Automatic Generation of Classical Invariants of Quantum Programs

Matthew Amy & Joseph Lunderville

School of Computing Science, Simon Fraser University

QIP
Raleigh, February 24th, 2025

M. Amy, J. Lunderville, *Linear and Non-linear Relational Analyses for Quantum Program Optimization*. POPL 2025, arXiv:2410.23493.

What is this talk about?

The classical (relational) invariant problem:

Given a QRAM program P, compute a logical/algebraic property characterizing the classical transitions induced by P — i.e. $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}_2^n$ such that

$$\langle \mathbf{x}' | P | \mathbf{x} \rangle \neq 0$$

Program invariants

A simple quantum program:

1. Prepare the state $|s\rangle = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathbf{x}\rangle$
2. For $i = 0..\left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$ do
    2.1 Apply oracle $U_f : |\mathbf{x}\rangle \mapsto (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle$
    2.2 Apply diffusion operator $2|s\rangle\langle s| - I$
3. Measure

Program invariants

A simple quantum program:

1. Prepare the state $|s\rangle = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathbf{x}\rangle$
2. For $i = 0.. \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor$ do
   2.1 Apply oracle $U_f : |\mathbf{x}\rangle \mapsto (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$
   2.2 Apply diffusion operator $2|s\rangle\langle s| - I$
3. Measure

Loop invariant: $|\psi\rangle \in \mathrm{span}\left\{ \frac{1}{\sqrt{M}} \sum_{f(\mathbf{x})=1} |\mathbf{x}\rangle, \frac{1}{\sqrt{2^n - M}} \sum_{f(\mathbf{x})=0} |\mathbf{x}\rangle \right\}$

Program invariants

A simple quantum program:

1. Prepare the state $|s\rangle = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathbf{x}\rangle$
2. For $i = 0..\left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$ do
    2.1 Apply oracle $U_f : |\mathbf{x}\rangle \mapsto (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle$
    2.2 Apply diffusion operator $2|s\rangle\langle s| - I$
3. Measure

Loop invariant: $|\psi\rangle \in \mathrm{span}\left\{ \frac{1}{\sqrt{M}} \sum_{f(\mathbf{x})=1} |\mathbf{x}\rangle, \frac{1}{\sqrt{2^n - M}} \sum_{f(\mathbf{x})=0} |\mathbf{x}\rangle \right\}$

State invariants = property of a set of states
Relational invariants = property of input/output pairs

But why classical invariants?

Computationally tractable + useful for verification & optimization!

- An ancilla is returned to the $|0\rangle$ state
- A gate has no effect on the state
- A control is statically eliminable
- A circuit implements modular exponentiation
- A diagonal gate D can quasi-commute through P

$$DP = PD'$$

Example: The phase folding optimization

1. Map Clifford+T circuit to string of $\pi/4$ Pauli exponentials

$$R(P_1)R(P_2)\cdots R(P_k)C$$

2. Use Pauli commutations to find pairs $P_i = \pm P_j$ that are adjacent and merge them

Example: The phase folding optimization

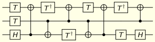
1. Map Clifford+T circuit to string of $\pi/4$ Pauli exponentials

$$R(P_1)R(P_2)\cdots R(P_k)C$$

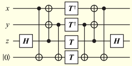
2. Use Pauli commutations to find pairs $P_i = \pm P_j$ that are adjacent and merge them

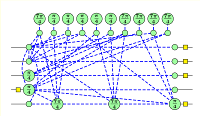
Many other ways, but all rely on circuit representations

$$\sum_{\mathbf{y}} e^{iP(\mathbf{x},\mathbf{y})}|A(\mathbf{x},\mathbf{y})\rangle$$

