Hoare meets Heisenberg: A Lightweight Logic for Quantum Programs

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

[1]Microsoft Quantum, Redmond, WA
[2]University of Chicago, Chicago, IL

We show that Gottesman's (1998) semantics for Clifford circuits based on the Heisenberg representation gives rise to a lightweight Hoare-like logic for efficiently characterizing a common subset of quantum programs. Our applications include (i) certifying whether auxiliary qubits can be safely disposed of, (ii) determining if a system is separable across a given bi-partition, (iii) checking the transversality of a gate with respect to a given stabilizer code, and (iv) computing post-measurement states for computational basis measurements. Further, this logic is extended to accommodate universal quantum computing by deriving Hoare triples for the T-gate, multiply-controlled unitaries such as the Toffoli gate, and some gate injection circuits that use associated magic states. A number of interesting results emerge from this logic, including a lower bound on the number of T gates necessary to perform a multiply-controlled Z gate.

1 Introduction

Quantum programs are notoriously complex in both the traditional and computational sense: They are hard to write correctly and extremely expensive to simulate. The same applies to program logics for quantum programs: It can be hard to come up with an assertion about a quantum program (typically an observable or a projector), and it is doubly hard to prove that it holds upon execution of a program. Typically this will either involve complex calculations or high-level reasoning. To address this problem, we propose a logic that uses the stabilizer formalism for efficient reasoning about Clifford circuits. We extend this system to handle universal quantum gate sets, both by explicitly adding the T gate and by showing how to handle arbitrary unitary gates. We also expand the system to handle measurement on stabilizer circuits and a restricted set of Clifford+T circuits. This system is designed for efficient analysis: In particular, given a precondition and a Clifford circuit, we can derive the most general postcondition in linear time. Given a non-Clifford circuit, determining the postcondition will double in the worst case for each non-Clifford gate in the circuit.

The starting point to understanding our system is the Heisenberg interpretation of quantum mechanics. This interpretation treats quantum operators as functions on operators rather than on quantum states. For instance, given an arbitrary quantum state $|\phi\rangle$,

Aarthi Sundaram: aarthi.sundaram@microsoft.com
Robert Rand: rand@uchicago.edu
Kartik Singhal: ks@cs.uchicago.edu
Brad Lackey: brad.lackey@microsoft.com

the Hadamard operator H satisfies

$$HZ\,|\phi\rangle = XH\,|\phi\rangle\,. \tag{1}$$

In other words, the operator H can be viewed as a function that takes Z to X and similarly takes X to Z. Gottesman [14] used this representation to present the rules for how the Clifford set (H, S and $CNOT$) operates on Pauli X and Z matrices. Hence, we can use Hoare-style triple to describe the action of H on both the X and Z operators.

$$\{\mathbf{X}\}\ H\ \{\mathbf{Z}\} \qquad \{\mathbf{Z}\}\ H\ \{\mathbf{X}\} \tag{2}$$

Note that it suffices to just specify how H acts on $\mathbf{X}$ and $\mathbf{Z}$ as we can derive the action of H on $\mathbf{Y}$ by treating the operator Y as iXZ (since $\sigma_y = i\sigma_x\sigma_z$). More specifically,

$$\begin{aligned} HY\,|\phi\rangle &= H(iXZ)\,|\phi\rangle \\ &= i(HX)Z\,|\psi\rangle \\ &= i(ZH)Z\,|\psi\rangle \\ &= iZ(HZ)\,|\psi\rangle \\ &= iZXH\,|\psi\rangle \\ &= -YH\,|\psi\rangle \end{aligned}$$

Throughout this work, we develop a logic motivated by this interpretation of Pauli matrices as predicates. Formally, the syntax of the logic, as found in Figure 4 and Figure 5, is axiomatic with the semantics described above being a sound interpretation. For example, we can represent the general form of this last deduction by the following deductive rule:

$$\frac{\{\mathbf{X}\}\ U\ \{\mathbf{A}\} \qquad \{\mathbf{Z}\}\ U\ \{\mathbf{B}\}}{\{\mathbf{Y}\}\ U\ \{\mathbf{iAB}\}}\ \mathrm{Y}$$

Here $\mathbf{A}$ and $\mathbf{B}$ are assumed to be Paulis, so the product of $\mathbf{A}$ and $\mathbf{B}$ is simply the third Pauli, possibly negated or multiplied by i. This is indicative (and a special case) of the kinds of rules we will use throughout the paper.

In Gottesman's paper, the end goal was to fully describe quantum programs and prove the *Gottesman-Knill theorem*, which shows that any Clifford circuit can be classically simulated efficiently. Our goal is to take the rules in eq. (2) and use them as a starting point to build a logical system for characterizing quantum programs (§2). Furthermore, we move beyond Clifford circuits and expand the predicates to characterize some magic states, the T gate, and other gates in the Clifford hierarchy (§7). A key feature of our system is that the predicates correspond to unitary Hermitian operators: when restricted to stabilizer quantum computing, these are (tensor products of) Pauli matrices, and for universal quantum computing, they are general unitary Hermitian matrices. Notationally, we use uppercase letters $U, V, \ldots$ to denote unitary gates or matrices and the boldface $\mathbf{U}, \mathbf{V}, \ldots$ to denote the corresponding predicates.

The semantics of stabilizer predicates In our system, a judgment of the form $\mathbf{P}(|\psi\rangle)$ admits a straightforward interpretation: $|\psi\rangle$ is a $+1$ eigenstate of P. As a result, $\{\mathbf{A}\}\ U\ \{\mathbf{B}\}$ means that U maps a $+1$ eigenstate of A to a $+1$ eigenstate of B. This closely mirrors the stabilizer formalism used for error correcting codes [13]. It works well as long as we restrict to Clifford circuits and are fine with very coarse judgments in the face of measurements. However, for more accurate judgments when measurements are performed and to work with more general gates, we will associate $\mathbf{P}(|\psi\rangle)$ with the fact that $|\psi\rangle$ lies in the image of the projection $\Pi_P^+ := \frac{1}{2}(I+P)$ i.e., $\frac{1}{2}(I+P)\,|\psi\rangle = |\psi\rangle$.

We use the tensor operand $\otimes$ to represent multi-qubit predicates. Using our first interpretation, $|\psi\rangle$ satisfies $\mathbf{A} \otimes \mathbf{B}$ if $|\psi\rangle$ is a $+1$-eigenstate of $A \otimes B$. Observe that this does not restrict $|\psi\rangle$ to be a product state $|\phi_1\rangle \otimes |\phi_2\rangle$ such $|\phi_1\rangle$ satisfies $\mathbf{A}$ and $|\phi_2\rangle$ satisfies $\mathbf{B}$. For instance, $\mathbf{A} \otimes \mathbf{B}$ holds of $|\psi'\rangle$ when $|\psi'\rangle = |\phi_1'\rangle \otimes |\phi_2'\rangle$ such that $-\mathbf{A}(|\phi_1'\rangle)$ (i.e., $|\phi_1'\rangle$ is a -1-eigenstate of A) and $-\mathbf{B}(|\phi_2'\rangle)$. Moreover, arbitrary superpositions of $|\psi\rangle$ and $|\psi'\rangle$ also satisfy $\mathbf{A} \otimes \mathbf{B}$.

In our predicate language, conjunction and intersection coincide: if $|\psi\rangle$ is a $+1$-eigenstate of both A and B, then it satisfies $\mathbf{A} \cap \mathbf{B}$. Note that for this to hold A and B must commute, because Pauli operators that do not commute will instead anticommute and have no common eigenvectors. In our projection semantics, a $|\psi\rangle$ that satisfies $\mathbf{P} \cap \mathbf{Q}$ is simultaneously in the image of the two projections Π_P^+ and Π_Q^+.

Finally, we use disjoint unions to represent post-measurement states when the outcome is probabilistic. In this case, $(\mathbf{A} \uplus \mathbf{B})(|\psi\rangle)$ denotes that $|\psi\rangle$ is either a $+1$-eigenstate A or a $+1$-eigenstate of B, without making any claims to the likelihood of which case is true. In the measurement context, it means that one outcome results in the system satisfying $\mathbf{A}$ and the other outcome satisfies $\mathbf{B}$. In our projection semantics, it implies that $|\psi\rangle$ is either in the image of Π_A^+ or in the image of Π_B^+.

While our statements about intersection and union are focused on the stabilizer formalism, and hence refer to Pauli types, they extend to commuting additive predicates as well. For additive predicates, failing to commute does mean they must anticommute and hence in complete generality the situation can be quite complex. In particular, the projection semantics of additive predicates is a traditional quantum logic, or orthomodular lattice of subspaces, for which the analogue of union (span of the two subspaces) does not distribute with the intersection.

Applications Our syntax and derivation rules for Clifford circuits and stabilizer states are methodically developed in §2. The full list of our rules are in Figures 4 and 5. The most straightforward use of our system is in characterizing properties of Clifford circuits, particularly entanglement and separability. For the textbook case of Deutsch's algorithm, we are easily able to verify three key properties: (i) the first qubit is $|0\rangle$ whenever the function is constant, (ii) the first qubit is $|1\rangle$ whenever the function is balanced, and (iii) that the two qubits are never entangled, and therefore the second can be safely discarded. These are three common and broadly useful properties to check.

Ideally, our predicates would be unique: any $\mathbf{A}$ and $\mathbf{B}$ that have the same set of eigenvectors should be equal. This would allow us to prove program equivalence, given fully descriptive predicates for a program (see §2.6). While this uniqueness does not hold by construction, we can obtain a canonical representation for our predicates that guarantees this property. Inspired by the *row echelon form* of a matrix, we describe in §3 an efficient algorithm to generate a canonical representation for intersections of predicates. This allows us to use our logic to *efficiently* track whether a given sub-system is separable from the rest of the system in §4. In §4.3, we generate and then disentangle a GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ to show how the logic is capable of tracking both the creation and destruction of entanglement.

A crucial method used by quantum circuits to extract or output classical information is measurement (usually in the computational basis). It is challenging to tune our logic to accommodate measurement in light of the fact that it requires managing the operation on all the basis states, unlike the evolution of a single Pauli operator. However, measurement on stabilizer states is well understood, and this allows us to construct a procedure to generate a measurement outcome and post-measurement as discussed in §5. In particular, when the measurement outcome is random, we use disjoint unions to capture the fact that the system could be in one of several states, depending on the outcome. As a simple example, applying a z-basis measurement on an $\mathbf{X}$ qubit to get a random 0 or 1 outcome is represented as

$$\frac{}{\{\mathbf{X}\}\ \mathsf{Meas}\ \{\mathbf{Z} \uplus -\mathbf{Z}\}}$$

Using all the elements described above, in §6, we demonstrate how our logic can be used to verify the working of a stabilizer error correcting code (the Steane code on 7 qubits [30]). Specifically, we (i) derive a predicate for a logical qubit in the Steane code; (ii) verify that the encoding circuit constructs the appropriate logical qubit state; and (iii) show the transversality of the H and S gates as well as the non-transversality of the T gate for the Steane code.

Additive predicates and their applications All the ideas discussed up to this point deal with the realm of stabilizer states and Clifford circuits, which are not universal for quantum computing. For instance, while we can add the axiom $\{\mathbf{Z}\}\ T\ \{\mathbf{Z}\}$ to our system, the stabilizer formalism is incapable of expressing the action of the T gate on $\mathbf{X}$. We address this shortcoming by developing *additive predicates* in §7, which are expressed as linear combinations of our basic predicates. This allows us to express the action of T on $\mathbf{X}$ as $\{\mathbf{X}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y})\right\}$.

Since the T-gate is not the only way to achieve universal quantum computation, we produce a straightforward algorithm for adding new gates to the system (such as the Toffoli) by fully deriving their corresponding rules. A particularly nice application has to do with multiply-controlled Z gates, which have very succinct postconditions when applied to $\mathbf{X}$ or $\mathbf{Z}$ qubits. In fact, comparing their derived rules to that of the T gate, we can easily show that synthesizing an n-controlled Z-gate requires at least $(2n-2)$ T-gates.

In §8, we discuss how to determine the postcondition of a single-qubit computational basis measurement given one- and two-qubit additive preconditions. Putting these pieces together in §8.3, we derive rules for gate injection circuits that use associated magic states to implement non-Clifford circuits. We focus on single-qubit unitaries that correspond to a rotation about the Z axis, i.e., that rotate qubits in the $\mathbf{X}/\mathbf{Y}$-plane by some angle θ.

Applying the logic in practice. We conclude with a discussion on the complexity of determining the most descriptive postcondition given a program and a precondition in §9. Unsurprisingly, fully characterizing a circuit with high T-depth proves to be intractable in the general case. However, proving interesting properties of circuits with a few T gates is often quite possible. Moreover, Clifford circuits can be efficiently characterized to any degree of precision, allowing us to flexibly analyze a broad range of quantum programs. Note that efficiency here means that the procedure scales linearly with the number of gates in the operation and polynomially in the size of the system.

We place our work in the context of related work in §10 and discuss possible future applications and extensions to this system in §11.

2 Our Hoare-style Logic and its Semantics

Here we present the internal syntax of our predicates and several semantic interpretations. We will extend this to more general predicates in §7 below. Our atomic predicates correspond to the Pauli matrices and are denoted $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$. We denote basic operators (or *gates*) by H, S, $CNOT$ and later T.

2.1 A Simple Quantum Language

Our language is given by the following grammar:

$$g := H\ i \mid S\ i \mid CNOT\ i\ j \mid T\ i \mid \text{Meas}\ i \mid g; g$$

where the semicolon corresponds to sequencing. T and Meas are both significantly more difficult to reason about than the other operators and will have their own sections devoted to them. Note that we can express other common operators like X, CZ, $T^\dagger$, and CCX (or $TOFF$) in terms of the operators above. We will introduce each of these in this and derive their associated pre- and postconditions.

2.2 Atomic Predicates

Our core interpretation for $\mathbf{X}, \mathbf{Y}$ and $\mathbf{Z}$ is that each of these predicates is inhabited by a single qubit state, the +1-eigenstate of the Pauli operators σ_x, σ_y, and σ_z. The following judgments hold using the standard quantum computing notation:

$$\mathbf{X}(|+\rangle) \qquad \mathbf{Y}(|i\rangle) \qquad \mathbf{Z}(|0\rangle)$$

We can also negate these operators to obtain their -1-eigenstates:

$$-\mathbf{X}(|-\rangle) \qquad -\mathbf{Y}(|-i\rangle) \qquad -\mathbf{Z}(|1\rangle)$$

Note that we can equally well read $-\mathbf{X}(|-\rangle)$ as "$|-\rangle$ is a +1-eigenstate of $-X$" or "$|-\rangle$ is a -1-eigenstate of X". We prefer the former since it will generalize better to multiplication by numbers other than -1 in subsequent sections.

Unlike $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, every single-qubit state is a +1 eigenvector of $\mathbf{I}$:

$$\forall\, |\psi\rangle\,, \mathbf{I}(|\psi\rangle)$$

In this sense, $\mathbf{I}$ corresponds to the proposition "True".

Note that all of our atomic predicates correspond to unitary and hermitian operators. This ensures that they all have +1-eigenstates. In fact, throughout this paper, our predicates will be unitary and hermitian and, with the exception of $\mathbf{I}$ (and $\mathbf{I}$ tensored with itself) of trace 0. This guarantees that they have an equal number of +1 and -1 eigenstates.

2.3 Basic Hoare Triples and Sequencing

To define our basic Hoare triples, we turn to the characterization of H, S and $CNOT$ by Gottesman [14]:

Proposition 1. *Given a unitary $U : A \to B$ in the Heisenberg interpretation, U takes every eigenstate of A to an eigenstate of B with the same eigenvalue.*

Proof. From eq. [1] in Gottesman [14], given a state $|\psi\rangle$ and an operator U,

$$UN|\psi\rangle = UNU^\dagger U|\psi\rangle\,.$$

In the Heisenberg interpretation, this can be denoted as $U : N \rightarrow UNU^\dagger$. Suppose that $|\psi\rangle$ is an eigenstate of N with eigenvalue λ and let $|\phi\rangle$ denote the state after U acts on $|\psi\rangle$. Then,

$$\lambda|\phi\rangle = U(\lambda|\psi\rangle) = UN|\psi\rangle = UNU^\dagger U|\psi\rangle = (UNU^\dagger)|\phi\rangle\,.$$

Hence, $|\phi\rangle$ is an eigenstate of the modified operator $UNU^\dagger$ with eigenvalue λ. □

Therefore, in our logic, $\{\mathbf{A}\}\ U\ \{\mathbf{B}\}$ will mean that U takes a $+1$ eigenstate of A to a $+1$ eigenstate of B.

