A Rich Type System for Quantum Programs

Aarthi Sundaram [1] Robert Rand [2] Kartik Singhal [2] Brad Lackey [1]

[1]Microsoft [2]University of Chicago

Overview

We present a type system inspired by the stabilizer formalism for Clifford circuits. Further, we extend it to effectively type the T gate and handle arbitrary unitary gates. Using this we can:

- certify the safe disposal and reuse of auxiliary qubits;
- determine separability across a given bi-partition;
- verify the transversality of a gate for stabilizer codes;
- type certain post-measurement states;
- type gate injection circuits that use associated magic states;
- derive types for multiply-controlled unitaries;
- lower bound the T count for multiply-controlled Z gates.

The Type System

The components of our type system for quantum programs are:

- **Ground types:** the 1-qubit Pauli gates $\{I, X, Y, Z\}$.
- **Algebraic operations:** scalar multiplication, additive types, multi-qubit types via tensors.
- **Arrow types:** that provide types to programs and operations in addition to states.
- **Intersection types:** to fully specify program behavior by combining specifications.
- **Union Types:** to capture the non-determinism of measurement.

The grammar generated by combining our components:

$$G := \mathbf{I} \mid \mathbf{X} \mid \mathbf{Y} \mid \mathbf{Z}$$
$$A := G \mid c\,A \mid A\,A \mid A + A \mid A \otimes A$$
$$T := A \mid T \to T \mid T \cap T \mid T \cup T$$

Programs are a sequence of the quantum gate operations. Using the Clifford + T gates as our universal gate set, programs in our type system are defined as follows:

$$P := H\ n \mid S\ n \mid CNOT\ n\ m \mid T\ n \mid P\ ;\ P$$

where $H\ n$ denotes applying the H gate to the n-th bit and ";" denotes the sequential application of gates.

The typing statement $P : \mathbf{V}$ is said to be true if P has type $\mathbf{V}$.

A valid typing statement for the control-σ_z gate:

$$CZ\ 0\ 1 := (H\ 1);\ (CNOT\ 0\ 1); (H\ 1)\ :\ \mathbf{X} \otimes \mathbf{I} \to \mathbf{X} \otimes \mathbf{Z}.$$

Remark: Our type system is amenable to any universal gate set of choice with a corresponding change to the basic arrow types.

Typing rules

A subset of our typing rules from [3] is listed below:

Ground Type Rules:

$$\frac{}{|+\rangle : \mathbf{X}} \quad \frac{}{|-\rangle : -\mathbf{X}} \quad \frac{}{|i\rangle : \mathbf{Y}} \quad \frac{}{|-i\rangle : -\mathbf{Y}} \quad \frac{}{|0\rangle : \mathbf{Z}} \quad \frac{}{|1\rangle : -\mathbf{Z}}$$

$$\frac{}{H : (\mathbf{X} \to \mathbf{Z}) \cap (\mathbf{Z} \to \mathbf{X})} \qquad \frac{}{S : (\mathbf{X} \to \mathbf{Y}) \cap (\mathbf{Z} \to \mathbf{Z})}$$

$$\frac{}{CNOT : (\mathbf{X} \otimes \mathbf{I} \to \mathbf{X} \otimes \mathbf{X}) \cap (\mathbf{I} \otimes \mathbf{Z} \to \mathbf{Z} \otimes \mathbf{Z})}$$

Tensor Rules:

$$\frac{\mathbf{T}[i] = \mathbf{A} \qquad \mathbf{T}[j] = \mathbf{B} \qquad U : \mathbf{A} \otimes \mathbf{B} \to \mathbf{C} \otimes \mathbf{D}}{U\ i\ j : \mathbf{T} \to \mathbf{T}\{i \mapsto \mathbf{C}; j \mapsto \mathbf{D}\}}\ \otimes_2$$

$$\frac{g : \mathbf{A} \otimes \mathbf{I} \to \mathbf{C} \otimes \mathbf{D} \qquad g : \mathbf{I} \otimes \mathbf{B} \to \mathbf{E} \otimes \mathbf{F}}{g : \mathbf{A} \otimes \mathbf{B} \to \mathbf{CE} \otimes \mathbf{DF}}\ \otimes\text{-MUL}$$

