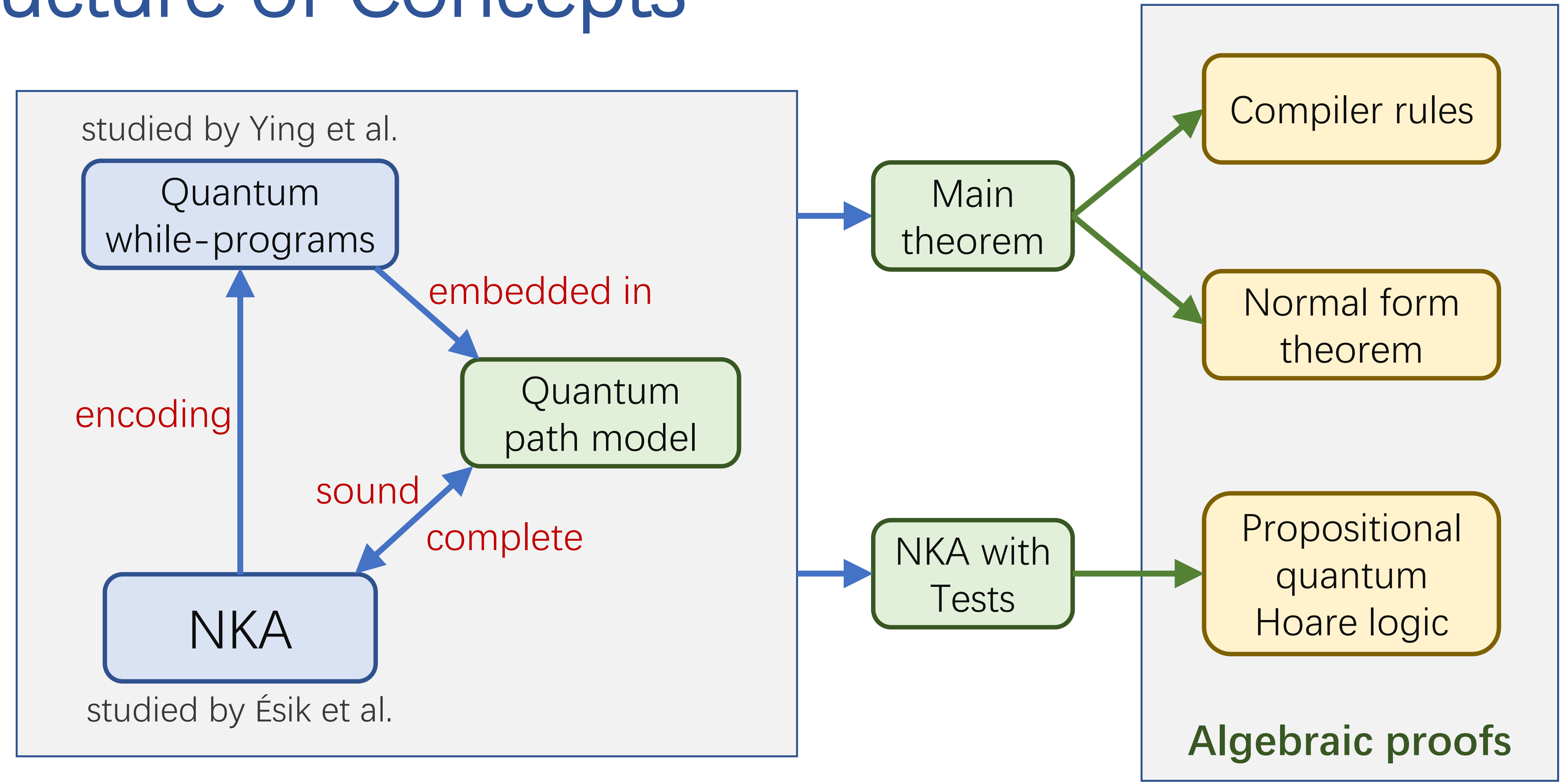
- *Main theorem*: algebraic derivation induces equivalence.