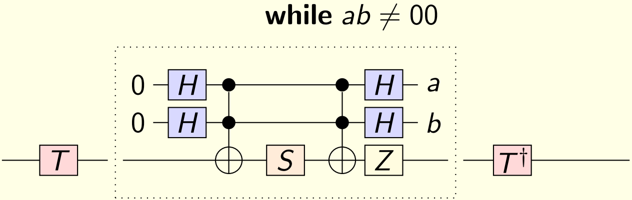


$$R(P_1)R(P_2)\cdots R(P_k)C$$



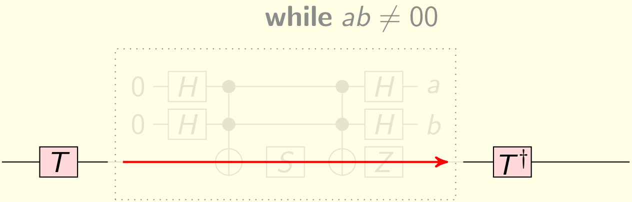


A real-world$^{\text{TM}}$ program



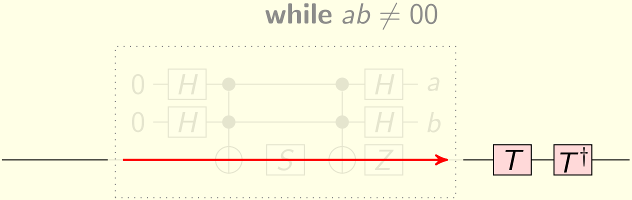
Not a circuit, so what can we do?

A real-world$^{\text{TM}}$ program



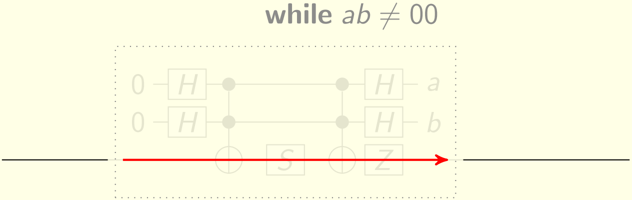
Loop satisfies the classical invariant $x' = x$

A real-world^{TM} program



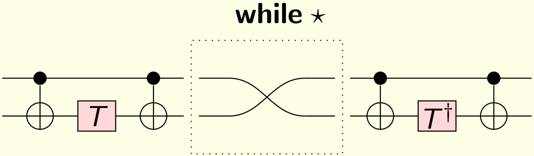
Loop satisfies the classical invariant $x' = x$

A real-world^{TM} program

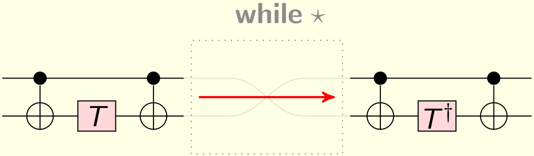


Loop satisfies the classical invariant $x' = x$

A slightly more challenging example

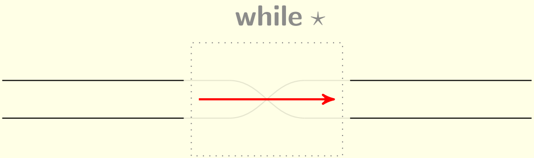


A slightly more challenging example



Loop satisfies the classical invariant $x \oplus y = x' \oplus y'$

A slightly more challenging example



Loop satisfies the classical invariant $x \oplus y = x' \oplus y'$

How can we formalize & compute these invariants?

A relational approach

Classical semantics $\mathcal{C}\llbracket U \rrbracket \subseteq \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ of a circuit U is the set of non-zero classical transitions:

$$(\mathbf{x}, \mathbf{x}') \in \mathcal{C}\llbracket U \rrbracket \iff \langle \mathbf{x}' | U | \mathbf{x} \rangle \neq 0$$

Naturally extends to non-deterministic QRAM programs

$$\Sigma ::= \textbf{skip} \mid q := |0\rangle \mid U\mathbf{q} \mid \textbf{meas}\ q$$
$$P \in \mathrm{RegExp}(\Sigma) ::= E \in \Sigma \mid P_1;\ P_2 \mid P_1 + P_2 \mid P^\star$$

Classical transitions = union over all possible runs $\pi \in \mathcal{L}(P)$:

$$(\mathbf{x}, \mathbf{x}') \in \mathcal{C}\llbracket P \rrbracket \iff \exists \pi \in \mathcal{L}(P). \langle \mathbf{x}' | \pi | \mathbf{x} \rangle \neq 0$$

Computing the classical transitions

Problem: can't compute $\mathcal{C}\llbracket P \rrbracket$
Solution: Any sound approximation $R \supseteq \mathcal{C}\llbracket P \rrbracket$ suffices

Simple approximation: interpret regular expressions on relations

$$
\begin{aligned}
\mathcal{R}\llbracket E \in \Sigma \rrbracket &= \{(\mathbf{x}, \mathbf{x}') \mid \langle \mathbf{x}' | E | \mathbf{x} \rangle \neq 0\} \\
\mathcal{R}\llbracket T_1;\ T_2 \rrbracket &= \mathcal{R}\llbracket T_2 \rrbracket \circ \mathcal{R}\llbracket T_1 \rrbracket \\
\mathcal{R}\llbracket T_1 + T_2 \rrbracket &= \mathcal{R}\llbracket T_1 \rrbracket \cup \mathcal{R}\llbracket T_2 \rrbracket \\
\mathcal{R}\llbracket T^* \rrbracket &= \cup_{k=0}^{\infty} \mathcal{R}\left\llbracket T^k \right\rrbracket
\end{aligned}
$$