Arrow and Sequence Rules:

$$\frac{g : \mathbf{A} \to \mathbf{A}' \qquad g : \mathbf{B} \to \mathbf{B}'}{g : (\mathbf{AB}) \to (\mathbf{A}'\mathbf{B}')}\ \text{MUL} \qquad \frac{g : \mathbf{A} \to \mathbf{A}'}{g : \mathbf{cA} \to \mathbf{cA}'}\ \text{SCALE}$$

$$\frac{g_1 : \mathbf{A} \to \mathbf{B} \qquad g_2 : \mathbf{B} \to \mathbf{C}}{g_1; g_2 : \mathbf{A} \to \mathbf{C}}\ \text{SEQ} \qquad \frac{g_1; (g_2; g_3) : \mathbf{A} \to \mathbf{A}'}{(g_1; g_2); g_3 : \mathbf{A} \to \mathbf{A}'}\ \text{ASSOC}$$

Intersection Rules:

$$\frac{g : \mathbf{A} \qquad g : \mathbf{B}}{g : \mathbf{A} \cap \mathbf{B}}\ \cap\text{-I} \qquad \frac{g : (\mathbf{A} \to \mathbf{A}') \cap (\mathbf{B} \to \mathbf{B}')}{g : (\mathbf{A} \cap \mathbf{B}) \to (\mathbf{A}' \cap \mathbf{B}')}\ \cap\text{-ARR-DIST}$$

Additive Type Rules:

$$\frac{}{T : (\mathbf{Z} \to \mathbf{Z}) \cap \left(\mathbf{X} \to \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Y})\right)} \qquad \frac{g : \mathbf{A} \to \mathbf{B} \qquad g : \mathbf{C} \to \mathbf{D}}{g : \mathbf{A} + \mathbf{C} \to \mathbf{B} + \mathbf{D}}\ \text{ADD}$$

$$\frac{U : \mathbf{A} \to \mathbf{B} + \mathbf{C} \qquad \mathbf{T}[i] = \mathbf{A}}{U\ i : \mathbf{T} \to \mathbf{T}\{i \mapsto \mathbf{B}\} + \mathbf{T}\{i \mapsto \mathbf{C}\}}\ \text{ADD}_2$$

Normalization Rules:

$$\frac{g : \mathbf{A} \to \mathbf{B} \cap \mathbf{C}}{g : \mathbf{A} \to \mathbf{B} \cap \mathbf{BC}}\ \cap\text{-MUL-R} \qquad \frac{g : \mathbf{A} \cap \mathbf{B} \to \mathbf{C}}{g : \mathbf{A} \cap \mathbf{AB} \to \mathbf{C}}\ \cap\text{-MUL-L}$$

Semantics

Gottesman's analysis [1] of Clifford gates via the Heisenberg interpretation forms the starting point for this type system.

Proposition: Given a unitary U, matrices A, B, let $U : A \to B$ imply that for all states $|\psi\rangle$, $UA|\psi\rangle = BU|\psi\rangle$. Then, U takes every eigenstate of A to an eigenstate of B with the same value.

This leads to an eigenvector-based semantics for our types:

- **Ground Types:** The basic types for states correspond to Pauli matrices. Specifically, $|\psi\rangle : \mathbf{A}$ implies that $|\psi\rangle$ is a $+1$-eigenstate of the Pauli matrix A. For example, $|0\rangle : \mathbf{Z}$ and $|1\rangle : -\mathbf{Z}$.
- **Program Types:** A program typed as $p : \mathbf{A} \to \mathbf{B}$ takes all $+1$-eigenstates of A to $+1$-eigenstates of B.

  $H : \mathbf{X} \to \mathbf{Z}$ and $T : \mathbf{Z} \to \mathbf{Z}$.
- **Multi-qubit systems:** Multi-qubit types are formed as tensors of single qubit types. Specifically, $|\psi\rangle : \mathbf{A} \otimes \mathbf{B}$ is a $+1$-eigenstate of $A \otimes B$. Note that $|\psi\rangle$ here could also be an entangled state.