Theorem. For quantum programs $P, Q, \{S_i\}_{i=1}^k, \{T_i\}_{i=1}^k$, where $[\![S_i]\!] = [\![T_i]\!]$ for all i. If

$$\vdash_{\text{NKA}} \left(\bigwedge_{i=1}^{k} \text{Enc}(S_i) = \text{Enc}(T_i)\right) \rightarrow \text{Enc}(P) = \text{Enc}(Q),$$

then $[\![P]\!] = [\![Q]\!]$. Here Enc is the encoding to algebraic expressions.

Structure of Concepts



Non-idempotent Kleene Algebra

- NKA removes idempotency from KA.
  - Many rules of KA are still in NKA.

- Facts about NKA:
  - Sound and complete models
    - Rational power series over $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ [Bloom&Ésik, 2009].
    - Weighted automata = RPS [Schützenberger, 1961].
  - Complexity
    - Deciding equation is PSPACE-complete.
    - Deciding inequality is undecidable [Eilenberg, 1974].

Axioms of NKA

Semiring Laws

$p + (q + r) = (p + q) + r;$
$p + q = q + p;$
$p + 0 = p;$
$p(qr) = (pq)r;$
$1p = p1 = p;$
$0p = p0 = 0;$
$p(q + r) = pq + pr;$
$(p + q)r = pr + qr;$
$\cancel{p + p = p}$

Star Laws

$1 + pp^* \leq p^*;$
$q + pr \leq r \to p^*q \leq r;$
$q + rp \leq r \to qp^* \leq r;$

Partial Order Laws

$p \leq p;$
$p \leq q \wedge q \leq p \to p = q;$
$p \leq q \wedge q \leq r \to p \leq r;$
$p \leq q \wedge r \leq s \to p + r \leq q + s;$
$p \leq q \wedge r \leq s \to pr \leq qs;$

Derivable rules in NKA
[Ésik&Kuich, 2004]

(fixed-point)
$a^* = 1 + aa^*$

(sliding)
$(ab)^*a = a(ba)^*$

(positivity)
$0 \leq a$

(unrolling)
$a^* = (aa)^*(1 + a)$

(denesting)
$(a + b)^* = a^*(ba^*)^* = (a^*b)^*a^*$

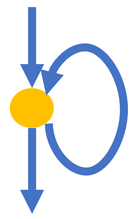
Encoding Quantum While-Programs

- Encode as “regular expressions”.

$$
\begin{aligned}
&\mathrm{Enc}(\mathbf{skip}) = 1; \qquad \mathrm{Enc}(q := |0\rangle) = \boxed{E([\![q := |0\rangle]\!])};\\
&\mathrm{Enc}(\mathbf{abort}) = 0; \qquad \mathrm{Enc}(\overline{q} := U[\overline{q}]) = \boxed{E([\![\overline{q} := U[\overline{q}]]\!])};\\
&\mathrm{Enc}(P_1; P_2) = \mathrm{Enc}(P_1) \cdot \mathrm{Enc}(P_2);\\
&\mathrm{Enc}(\mathbf{case}\ M[\overline{q}] \xrightarrow{i} P_i\ \mathbf{end}) = \sum_i \boxed{E(\mathcal{M}_i)} \cdot \mathrm{Enc}(P_i);\\
&\mathrm{Enc}(\mathbf{while}\ M[\overline{q}] = 1\ \mathbf{do}\ P\ \mathbf{done}) = (\boxed{E(\mathcal{M}_1)} \cdot \mathrm{Enc}(P))^* \cdot \boxed{E(\mathcal{M}_0)}
\end{aligned}
$$