Computing the classical transitions

Problem: can't compute $\mathcal{C}[\![P]\!]$
Solution: Any sound approximation $R \supseteq \mathcal{C}[\![P]\!]$ suffices

Simple approximation: interpret regular expressions on relations

$$\mathcal{R}[\![E \in \Sigma]\!] = \{(\mathbf{x}, \mathbf{x}') \mid \langle \mathbf{x}' | E | \mathbf{x} \rangle \neq 0\}$$
$$\mathcal{R}[\![T_1;\ T_2]\!] = \mathcal{R}[\![T_2]\!] \circ \mathcal{R}[\![T_1]\!]$$
$$\mathcal{R}[\![T_1 + T_2]\!] = \mathcal{R}[\![T_1]\!] \cup \mathcal{R}[\![T_2]\!]$$
$$\mathcal{R}[\![T^*]\!] = \cup_{k=0}^{\infty} \mathcal{R}\left[\!\!\left[T^k\right]\!\!\right]$$

$\Longrightarrow$ Computable, but exponential-time
(and not really logical)

Affine subspaces

Clifford+T gates implement affine (classical) transitions

$$\begin{aligned} T : |x\rangle &\mapsto \omega^x |x\rangle \\ X : |x\rangle &\mapsto |1+x\rangle \\ \mathrm{CNOT} : |x,y\rangle &\mapsto |x, x+y\rangle \\ H : |x\rangle &\mapsto \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_2} (-1)^{xy} |y\rangle \end{aligned}$$

Viewed as subsets of $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \simeq \mathbb{Z}_2^{2n}$, the classical semantics are exactly affine subspaces

$$\begin{aligned} \mathcal{C}[\![T]\!] &= \{(x,x) \mid x \in \mathbb{Z}_2\} && = \langle x' = x \rangle \\ \mathcal{C}[\![X]\!] &= \{(x,1+x) \mid x \in \mathbb{Z}_2\} && = \langle x' = 1 + x \rangle \\ \mathcal{C}[\![CNOT]\!] &= \{(x,y,x,x+y) \mid x,y \in \mathbb{Z}_2\} && = \langle x' = x, y' = x + y \rangle \\ \mathcal{C}[\![H]\!] &= \{(x,x') \mid x,x' \in \mathbb{Z}_2\} && = \langle \emptyset \rangle \end{aligned}$$

The affine subspace domain

Lattice of affine subspaces $\mathcal{S}(\mathbb{Z}_2^{2n})$ of $\mathbb{Z}_2^{2n}$ forms a Kleene algebra (coherently interpret regular expressions)

$$(\mathcal{S}(\mathbb{Z}_2^{2n}), 0, 1, \cdot, \sqcup, (\cdot)^\star)$$

where

- $0 = \{0\}$
- $1 = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \mathbb{Z}_2^n\}$
- $S \cdot S'$ is relational composition (projection & intersection)
- $S \sqcup S'$ is least-upper-bound (i.e. subspace union)
- $S^\star = \sqcup_{i=0}^{\infty} S_i$ where $S_i \sqsubseteq S_{i+1}$

The affine subspace domain

Lattice of affine subspaces $\mathcal{S}(\mathbb{Z}_2^{2n})$ of $\mathbb{Z}_2^{2n}$ forms a Kleene algebra (coherently interpret regular expressions)

$$(\mathcal{S}(\mathbb{Z}_2^{2n}), 0, 1, \cdot, \sqcup, (\cdot)^\star)$$

where

- $0 = \{0\}$
- $1 = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \mathbb{Z}_2^n\}$
- $S \cdot S'$ is relational composition (projection & intersection)
- $S \sqcup S'$ is least-upper-bound (i.e. subspace union)
- $S^\star = \sqcup_{i=0}^{\infty} S_i$ where $S_i \sqsubseteq S_{i+1}$