As a result, our basic Hoare triples for H and S follow precisely from Gottesman (we will postpone the introduction of $CNOT$ until the next section):

$$\frac{}{\{\mathbf{X}\}\ H\ \{\mathbf{Z}\}} \qquad \frac{}{\{\mathbf{Z}\}\ H\ \{\mathbf{X}\}} \qquad \frac{}{\{\mathbf{X}\}\ S\ \{\mathbf{Y}\}} \qquad \frac{}{\{\mathbf{Z}\}\ S\ \{\mathbf{Z}\}}$$

So, for instance, H[1] takes $|+\rangle$ to $|0\rangle$.

Note that every qubit is an $+1$-eigenstate of I, and similarly, every quantum state is an $+1$-eigenstate of I^k (our notation for $I^{\otimes k}$ where k is the number of qubits in the system) so we have the following rule for any single qubit unitary U:

$$\frac{}{\{\mathbf{I}\}\ U\ \{\mathbf{I}\}}\ \mathbf{I}$$

We adopt the standard sequencing rule from Hoare logic:

$$\frac{\{\mathbf{A}\}\ p_1\ \{\mathbf{B}\} \qquad \{\mathbf{B}\}\ p_2\ \{\mathbf{C}\}}{\{\mathbf{A}\}\ p_1; p_2\ \{\mathbf{C}\}}\ \textsc{seq} \tag{3}$$

For instance, here is our derivation of the postcondition for applying $Z = S; S$ to a state satisfying $\mathbf{Z}$:

$$\frac{\dfrac{}{\{\mathbf{Z}\}\ S\ \{\mathbf{Z}\}} \qquad \dfrac{}{\{\mathbf{Z}\}\ S\ \{\mathbf{Z}\}}}{\{\mathbf{Z}\}\ S; S\ \{\mathbf{Z}\}}\ \textsc{seq}$$

Since S has $\mathbf{Y}$ as a postcondition given the precondition $\mathbf{X}$ and our basic Hoare judgments only have $\mathbf{X}$ and $\mathbf{Z}$ preconditions, we will need to introduce rules for coefficients and multiplication that generalize the $\mathbf{Y}$ rule presented in the introduction:

$$\frac{\{\mathbf{A}\}\ p\ \{\mathbf{B}\}}{\{\mathbf{cA}\}\ p\ \{\mathbf{cB}\}}\ \textsc{scale} \qquad \frac{\{\mathbf{A}\}\ p\ \{\mathbf{B}\} \qquad \{\mathbf{C}\}\ p\ \{\mathbf{D}\}}{\{\mathbf{AC}\}\ p\ \{\mathbf{BD}\}}\ \textsc{mul} \tag{4}$$

In SCALE, $\mathbf{c}$ can be any complex number, although in any derivation that stays within the Clifford group, non-vacuous predicates will only use $c \in \{-1, i, -i\}$. We should note that there is no matrix multiplication happening when we apply the MUL rule: There are only 16 possible combinations of two Paulis, each of which produces a Pauli, so we can efficiently simplify these symbolically. The same is true for $c \in \{1, -1, i, -i\}$. We should also note

[1] For readability, we use U as shorthand for U applied to qubit 1 when U is a one qubit unitary, and V as shorthand for $V\ 1\ 2$ when V is a two-qubit unitary, particularly when these are applied to one- and two-qubit states, respectively. We discuss applying unitaries to larger states in §2.4.

that many intermediate deductions will prove vacuous: For instance, we can easily derive that $\{\mathbf{XZ}\}\ H\ \{\mathbf{ZX}\}$ which simplifies to $\{-\mathbf{iY}\}\ H\ \{\mathbf{iY}\}$. In itself, this is not useful, as neither $-iY$ nor iY have $+1$-eigenvectors. However, by applying the scale rule with $c = i$, we get $\{\mathbf{Y}\}\ H\ \{-\mathbf{Y}\}$, which is certainly meaningful.

We can now derive a postcondition for Z given the precondition $\mathbf{X}$:

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

In this deduction, $\mathbf{XZ}$ is simply a notation for $-\mathbf{iY}$ included for readability. Likewise, $\mathbf{YZ}$ is simply $\mathbf{iX}$.

Defining X as $H;Z;H$ and Y as $S;X;Z;S$, we can similarly verify that $\{\mathbf{X}\}\ X\ \{\mathbf{X}\}$, $\{\mathbf{Z}\}\ X\ \{-\mathbf{Z}\}$, $\{\mathbf{X}\}\ Y\ \{-\mathbf{X}\}$, and $\{\mathbf{Z}\}\ Y\ \{-\mathbf{Z}\}$.

2.4 Predicates over multi-qubit systems

In order to do anything interesting, we're going to need to consider multi-qubit systems. We can write a predicate $\mathbf{P}_1 \otimes \mathbf{P}_2 \otimes \cdots \otimes \mathbf{P}_n$ for Pauli predicates $\mathbf{P_i}$ to characterize an n qubit system following our semantics. We use $\mathbf{T}[i]$ to refer to $\mathbf{P}_i$ from that tensor product and $U\ i$ to apply U to the i^{th} qubit in a quantum state. We can therefore introduce the following rule for applying a single-qubit operator to a multi-qubit state:

$$\dfrac{\mathbf{T}[i] = \mathbf{A} \qquad U : \mathbf{A} \to \mathbf{B}}{\{\mathbf{T}\}\ U\ i\ \{\mathbf{T}[\mathbf{i} \mapsto \mathbf{B}]\}}\ \otimes_1 \tag{5}$$

Here $\mathbf{T}\{i \mapsto \mathbf{B}\}$ replaces the predicate for the i^{th} qubit in the tensor product with $\mathbf{B}$.

We can now introduce the Hoare triples corresponding to Gottesman's rules for $CNOT$:

$$\dfrac{}{\{\mathbf{X} \otimes \mathbf{I}\}\ \ CNOT\ \ \{\mathbf{X} \otimes \mathbf{X}\}} \qquad\qquad \dfrac{}{\{\mathbf{I} \otimes \mathbf{X}\}\ \ CNOT\ \ \{\mathbf{I} \otimes \mathbf{X}\}}$$

$$\dfrac{}{\{\mathbf{Z} \otimes \mathbf{I}\}\ \ CNOT\ \ \{\mathbf{Z} \otimes \mathbf{I}\}} \qquad\qquad \dfrac{}{\{\mathbf{I} \otimes \mathbf{Z}\}\ \ CNOT\ \ \{\mathbf{Z} \otimes \mathbf{Z}\}}$$

To apply $CNOT$ to multi-qubit states, we'll need a new rule:

$$\dfrac{\mathbf{T}[i] = \mathbf{A} \qquad \mathbf{T}[j] = \mathbf{B} \qquad \{\mathbf{A} \otimes \mathbf{B}\}\ U\ \{\mathbf{C} \otimes \mathbf{D}\}}{\{\mathbf{T}\}\ U\ i\ j\ \{\mathbf{T}[\mathbf{i} \mapsto \mathbf{C}; \mathbf{j} \mapsto \mathbf{D}]\}}\ \otimes_2 \tag{6}$$

Note that we'll often need to use this in conjunction with the MUL rule, where multiplication distributes over addition. Consider this simple derivation:

$$\dfrac{\begin{array}{c}(\mathbf{Z} \otimes \mathbf{Y} \otimes \mathbf{X})[1] = \mathbf{Z} \qquad (\mathbf{Z} \otimes \mathbf{Y} \otimes \mathbf{X})[3] = \mathbf{X} \\ \dfrac{\{\mathbf{Z} \otimes \mathbf{I}\}\ \ CNOT\ \ \{\mathbf{Z} \otimes \mathbf{I}\} \qquad \{\mathbf{I} \otimes \mathbf{X}\}\ \ CNOT\ \ \{\mathbf{I} \otimes \mathbf{X}\}}{\{\mathbf{Z} \otimes \mathbf{X}\}\ \ CNOT\ \ \{\mathbf{Z} \otimes \mathbf{X}\}}\ \text{MUL}\end{array}}{\{\mathbf{Z} \otimes \mathbf{Y} \otimes \mathbf{X}\}\ \ CNOT\ 1\ 3\ \ \{\mathbf{Z} \otimes \mathbf{Y} \otimes \mathbf{X}\}}\ \otimes_2$$

Note that multiplication distributes componentwise over tensors. Note that sometimes we will obtain a coefficient of -1 when multiplying two terms; we move these to the outside of the tensor so that $\mathbf{X} \otimes -\mathbf{Z}$ becomes $-(\mathbf{X} \otimes \mathbf{Z})$ (the parentheses are generally not needed as a result).

We note that the identity rule also applies to the $CNOT$ gate:

$$\frac{}{\{\mathbf{I} \otimes \mathbf{I}\}\ CNOT\ \{\mathbf{I} \otimes \mathbf{I}\}}\ \mathbf{I}_2$$

On this basis, it is easy to show that $\mathbf{I}^k$ is a universal predicate for all quantum programs, where $\mathbf{I}^k$ corresponds to $I^{\otimes k}$ and k is greater than or equal to the number of qubits in our program.

2.5 Intersections and Consequence Rules

If we want to fully describe an operator's behavior, we need to add conjunctions; or, from the perspective of describing a set of eigenstates, intersections. The derivation rule for intersection is exactly what we would expect:

$$\frac{\{\mathbf{A}\}\ p\ \{\mathbf{B}\} \qquad \{\mathbf{C}\}\ p\ \{\mathbf{D}\}}{\{\mathbf{A} \cap \mathbf{C}\}\ p\ \{\mathbf{B} \cap \mathbf{D}\}}\ \cap \tag{7}$$

Of course, if $\{\mathbf{A}\}\ p\ \{\mathbf{B} \cap \mathbf{C}\}$ is a valid triple, then $\{\mathbf{A}\}\ p\ \{\mathbf{B}\}$ should as well – we're simply weakening the postcondition. Similarly, we should be able to strengthen the precondition to $\mathbf{A} \cap \mathbf{E}$, even if this winds up being the empty set. This brings us to the rule of consequence:

$$\frac{\mathbf{A}' \Rightarrow \mathbf{A} \qquad \{\mathbf{A}\}\ g\ \{\mathbf{B}\} \qquad \mathbf{B} \Rightarrow \mathbf{B}'}{\{\mathbf{A}'\}\ g\ \{\mathbf{B}'\}}\ \text{CONS}$$

Note that $\Rightarrow$ is not general implication: In order to make the logic simple and syntax directed, we do not want to allow for arbitrary linear algebraic or even logical rewriting in the predicates. Instead, we have a small number of implication rules, mostly related to intersections (the remaining rules will appear with their associated connectives and are summarized in fig. 5):

$$\begin{aligned}
&\mathbf{A} \cap \mathbf{B} \Rightarrow \mathbf{A}\\
&\mathbf{A} \cap \mathbf{B} \Rightarrow \mathbf{B} \cap \mathbf{A}\\
&\mathbf{A} \cap (\mathbf{B} \cap \mathbf{C}) \Leftrightarrow (\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C}
\end{aligned}$$

One linear algebraic rule is important and will be used repeatedly in our normalization section (§3), however. Consider the following derivation for $CNOT$:

$$\frac{\{\mathbf{Z} \otimes \mathbf{I}\}\ CNOT\ \{\mathbf{Z} \otimes \mathbf{I}\} \qquad \{\mathbf{I} \otimes \mathbf{Z}\}\ CNOT\ \{\mathbf{Z} \otimes \mathbf{Z}\}}{\{\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{I} \otimes \mathbf{Z}\}\ CNOT\ \{\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z}\}}\ \cap$$

This should become quite easy to interpret: $\mathbf{Z} \otimes \mathbf{I}$ characterizes states where the first qubit is $|0\rangle$ and $\mathbf{I} \otimes \mathbf{Z}$ does the same for the second qubit. Hence, their intersection describes exclusively the state $|00\rangle$. However, while we can check mathematically that $\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z}$ describes exactly the same state, it is rather less obvious from looking at it. Hence, we introduce the rule

$$\mathbf{A} \cap \mathbf{B} \Leftrightarrow \mathbf{A} \cap \mathbf{AB}$$

where multiplication distributes component-wise over tensors.

The argument that this rule is sound is slightly subtle: if $|\psi\rangle : \mathbf{A} \cap \mathbf{B}$ then in our semantics $|\psi\rangle$ is a +1-eigenstate of both (multi-qubit) Pauli operators A and B. But then $|\psi\rangle$ is also a +1-eigenstate of AB. The converse is also true (as $A^2 = I$), and so semantically, $\mathbf{A} \cap \mathbf{B}$ and $\mathbf{A} \cap \mathbf{AB}$ refer to the same set of states.

Hence we get

$$\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z} \Rightarrow \mathbf{Z} \otimes \mathbf{I} \cap \mathbf{ZZ} \otimes \mathbf{ZI} \rightsquigarrow \mathbf{I} \otimes \mathbf{Z}$$

where $\rightsquigarrow$ denotes simplification of predicates. Hence we can derive the desired triple

$$\{\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{I} \otimes \mathbf{Z}\} \ \mathit{CNOT} \ \{\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{I} \otimes \mathbf{Z}\}$$

2.6 Fully Descriptive Predicates

Finally, we will often want a complete description of a given gate or circuit C. As in [14], any Pauli operator can be generated as the tensor product of weight one Pauli operators, so instead of making 2^n judgements to characterize an n-qubit Clifford circuit C it suffices to make the $2n$ judgements

$$\{\mathbf{I} \otimes \cdots \otimes \mathbf{X} \otimes \cdots \otimes \mathbf{I}\} \ C \ \{\mathbf{P_j}\} \quad \text{and} \quad \{\mathbf{I} \otimes \cdots \otimes \mathbf{Z} \otimes \cdots \otimes \mathbf{I}\} \ C \ \{\mathbf{Q_j}\}$$

for each position j.

To succinctly give this characterization, it is useful to add new syntax and corresponding deductive rule (note that this isn't strictly part of the Hoare logic):

$$\frac{\forall i, \{\mathbf{P_i}\} \ p \ \{\mathbf{Q_i}\}}{\{\{\mathbf{P_1} \parallel \mathbf{P_2} \parallel \cdots \parallel \mathbf{P_n}\}\} \ p \ \{\{\mathbf{Q_1} \parallel \mathbf{Q_2} \parallel \cdots \parallel \mathbf{Q_n}\}\}} \parallel$$

This gives us the following information-theoretically complete description of CNOT:

$$\{\{\mathbf{X} \otimes \mathbf{I} \parallel \mathbf{I} \otimes \mathbf{X} \parallel \mathbf{Z} \otimes \mathbf{I} \parallel \mathbf{I} \otimes \mathbf{Z}\}\} \ \mathit{CNOT} \ \{\{\mathbf{X} \otimes \mathbf{X} \parallel \mathbf{I} \otimes \mathbf{X} \parallel \mathbf{Z} \otimes \mathbf{I} \parallel \mathbf{Z} \otimes \mathbf{Z}\}\}$$

2.7 Example: Deutsch's Algorithm

A complete list of our rules and grammar for Pauli predicates is given in Figures 4 and 5. Here, we show an example of how we can apply these rules to make non-trivial judgments about quantum programs.

Many quantum circuits introduce ancillary qubits that perform some classical computation and are then discarded in a basis state. Several efforts have been made to verify this behavior: The Quipper [15] and Q# [32] languages allow us to *assert* that ancillae are separable and can be safely discarded, while $\mathcal{Q}$WIRE allows us to manually verify this [26]. More recently, Silq [3] allows us to define "qfree" functions that never put qubits into a superposition. We can use our logic to avoid this restriction and automatically guarantee ancilla correctness by showing that the ancillae are discarded as they satisfy the predicate $\mathbf{Z}$ and, more specifically, are separable from the rest of the system.

A simple example to demonstrate this ability to safely discard auxiliary qubits is Deutsch's algorithm [9]. Given a function $f : \{0, 1\} \to \{0, 1\}$, the algorithm uses oracle access to f and a single auxiliary qubit to determine if f has a constant value or is balanced.

We want to show that the qubit y is never entangled with qubit x despite the application of the oracle $U_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$. In this case, it would be safe to discard qubit y just after the dotted line in Figure 1 (i.e., even before measurement destroys any hypothetical entanglement).