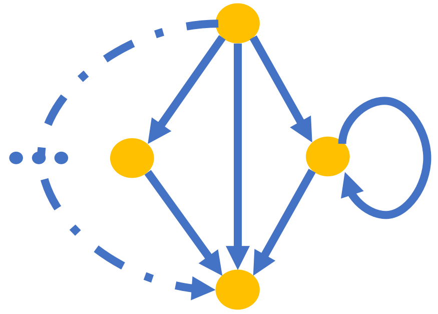
E: elementary operations ⇒ symbols

- Kleene star: $\mathcal{E}^* = \mathcal{E}^0 + \mathcal{E}^1 + \mathcal{E}^2 + \cdots$
  - “$*$” is partially defined for quantum channels.
  - $\mathcal{E}_I^* = \mathcal{E}_I + \mathcal{E}_I + \mathcal{E}_I + \cdots$: divergent sum

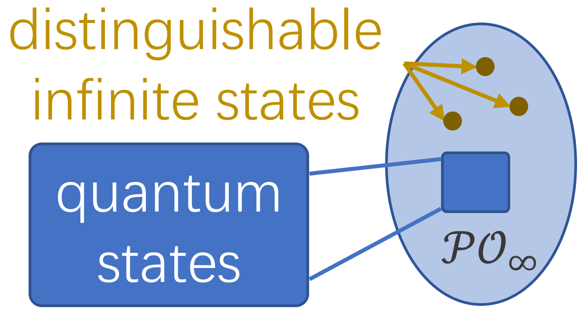


- Aim for a total Kleene star function.

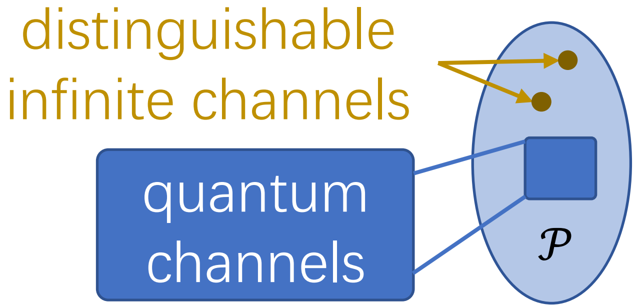
Quantum Path Model



- Quantum processes take *sum of all paths*.
  - $\mathcal{M}_0(\sum_n |0\rangle\langle 0|) = \sum_n |0\rangle\langle 0|\,, \quad \mathcal{M}_0(\sum_n |1\rangle\langle 1|) = 0.$
  - Need to distinguish different infinities.



- Quantum path model
  - $\mathcal{PO}_\infty$: generalization of *quantum states*
    - Equivalence classes of quantum state multisets.
    - Embeds quantum states.
  - $\mathcal{P}$: generalization of *quantum channels*
    - *Linear* and *monotone* transformations of $\mathcal{PO}_\infty$.
    - Embeds quantum channels.

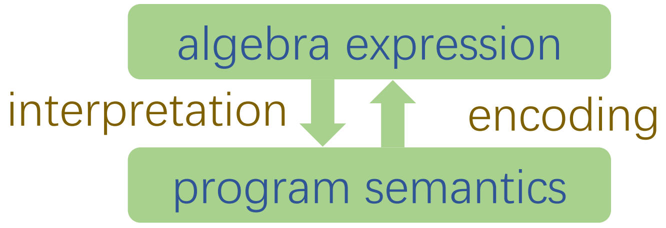


Quantum Interpretation

- QI interprets expressions into QPM.
  - $\mathrm{int} = (\mathcal{H}, \mathrm{eval})$.
  - eval: symbols ⇒ quantum channels.

$$\mathcal{Q}_{\mathrm{int}}(0) = \mathcal{O}_{\mathcal{H}}, \qquad \mathcal{Q}_{\mathrm{int}}(e+f) = \mathcal{Q}_{\mathrm{int}}(e) + \mathcal{Q}_{\mathrm{int}}(f),$$
$$\mathcal{Q}_{\mathrm{int}}(1) = \mathcal{I}_{\mathcal{H}}, \qquad \mathcal{Q}_{\mathrm{int}}(e \cdot f) = \mathcal{Q}_{\mathrm{int}}(e); \mathcal{Q}_{\mathrm{int}}(f),$$
$$\mathcal{Q}_{\mathrm{int}}(a) = \langle \mathrm{eval}(a) \rangle^{\uparrow}, \qquad \mathcal{Q}_{\mathrm{int}}(e^*) = \mathcal{Q}_{\mathrm{int}}(e)^*.$$

- QI inverts encoding:
  - $\mathcal{Q}_{\mathrm{int}}(\mathrm{Enc}(P)) = \langle [\![P]\!] \rangle^{\uparrow}$.