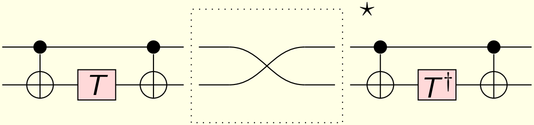
Proposition

$S^\star$ stabilizes in $\Omega(2n)$ iterations

Affine relational invariants

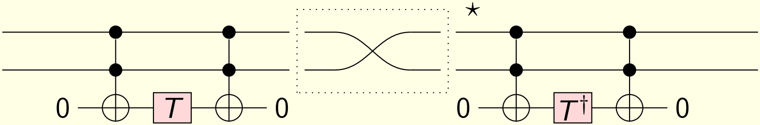
Proposition

Given a QRAM program P, an affine subspace soundly approximating $\mathcal{C}[\![P]\!]$ can be computed in polynomial time



Loop invariant $S = \langle x' \oplus y' = x \oplus y \rangle$ allows canceling the T gates by canonicalizing the conditions $x \oplus y$ and $x' \oplus y'$ modulo S

What if we need more precision?



- The non-linear loop invariant $x'y' = xy$ allows eliminating both T gates
- The strongest affine loop invariant $\langle x' \oplus y' = x \oplus y \rangle$ is unable to prove the relation $x'y' = xy$

  $\implies$ need non-linear relations for this optimization!

From affine subspaces to varieties

Replace affine subspaces with affine varieties and affine relations with polynomial ideals

$$I = \mathbb{I}(V) = \{f \in \mathbb{Z}_2[\mathbf{X}, \mathbf{X}'] \mid f(\mathbf{x}, \mathbf{x}') = 0 \; \forall (\mathbf{x}, \mathbf{x}') \in V\}.$$

Gröbner basis methods suffice to implement KA operators

From affine subspaces to varieties

Replace affine subspaces with affine varieties and affine relations with polynomial ideals

$$I = \mathbb{I}(V) = \{f \in \mathbb{Z}_2[\mathbf{X}, \mathbf{X}'] \mid f(\mathbf{x}, \mathbf{x}') = 0 \; \forall(\mathbf{x}, \mathbf{x}') \in V\}.$$

Gröbner basis methods suffice to implement KA operators

Notes:

- Precise for the compositional model $\mathcal{R}[\![P]\!]$
- Gives all polynomial relations implied by the variety $\mathcal{R}[\![P]\!]$

Proposition (Hilbert's strong Nullstellensatz for $\mathbb{Z}_2$)

$$\mathbb{I}(\mathbb{V}(I)) = I + \langle X_i^2 - X_i \mid X_i \in \mathbf{X} \rangle$$

The catch

Sequential composition is not precise in any classical domain!

$$\mathcal{R}\llbracket H \rrbracket \circ \mathcal{R}\llbracket H \rrbracket = \mathbb{Z}_2^2 \circ \mathbb{Z}_2^2 = \mathbb{Z}_2^2$$

$$\mathcal{R}\llbracket HH \rrbracket = \mathcal{R}\llbracket I \rrbracket = \langle x = x' \rangle \neq \mathbb{Z}_2^2$$

The catch

Sequential composition is not precise in any classical domain!

$$\mathcal{R}\left[\!\left[H\right]\!\right] \circ \mathcal{R}\left[\!\left[H\right]\!\right] = \mathbb{Z}_2^2 \circ \mathbb{Z}_2^2 = \mathbb{Z}_2^2$$

$$\mathcal{R}\left[\!\left[HH\right]\!\right] = \mathcal{R}\left[\!\left[I\right]\!\right] = \langle x = x' \rangle \neq \mathbb{Z}_2^2$$

Solution: use the sum-over-paths to generate precise transition relations for the sequential (circuit) fragment!

$$U : |\mathbf{x}\rangle \mapsto \sum_{\mathbf{y} \in \mathbb{Z}_2^k} \Phi(\mathbf{x}, \mathbf{y}) |f_1(\mathbf{x}, \mathbf{y})\rangle \otimes \cdots \otimes |f_n(\mathbf{x}, \mathbf{y})\rangle$$

Interference & the sum-over-paths

$$(\!|U|\!) = |\mathbf{x}\rangle \mapsto \sum_{\mathbf{y}\in\mathbb{Z}_2^k} \Phi(\mathbf{x},\mathbf{y})|f_1(\mathbf{x},\mathbf{y})\rangle \otimes \cdots \otimes |f_n(\mathbf{x},\mathbf{y})\rangle$$

- Can compute $(\!|U|\!)$ in poly-time
- The ideal $I = \exists \mathbf{Y}.\langle X_1' = f_1(\mathbf{X},\mathbf{Y}), \ldots, X_n' = f_n(\mathbf{X},\mathbf{Y})\rangle$ soundly approximates $\mathcal{C}\,[\![U]\!]$
- Can increase the precision of the ideal by re-writing[1] and analyzing interference

$$(\!|U|\!) = \sum_{y\in\mathbb{Z}_2} (-1)^{yP}(\!|U'|\!) \implies I \sqcap \langle P = 0\rangle \text{ is sound}$$

[1] M. Amy, Towards large-scale functional verification of universal quantum circuits. QPL 2018.