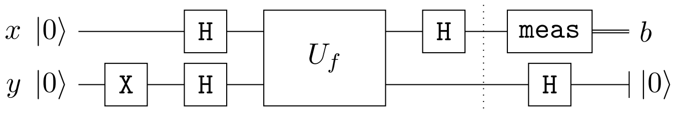

Figure 1: Deutsch's algorithm to check if $f : \{0, 1\} \to \{0, 1\}$ is constant or balanced

Before analyzing the circuit, consider the possible behaviors for f. Acting on a single bit, one can conclude that $f(x) \in \{0, 1, x, (1-x)\}$. It is easy to derive the oracle application by a case-by-case analysis:

$$\texttt{U}_\texttt{f}\ \texttt{1 2} = \begin{cases} \texttt{I 2} & \text{if } f(x) = 0 \\ \texttt{X 2} & \text{if } f(x) = 1 \\ \texttt{CNOT 1 2} & \text{if } f(x) = x \\ \texttt{X 1; CNOT 1 2; X 1} & \text{if } f(x) = 1 - x. \end{cases} \tag{8}$$

Clearly, the first two cases are not entangling gates. The last case is a 0-controlled *CNOT* which is equivalent to the *CNOT* gate for our purposes. Hence, we analyze the circuit for the case where $\texttt{U}_\texttt{f}\ \texttt{1 2} \equiv \texttt{CNOT 1 2}$. The precondition for this circuit is two qubits initialized in the computational basis, or equivalently $\mathbf{Z} \otimes \mathbf{I} \cap \mathbf{I} \otimes \mathbf{Z}$. Instead of building a full proof tree for `deutsch`, we'll use the standard approach for Hoare logic, in which we write an annotated program with the intermediate predicates in between the commands. For convenience, we'll do our derivations in parallel, rather than combining them with the $\cap$ rule at the end:

```
deutsch :=
  {I ⊗ Z ∩ Z ⊗ I}
  X 2;        (* y is set to 1 *)
  {-I ⊗ Z ∩ Z ⊗ I}
  H 1;
  {-I ⊗ Z ∩ X ⊗ I}
  H 2;
  {-I ⊗ X ∩ X ⊗ I}
  Uf 1 2;   (* Uf = CNOT *)
  {-I ⊗ X ∩ X ⊗ X}
  H 1;
  {-I ⊗ X ∩ Z ⊗ X} ⇒ (∩-mul)
  {I ⊗ -X ∩ -Z ⊗ I}
```

The last line is obtained through the ∩-MUL rule and the distributivity of negation. This is precisely what Deutsch's algorithm is supposed to produce – two separable qubits (implied by $\mathbf{A} \otimes \mathbf{I}$, see §4), the first of which is an eigenstate of $-Z$, corresponding to a $|1\rangle$ qubit. Note that we could return the second qubit to $\mathbf{Z}$ by applying a Hadamard and an X. However, as we statically verified that the ancillary y qubit is unentangled with x, we may freely discard it and optimize away the final `H 2`; `X 2`.

This derivation could also similarly be extended to the more generic Deutsch-Jozsa algorithm [10]. This, of course, would require extending both the language and logic to deal with recursion. We leave this challenge for future work.

3 Normal Forms

Our intersection predicates have the property that there exists a canonical form with which to describe them. This allows us to verify the equality of intersection predicates by verifying the equality of their canonical forms. The canonical form we use is inspired by the *row echelon form* of a matrix, in which every row has its first nonzero term before any subsequent row. We translate this into $\mathbf{I}$ being 0 and further impose that $\mathbf{X} \prec \mathbf{Y} \prec \mathbf{Z} \prec \mathbf{I}$ so $\mathbf{I} \otimes \mathbf{X}$ precedes $\mathbf{I} \otimes \mathbf{Z}$. Further, an intersection predicate involving commuting, independent terms can be viewed as a matrix with each term corresponding to a row and each column corresponding to a qubit. Then, in the canonical form, any column contains at most one $\mathbf{X}$, and any column without an $\mathbf{X}$ has at most one $\mathbf{Z}$. The unique $\mathbf{X}$ or $\mathbf{Z}$ in each column will be called the $\mathbf{X}$ or $\mathbf{Z}$ pivot.

The implication rule for intersection predicates, $\mathbf{A} \cap \mathbf{B} \Leftrightarrow \mathbf{A} \cap \mathbf{AB}$, will be useful to reduce the predicates to their canonical forms. Given an n-qubit intersection predicate with m independent terms $\mathbf{A}_{(1)} \cap \ldots \cap \mathbf{A}_{(m)}$, do the following:

1. Let $\mathcal{P}$ be an ordered set of indices, initialized to $\emptyset$.
2. For each qubit $i = 1 \ldots n$:
    - For the first term $j \notin \mathcal{P}$ such that $\mathbf{A}_{(j)}[i] \in \{\mathbf{X}, \mathbf{Y}\}$
        - Update $\mathcal{P} \leftarrow \mathcal{P} \cup \{j\}$.
        - For terms $k \neq j$, if $\mathbf{A}_{(k)}[i] \in \{\mathbf{X}, \mathbf{Y}\}$, rewrite $\mathbf{A}_{(k)} \leftarrow \mathbf{A}_{(j)}\mathbf{A}_{(k)}$.
    - If there is no term with $\mathbf{X}$ or $\mathbf{Y}$ on qubit i , for the first term $j \notin \mathcal{P}$ such that $\mathbf{A}_{(j)}[i] = \mathbf{Z}$:
        - Update $\mathcal{P} \leftarrow \mathcal{P} \cup \{j\}$.
        - For terms $k \neq j$, if $\mathbf{A}_{(k)}[i] = \mathbf{Z}$, rewrite $\mathbf{A}_{(k)} \leftarrow \mathbf{A}_{(j)}\mathbf{A}_{(k)}$.
    - If no term contains $\mathbf{X}$, $\mathbf{Y}$, or $\mathbf{Z}$ on qubit i proceed.
3. We order the terms as follows:
    - For the terms in $\mathcal{P}$, place them in the order in which they appear in $\mathcal{P}$.
    - Order the remaining terms lexicographically.

Notice that each term can be added to $\mathcal{P}$ at most once, and this, along with the ordering of terms, makes the canonical form unique. Further, by viewing the ith term in $\mathcal{P}$ to be the $\mathbf{X}-, \mathbf{Y}-$ or $\mathbf{Z}-$pivot for qubit i, this procedure is functionally equivalent to row echelonization for matrices and can be computed using $O(n^3)$ operations.

Note that this normalization process is functionally similar to the reduction of a stabilizer code to a standard form; see, for example, [22, §10.5.7]. Given the standard form of a stabilizer code, there are efficient methods for generating its encoding circuit using only Clifford gates [7]. In particular, if we are given a state that can be described with a complete Pauli predicate, we know that we can efficiently construct a Clifford circuit from the normal form of the predicate that prepares the given state. We capture this in the following formal statement.

Proposition 2. *Let $|\psi\rangle$ be an n-qubit state. Then $\mathbf{P}_{(1)} \cap \cdots \cap \mathbf{P}_{(n)}(|\psi\rangle)$ if and only if $|\psi\rangle$ can be prepared from $|0 \ldots 0\rangle$ with a Clifford circuit. That is, for any set of commuting Pauli operators $P_{(1)}, \ldots, P_{(n)}$ there exists a Clifford operator $C : \mathbf{Z}_j \to \mathbf{P}_{(j)}$ for each $j = 1, \ldots, n$.*

Example 3. *Consider the following predicate:*

$$\mathbf{X} \otimes \mathbf{X} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z}.$$

Conveniently, the first term contains an $\mathbf{X}$ on qubit 1. However, no subsequent terms have an $\mathbf{X}$ on this qubit, so we move on to qubit 2.

For the second qubit, no $\mathbf{X}$*'s remain in pivot terms, so we take the* $\mathbf{Z}$ *in the second term,* $\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{I}$*. The third term is now rewritten as:*

$$\begin{aligned}&(\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{Z})(\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{I})\\ =\ &\mathbf{ZZ}\otimes\mathbf{ZZ}\otimes\mathbf{ZI}\\ =\ &\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{Z}.\end{aligned}$$

For the last qubit, there is only one term with a $\mathbf{X}$ *or* $\mathbf{Z}$ *in the third position, so we are done.*

The entire procedure yields the normal form:

$$\mathbf{X}\otimes\mathbf{X}\otimes\mathbf{I}\cap\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{I}\cap\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{Z}.$$

An essential property of the normal form is that it is oblivious to the original ordering of the terms. For instance, in Example 3, if we had first swapped the 2nd and 3rd terms then $\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{Z}$ would have been the pivot for the second qubit and we would replace the 3rd term with $\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{Z}$. We would then use the third term as our pivot, replacing the second term ($\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{Z}$) with $\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{I}$. The entire procedure yields $\mathbf{X}\otimes\mathbf{X}\otimes\mathbf{I}\cap\mathbf{Z}\otimes\mathbf{Z}\otimes\mathbf{I}\cap\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{Z}$ just as before.

Since all of our normalization operations are justified by the one implication rule, associativity, and commutativity rules, the following simplification rule is admissible:

$$\frac{\{\mathbf{A}\}\ g\ \{\mathbf{B}\}}{\{\mathbf{A}\}\ g\ \{\text{norm}(\mathbf{B})\}}\ \textsc{Norm}$$

where norm is our normalization procedure. This is the rule we will apply in practice before making separability judgments.

4 Separability

In this section, we present the first application of our Hoare style logic—the ability to make judgments on whether a given sub-system is separable from the remainder of the system. We start with determining whether a single qubit is separable before moving to multi-qubit sub-systems.

4.1 Single qubit separability

Following the core semantics that a predicate refers to the +1-eigenstate of its semantic operator, we first prove a statement about the separable eigenstates of some operators. For notational simplicity, we state the following proposition with a focus on the first qubit; however, the result holds for any operator of the form $I^{k-1}\otimes U\otimes I^{n-k}$

Proposition 4. *For any* 2×2 *unitary, Hermitian matrix* U*, the eigenstates of* $U\otimes I^{n-1}$ *are all vectors of the form* $|u\rangle\otimes|\psi\rangle$ *where* $|u\rangle$ *is an eigenstate of* U *and* $|\psi\rangle\in\mathbb{C}^{2^{n-1}}$ *is an arbitrary state.*

Proof. Let $|\phi\rangle$ be the λ-eigenstate and $\left|\phi^{\perp}\right\rangle$ be the $(-\lambda)$-eigenstate of U where $\lambda\in\{1,-1\}$. Note that $\{|\phi\rangle,\left|\phi^{\perp}\right\rangle\}$ forms a single-qubit basis.

First, consider states of the form $|\gamma\rangle=|u\rangle\otimes|\psi\rangle$ where $|u\rangle\in\{|\phi\rangle,\left|\phi^{\perp}\right\rangle\}$ and $|\psi\rangle\in\mathbb{C}^{2^{n-1}}$. Clearly,

$$(U\otimes I^{n-1})\,|\gamma\rangle=(U\otimes I^{n-1})(|u\rangle\otimes|\psi\rangle)=(U\,|u\rangle)\otimes|\psi\rangle=\lambda_u\,|u\rangle\otimes|\psi\rangle\,.$$

Hence, every state of the form of $|\gamma\rangle$ is an eigenstate of $U \otimes I^{n-1}$. Additionally, note that by similar reasoning, for every separable state $|\gamma\rangle = |v\rangle \otimes |\psi\rangle$, where $|v\rangle \notin \{|\phi\rangle, \left|\phi^{\perp}\right\rangle\}$, is not an eigenstate of $U \otimes I^{n-1}$.

Now we show that any state not in this separable form cannot be an eigenstate of $U \otimes I^{n-1}$. By way of contradiction assume that $|\delta\rangle$ is an eigenstate of $U \otimes I^{n-1}$ with $(U \otimes I^{n-1})|\delta\rangle = \mu |\delta\rangle$. Expand

$$|\delta\rangle = \alpha |\phi\rangle \otimes |\psi_1\rangle + \beta \left|\phi^{\perp}\right\rangle \otimes |\psi_2\rangle$$

where $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^{2^{n-1}}$. Then we compute

$$\begin{aligned}(U \otimes I^{n-1})|\delta\rangle &= \alpha(U|\phi\rangle) \otimes |\psi_1\rangle + \beta(U\left|\phi^{\perp}\right\rangle) \otimes |\psi_2\rangle \\ &= \lambda\alpha |\phi\rangle \otimes |\psi_1\rangle - \lambda\beta \left|\phi^{\perp}\right\rangle \otimes |\psi_2\rangle \\ &= \mu\alpha |\phi\rangle \otimes |\psi_1\rangle + \mu\beta \left|\phi^{\perp}\right\rangle \otimes |\psi_2\rangle\end{aligned}$$

where we have used that $|\phi\rangle$ and $\left|\phi^{\perp}\right\rangle$ are the $+\lambda$ and $-\lambda$ eigenvalues of U respectively. As the components of the expansion are orthogonal to each other, μ must satisfy:

$$\mu\alpha = \lambda\alpha \text{ and } \mu\beta = -\lambda\beta.$$

Since $U \otimes I^{n-1}$ is unitary, $\lambda \neq 0$ and we either have (i) $\alpha = 0$, $\mu = -\lambda$, and $|\delta\rangle = \left|\phi^{\perp}\right\rangle \otimes |\psi_2\rangle$ or (ii) $\beta = 0$, $\mu = +\lambda$, and $|\delta\rangle = |\phi\rangle \otimes |\psi_1\rangle$. In either case, $|\delta\rangle$ has a separable form as claimed. □

As every Pauli matrix is both Hermitian and unitary, combining Propositions 1 and 4, we immediately obtain the following corollary:

Corollary 5. *Every term of the form* $\mathbf{I}^{i-1} \otimes \mathbf{U} \otimes \mathbf{I}^{n-i}$ *is separable, for any* $U \in \{\pm X, \pm Y, \pm Z\}$. *That is, the* i^{th} *factor satisfies the predicate* $\mathbf{U}$ *and is not entangled with the rest of the system.*

Following Gottesman's notation, let $\mathbf{U}_k$ be the n-qubit predicate where the k^{th} factor satisfies the single-qubit predicate $\mathbf{U}$ and is separable from the rest of the system. For example, the predicate $\mathbf{X}_1 \equiv \mathbf{X} \otimes \mathbf{I}$ describes the set of two separable qubits where the first qubit is in the $\mathbf{X}$ eigenstate[2]. The two-qubit product state $|0\rangle \otimes |+\rangle$ satisfies the intersection predicate $\mathbf{Z}_1 \cap \mathbf{X}_2$ to signify that each qubit is separable from the other. Corollary 5 then justifies the following separability-based simplification rules:

$$\mathbf{I}^{k-1} \otimes \mathbf{B} \otimes \mathbf{I}^{n-k} \Leftrightarrow \mathbf{B}_k$$

Since A being separable in a larger system B implies that the rest of B is separable from A, we can add the following rules for distributing separability judgments across intersections:

$$\text{If } \mathbf{T}[k] \in \{\mathbf{B}, \mathbf{I}\},\ \mathbf{B}_k \cap \mathbf{T} \Leftrightarrow \mathbf{B}_k \cap \mathbf{T}_{[n]\setminus\{k\}}$$

Using these rules, we can re-write $\mathbf{X}_1 \cap (\mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{Z})$ as $\mathbf{X}_1 \cap (\mathbf{Z} \otimes \mathbf{Z})_{2,3}$.

[2] For precision, we should say $\mathbf{X}_{1\in[2]}$ to indicate the size of the system, but this will always be clear from the context.

4.2 Multi-qubit separability

While Corollary 5 can be used to identify if a single qubit is separable from the rest of the system, we would also like to make judgments about a multi-qubit subsystem $S \subset \{1, \dots, n\}$ being separable from $\{1, \dots, n\} \setminus S$. Generalizing Proposition 4 will help us in this regard. However, we only generalize it for the case when the unitaries are Pauli matrices (rather than generic Hermitian matrices). The following fact about Pauli matrices adapted from Nielsen and Chuang [22, Prop. 10.5] by setting $n \leftarrow k, k \leftarrow 0$, will be useful for the proof.

Fact 6. *For k-qubit Pauli matrices $V \in \{\pm I, \pm X, \pm Y, \pm Z\}^k$ such that $V \neq I^k$, the eigenvalue $\lambda \in \{-1, 1\}$ has an eigenspace of dimension 2^{k-1}. For k independent, commuting k-qubit Pauli matrices $U_{(1)}, \dots U_{(k)}$, the joint eigenspace for an eigenvalue tuple $(\lambda_1, \dots, \lambda_k)$ has dimension 1.*

This fact can be intuitively argued from the observation that each Pauli matrix divides the total 2^k-dimensional Hilbert space into two sub-spaces of the same dimension, each corresponding to the $+1$ or -1 eigenvalues. The k-tuple then identifies a 1-dimensional subspace at the intersection of the corresponding eigenspaces for $U_{(1)}, \dots, U_{(k)}$.