- Axioms of NKA are sound and complete w.r.t. quantum interpretation.

Theorem. For expressions e, f over a finite alphabet, there is
$$\vdash_{\mathrm{NKA}} e = f \quad \Leftrightarrow \quad \forall \mathrm{int}: \ \mathcal{Q}_{\mathrm{int}}(e) = \mathcal{Q}_{\mathrm{int}}(f)$$

Insight: NKA captures all equations for quantum.

- Soundness leads to the *main theorem*.

Verifying Compiler Rule

- Revisit loop unrolling

$$\vdash_{\text{NKA}} m_1 m_1 = m_1 \wedge m_1 m_0 = 0 \rightarrow$$
$$(m_0 p)^* m_1 = (m_0 p(m_0 p + m_1 \cdot 1))^* m_1.$$

Derivable equations in NKA:

(denesting)	(fixed-point)	(unrolling)
$(a+b)^* = a^*(ba^*)^*$	$a^* = 1 + aa^*$	$a^* = (aa)^*(1+a)$

- Main theorem ⇒ $[\![\text{Unrolling1}]\!] = [\![\text{Unrolling2}]\!]$ if $\mathcal{M}_i \circ \mathcal{M}_j = \delta_{ij}\mathcal{M}_i$.

- More examples in the paper
  - Quantum specific rule: loop boundary cancellation
  - Real world application: quantum signal processing

Quantum Böhm-Jacopini Theorem

- A normal form theorem:

> ***Theorem.*** For quatum program P, there is a quantum program with one **while** loop that is equivalent to $P; p_{\mathcal{C}} := |0\rangle$.
> Here $\mathcal{C}$ is an auxiliary classical space.

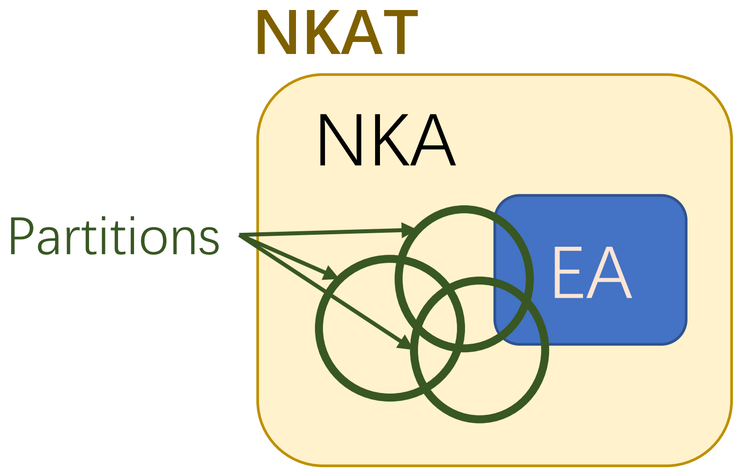
- Observed in [Yu, 2019]. We give an algebraic proof to it.
- Idea:
  - Reconstruct control flows.
  - Prove equivalences via NKA.

NKA with Tests (NKAT)

- Classical tests serve two functionalities:
  - Property test and branch guard.
- Quantum: separate concepts.

	Property test	Branch guard
Classical test	✓	✓
Quantum predicate	✓	✗
Quantum measurement	✗	✓

- NKA with Tests
  - Quantum predicates: an effect algebra.
    - EA $(\mathcal{L}, \oplus, 0, e)$: 5 axioms.
    - EA is embedded in NKA.
  - Quantum measurements: partitions $(m_i)_{i \in I}$.
    - $m_i \mathcal{L} \subseteq \mathcal{L}$ and $\sum_{i \in I} m_i e = e$.