  Let $|\psi\rangle := 0.8\,|00\rangle + 0.6\,|11\rangle$. Then, $|\psi\rangle : \mathbf{Z} \otimes \mathbf{Z}$.
- **Intersection Types:** When $|\psi\rangle : \mathbf{A} \cap \mathbf{B}$, then $|\psi\rangle : \mathbf{A}$ and $|\psi\rangle : \mathbf{B}$ implying that $|\psi\rangle$ is a simultaneous $+1$-eigenstate of A and B. When A and B are Pauli operators, they must commute as anti-commuting Pauli operators do not have common eigrnvectors.

  Let $|\Phi^+\rangle := \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Then, $|\Phi^+\rangle : (\mathbf{X} \otimes \mathbf{X}) \cap (\mathbf{Z} \otimes \mathbf{Z})$.
- **Union Types:** When $|\psi\rangle : \mathbf{A} \cup \mathbf{B}$, then $|\psi\rangle$ is either a $+1$-eigenstate of A or a $+1$-eigenstate of B. In the measurement context, it implies that one outcome has a post-measurement type $\mathbf{A}$ and the other outcome has type $\mathbf{B}$.

  $|+\rangle : \mathbf{X}$ when measured results in a type $\mathbf{Z} \cup -\mathbf{Z}$ since there is an equal probability of obtaining 0 or 1 as the outcome.
- **Additive Types:** A Hermitian, unitary matrix $M = \sum_j c_j P_j$ where $c_j \in \mathbb{R}$ and the P_js are Pauli matrices gives a corresponding additive type $\mathbf{M} = \sum_j \mathbf{c}_j \mathbf{P}_j$ and $|\psi\rangle : \mathbf{M}$ iff $M\,|\psi\rangle = |\psi\rangle$.

  Let $|\psi\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}\,|1\rangle\right)$. Then, $|\psi\rangle : \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Y})$.

Applying our rules

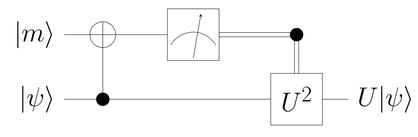
1. Deriving $S; S \equiv Z$

To show that $S; S \equiv Z$, it is enough to show that the action of both is the same on $\mathbf{X}$ and $\mathbf{Z}$ types. Since $S : \mathbf{Z} \to \mathbf{Z}$, we directly get $S; S : \mathbf{Z} \to \mathbf{Z}$ using the SEQ rule. The action on $\mathbf{X}$ becomes:

$$\dfrac{\dfrac{\dfrac{}{S : \mathbf{X} \to \mathbf{Y}} \qquad \dfrac{\dfrac{}{S : \mathbf{Z} \to \mathbf{Z}} \qquad \dfrac{}{S : \mathbf{Z} \to \mathbf{Z}}}{S : \mathbf{XZ} \to \mathbf{YZ}}\ \text{MUL}}{S : \mathbf{Y} \to \mathbf{iYZ}}\ \text{SCALE}}{S; S : \mathbf{X} \to -\mathbf{X}}\ \text{SEQ}$$

where the SCALE rule used $\mathbf{Y} = \mathbf{iXZ}$.

2. Typing a gate injection circuit



Let $|m\rangle : \mathbf{M} = \cos\theta \cdot \mathbf{X} + \sin\theta \cdot \mathbf{Y}$ and $U : (\mathbf{X} \to \mathbf{M}) \cap (\mathbf{Z} \to \mathbf{Z})$.

We verify the above circuit implements U.

Showing $\mathbf{Z} \to \mathbf{Z}$: our input is $|m\rangle \otimes |0\rangle : (\mathbf{M} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z})$. Then

$$(\cos\theta \cdot \mathbf{X} + \sin\theta \cdot \mathbf{Y}) \otimes \mathbf{I} \overset{NOTC}{\longrightarrow} \cos\theta \cdot \mathbf{X} \otimes \mathbf{I} + \sin\theta \cdot \mathbf{Y} \otimes \mathbf{Z}$$
$$\mathbf{I} \otimes \mathbf{Z} \overset{NOTC}{\longrightarrow} \mathbf{I} \otimes \mathbf{Z}.$$

We have Meas $1 : \mathbf{I} \otimes \mathbf{Z} \to [\mathbf{Z} \otimes \mathbf{I} \cup (-\mathbf{Z}) \otimes \mathbf{I}] \cap (\mathbf{I} \otimes \mathbf{Z})$.