Fact 6 requires the k-qubit Pauli matrices to be independent and pairwise commuting. It is straightforward to check independence by ensuring that multiplying any combination of the k matrices together does not yield the $\mathbf{I}^k$ term. Pairwise commutativity can also be directly determined using the following fact, which follows immediately from the fact that distinct Pauli matrices from $\{X, Y, Z\}$ anticommute.

Fact 7. *Given $A = A_1 \otimes \dots \otimes A_k$ and $B = B_1 \otimes \dots \otimes B_k$, where the A_is and B_is are Pauli matrices, A and B will commute precisely when there is an even number of positions where A_i and B_i are both from $\{X, Y, Z\}$ but $A_i \neq B_i$.*

We can now state the conditions under which a set of Pauli operators could correspond to a separable sub-system.

Proposition 8. *For independent, commutative, non-identity k-qubit matrices $U_{(1)}, \dots, U_{(k)} \in \{\pm I, \pm X, \pm Y, \pm Z\}^k$ such that $U_{(i)} \cap U_{(j)} \neq \emptyset$ for all $i \neq j$, the eigenstate of $(I^{n-k} \otimes U_{(1)}) \cap \dots \cap (I^{n-k} \otimes U_{(k)})$ are all vectors of the form $|u\rangle \otimes |\Psi\rangle$ where $|\Psi\rangle$ is an eigenstate of $U_{(1)}, \dots, U_{(k)}$.*

Proof. First, it is clear that any state of the form $|u\rangle \otimes |\Psi\rangle$ where $|\Psi\rangle$ is an eigenstate of $U_{(1)}, \dots, U_{(k)}$ is an eigenstate of $I^{n-k} \otimes U_{(1)}, \dots, I^{n-k} \otimes U_{(k)}$. This implies that it is also an eigenstate of $(I^{n-k} \otimes U_{(1)}) \cap \dots \cap (I^{n-k} \otimes U_{(k)})$.

To prove the inverse direction, assume by way of contradiction that there exists an entangled n-qubit state $|\delta\rangle$ that is an eigenstate of $(I \otimes U_{(i)}$ with eigenvalue $\lambda_i \in \{-1, 1\}$ for each $i \in \{1, \dots, k\}$. Let the n-qubit state $|\delta\rangle$ be written in terms of its *Schmidt* (singular value) decomposition across the $(n-k, k)$ qubit bipartition as

$$|\delta\rangle = \sum_{j=1}^{K} \alpha_j |\phi_j\rangle \otimes |\gamma_j\rangle$$

where $\{|\phi_i\rangle\}_i$ and $\{|\gamma_i\rangle\}_i$ are orthonormal vectors in each of their respective subsystems.

$$\begin{aligned}
\forall i \in \{1,\ldots,k\} \quad (I \otimes U_{(i)})\,|\delta\rangle &= \sum_j \alpha_j (I\,|\phi_j\rangle) \otimes (U_{(i)}\,|\gamma_j\rangle) \\
&= \lambda_i \sum_j \alpha_j\,|\phi_j\rangle \otimes |\gamma_j\rangle \\
&= \sum_j \alpha_j\,|\phi_j\rangle \otimes (\lambda_i\,|\gamma_j\rangle) \\
&\Rightarrow \forall i,j, \quad U_{(i)}\,|\gamma_j\rangle = \lambda_i\,|\gamma_j\rangle\,. \\
&\Rightarrow \forall i,j, \quad \lambda_i U_{(i)}\,|\gamma_j\rangle = |\gamma_j\rangle \quad \text{Since, } \lambda_i \in \{-1,1\}. \qquad (9)
\end{aligned}$$

As $\{|\gamma_i\rangle\}_i$ forms a set of orthonormal vectors, the span of these vectors is contained in the eigenspace for the eigenvalue tuple $(+1,+1,\ldots,+1)$ corresponding to $\lambda_1 U_{(1)},\ldots,\lambda_k U_{(k)}$ respectively. Additionally, when $U_{(i)}$ is a k-qubit Pauli matrix, $\lambda_i U_{(i)}$ is also in $\{\pm I, \pm X, \pm Y, \pm Z\}^k$. Then, from Fact 6, the joint eigenspace for the all-1s tuple has dimension 1. Specifically, there exists only a single $|\gamma\rangle$ that satisfies Equation (9). Hence, $K = 1$ contradicting the assumption that $|\delta\rangle$ is entangled across the $(n-k,k)$ qubit bi-partition. □

Extending the $\mathbf{U}_i$ notation to the multi-qubit setting where $K \subset \{1,\ldots,n\}$ and $0 < |K| < n$, let $(\mathbf{U})_K$ be the predicate such that qubits in K are separable from the $\{1,\ldots,n\} \setminus K$ sub-system. Formally, we define $\mathbf{U}_K := \left(\cap_{j=1}^{|K|} \mathbf{U}_{(j)}\right)_K$ where each $\mathbf{U}_{(j)}$ is a non-trivial $|K|$-qubit non-identity Pauli string.

For example, consider a 2-qubit predicate $(\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})$ whose joint eigenspace is spanned by the two maximally entangled Bell states $\{|\Phi^+\rangle, |\Psi^-\rangle\}$. In an n-qubit state satisfying this predicate on the first and third qubits, these qubits being maximally entangled are disjoint from the rest of the system, and hence, they satisfy the predicate

$$(\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{1,3} = (\mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I}^{n-3}) \cap (\mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I}^{n-3}).$$

If the second and fourth qubits are similarly entangled, the system satisfies the predicate $(\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{1,3} \cap (\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{2,4}$. This idea to gather the nontrivial factors within a subsystem is not unique to our work and has been previously employed by Honda [17] to determine the entangled components in his static analysis framework.

Combining this representation with Propositions 1 and 8, we obtain the following corollary:

Corollary 9. *Let $K \subset \{1,\ldots,n\}$ with $|K| = k$ and $\overline{K} := \{1,\ldots,n\} \setminus K$. Every intersection predicate 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 as a sub-term is separable across the bi-partition $(K, \overline{K})$. That is, the factors in K are separable from the $\overline{K}$ subsystem.*

Given a canonical n-qubit intersection predicate with m independent terms $\mathbf{A}_{(1)} \cap \ldots \cap \mathbf{A}_{(m)}$, finding if a subsystem of qubits $K \subset \{1,\ldots,n\}$ with $|K| = k < m$, is separable from the remaining system can be determined in a straightforward way. We first verify that every qubit in K has a pivot; otherwise, some qubit in K has $\mathbf{I}$ in all terms, and we can conclude that K is not separable from the remaining system. If every qubit in K has a pivot, we run the following procedure:

- Let $\mathbf{A}_{(j_1)},\ldots,\mathbf{A}_{(j_k)}$ be the k terms which have the pivots for qubits in K.

- For each $i = 2 \ldots k$, check that $\mathbf{A}_{(j_i)}$ commutes with $\mathbf{A}_{(j_1)}$ using Fact 7.[3]
- For each $i = 1 \ldots k$, check that the term $\mathbf{A}_{(j_i)}$ has an $\mathbf{I}$ for every qubit $\ell \in \overline{K}$.

Corollary 9 justifies our multi-qubit separability rules when $S = \{j_1, \ldots, j_k\} \subset [n]$

$$\mathbf{B} \cap \mathbf{T}_{(1)} \cap \ldots \cap \mathbf{T}_{(k)} \Leftrightarrow \mathbf{B}_{\overline{S}} \cap \Big(\mathbf{C}_{(1)} \cap \ldots \cap \mathbf{C}_{(k)}\Big)_S,$$
$$\text{where } \forall_{j\in[k]}\ \mathbf{T}_{(j)}[S] = \mathbf{C}_{(j)} \forall_{j\in[k]}\ \mathbf{T}_{(j)}[\overline{S}] = \mathbf{I}^{n-k}\mathbf{B}[S] = \mathbf{I}^k$$

Example 10. *Continuing from Example 3, consider the predicate*

$$\mathbf{X} \otimes \mathbf{X} \otimes \mathbf{I} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I} \cap \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Z}.$$

As $(\mathbf{X} \otimes \mathbf{X})$ *and* $(\mathbf{Z} \otimes \mathbf{Z})$ *are two independent and commuting operators, the first two terms with* $\mathbf{I}$ *on the third qubit ensure that we can apply Corollary 9 to determine that the first two qubits are separable from the third. We can write this as:*

$$(\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{1,2} \cap \mathbf{Z}_3.$$

4.3 Application: GHZ state, Entanglement Creation and Disentanglement

To demonstrate how we can track the possibly entangling and disentangling properties of the *CNOT* gate, we can look at the example of creating the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ starting from $|000\rangle$ and then disentangling it. A similar example was considered by Honda [17] to demonstrate how his system can track when *CNOT* displays either its entangling or disentangling behavior. One crucial difference is that Honda uses the denotational semantics of density matrices which, in practice, would scale poorly with the size of the program being validated. Our approach is closer to that of Perdrix [24, 23] in terms of design and scalability but capable of showing separability where the prior systems could not.

We will consider the following GHZ program acting on the initial state $\mathbf{Z}_1 \cap \mathbf{Z}_2 \cap \mathbf{Z}_3$. We first follow the derivation for $\mathbf{Z}_1$:

```
Definition GHZ :=
  {Z₁} ⇒
  {Z ⊗ I ⊗ I}
  H 1;
  {X ⊗ I ⊗ I}
  CNOT 1 2;
  {X ⊗ X ⊗ I}
  CNOT 2 3
  {X ⊗ X ⊗ X}
```

Repeating the derivation for $\mathbf{Z}_2$ and $\mathbf{Z}_3$, we obtain:

$$\{\mathbf{Z_2}\}\ \texttt{GHZ}\ \{\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}\}$$
$$\{\mathbf{Z_3}\}\ \texttt{GHZ}\ \{\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}\}$$

If we now apply `CNOT 3 1`, we get the following specifications:

$$\{\mathbf{Z_1}\}\ \texttt{GHZ}\ \{\mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X}\}\ \texttt{CNOT 3 1}\ \{\mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X}\}$$
$$\{\mathbf{Z_2}\}\ \texttt{GHZ}\ \{\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}\}\ \texttt{CNOT 3 1}\ \{\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z}\}$$
$$\{\mathbf{Z_3}\}\ \texttt{GHZ}\ \{\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}\}\ \texttt{CNOT 3 1}\ \{\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}\}$$

[3] This ensures that in all terms where the qubits in $\overline{K}$ are pivots, the terms have an $\mathbf{I}$ for all qubits in K.

If we want to analyze the output of this program on $\mathbf{Z_1} \cap \mathbf{Z_2} \cap \mathbf{Z_3}$, we can apply the following normalization steps (the first and second row serving as the first and second pivots):

$$\begin{aligned}
&\{\mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \cap \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}\} \Rightarrow \\
&\{\mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \cap \mathbf{IZ} \otimes \mathbf{ZZ} \otimes \mathbf{ZZ}\} \ \rightsquigarrow \\
&\{\mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \cap \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{I}\}.
\end{aligned}$$

Recognizing that the first qubit can now be separated from the other two, we obtain $\mathbf{Z}_1 \cap (\mathbf{X} \otimes \mathbf{X} \cap \mathbf{Z} \otimes \mathbf{Z})_{2,3}$, that is, a $\mathbf{Z}$ qubit and a Bell pair.

Returning to the unnormalized program, if we finally apply `CNOT 3 2`, we get

$$\begin{aligned}
&\{\mathbf{Z_1}\}\ \texttt{GHZ; CNOT 3 1; CNOT 3 2}\ \{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X}\} \\
&\{\mathbf{Z_2}\}\ \texttt{GHZ; CNOT 3 1; CNOT 3 2}\ \{\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}\} \\
&\{\mathbf{Z_3}\}\ \texttt{GHZ; CNOT 3 1; CNOT 3 2}\ \{\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I}\}
\end{aligned}$$

to which we can apply the intersection rule and single-qubit separability rules to obtain

$$\{\mathbf{Z_1} \cap \mathbf{Z_2} \cap \mathbf{Z_3}\}\ \texttt{GHZ; CNOT 3 1; CNOT 3 2}\ \{\mathbf{Z_1} \cap \mathbf{Z_2} \cap \mathbf{X_3}\}$$

showing that the whole procedure moves the $\mathbf{X}$ generated by the initial Hadamard gate to the third position.

5 Measurement

It is challenging to turn Gottesman's semantics for measurement into an efficient deductive system because it looks at its operation on all the basis states rather than simply the evolution of a single Pauli operator. Namely, it adds significant computational complexity, while our prior deductive rules were linear in the number of qubits. Nonetheless, our normalization in §3 parallels that in the stabilizer formalism, and the action of measurement on stabilizer groups is well-understood [14]. This produces a method for inferring the postconditions for measurement that is quadratic in the number of qubits in the worst case [1].

5.1 Union predicates

Before discussing how we check measurement, it helps to consider how we can represent post-measurement states. Unlike unitary gate application, which is deterministic, implying that each input predicate has a specified output predicate, not all measurements have deterministic outcomes. While we do not want to use our logic system to verify the probabilities of measurement outcomes, it would be useful to be able to compute the possible post-measurement states for the system. With this, we could still track how the system evolves with subsequent operations depending on the measurement results.

We use the union connective, $\mathbf{A} \uplus \mathbf{B}$, to denote that the system either satisfies the predicate $\mathbf{A}$ or predicate $\mathbf{B}$. We show how to use this in the context of measurement with this simple example.

Example 11 (Measuring $|+\rangle$)**.** *Consider the single qubit in the $|+\rangle$ state on which a computational basis measurement is performed. The outcome has equal probability to be* 0 *or* 1 *which we cast as qubits in states $|0\rangle : \mathbf{Z}$ and $|1\rangle : -\mathbf{Z}$ respectively. We represent this in our logic system as*

$$\frac{}{\{\mathbf{X}\}\ \mathit{Meas}\ \{\mathbf{Z} \uplus -\mathbf{Z}\}}$$

Applying a gate to a union predicate distributes across the union, and each term in the union evolves separately. This gives the following rule for unions:

$$\frac{\{\mathbf{A}\}\ g\ \{\mathbf{A}'\} \qquad \{\mathbf{B}\}\ g\ \{\mathbf{B}'\}}{\{\mathbf{A} \uplus \mathbf{B}\}\ g\ \{\mathbf{A}' \uplus \mathbf{B}'\}}\ \uplus$$

As with intersections, the ordering of the terms does not matter, with commutativity and associativity holding for unions as well, leading to the following implications:

$$\begin{aligned}&\mathbf{A} \Rightarrow \mathbf{A} \uplus \mathbf{B}\\ &\mathbf{A} \uplus \mathbf{B} \Rightarrow \mathbf{B} \uplus \mathbf{A}\\ &\mathbf{A} \uplus (\mathbf{B} \uplus \mathbf{C}) \Rightarrow (\mathbf{A} \uplus \mathbf{B}) \uplus \mathbf{C}\end{aligned}$$

5.2 Predicates for post-measurement states

For ease of exposition, we will assume that we are performing a Z-basis measurement on the j^{th} qubit of an n qubit system. In §3 we introduced a normalization procedure for intersection predicates. There, we constructed the normal form by examining each qubit in turn $i = 1, \ldots, n$, and looked for an intersection term whose i^{th} factor is $\mathbf{X}$, $\mathbf{Y}$, or $\mathbf{Z}$. As there, let us write $\mathbf{A}_{(1)} \cap \cdots \cap \mathbf{A}_{(m)}$ for the pre-measurement predicate. Now however, we begin by searching for an i, such that its j^{th} factor $\mathbf{A}_{(i)}[j] \in \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$.

1. If there exists an i such that $\mathbf{A}_{(i)}[j] = \mathbf{X}$ or $\mathbf{A}_{(i)}[j] = \mathbf{Y}$, then the measurement outcome is uniformly random:
   (a) Replace $\mathbf{A}_{(k)} \leftarrow \mathbf{A}_{(i)} A_{(k)}$ for all $k \neq i$ with $\mathbf{A}_{(k)}[j] \in \{\mathbf{X}, \mathbf{Y}\}$.
   (b) Let $\mathbf{U}' = \mathbf{A}_{(1)} \cap \cdots \cap \mathbf{A}_{(i-1)} \cap \mathbf{A}_{(i+1)} \cap \cdots \cap \mathbf{A}_{(m)}$.
   (c) The post-measurement state satisfies the predicate $(\mathbf{Z}_j \cap \mathbf{U}') \uplus (-\mathbf{Z}_j \cap \mathbf{U}')$.
   (d) Normalize each branch of the union separately to get the normalized post-measurement predicate.