Propositional Quantum Hoare Logic

- NKAT encodes quantum Hoare triples:

$$\models_{par} \{A\}P\{B\} \quad \Leftrightarrow \quad \mathrm{Enc}(P)\bar{b} \leq \bar{a}$$

- Propositional QHL (a fragment of QHL [Ying, 2011])

$$
\begin{array}{llll}
\text{(Ax.Sk)} & \{A\}\ \mathbf{skip}\ \{A\} & \text{(R.OR)} & \dfrac{A \sqsubseteq A' \quad \{A'\}P\{B'\} \quad B' \sqsubseteq B}{\{A\}P\{B\}} \\
\text{(Ax.Ab)} & \{I_{\mathcal{H}}\}\ \mathbf{abort}\ \{O_{\mathcal{H}}\} & \text{(R.IF)} & \dfrac{\{A_i\}P_i\{B\} \text{ for all } i}{\{\sum_i \mathcal{M}_i^\dagger(A_i)\}\mathbf{case}\ M \xrightarrow{i} P_i\ \mathbf{end}\{B\}} \\
\text{(R.SC)} & \dfrac{\{A\}P_1\{B\} \quad \{B\}P_2\{C\}}{\{A\}P_1;P_2\{C\}} & \text{(R.LP)} & \dfrac{\{B\}P\{C\} \quad C = \mathcal{M}_0^\dagger(A) + \mathcal{M}_1^\dagger(B)}{\{C\}\mathbf{while}\ M = 1\ \mathbf{do}\ P\ \mathbf{done}\{A\}}
\end{array}
\quad \Leftrightarrow \quad
\begin{cases}
\text{(Ax.Sk)}: & 1\bar{a} \leq \bar{a}, \\
\text{(Ax.Ab)}: & 0\bar{0} \leq \bar{1}, \\
\text{(R.OR)}: & a \leq a' \wedge p\overline{b'} \leq \overline{a'} \wedge b' \leq b \to p\bar{b} \leq \bar{a}, \\
\text{(R.IF)}: & \left(\bigwedge_{i\in I} p_i\bar{b} \leq \overline{a_i}\right) \to (\sum_{i\in I} m_i p_i)\bar{b} \leq \overline{\sum_i m_i a_i}, \\
\text{(R.SC)}: & p_1\bar{b} \leq \bar{a} \wedge p_2\bar{c} \leq \bar{b} \to p_1p_2\bar{c} \leq \bar{a}, \\
\text{(R.LP)}: & \overline{pm_0a + m_1b} \leq \bar{b} \to (m_1p)^*m_0\bar{a} \leq \overline{m_0a + m_1b}.
\end{cases}
$$

- Algebraic reasoning is easier than matrix analysis.

Future Directions

- Applications
  - Quantum NetKAT for quantum software-defined networks?
  - Finer characterizations of quantum measurements?
- Automation
  - Bisimulation and co-algebra for NKA?
    - Faster equivalence checking of NKA equations.
    - Algorithms deciding Horn formulae.
  - Formal systems in Coq?

Q&A

Thanks!

References

- [Ésik&Kuich, 2004] Zoltán Ésik and Werner Kuich.2004. Inductive ⋆-semirings. *Theoretical Computer Science* 324, 1 (2004), 3–33
- [Bloom&Ésik, 2009] Stephen L Bloom and Zoltán Ésik. 2009. Axiomatizing rational power series over natural numbers. *Information and Computation* 207, 7 (2009), 793–811.
- [Schützenberger, 1961] M.P. Schützenberger. 1961. On the definition of a family of automata. *Information and Control* 4, 2 (1961), 245 – 270.
- [Eilenberg, 1974] Samuel Eilenberg. 1974. *Automata, languages, and machines.* Academic press.
- [Yu, 2019] Nengkun Yu. 2019. Quantum Temporal Logic. *arXiv e-prints*, Article arXiv:1908.00158 (July 2019).
- [Ying, 2011] Mingsheng Ying. 2011. Floyd–Hoare Logic for Quantum Programs. *ACM Transactions on Programming Languages and Systems* 33, 6 (2011).