Is this useful?

Application: integrated program optimizations

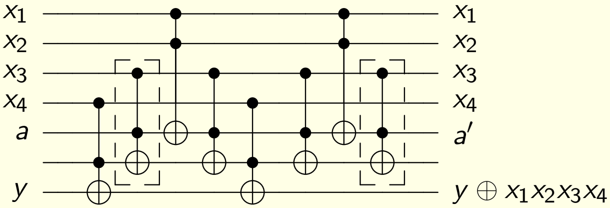
- Implemented[2] invariant generation on openQASM 3.0
- Finds non-trivial optimizations based on loop invariants
- Deep integration of optimization in compilers for hybrid workflows

Benchmark	n	Original	$\mathbf{PF}_{\mathrm{Aff}}$		$\mathbf{PF}_{\mathrm{Pol}}$		Generated loop invariant
		$\#\ T$	$\#\ T$	time (s)	$\#\ T$	time (s)	
RUS	3	16	10	0.30	8	0.35	$\langle z' + z \rangle$
Grover	129	$1736e9$	$1470e9$	1.98	TIMEOUT		–
Reset-simple	2	2	1	0.15	1	0.23	–
If-simple	2	2	0	0.18	0	0.16	–
Loop-simple	2	2	0	0.17	0	0.16	$\langle x' + x, y + y' + xy + xy' \rangle$
Loop-h	2	2	0	0.16	0	0.16	$\langle y' + y \rangle$
Loop-nested	2	3	2	0.17	2	0.18	$\langle x' + x \rangle$, $\langle x' + x \rangle$
Loop-swap	2	2	0	0.30	0	0.20	$\langle x' + y' + x + y, x' + xy + xx' + yx' \rangle$
Loop-nonlinear	3	30	18	0.44	0	0.26	$\langle x' + x, z' + z, y' + y + xy + xy' \rangle$
Loop-null	2	4	1	0.18	1	0.17	$\langle x' + x, y' + y \rangle$

[2] https://github.com/meamy/feynman

Application: circuit optimization

- Strictly outperforms existing phase folding approaches
- Recovers previous[3] hand-optimized k-control Toffoli

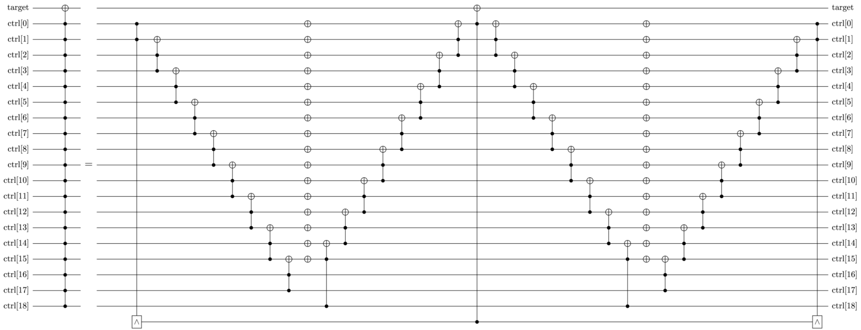


- Requires inferring the equality $a' = a$
- As $k \to \infty$, reduces T-count by $1/3$ to $8(k-1)$
- Previously unachievable by automated means

[3] D. Maslov, *On the advantages of using relative phase Toffolis with an application to multiple control Toffoli optimization* Phys Rev. A 2016.

A compact & efficient multiply-controlled Toffoli

Recent[4] $2(k-2)+1$-Toffoli in constant clean space:



- Previous optimizers: T-count $11(k-2)+7$
- Invariant approach: T-count $8(k-2)+7$

Halves the T-count of the best previous construction!

[4] T. Khattar, C. Gidney, *Rise of conditionally clean ancillae for optimizing quantum circuits*. arXiv:2407.17966

Other applications?

- Verification
- Hybrid program design
  - E.g. repeat-until-success circuits
- Error correction
  - Fully precise for QRAM programs with Clifford operations
  - Space-time codes?

Thank you!