2. If no i has $\mathbf{A}_{(i)}[j] \in \{\mathbf{X}, \mathbf{Y}\}$ find an i such that $\mathbf{A}_{(i)}[j] = \mathbf{Z}$. When this is the case, the outcome is deterministic as some combination of the intersection terms is $\mathbf{Z}_j$ or $-\mathbf{Z}_j$ [1]:[4]
   (a) Using the implication that $\mathbf{A} \cap \mathbf{B} \Leftrightarrow \mathbf{A} \cap \mathbf{AB}$, obtain $\pm\mathbf{Z}_j$ as an intersection term (our normalization procedure ensures this can be done efficiently). Let the rest of the intersection be $\mathbf{U}$.
   (b) Normalize the term $(\pm\mathbf{Z}_j \cap \mathbf{U})$ to obtain the normalized post-measurement predicate.

3. If all $A_{(i)}[j] = \mathbf{I}$ then the post-measurement state will satisfy the predicate

$$(\mathbf{Z}_1 \cap \mathbf{A}_{(1)} \cap \cdots \cap \mathbf{A}_{(m)}) \uplus (-\mathbf{Z}_1 \cap \mathbf{A}_{(1)} \cap \cdots \cap \mathbf{A}_{(m)}).$$

   Normalize each branch of the union separately to get the normalized post-measurement predicate.

[4] We refer the interested reader to the discussion following Proposition 3 in Aaronson and Gottesman [1] for details on why this fact holds.

Observe that case (3) can occur only when an $m < n$–that is, the predicate is underdetermined. This will commonly be the case while dealing with the physical qubit predicates for stabilizer-based error-correcting codes. Finally, by construction, the measured qubit satisfies the predicate $\mathbf{Z}$ or $-\mathbf{Z}$ and is separable from the rest of the system.

Example 12. *As an example of our normalization and measurement rules, consider measuring the first qubit in the z-basis, a state satisfying the predicate* $\mathbf{X} \otimes \mathbf{X}$*. According to our rules above, we remove this term when considering the post-measurement predicate; that is, we know nothing of the resulting predicate except the consequence of the measurement. In particular, rule (1) above states our post-measurement predicate is of the form* $\mathbf{Z}_1 \uplus -\mathbf{Z}_1$*. To validate this in the semantics, we note* $\mathbf{X} \otimes \mathbf{X}(|\psi\rangle)$ *if and only if*

$$|\psi\rangle = \alpha\,|{+}{+}\rangle + \beta\,|{-}{-}\rangle = \tfrac{1}{\sqrt{2}}\,|0\rangle \otimes (\alpha\,|+\rangle + \beta\,|-\rangle) + \tfrac{1}{\sqrt{2}}\,|1\rangle \otimes (\alpha\,|+\rangle - \beta\,|-\rangle).$$

Regardless of measuring 0 *or* 1*, the resulting state in the other qubit is arbitrary. Hence the postcondition is indeed of the form* $(\mathbf{Z} \otimes \mathbf{I}) \uplus (-\mathbf{Z} \otimes \mathbf{I}) = \mathbf{Z}_1 \uplus -\mathbf{Z}_1$*.*

5.3 Example: Measuring a GHZ state

Continuing our analysis of the GHZ state from §4.3, the circuit `GHZ` has the postcondition

$$(\mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X}) \cap (\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}).$$

To compute the output of `GHZ; MEAS 1`, we enact the above program. Fortunately, our intersection already has the requisite form, with the first term being the only one with an $\mathbf{X}$ in the initial position. We remove the term $(\mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X})$ and replace the intersection with

$$(\mathbf{Z}_1 \cap (\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z})) \uplus (-\mathbf{Z}_1 \cap (\mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z}))$$

We normalize each branch of the union as per §3 to obtain

$$(\mathbf{Z}_1 \cap \mathbf{Z}_2 \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z})) \uplus (-\mathbf{Z}_1 \cap -\mathbf{Z}_2 \cap (\mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{Z})).$$

Finally, the last term can also be simplified to give $(\mathbf{Z}_1 \cap \mathbf{Z}_2 \cap \mathbf{Z}_3) \uplus (-\mathbf{Z}_1 \cap -\mathbf{Z}_2 \cap -\mathbf{Z}_3)$.
□

6 Application: Error-correcting Codes

We can also use our logic system to analyze error-correcting codes. In this section, we consider the 7-qubit Steane [29] code. Recall that the Steane code encodes a single qubit into 7 qubits and has the ability to detect errors on 2 qubits and correct all single-qubit errors. The stabilizers and logical operators for the Steane code are generated by:

$$\begin{array}{ccc} g_1 = IIIXXXX & g_2 = IXXIIXX & \overline{X} = XXXXXXX \\ g_3 = XIXIXIX & g_4 = IIIZZZZ & \overline{Z} = ZZZZZZZ \\ g_5 = IZZIIZZ & g_6 = ZIZIZIZ & \end{array}$$

We realize $|0\rangle$ in this setup through the logical state $|0_L\rangle$ defined by projecting the all 0s state using the stabilizer generators of the code:

$$|0_L\rangle \propto \frac{1}{2^6}\Pi_{i=1}^{6}(I + g_i)\,|0000000\rangle$$

By virtue of being the logical 0 state, it should also be stabilized by the logical-σ_Z equivalent $\overline{Z}$. In other words, $|0_L\rangle$ is uniquely stabilized by $g_1, \ldots, g_6$ and $\overline{Z}$. In our system, this means that $|0_L\rangle : \mathbf{Z}_L$ where $\mathbf{Z}_L$ is the 7-term intersection predicate

$$\begin{aligned} \mathbf{Z}_L &:= \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \cap \overline{\mathbf{Z}} \\ &= \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X} \\ &\cap \ldots \cap \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{Z} \\ &\cap \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{Z} \end{aligned} \tag{10}$$

By a similar argument, $|+_L\rangle : \mathbf{X}_L$ where $\mathbf{X}_L = \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \cap \overline{\mathbf{X}}$. All states in the Steane code space are stabilized by $g_1, \ldots, g_6$. Then, we can associate the following predicate to the logical Steane code space as

$$\mathbf{St_7} := \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \qquad \text{and} \qquad \mathbf{Z}_L = \mathbf{St_7} \cap \overline{\mathbf{Z}}; \quad \mathbf{X}_L = \mathbf{St_7} \cap \overline{\mathbf{X}}.$$

Being consistent with the equation above, we can conclude that $|+i_L\rangle : \mathbf{Y}_L$ where

$$\mathbf{Y}_L := \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \cap \overline{\mathbf{Y}} \qquad \text{where} \qquad \overline{Y} = i\overline{XZ}.$$

Further, we use $\mathbf{Y}_L = i\mathbf{X}_L\mathbf{Z}_L$ as syntactic sugar to derive the action of any gate on $\mathbf{Y}_L$. In this scenario, we can manipulate the predicates at the logical level, i.e., $\{\mathbf{X}_L, \mathbf{Y}_L, \mathbf{Z}_L\}$ as if they share the same algebraic relations as their corresponding Pauli counterparts, $\{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$.

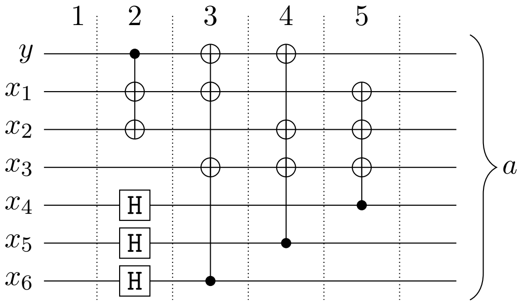

Figure 2: Encoding circuit for the Steane $[[7, 1, 3]]$ code

Consider the Steane code unitary encoding circuit `Enc−St` given in Figure 2 where a data qubit y is converted into a logical qubit a. By construction, it takes $|a\rangle \otimes |000000\rangle \to |a_L\rangle$ for $a \in \{0, 1, +, -\}$. Consider $a = 0$ for instance. Then we can describe the action of `Enc−St` in our system as follows:

1. start with the precondition $\mathbf{Z}_y \cap \mathbf{Z}_{x_1} \cap \ldots \cap \mathbf{Z}_{x_6}$;

2. apply each gate from Figure 2 using the axioms for H and $CNOT$;

3. normalize the output.

A straightforward computation (an exercise left to the reader) will show that we indeed obtain norm($\mathbf{Z}_L$) as the output. Extending this argument, we characterize `Enc − St` as:

$$\{\mathbf{Z_y} \cap \mathbf{Z_{x_1}} \cap \ldots \cap \mathbf{Z_{x_6}}\} \ \texttt{Enc}-\texttt{St} \ \{\text{norm}(\mathbf{Z_L})\}$$
$$\{\mathbf{X_y} \cap \mathbf{Z_{x_1}} \cap \ldots \cap \mathbf{Z_{x_6}}\} \ \texttt{Enc}-\texttt{St} \ \{\text{norm}(\mathbf{X_L})\}$$

Another application of our system is verifying the transversality of a gate with respect to a code. For instance, it is straightforward to verify that $\mathtt{H_L} := \mathtt{H\ y;\ H\ x_1;\ H\ x_2;\ H\ x_3;\ H\ x_4;\ H\ x_5;\ H\ x_6}$ is transversal for the Steane code i.e.,

$$\{\mathbf{X_L}\}\ H_L\ \{\mathbf{Z_L}\} \qquad \text{and} \qquad \{\mathbf{Z_L}\}\ H_L\ \{\mathbf{X_L}\} \tag{11}$$

Clearly, $\{\mathbf{g_1} \cap \mathbf{g_2} \cap \mathbf{g_3}\}\ H_L\ \{\mathbf{g_4} \cap \mathbf{g_5} \cap \mathbf{g_6}\}$ and vice-versa. Hence, $\{\mathbf{St_7}\}\ H_L\ \{\mathbf{St_7}\}$. Further, $\left\{\overline{\mathbf{X}}\right\}\ H_L\ \left\{\overline{\mathbf{Z}}\right\}$ and vice-versa. Therefore, H_L takes $\mathbf{Z}_L = \mathbf{St_7} \cap \overline{\mathbf{Z}}$ to $\mathbf{St_7} \cap \overline{\mathbf{X}} = \mathbf{X}_L$ and vice-versa.

In a similar vein, we can prove that the operation $U = \mathtt{S\ y;\ S\ x_1;\ S\ x_2;\ S\ x_3;\ S\ x_4;\ S\ x_5;\ S\ x_6}$ is not the logical-S gate S_L. Firstly, the triple for the logical-S should satisfy

$$\{\mathbf{Z_L}\}\ S_L\ \{\mathbf{Z_L}\} \qquad \text{and} \qquad \{\mathbf{X_L}\}\ S_L\ \{\mathbf{Y_L}\}$$

Now, $\left\{\mathbf{g_4} \cap \mathbf{g_5} \cap \mathbf{g_6} \cap \overline{\mathbf{Z}}\right\}\ U\ \left\{\mathbf{g_4} \cap \mathbf{g_5} \cap \mathbf{g_6} \cap \overline{\mathbf{Z}}\right\}$ as the S acts only on $\mathbf{Z}$ or $\mathbf{I}$. In the case of $\{\mathbf{g_1}, \mathbf{g_2}, \mathbf{g_3}, \overline{\mathbf{X}}\}$, the $\mathbf{X}$s are converted to $\mathbf{Y}$s such that the predicates are changed on output. Clearly, $\left\{\overline{\mathbf{X}}\right\}\ U\ \{\mathbf{Y^7}\}$ but $\mathbf{Y}^7 = -\mathbf{i}\overline{\mathbf{XZ}} = -\overline{\mathbf{Y}}$. Let us take $\mathbf{g_1} \cap \mathbf{g_4}$ to see how the remaining stabilizers would evolve:

$$\dfrac{\dfrac{\{\mathbf{g_1} \cap \mathbf{g_4}\}\ U\ \{(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y}) \cap \mathbf{g_4}\}}{\{\mathbf{g_1} \cap \mathbf{g_4}\}\ U\ \{(\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y})\mathbf{g_4} \cap \mathbf{g_4}\}}\ \text{CONS}}{\{\mathbf{g_1} \cap \mathbf{g_4}\}\ U\ \{\mathbf{g_1} \cap \mathbf{g_4}\}}$$

$$\begin{aligned}\{g_1 \cap g_4\}\ U\ &\{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y}) \cap g_4\} \Rightarrow \\ &\{\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y} \otimes \mathbf{Y})g_4 \cap g_4\} \rightsquigarrow \\ &\{g_1 \cap g_4\}\end{aligned}$$

Extending this reasoning to $(\mathbf{g_2} \cap \mathbf{g_5})$ and $(\mathbf{g_3} \cap \mathbf{g_6})$, $\{\mathbf{St_7}\}\ U\ \{\mathbf{St_7}\}$. Putting the pieces together, $\{\mathbf{Z_L}\}\ U\ \{\mathbf{Z_L}\}$ but U takes $\mathbf{X}_L$ to $\mathbf{St_7} \cap -\overline{\mathbf{Y}} = -\mathbf{Y}_L$. By contrast, defining

$$\mathtt{S_L} := \mathtt{Z\ y;\ S\ y;\ Z\ x_1; S\ x_1\ Z\ x_2;\ S\ x_2;\ Z\ x_3;\ S\ x_3;\ Z\ x_4;\ S\ x_4;\ Z\ x_5;\ S\ x_5;\ Z\ x_6;\ S\ x_6}$$

gives us the desired behavior.

We would also like to show that the T-gate is not transversal for the Steane code. However, with T not being a Clifford gate, we find that Pauli predicates are insufficient to describe it fully. For this, we consider the additive extension to our logic system in subsequent sections and demonstrate this in Example 16.

6.1 Logical Multi-qubit predicates

Extending the discussion on logical qubits and quantum error correcting codes to multi-qubit logical states requires us to add some additional rules to our system.

Separable states Describing states where each qubit is separable will be the most straightforward of these. A simple example is with the state $|01\rangle : \mathbf{X}_1 \cap \mathbf{Z}_2$. Correspondingly the state $|0_L 1_L\rangle : (\mathbf{X}_L)_{\underline{1}} \cap (\mathbf{Z}_L)_{\underline{2}}$ where $\underline{1}, \underline{2}$ represent the logical qubits. From the point of the physical qubits $\underline{1}, \underline{2}$ denote the sets of physical qubits that encode each logical qubit. For instance, for the 7-qubit Steane code, $\underline{1} := (y, x_1, \ldots, x_6)$ and $\underline{2} := (y', x'_1, \ldots, x'_6)$. Formally, we get,

$$(\mathbf{X}_L)_{\underline{1}} \cap (\mathbf{Z}_L)_{\underline{2}} = (\mathbf{g_1} \cap \ldots \mathbf{g_6} \cap \overline{\mathbf{X}})_{\underline{1}} \cap (\mathbf{g_1} \cap \ldots \mathbf{g_6} \cap \overline{\mathbf{Z}})_{\underline{2}}$$

Entangled multi-qubit states To express the predicate for two logical qubits as, say, $\mathbf{X}_L \otimes_L \mathbf{Z}_L$, and effectively tracking their evolution requires more advanced notions such as a logical tensor product $\otimes_L$ between logical predicates and further rules on how tensor products behave with intersections. For the sake of this example, we consider a logical tensor operation $\otimes_L$ that acts as follows:

- Consider two basic logical predicates $\mathbf{A}_L, \mathbf{B}_L$ for $A, B \in \{X, Z\}$
- Order their intersection terms as $\mathbf{A}_L = \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \cap \overline{\mathbf{A}}$ and $\mathbf{B}_L = \mathbf{g_1} \cap \ldots \cap \mathbf{g_6} \cap \overline{\mathbf{B}}$
- Define $\mathbf{A}_L \otimes_L \mathbf{B}_L$:=$(\mathbf{St_7} \otimes \mathbf{I}^7) \cap (\mathbf{I}^7 \otimes \mathbf{St_7}) \cap (\overline{\mathbf{A}} \otimes \overline{\mathbf{B}})$.