- Regardless of outcome, the second wire has output type $\mathbf{Z}$.

Showing $\mathbf{X} \to \mathbf{M}$: our input is $|m\rangle \otimes |+\rangle : (\mathbf{I} \otimes \mathbf{X}) \cap (\mathbf{M} \otimes \mathbf{I})$ and

$$\mathbf{I} \otimes \mathbf{X} \overset{NOTC}{\longrightarrow} \mathbf{X} \otimes \mathbf{X}$$
$$(\cos\theta \cdot \mathbf{X} + \sin\theta \cdot \mathbf{Y}) \otimes \mathbf{I} \overset{NOTC}{\longrightarrow} \cos\theta \cdot \mathbf{X} \otimes \mathbf{I} + \sin\theta \cdot \mathbf{Y} \otimes \mathbf{Z}.$$

We use the $\cap$-MUL-R rule to rewrite the resulting type as

$$(\mathbf{X} \otimes \mathbf{X}) \cap (\cos\theta \cdot \mathbf{I} \otimes \mathbf{X} + \sin\theta \cdot \mathbf{Z} \otimes \mathbf{Y}).$$

Now, measurement has

$$\begin{aligned}\text{Meas } 1 : (\cos\theta \cdot \mathbf{I} \otimes \mathbf{X} + \sin\theta \cdot \mathbf{Z} \otimes \mathbf{Y}) \to \\ [(\mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes (\cos\theta \cdot \mathbf{X} + \sin\theta \cdot \mathbf{Y}))] \cup \quad \text{(measured 0)} \\ [((-\mathbf{Z}) \otimes \mathbf{I}) \cap (\mathbf{I} \otimes (\cos\theta \cdot \mathbf{X} - \sin\theta \cdot \mathbf{Y}))] \quad \text{(measured 1)}\end{aligned}$$

- On outcome 0 the output type is $\mathbf{M}$.
- On outcome 1 we need to apply U^2 to obtain type $\mathbf{M}$.

Determining Separability

Single qubit separability

The following conditions allow us to determine if some single qubit is separable from the rest of the system.

Proposition: For any 2×2 unitary, Hermitian matrix U, the eigenstates of $I^{i-1} \otimes U \otimes I^{n-i}$ are all vectors of the form $|\phi\rangle \otimes |u\rangle \otimes |\psi\rangle$ where $|u\rangle$ is an eigenstate of U and $|\phi\rangle$, $|\psi\rangle$ are arbitrary states.

For our basic types made of Pauli matrices that are both Hermitian and unitary, we get:

Result: Every term of type $\mathbf{I}^{i-1} \otimes \mathbf{U} \otimes \mathbf{I}^{n-i}$ is separable, for any $U \in \{\pm X, \pm Y, \pm Z\}$. That is, the i^{th} factor has type $\mathbf{U}$ and is not entangled with the rest of the system.

We define $\mathbf{A}_i$ to be the n-qubit type where the i^{th} factor has type $\mathbf{A}$ and is separable for the rest of the system.

$$|0\rangle \otimes |+\rangle : (\mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{X}) \equiv \mathbf{Z}_1 \cap \mathbf{X}_2$$

Multi-qubit separability

Using a fact from [2] that the joint eigenspace of k independent, commuting k-qubit Pauli operators where each operator has eigenvalue +1 has dimension 1, we get condition to determine multi-qubit separability:

Result: Let $K \subset \{1, \ldots, n\}$ with $|K| = k$. Every intersection type that contains the term $\bigcap_{j=1}^{k} \left(\mathbf{U}_{(j)} \otimes \mathbf{I}^{n-k}\right)$ where each of the $\mathbf{U}_{(j)}$s acts on K, is pair-wise commuting and independent such that the factors in K are separable from the rest.

Let $(\mathbf{U})_K$ denote the type such that qubits in K are separable from the rest of the system.