Not that this definition is not arbitrary, but it can, in fact, be derived from existing rules in our system along with the assumption that the tensor distributes across intersections when the terms involved commute, i.e.,

$$\frac{\{\mathbf{T}\}\ g\ \{(\mathbf{A} \cap \mathbf{B}) \otimes \mathbf{C}\}}{\{\mathbf{T}\}\ g\ \{(\mathbf{A} \otimes \mathbf{I}) \cap (\mathbf{B} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{C})\}}\ \cap\text{-}\otimes\text{-DIST} \tag{12}$$

Recalling that $\mathbf{St_7} = \mathbf{g_1} \cap \ldots \cap \mathbf{g_6}$, we can fully expand the $\otimes_L$ expression as

$$\mathbf{A}_L \otimes_L \mathbf{B}_L {=} (\mathbf{g_1} \otimes \mathbf{I}^7) \cap \ldots \cap (\mathbf{g_6} \otimes \mathbf{I}^7) \cap (\mathbf{I}^7 \otimes \mathbf{g_1}) \cap \ldots \cap (\mathbf{I}^7 \otimes \mathbf{g_6}) \cap (\overline{\mathbf{A}} \otimes \overline{\mathbf{B}})$$

Now, the question becomes: can we show the transversality of *CNOT* with respect to the Steane code? We can begin by defining:

$$\mathtt{CNOT_L}\ \underline{1}\ \underline{2} := \mathtt{CNOT\ y\ y'};\ \mathtt{CNOT\ x_1\ x_1'};\ \mathtt{CNOTx_2\ x_2'};\ \mathtt{CNOT\ x_3\ x_3'};$$
$$\mathtt{CNOT\ x_4\ x_4'};\ \mathtt{CNOT\ x_5\ x_5'};\ \mathtt{CNOT\ x_6\ x_6'};.$$

Using the behavior of *CNOT* from Table 2, we need to show that

$$\begin{array}{ll} \{\mathbf{X_L} \otimes \mathbf{I_L}\}\ CNOT_L\ \{\mathbf{X_L} \otimes \mathbf{X_L}\} & \{\mathbf{I_L} \otimes \mathbf{X_L}\}\ CNOT_L\ \{\mathbf{I_L} \otimes \mathbf{X_L}\} \\ \{\mathbf{I_L} \otimes \mathbf{Z_L}\}\ CNOT_L\ \{\mathbf{Z_L} \otimes \mathbf{Z_L}\} & \{\mathbf{Z_L} \otimes \mathbf{I_L}\}\ CNOT_L\ \{\mathbf{Z_L} \otimes \mathbf{I_L}\} \end{array} \tag{13}$$

Here, by $\mathbf{I}_L$, we mean any state that lies in the codespace of the Steane code, and so,

$$\mathbf{I}_L := \mathbf{g_1} \cap \ldots \cap \mathbf{g_6}.$$

It will be easier to derive the action of $CNOT_L$ by understanding its actions on each of the stabilizers and logical operators for the Steane code as all logical predicates use these as the building blocks. Applying $CNOT_L$ to each of the operators gate-wise, we get:

- For the X-terms, i.e., for $\mathbf{A} \in \{\mathbf{g_1}, \mathbf{g_2}, \mathbf{g_3}, \overline{\mathbf{X}}\}$

$$\left\{\mathbf{A} \otimes \mathbf{I^7}\right\}\ CNOT_L\ \{\mathbf{A} \otimes \mathbf{A}\} \quad \text{and} \quad \left\{\mathbf{I^7} \otimes \mathbf{A}\right\}\ CNOT_L\ \left\{\mathbf{I^7} \otimes \mathbf{A}\right\} \tag{14}$$

- For the Z-term, i.e., for $\mathbf{A} \in \{\mathbf{g_4}, \mathbf{g_5}, \mathbf{g_6}, \overline{\mathbf{Z}}\}$

$$\left\{\mathbf{A} \otimes \mathbf{I^7}\right\}\ CNOT_L\ \left\{\mathbf{A} \otimes \mathbf{I^7}\right\} \quad \text{and} \quad \left\{\mathbf{I^7} \otimes \mathbf{A}\right\}\ CNOT_L\ \{\mathbf{A} \otimes \mathbf{A}\} \tag{15}$$

As the term $(\mathbf{St_7} \otimes \mathbf{I}^7) \cap (\mathbf{I}^7 \otimes \mathbf{St_7})$ appears in every predicate for entangled states, we first derive the action of $CNOT_L$ on it.

$$\cfrac{\cfrac{\left\{(\mathbf{St_7} \otimes \mathbf{I^7}) \cap (\mathbf{I^7} \otimes \mathbf{St_7})\right\} \ \ CNOT_L \ \ \left\{\bigcap_{\mathbf{i=1}}^{\mathbf{6}} (\mathbf{g_i} \otimes \mathbf{g_i}) \bigcap_{\mathbf{i=4}}^{\mathbf{6}} (\mathbf{g_i} \otimes \mathbf{I^7}) \bigcap_{\mathbf{i=1}}^{\mathbf{3}} (\mathbf{I^7} \otimes \mathbf{g_i})\right\}}{\left\{(\mathbf{St_7} \otimes \mathbf{I^7}) \cap (\mathbf{I^7} \otimes \mathbf{St_7})\right\} \ \ CNOT_L \ \ \left\{\bigcap_{\mathbf{i=1}}^{\mathbf{6}} (\mathbf{g_i} \otimes \mathbf{I^7}) \bigcap_{\mathbf{i=1}}^{\mathbf{6}} (\mathbf{I^7} \otimes \mathbf{g_i})\right\}} \ \textsc{cons}}{\left\{(\mathbf{St_7} \otimes \mathbf{I^7}) \cap (\mathbf{I^7} \otimes \mathbf{St_7})\right\} \ \ CNOT_L \ \ \left\{(\mathbf{St_7} \otimes \mathbf{I^7}) \cap (\mathbf{I^7} \otimes \mathbf{St_7})\right\}} \tag{16}$$

Now, using eqs. (14) to (16), we can derive the action of $CNOT_L$ on the remaining logical predicates. Taking $\mathbf{X}_L \otimes \mathbf{I}_L = (\mathbf{St_7} \otimes \mathbf{I}^7) \cap (\mathbf{I}^7 \otimes \mathbf{St_7}) \cap (\overline{\mathbf{X}} \otimes \mathbf{I}^7)$ as an example,

$$\cfrac{\{\mathbf{X_L} \otimes \mathbf{I_L}\} \ \ CNOT_L \ \ \left\{(\mathbf{St_7} \otimes \mathbf{I^7}) \cap (\mathbf{I^7} \otimes \mathbf{St_7}) \cap (\overline{\mathbf{X}} \otimes \overline{\mathbf{X}})\right\}}{\{\mathbf{X_L} \otimes \mathbf{I_L}\} \ \ CNOT_L \ \ \{\mathbf{X_L} \otimes \mathbf{X_L}\}} \ \textsc{cons}$$

Similarly, for the other three cases, we can directly get

$$\begin{gathered}
\{\mathbf{Z_L} \otimes \mathbf{I_L}\} \ \ CNOT_L \ \ \{\mathbf{Z_L} \otimes \mathbf{I_L}\} \\
\{\mathbf{I_L} \otimes \mathbf{X_L}\} \ \ CNOT_L \ \ \{\mathbf{I_L} \otimes \mathbf{X_L}\} \\
\{\mathbf{I_L} \otimes \mathbf{Z_L}\} \ \ CNOT_L \ \ \{\mathbf{Z_L} \otimes \mathbf{Z_L}\}
\end{gathered}$$

thereby satisfying Equation (13) and confirming the transversality of $CNOT$ for the Steane code.

7 Additive Predicates

7.1 The Clifford + T set

Up to this point, we have focused on Hoare triples of Clifford operations, which are not universal for quantum computation. The easiest path from the Clifford set to a universal set is adding the T operator to our language. Appealing to Gottesman's original Heisenberg formalism $T\sigma_z T^\dagger = \sigma_z$, and so we can use the triple $\{\mathbf{Z}\} \ T \ \{\mathbf{Z}\}$. Unfortunately,

$$T\sigma_x T^\dagger = \tfrac{1}{\sqrt{2}} \left(\begin{smallmatrix} 0 & 1-i \\ 1+i & 0 \end{smallmatrix}\right)$$

is not in the Pauli group and hence not expressible in our logic using Pauli predicates.

Yet, $\frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 0 & 1-i \\ 1+i & 0 \end{smallmatrix}\right)$ can be rewritten as the weighted sum of Pauli matrices $\frac{1}{\sqrt{2}}(\sigma_x + \sigma_y)$, so if our judgments distribute over addition, we can expand it to deal with *additive* predicates $\mathbf{A} + \mathbf{B}$. Indeed $U(A + B)U^\dagger = UAU^\dagger + UBU^\dagger$. To incorporate terms involving added predicates, we extend our grammar to include words of the form $\mathbf{G} + \mathbf{G}$, where $\mathbf{G}$ is the language of Pauli predicates. Throughout, we will use the shorthand $\mathbf{A} - \mathbf{B} = \mathbf{A} + (-\mathbf{B})$. We extend our judgments with the rule

$$\cfrac{\{\mathbf{A}\} \ U \ \{\mathbf{C}\} \qquad \{\mathbf{B}\} \ U \ \{\mathbf{D}\}}{\{\mathbf{A} + \mathbf{B}\} \ U \ \{\mathbf{C} + \mathbf{D}\}} \ \textsc{add} \tag{17}$$

Note that this will so frequently be combined with our SCALE rule (which can now see a broader range of coefficients c) to deal with additive predicates that we will tend to apply them together.

Example 13 (*T* on precondition $\mathbf{Y}$)**.** *We prove the behavior of T on precondition $\mathbf{Y}$ explicitly:*

$$\frac{\overline{\{\mathbf{X}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y})\right\}} \qquad \overline{\{\mathbf{Z}\}\ T\ \{\mathbf{Z}\}}}{\{\mathbf{Y}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{Y}-\mathbf{X})\right\}}\ \textit{MUL+SCALE}$$

Example 14 (Composing *T*)**.** *We prove that $T;T$ provides the same triples as S. This is trivially true on $\mathbf{Z}$ since both S and T take precondition $\mathbf{Z}$ to postcondition $\mathbf{Z}$. We prove the $T;T$ reproduces the correct postcondition on $\mathbf{X}$ explicitly:*

$$\frac{\overline{\{\mathbf{X}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y})\right\}} \qquad \overset{\textit{ADD+SCALE}}{\dfrac{\overline{\{\mathbf{X}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y})\right\}} \qquad \overline{\{\mathbf{Y}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{Y}-\mathbf{X})\right\}}}{\left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y})\right\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}+\mathbf{Y}+\mathbf{Y}-\mathbf{X}))\right\}}}}{\{\mathbf{X}\}\ T;T\ \{\mathbf{Y}\}}\ \textit{SEQ}$$

Example 15 (Typing $T^\dagger$)**.** *Finally, it is useful to know the triples of $T^\dagger$, which we'll define as $Z;S;T$. Again one trivially has $\{\mathbf{Z}\}\ T^\dagger\ \{\mathbf{Z}\}$, so we simply prove its behavior on $\mathbf{X}$ as follows:*

$$\frac{\dfrac{\overline{\{\mathbf{X}\}\ Z\ \{-\mathbf{X}\}} \qquad \overline{\{-\mathbf{X}\}\ S\ \{-\mathbf{Y}\}}}{\{\mathbf{X}\}\ Z;S\ \{-\mathbf{Y}\}}\ \textit{SEQ} \qquad \overline{\{-\mathbf{Y}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}-\mathbf{Y})\right\}}}{\{\mathbf{X}\}\ Z;S;T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X}-\mathbf{Y})\right\}}\ \textit{SEQ}$$

Example 16 (Steane code non-transversality of *T*)**.** *Now that we have the triple for T, the logical-T gate for the Steane code T_L should satisfy*

$$\{\mathbf{Z}_L\}\ T_L\ \{\mathbf{Z}_L\}\ \textit{and}\ \{\mathbf{X}_L\}\ T_L\ \{\tfrac{1}{\sqrt{2}}(\mathbf{X}_L+\mathbf{Y}_L)\}$$

where we use the descriptions from §6 for $\mathbf{Z}_L, \mathbf{X}_L$ and $\mathbf{Y}_L$. However, we can easily show that the operation $U :=$ `T y; T x`$_1$`; T x`$_2$`; T x`$_3$`; T x`$_4$`; T x`$_5$`; T x`$_6$ does not satisfy this behavior. In fact, U acting on $\mathbf{St_7}$ changes the output as any stabilizer containing an $\mathbf{X}$ is converted into a non-trivial additive predicate. Then, T applied to $\mathbf{St_7}$ becomes a predicate containing states outside both the Steane code space as well as the larger stabilizer state space. For instance

$$\{\mathbf{g_1}\}\ U\ \{\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{I}\otimes\tfrac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Y})\otimes\tfrac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Y})\otimes\tfrac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Y})\otimes\tfrac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Y})\},$$

which is clearly not a simple tensor product of Paulis as a stabilizer is expected to be.

Proposition 17. *Let $|\psi\rangle$ be an n-qubit state satisfying $\left(\frac{1}{\sqrt{2}}(\mathbf{P}_0+\mathbf{P}_1)\cap\mathbf{P}_2\cdots\cap\mathbf{P}_n\right)$ with P_0, P_1 anticommuting. Then $|\psi\rangle$ can be prepared from $|0\ldots0\rangle$ with a Clifford plus one T-gate circuit.*

Proof. As P_0, P_1 are anticommuting, by Theorem 42 there exists a Clifford circuit C such that $\{\mathbf{P}_0\}\ C\ \{-\mathbf{X}\otimes\mathbf{I}\otimes\cdots\mathbf{I}\}$ and $\{\mathbf{P}_1\}\ C\ \{\mathbf{Y}\otimes\mathbf{I}\otimes\cdots\mathbf{I}\}$. Hence

$$\left[\left(\tfrac{1}{\sqrt{2}}(\mathbf{X}+\mathbf{Y})\otimes\mathbf{I}^{\otimes(n-1)}\right)\cap\mathbf{P}'_2\cdots\cap\mathbf{P}'_n\right](C\,|\psi\rangle).$$

Note that each P'_j $(j=2,\ldots,n)$ must commute with $\frac{1}{\sqrt{2}}(X+Y)\otimes I^{\otimes(n-1)}$ and hence $P_j = I\otimes Q_j$ or $P_j = \sigma_z\otimes Q_j$. In either case, apply a $T^\dagger$-gate to the first qubit gives $T_1^\dagger : \mathbf{P}'_j \to \mathbf{P}'_j$. Consequently,

$$\left[\left(\mathbf{X}\otimes\mathbf{I}^{\otimes(n-1)}\right)\cap\mathbf{P}'_2\cdots\cap\mathbf{P}'_n\right](T_1^\dagger C\,|\psi\rangle).$$

Now, we can apply Proposition 2 and obtain a Clifford C' such that $C'T_1^\dagger C\,|\psi\rangle$ satisfies $\mathbf{Z}_1 \cap \cdots \cap \mathbf{Z}_n$. Therefore $(C'T_1^\dagger C)^\dagger$ is our desired circuit. □

Note that there is a converse of this result. One can always squander the single T-gate by applying it directly to $|0\ldots 0\rangle$. But presuming this is not the case, and we prepare a state on which T acts nontrivially, then additional Clifford gates can only produce predicates of the form $\frac{1}{\sqrt{2}}(\mathbf{P}_0 + \mathbf{P}_1) \cap \mathbf{P}_2 \cdots \cap \mathbf{P}_n$ with P_0, P_1 anticommuting.

7.2 Example: Hoare triple for Toffoli

Now that we have a judgment for T, we can use it to derive a valid Hoare triple for Toffoli via the latter's standard decomposition into T, H and $CNOT$ gates:

```
TOFFOLI a b c :=
  H c; CNOT b c; T† c; CNOT a c; T c; CNOT b c; T† c;
  CNOT a c; T b; T c; H c; CNOT a b; T a; T† b; CNOT a b.
```

Showing that $\{\mathbf{Z_1} \cap \mathbf{Z_2}\}$ `TOFFOLI` $\{\mathbf{Z_1} \cap \mathbf{Z_2}\}$ proves remarkably straightforward:

$$\begin{array}{rl}
 & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{H c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{CNOT b c; T}^\dagger\texttt{ c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{CNOT a c; T c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{CNOT b c; T}^\dagger\texttt{c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{CNOT a c; T b; T c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{H c;} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\} \\
\texttt{CNOT a b; T a; T}^\dagger\texttt{b;} & \{Z \otimes I \otimes I \cap Z \otimes Z \otimes I\} \\
\texttt{CNOT a b.} & \{Z \otimes I \otimes I \cap I \otimes Z \otimes I\}
\end{array}$$

Note that the trailing T and $T^\dagger$s are all applied to $\mathbf{I}$ or $\mathbf{Z}$ and therefore have no effect on the predicates. (We combine them with the previous commands for conciseness.) Noticeably, the derivation that $\{\mathbf{X_3}\}$ `TOFFOLI` $\{\mathbf{X_3}\}$ also proves trivial (since `H c` immediately converts the $\mathbf{X}$ to a $\mathbf{Z}$), showing that a $|+\rangle$ in the third position is not entangled by a Toffoli gate. By contrast, Toffoli's action on $\mathbf{Z}_3$ does get a bit messy[5]:

$$\begin{array}{rl}
 & \{I \otimes I \otimes Z\} \\
\texttt{H c;} & \{I \otimes I \otimes X\} \\
\texttt{CNOT b c;} & \{I \otimes I \otimes X\} \\
\texttt{T}^\dagger\texttt{ c;} & \{I \otimes I \otimes X - I \otimes I \otimes Y\} \\
\texttt{CNOT a c;} & \{I \otimes I \otimes X - Z \otimes I \otimes Y\} \\
\texttt{T c;} & \{I \otimes I \otimes X + I \otimes I \otimes Y - Z \otimes I \otimes Y + Z \otimes I \otimes X\} \\
\texttt{CNOT b c;} & \{I \otimes I \otimes X + I \otimes Z \otimes Y - Z \otimes Z \otimes Y + Z \otimes I \otimes X\} \\
\texttt{T}^\dagger\texttt{ c;} & \{I \otimes I \otimes X - I \otimes I \otimes Y + I \otimes Z \otimes X + I \otimes Z \otimes Y - \\
 & \;\; Z \otimes Z \otimes X - Z \otimes Z \otimes Y + Z \otimes I \otimes X - Z \otimes I \otimes Y\} \\
\texttt{CNOT a c; T b;} & \{I \otimes I \otimes X - Z \otimes I \otimes Y + I \otimes Z \otimes X + Z \otimes Z \otimes Y - \\
 & \;\; Z \otimes Z \otimes X - I \otimes Z \otimes Y + Z \otimes I \otimes X - I \otimes I \otimes Y\}
\end{array}$$

[5] We leave off the coefficients for readability's sake, but this derivation, while wholly mechanical, can be difficult to follow to the end. The reader may wish to skip to the final steps of the deduction.

$$\begin{aligned}
\texttt{T c;}\quad & \{I\otimes I\otimes X + I\otimes I\otimes Y - Z\otimes I\otimes Y + Z\otimes I\otimes X\ + \\
& I\otimes Z\otimes X + I\otimes Z\otimes Y + Z\otimes Z\otimes Y - Z\otimes Z\otimes X\ - \\
& Z\otimes Z\otimes X - Z\otimes Z\otimes Y - I\otimes Z\otimes Y + I\otimes Z\otimes X\ + \\
& Z\otimes I\otimes X + Z\otimes I\otimes Y - I\otimes I\otimes Y + I\otimes I\otimes X\} \\
\texttt{H c;}\quad & \{I\otimes I\otimes Z - I\otimes I\otimes Y + Z\otimes I\otimes Y + Z\otimes I\otimes Z\ + \\
& I\otimes Z\otimes Z - I\otimes Z\otimes Y - Z\otimes Z\otimes Y - Z\otimes Z\otimes Z\ - \\
& Z\otimes Z\otimes Z + Z\otimes Z\otimes Y + I\otimes Z\otimes Y + I\otimes Z\otimes Z + \\
& Z\otimes I\otimes Z - Z\otimes I\otimes Y + I\otimes I\otimes Y + I\otimes I\otimes Z\} \\
\texttt{CNOT a b;}\quad & \{I\otimes I\otimes Z - I\otimes I\otimes Y + Z\otimes I\otimes Y + Z\otimes I\otimes Z\ + \\
& Z\otimes Z\otimes Z - Z\otimes Z\otimes Y - I\otimes Z\otimes Y - I\otimes Z\otimes Z\ - \\
& I\otimes Z\otimes Z + I\otimes Z\otimes Y + Z\otimes Z\otimes Y + Z\otimes Z\otimes Z + \\
& Z\otimes I\otimes Z - Z\otimes I\otimes Y + I\otimes I\otimes Y + I\otimes I\otimes Z\} \\
\texttt{T a; T}^\dagger\texttt{ b;}\quad & \{I\otimes I\otimes Z - I\otimes I\otimes Y + Z\otimes I\otimes Y + Z\otimes I\otimes Z\ + \\
& Z\otimes Z\otimes Z - Z\otimes Z\otimes Y - I\otimes Z\otimes Y - I\otimes Z\otimes Z\ - \\
& I\otimes Z\otimes Z + I\otimes Z\otimes Y + Z\otimes Z\otimes Y + Z\otimes Z\otimes Z\ + \\
& Z\otimes I\otimes Z - Z\otimes I\otimes Y + I\otimes I\otimes Y + I\otimes I\otimes Z\} \\
\texttt{CNOT a b;}\quad & \{I\otimes I\otimes Z - I\otimes I\otimes Y + Z\otimes I\otimes Y + Z\otimes I\otimes Z + \\
& I\otimes Z\otimes Z - I\otimes Z\otimes Y - Z\otimes Z\otimes Y - Z\otimes Z\otimes Z\ - \\
& Z\otimes Z\otimes Z + Z\otimes Z\otimes Y + I\otimes Z\otimes Y + I\otimes Z\otimes Z\ + \\
& Z\otimes I\otimes Z - Z\otimes I\otimes Y + I\otimes I\otimes Y + I\otimes I\otimes Z\} \\
\Longrightarrow\quad & \{I\otimes I\otimes Z + Z\otimes I\otimes Z + I\otimes Z\otimes Z - Z\otimes Z\otimes Z\ - \\
& Z\otimes Z\otimes Z + I\otimes Z\otimes Z + Z\otimes I\otimes Z + I\otimes I\otimes Z\} \\
\Longrightarrow\quad & \{I\otimes I\otimes Z + Z\otimes I\otimes Z + I\otimes Z\otimes Z - Z\otimes Z\otimes Z\}
\end{aligned}$$

Note that, despite the presence of seven T or $T^\dagger$-gates (and hence a potential of 128 summands appearing in the additive predicate), only four of them enlarged the term – all T or $T^\dagger$ gates applied to either of the first two qubits failed to change the predicates. The $\mathbf{X}$s all left the picture once we applied the second Hadamard, and the $\mathbf{Y}$s all canceled out, leaving only $\mathbf{Z}$s and $\mathbf{I}$s. In fact, every summand has a $\mathbf{Z}$ in the last position, and the first predicate leaves us no way to introduce a negative on the $\mathbf{Z}$.

Hence, we can conclude that Toffoli satisfies the triple

$$\{\mathbf{Z_1} \cap \mathbf{Z_2} \cap \mathbf{Z_3}\}\ \texttt{TOFFOLI}\ \{\mathbf{Z_1} \cap \mathbf{Z_2} \cap \mathbf{Z_3}\}$$

7.3 General additive predicates

Clifford+T, as studied in the previous section, is universal in that all unitaries can be approximated as a composition of such gates. However, one often wishes to do an exact analysis or simply use a different universal gate set. Recall that we say $|\psi\rangle$ satisfies a predicate $\mathbf{P}$ if $|\psi\rangle$ is a $+1$-eigenstate of the (multi-qubit) Pauli operator P. The critical feature of Pauli operators is they are unitary, Hermitian, and (except in the case of the identity) trace zero. Thus, unitary, Hermitian, and trace zero operators form a natural basis to extend Pauli predicates. Note that the Pauli operators form a linear basis of the vector space of all linear operators, and so for any unitary and Hermitian operator M, we can write $M = \sum_j c_j P_j$ for some (real) coefficients c_j and Pauli operators P_j.

Definition 18. *An* additive predicate *is an expression of the form* $\mathbf{M} = \sum_j c_j \mathbf{P}_j$ *where* $c_j \in \mathbb{R}$ *and* $\mathbf{P}_j$ *are Pauli predicates, such that the operator* $M = \sum_j c_j P_j$ *is unitary, Hermitian, and trace zero. We say a state* $|\psi\rangle$ *satisfies* $\mathbf{M}$*, written* $\mathbf{M}(|\psi\rangle)$*, if* $M\,|\psi\rangle = |\psi\rangle$*.*

Lemma 19. *A one-qubit additive predicate has the form* $\mathbf{M} = a\mathbf{X} + b\mathbf{Y} + c\mathbf{Z}$ *with* $a^2 + b^2 + c^2 = 1$.

Proof. Any one-qubit operator may written $M = tI + a\sigma_x + b\sigma_y + c\sigma_z$. As M is Hermitian $t, a, b, c \in \mathbb{R}$. But M is also unitary so

$$I = M^2 = (t^2 + a^2 + b^2 + c^2)I + 2ta\sigma_x + 2tb\sigma_y + 2tc\sigma_z.$$

Hence $t = 0$, and therefore M has trace zero and $a^2 + b^2 + c^2 = 1$. □

This lemma shows that 1-qubit additive predicates are particularly simple in that they form a representation of the familiar Bloch sphere.

Proposition 4 on separability was stated at a level of generality that supports additive predicates as follows.

Corollary 20. *Let* $\mathbf{I}^{(k-1)} \otimes \mathbf{M} \otimes \mathbf{I}^{(n-k)}$ *be an additive predicate, and suppose* $|\psi\rangle$ *satisfies* $\mathbf{I}^{(k-1)} \otimes \mathbf{M} \otimes \mathbf{I}^{(n-k)}$. *Then the* k^{th} *qubit of* $|\psi\rangle$ *is unentangled from the rest of the system.*

7.4 Logic of general unitary maps

The logic of Clifford operators carries over to general unitaries. With Cliffords, we claimed that a complete description of an n-qubit operator could be deduced based on examining the preconditions $\mathbf{X}_j$ and $\mathbf{Z}_j$ as $j = 1, \ldots, n$. In the case of 1-qubit unitaries consider the triple $\{\mathbf{M}\}\ U\ \{\mathbf{N}\}$. Using $|m\rangle$ and $|n\rangle$ for one-qubit states that satisfy $\mathbf{M}(|M\rangle)$ and $\mathbf{N}(|n\rangle)$, we have $U\,|m\rangle\langle m|\,U^\dagger = |n\rangle\langle n|$, which in turn implies $UMU^\dagger = N$. If $\mathbf{M} = a\mathbf{X} + b\mathbf{Y} + c\mathbf{Z}$ then also $M = a\sigma_x + b\sigma_y + c\sigma_z$, and thus

$$N = U(a\sigma_x + b\sigma_y + c\sigma_z)U^\dagger = aU\sigma_xU^\dagger + bU\sigma_yU^\dagger + cU\sigma_zU^\dagger.$$

That is, if we merely knew $\{\mathbf{X}\}\ U\ \{\mathbf{N_x}\}$ and $\{\mathbf{Z}\}\ U\ \{\mathbf{N_z}\}$ then we can deduce $\{\mathbf{Y}\}\ U\ \{\mathbf{N_y}\}$, where

$$N_y = U\sigma_yU^\dagger = iU\sigma_xU^\dagger U\sigma_zU^\dagger = iN_xN_z,$$

and so deduce $N = aN_x + bN_y + cN_z$. In other words, knowing the postconditions of U on preconditions $\mathbf{X}$ and $\mathbf{Z}$ suffices to prove the behavior of U on any additive predicate precondition.

This extends to multi-qubit unitaries as expected. If we know how an n-qubit unitary U behaves on preconditions $\mathbf{X}_j$ and $\mathbf{Z}_j$ for any $j = 1, \ldots, n$, then we can compute $UPU^\dagger$ for any n-qubit Pauli operator. From this we can then compute the postcondition of U with any additive predicate $\mathbf{M}$ as precondition from $UMU^\dagger = \sum_j c_jUP_jU^\dagger$. That is, each unitary can be viewed as a matrix acting on Pauli operators, which Gosset et al. [12] refer to the "channel" representation of U. In particular, we see that as a Clifford operators only permutes Pauli operators (possibly with a sign change) its matrix only contains values −1, 0, or 1. From above, the channel representation of a T-gate has coefficients of the form $\frac{c}{2^{s/2}}$ for $c \in \{-1, 0, 1\}$ and $s \in \{0, 1\}$ (see also [12, Equation (6.2)]). With a straightforward induction argument we prove the following result.

Theorem 21. *Let* U *be a unitary circuit on* n *qubits composed of* t *number of* T*-gates and an arbitrary number of Clifford gates, and suppose* $\{\mathbf{X_j}\}\ U\ \{\mathbf{M_j}\}$ *and* $\{\mathbf{Z_j}\}\ U\ \{\mathbf{N_j}\}$ *for additive predicates* $\mathbf{M}_j$ *and* $\mathbf{N}_j$*, for each* $j = 1, \ldots, n$. *Then every coefficient of* $\mathbf{M}_j$ *and* $\mathbf{N}_j$ *is of the form* $\frac{c}{2^{s/2}}$ *where* $c, s \in \mathbb{Z}$ *and* $s \leq t$.

Proof. Inductively, if $t = 0$, then U is a Clifford operator, and so each $\mathbf{M}_j$ and $\mathbf{N}_j$ is a Pauli predicate, and hence as additive predicates, all their coefficients are in $\{-1, 0, 1\}$ as desired.

Suppose the statement is true for all unitary circuits containing at most $t-1$ number of T-gates, and suppose U is a unitary circuit with t number of T-gates. Suppose $U = C \circ U'$ with C a Clifford operator. We claim U' has the same assumptions and requirements as U: clearly U' also contains t number of T-gates, and if $\{\mathbf{X_j}\}\ U'\ \left\{\mathbf{M'_j}\right\}$ and $\{\mathbf{Z_j}\}\ U'\ \left\{\mathbf{N'_j}\right\}$ then we must have $\left\{\mathbf{M'_j}\right\}\ C\ \{\mathbf{M_j}\}$ and $\left\{\mathbf{N'_j}\right\}\ C\ \{\mathbf{N_j}\}$; since C is a Clifford operator the coefficients of $\mathbf{M}_j$ (respectively $\mathbf{N}_j$) are the same as those of $\mathbf{M}'_j$ (respectively $\mathbf{N}'_j$) up to sign changes and reordering.

Therefore we may assume $U = T_k \circ U'$, where T_k represents a T-gate operating on the k-th qubit. For notational convenience, let us assume $k = 1$ as the general case will follow identically. As above assume $\{\mathbf{X_j}\}\ U'\ \left\{\mathbf{M'_j}\right\}$ and $\{\mathbf{Z_j}\}\ U'\ \left\{\mathbf{N'_j}\right\}$, and let us write

$$M'_j = I \otimes \left(\sum_J c_{J,0} P_{J,0}\right) + \sigma_x \otimes \left(\sum_J c_{J,1} P_{J,1}\right) + \sigma_y \otimes \left(\sum_J c_{J,2} P_{J,2}\right) + \sigma_z \otimes \left(\sum_J c_{J,0} P_{J,0}\right)$$

where each $P_{J,l}$ is a $(n-1)$-qubit Pauli operator. Inductively each coefficient satisfies $2^{(t-1)/2} c_{J,l} \in \mathbb{Z}$. Then $T_1 : \mathbf{M}'_j \to \mathbf{M}_j$ and so

$$\begin{aligned} M_j &= I \otimes \left(\sum_J c_{J,0} P_{J,0}\right) + \tfrac{1}{\sqrt{2}}(\sigma_x + \sigma_y) \otimes \left(\sum_J c_{J,1} P_{J,1}\right) \\ &+\ \tfrac{1}{\sqrt{2}}(-\sigma_x + \sigma_y) \otimes \left(\sum_J c_{J,2} P_{J,2}\right) + \sigma_z \otimes \left(\sum_J c_{J,0} P_{J,0}\right) \\ &= I \otimes \left(\sum_J c_{J,0} P_{J,0}\right) + \sigma_x \otimes \left(\sum_J \frac{c_{J,1} - c_{J,2}}{\sqrt{2}} P_{J,1}\right) \\ &+\ \sigma_y \otimes \left(\sum_J \frac{c_{J,1} + c_{J,2}}{\sqrt{2}} P_{J,2}\right) + \sigma_z \otimes \left(\sum_J c_{J,0} P_{J,0}\right). \end{aligned}$$

Finally, $2^{t/2} \cdot \frac{c_{J,1} \pm c_{J,2}}{\sqrt{2}} = 2^{(t-1)/2}(c_{J,1} \pm c_{J,2}) \in \mathbb{Z}$. The same argument works for the $\mathbf{N}_j$. □

Note that certain unitaries, those that are Hermitian and have trace zero, also define an additive predicate. This was clear for Pauli operators in the context of Pauli predicates: $\mathbf{X}$ is a predicate as well as satisfying triples $\{\mathbf{X}\}\ \sigma_x\ \{\mathbf{X}\}$ and $\{\mathbf{Z}\}\ \sigma_x\ \{-\mathbf{Z}\}$. It is straightforward to check when a unitary is also Hermitian (up to a global phase) using Hoare-style triples. A Hermitian unitary has $U = U^\dagger = U^{-1}$ and so $U^2 = I$. Thus U is Hermitian if one can show $\{\mathbf{X}_j\}\, U\, \{\mathbf{X}_j\}$ and $\{\mathbf{Z}_j\}\, U\, \{\mathbf{Z}_j\}$ for all $j = 1, \ldots, n$.