Let $|\psi\rangle : (\mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I}) \cap (\mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{X})$. Here, $(\mathbf{X} \otimes \mathbf{X})$ and $(\mathbf{Z} \otimes \mathbf{Z})$ on qubits $\{1, 3\}$ are independent and commuting. Hence, $|\psi\rangle : (\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{1,3} \cap (\mathbf{Z} \otimes \mathbf{X})_{2,4}$.

Error Correcting Codes

Definition. Given a stabilizer code with generators $g_1, \ldots g_k$ and logical operators $\overline{X}, \overline{Z}$, our logical qubit types are

$$\mathbf{Z_L} := \mathbf{g}_1 \cap \cdots \cap \mathbf{g}_k \cap \overline{\mathbf{Z}} \qquad \mathbf{X_L} := \mathbf{g}_1 \cap \cdots \cap \mathbf{g}_k \cap \overline{\mathbf{X}}$$

For the Steane code with transversal H and S gates, we derive

$$H^7 : (\mathbf{X_L} \to \mathbf{Z_L}) \cap (\mathbf{Z_L} \to \mathbf{X_L})$$
$$S^7 : (\mathbf{X_L} \to \mathbf{Y_L}) \cap (\mathbf{Z_L} \to \mathbf{Z_L})$$

Similarly, we can show that $CNOT$ is transversal while the T gate is not as it doesn't produce the desired type.

Typing controlled unitaries

The full type of a general n-qubit unitary U is intractable to compute. For (multiply-)controlled unitaries, we can infer their types.

Definition. $\mathbf{Re}(U) = \frac{1}{2}(U + U^\dagger)$ and $\mathbf{Im}(U) = \frac{1}{2i}(U - U^\dagger)$.

Lemma: If $U : \mathbf{P} \to \mathbf{V}(\mathbf{P})$ for any n-qubit Pauli $\mathbf{P}$:

1. control-$U : \mathbf{Z} \otimes \mathbf{I} \to \mathbf{Z} \otimes \mathbf{I}$.
2. control-$U : \mathbf{X} \otimes \mathbf{I} \to \mathbf{X} \otimes \mathbf{Re}(U) + \mathbf{Y} \otimes \mathbf{Im}(U)$.
3. control-$U : \mathbf{I} \otimes \mathbf{P} \to \mathbf{I} \otimes \frac{1}{2}(\mathbf{P} + \mathbf{V}(\mathbf{P})) + \mathbf{Z} \otimes \frac{1}{2}(\mathbf{P} - \mathbf{V}(\mathbf{P}))$

If U is also Hermitian, so is control^k-U for any $k \geq 1$ and so also has an additive type we denote $\mathbf{C}^k\mathbf{U}$.

Theorem: $\mathbf{C}^k\mathbf{U} = \mathbf{I}^{\otimes(k+n)} - \frac{1}{2^k}(\mathbf{I} - \mathbf{Z})^{\otimes k} \otimes (\mathbf{I}^{\otimes n} - \mathbf{U})$.

In particular $\mathbf{C}^k\mathbf{Z} = \mathbf{I}^{\otimes(k+1)} - \frac{1}{2^k}(\mathbf{I} - \mathbf{Z})^{k+1}$.

Result: We have control^k-$\sigma_z : \mathbf{Z}_j \to \mathbf{Z}_j$ and

control^k-$\sigma_z : \mathbf{X}_j \to \mathbf{X}_j - \frac{1}{2^{k-1}}(\mathbf{I} - \mathbf{Z})^{\otimes(j-1)} \otimes \mathbf{X} \otimes (\mathbf{I} - \mathbf{Z})^{\otimes(k+1-j)}$.

Putting the all the pieces together, we get

Result: Any Clifford + T circuit that synthesizes control^k-σ_z contains at least $(2k - 2)$ T gates.

References

[1] Daniel Gottesman. The Heisenberg Representation of Quantum Computers. *arXiv preprint quant-ph/9807006*, 1998.

[2] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge, 2010. doi:10.1017/CBO9780511976667.

[3] Aarthi Sundaram, Robert Rand, Kartik Singhal, and Brad Lackey. A Rich Type System for Quantum Programs. *arXiv*, 2022. doi:10.48550/arXiv.2101.08939.