Example 22. *The Hadamard gate satisfies $\{\mathbf{X}\}\ H\ \{\mathbf{Z}\}$ and $\{\mathbf{Z}\}\ H\ \{\mathbf{X}\}$, and is also Hermitian, and so defines an additive predicate $\mathbf{H}$. It is straightforward to verify $\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z})$ by writing out H and $\frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ in the computational basis and comparing the resulting matrices. However, we can deduce this expression (again up to a global sign change) from the triples above. From the lemma above we know $H = a\sigma_x + b\sigma_y + c\sigma_z$; just using the Pauli relations*

$$\begin{aligned} H\sigma_x H &= (a^2 - b^2 - c^2)\sigma_x + 2ab\sigma_y + 2ac\sigma_z &= \sigma_z \\ H\sigma_z H &= 2ac\sigma_x + 2bc\sigma_y + (c^2 - a^2 - b^2)\sigma_z &= \sigma_x. \end{aligned}$$

And so we obtain the quadratic system

$$\begin{aligned} 0 &= a^2 - b^2 - c^2 = ab = bc \\ 1 &= 2ac = a^2 + b^2 + c^2. \end{aligned}$$

This is easy to solve by noting $1 = (a^2 + b^2 + c^2) + (a^2 - b^2 - c^2) = 2a^2$ *and so* $a = c = \pm\frac{1}{\sqrt{2}}$ *and* $b = 0$.

While a general unitary U is not Hermitian, we can construct additive predicates associated with U by adding an ancillary qubit. This is based on the real and imaginary parts of U as defined as follows.

Definition 23. *Given any operator U define its* real part *as* $\mathrm{Re}(U) = \frac{1}{2}(U + U^\dagger)$ *and* imaginary part *as* $\mathrm{Im}(U) = \frac{1}{2i}(U - U^\dagger)$.

Clearly, both $\mathrm{Re}(U)$ and $\mathrm{Im}(U)$ are Hermitian; however, neither is generally unitary. Nonetheless, we claim they do satisfy $\mathrm{Re}(U)^2 + \mathrm{Im}(U)^2 = I$ and $\mathrm{Re}(U) \cdot \mathrm{Im}(U) = \mathrm{Im}(U) \cdot \mathrm{Re}(U)$, and so look like the blocks in a 2×2 block unitary. Hence we could extend them to a unitary with an additional qubit.

Lemma 24. *Let U be unitary and $\mathrm{Re}(U), \mathrm{Im}(U)$ be as above. Let P and Q be any anticommuting Pauli operators (on any number of qubits). Then $P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U)$ is unitary, Hermitian, and trace zero.*

Proof. As $P, Q, \mathrm{Re}(U), \mathrm{Im}(U)$ are all Hermitian so is $P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U)$. Similarly, since P, Q anticommute, neither is the identity, and hence

$$\mathrm{tr}(P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U)) = \mathrm{tr}(P)\,\mathrm{tr}(\mathrm{Re}(U)) + \mathrm{tr}(Q)\,\mathrm{tr}(\mathrm{Im}(U)) = 0.$$

Finally, compute

$$\begin{aligned} &(P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U))^2 \\ &\quad = I \otimes (\mathrm{Re}(U)^2 + \mathrm{Im}(U)^2) + PQ \otimes \mathrm{Re}(U)\mathrm{Im}(U) + QP \otimes \mathrm{Im}(U)\mathrm{Re}(U). \end{aligned}$$

So, to finish, we merely complete our claims from above:

$$\mathrm{Re}(U)^2 + \mathrm{Im}(U)^2 = \frac{1}{4}(U^2 + 2I + (U^\dagger)^2) - \frac{1}{4}(U^2 - 2I + (U^\dagger)^2) = I$$

and

$$\mathrm{Re}(U)\mathrm{Im}(U) = \frac{1}{4i}(U^2 - (U^\dagger)^2) = \mathrm{Im}(U)\mathrm{Re}(U).$$

□

For example if $P = \sigma_x$ and $Q = \sigma_z$ then

$$P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U) = \begin{pmatrix} \mathrm{Im}(U) & \mathrm{Re}(U) \\ \mathrm{Re}(U) & -\mathrm{Im}(U) \end{pmatrix}.$$

Definition 25. *Let U be a n-qubit unitary, and $P, Q \in \{\sigma_x, \sigma_y, \sigma_z\}$ be distinct. Then the additive predicate of U relative to P, Q is the $(n+1)$-qubit additive predicate corresponding to $P \otimes \mathrm{Re}(U) + Q \otimes \mathrm{Im}(U)$. We denote this as $\mathbf{P} \otimes \mathbf{Re}(U) + \mathbf{Q} \otimes \mathbf{Im}(U)$ (despite that neither $\mathbf{Re}(U)$ and $\mathbf{Im}(U)$ are predicates themselves).*

7.5 Example: Triples satisfied by controlled unitaries

Consider the triples for the controlled-phase gate:

$$\begin{array}{ll} \{\mathbf{I}\otimes\mathbf{X}\}\,\texttt{control-}\sigma_z\,\{\mathbf{Z}\otimes\mathbf{X}\}, & \{\mathbf{X}\otimes\mathbf{I}\}\,\texttt{control-}\sigma_z\,\{\mathbf{X}\otimes\mathbf{Z}\}, \\ \{\mathbf{I}\otimes\mathbf{Z}\}\,\texttt{control-}\sigma_z\,\{\mathbf{I}\otimes\mathbf{Z}\}, & \{\mathbf{Z}\otimes\mathbf{I}\}\,\texttt{control-}\sigma_z\,\{\mathbf{Z}\otimes\mathbf{I}\}. \end{array}$$

Note $\{\mathbf{X}\}\,\sigma_z\,\{-\mathbf{X}\}$ and $\{\mathbf{Z}\}\,\sigma_z : \{\mathbf{Z}\}$. One is naturally led to the question: could we have deduced the appropriate postconditions of $\texttt{control-}\sigma_z$ from those of σ_z? More generally, can we deduce the triples of $\texttt{control-}U$ from the triples of U? Unfortunately, the answer must be no for a general unitary as this would imply "control-" is a functor of some sort, which is not the case. Nonetheless, we can deduce the triples of control-U from those of U *and* its additive predicate $\mathbf{X}\otimes\mathbf{Re}(U)+\mathbf{Y}\otimes\mathbf{Im}(U)$.

Consider $\texttt{control-}U$, and decompose our Hilbert space along the control bit $\mathfrak{H} = \mathfrak{H}_0 \oplus \mathfrak{H}_1$. Namely, with respect to this decomposition $\texttt{control-}U$ is the matrix operator

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

The component of our state where the control bit is $|0\rangle$ lives in $\mathfrak{H}_0$ where $\texttt{control-}U$ is trivial, but the component of the state where the control bit is $|1\rangle$ lives in $\mathfrak{H}_1$ where $\texttt{control-}U$ act as U. We use this representation to assert the judgments involving controlled operations in the following lemma.

Lemma 26. *Let U be any n-qubit unitary. Then the following triples are valid for the controlled U:*

1. $\{\mathbf{Z}\otimes\mathbf{I}\}$ *$\texttt{control-}U$* $\{\mathbf{Z}\otimes\mathbf{I}\}$, *and*
2. $\{\mathbf{X}\otimes\mathbf{I}\}$ *$\texttt{control-}U$* $\{\mathbf{X}\otimes\mathbf{Re}(U)+\mathbf{Y}\otimes\mathbf{Im}(U)\}$.

If P is any n-qubit Pauli, and $\{\mathbf{P}\}\,U\,\{\mathbf{V}\}$ then

(3) $\{\mathbf{I}\otimes\mathbf{P}\}$ *$\texttt{control-}U$* $\{\mathbf{I}\otimes\frac{1}{2}(\mathbf{P}+\mathbf{V})+\mathbf{Z}\otimes\frac{1}{2}(\mathbf{P}-\mathbf{V})\}$.

Proof. For (1), we simply note:

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}.$$

For (2), again, we compute

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} = \begin{pmatrix} 0 & U^\dagger \\ U & 0 \end{pmatrix}.$$

But now, similar to above, we compute

$$\begin{aligned} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\begin{pmatrix} 0 & U^\dagger \\ U & 0 \end{pmatrix} &= \begin{pmatrix} U & 0 \\ 0 & U^\dagger \end{pmatrix} \\ &= \left(\tfrac{1}{2}(I+\sigma_z)\otimes U + \tfrac{1}{2}(I-\sigma_z)\otimes U^\dagger\right). \end{aligned}$$

Therefore

$$\begin{pmatrix} 0 & U^\dagger \\ U & 0 \end{pmatrix} = (\sigma_x\otimes I)\left(\tfrac{1}{2}(I+\sigma_z)\otimes U + \tfrac{1}{2}(I-\sigma_z)\otimes U^\dagger\right)$$

$$
\begin{aligned}
&= (\sigma_x \otimes I)\left(I \otimes \tfrac{1}{2}(U+U^\dagger) + \sigma_z \otimes \tfrac{1}{2}(U-U^\dagger)\right)\\
&= \sigma_x \otimes \mathrm{Re}(U) + \sigma_y \otimes \mathrm{Im}(U).
\end{aligned}
$$

Finally, for (3), we compute

$$
\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix}\begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & UPU^\dagger \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & V \end{pmatrix}.
$$

In the computational basis $\frac{1}{2}(I+\sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\frac{1}{2}(I-\sigma_z) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore

$$
\begin{aligned}
\begin{pmatrix} P & 0 \\ 0 & V \end{pmatrix} &= \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & V \end{pmatrix}\\
&= \tfrac{1}{2}(I+\sigma_z)\otimes P + \tfrac{1}{2}(I-\sigma_z)\otimes V\\
&= I \otimes \tfrac{1}{2}(P+V) + \sigma_z \otimes \tfrac{1}{2}(P-V).
\end{aligned}
$$

□

Example 27. *Recall* $\{\mathbf{Z}\}\ S\ \{\mathbf{Z}\}$ *and* $\{\mathbf{X}\}\ S\ \{\mathbf{Y}\}$. *It is straightforward to verify that* $\mathrm{Re}(S) = \frac{1}{2}(I+\sigma_z)$ *and* $\mathrm{Im}(S) = \frac{1}{2}(I-\sigma_z)$. *Thus, we have*

$$
\begin{aligned}
&\{\mathbf{Z}\otimes\mathbf{I}\}\ \texttt{control-}S\ \{\mathbf{Z}\otimes\mathbf{I}\}\\
&\{\mathbf{X}\otimes\mathbf{I}\}\ \texttt{control-}S\ \left\{\left(\mathbf{X}\otimes\tfrac{1}{2}(\mathbf{I}+\mathbf{Z})\right) + \left(\mathbf{Y}\otimes\tfrac{1}{2}(\mathbf{I}-\mathbf{Z})\right)\right\}\\
&\qquad\qquad\qquad\quad \rightsquigarrow \left\{\left(\tfrac{1}{2}(\mathbf{X}+\mathbf{Y})\otimes\mathbf{I}\right) + \left(\tfrac{1}{2}(\mathbf{X}-\mathbf{Y})\otimes\mathbf{Z}\right)\right\}\\
&\{\mathbf{I}\otimes\mathbf{Z}\}\ \texttt{control-}S\ \{\mathbf{I}\otimes\mathbf{Z}\}\\
&\{\mathbf{I}\otimes\mathbf{X}\}\ \texttt{control-}S\ \left\{\left(\mathbf{I}\otimes\tfrac{1}{2}(\mathbf{X}+\mathbf{Y})\right) + \left(\mathbf{Z}\otimes\tfrac{1}{2}(\mathbf{X}-\mathbf{Y})\right)\right\}.
\end{aligned}
$$

Note that by Theorem 21, any unitary Clifford+T circuit that synthesizes `control-`*S requires at least 2 T-gates.*

Theorem 28. *Let U be a n-qubit Hermitian unitary with trace zero, and let* $\mathbf{U}$ *be its associated additive predicate. Then for each $k \geq 0$, we have* $\texttt{control}^k\texttt{-}U$ *is also a Hermitian unitary of trace zero, and its associated additive predicate is given by*

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

Proof. As above, we write the operator relation

$$
\begin{aligned}
\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} &= \tfrac{1}{2}(I+\sigma_z)\otimes I + \tfrac{1}{2}(I-\sigma_z)\otimes U\\
&= I\otimes\tfrac{1}{2}(I+U) + \sigma_z\otimes\tfrac{1}{2}(I-U).
\end{aligned}
$$

Now we can prove the theorem by induction. Clearly, the $k = 0$ case holds:

$$
\mathbf{U} = \mathbf{C}^0\mathbf{U} \rightsquigarrow \mathbf{I}^n - (\mathbf{I}^n - \mathbf{U}).
$$

Inductively suppose $\mathbf{C}^k\mathbf{U} = \mathbf{I}^{(k+n)} - \frac{1}{2^k}(\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{I}^n - \mathbf{U})$ then using the relation above

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

$$\begin{aligned}&\rightsquigarrow \mathbf{I} \otimes \tfrac{1}{2}(\mathbf{I}^{(k+n)} + \mathbf{I}^{(k+n)} - \tfrac{1}{2^k}(\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{I}^n - \mathbf{U}))\\ &\quad + \mathbf{Z} \otimes \tfrac{1}{2}(\mathbf{I}^{(k+n)} - \mathbf{I}^{(k+n)} + \tfrac{1}{2^k}(\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{I}^n - \mathbf{U}))\\ &\rightsquigarrow \mathbf{I}^{(k+1+n)} - \tfrac{1}{2^{k+1}}\mathbf{I} \otimes (\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{I}^n - \mathbf{U})\\ &\quad + \tfrac{1}{2^{k+1}}\mathbf{Z} \otimes (\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{I}^n - \mathbf{U})\\ &\rightsquigarrow \mathbf{I}^{(k+1+n)} - \tfrac{1}{2^{k+1}}(\mathbf{I}-\mathbf{Z})^{(k+1)} \otimes (\mathbf{I}^n - \mathbf{U})).\end{aligned}$$

□

Corollary 29. $\mathbf{C}^{k-1}\mathbf{Z} = \mathbf{I}^k - \frac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^k$.

As a simple example of the utility of the above formulation, we can easily derive a complete set of triples for an arbitrarily multiply controlled Z operator as follows.

Theorem 30. *We have*

$$\begin{aligned}&\{\mathbf{Z}_j\}\ \texttt{control}^k\text{-}\sigma_z\ \{\mathbf{Z}_j\}\\ &\{\mathbf{X}_j\}\ \texttt{control}^k\text{-}\sigma_z\ \left\{\mathbf{X}_j - \frac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^{j-1} \otimes \mathbf{X} \otimes (\mathbf{I}-\mathbf{Z})^{(k+1-j)}\right\}.\end{aligned}$$

Proof. As $\texttt{control}^k$-σ_z is symmetric, it suffices to prove these statements for $j = 1$. For the first, we already have

$$\{\mathbf{Z} \otimes \mathbf{I}^k\}\texttt{control}-(\texttt{control}^{k-1}\text{-}\sigma_z)\ \{\mathbf{Z} \otimes \mathbf{I}^k\}$$

from (1) of Lemma 26. Now from Lemma 26 part (2), and that $\texttt{control}^{k-1}$-σ_z is Hermitian, we have

$$\{\mathbf{X} \otimes \mathbf{I}^k\}\ \texttt{control}-(\texttt{control}^{k-1}\text{-}\sigma_z)\ \{\mathbf{X} \otimes \mathbf{C}^{k-1}\mathbf{Z}\}.$$

Then the result follows from the previous corollary. □

Corollary 31. *Any unitary Clifford+T circuit that synthesizes* $\texttt{control}^k$-σ_z *contains at least* $(2k-2)$ *T-gates.*

Note that this corollary does not provide a sharp bound. For example, Gosset et al. [12] provide an algorithm that explicitly computes the optimal T-count of the Toffoli gate to be seven. However, our bound only provides the lower bound of two.

Lemma 32. *For any unitary U we have*

1. $\mathrm{Re}(\texttt{control}^k\text{-}U) = \texttt{control}^k\text{-}(\mathrm{Re}(U))$, *and*
2. $\mathrm{Im}(\texttt{control}^k\text{-}U) = \frac{1}{2^k}(I-\sigma_z)^k \otimes \mathrm{Im}(U)$.

Proof. Note that

$$\frac{1}{2}\left[\begin{pmatrix} I & 0\\ 0 & U\end{pmatrix} + \begin{pmatrix} I & 0\\ 0 & U^\dagger\end{pmatrix}\right] = \begin{pmatrix} I & 0\\ 0 & \frac{1}{2}(U+U^\dagger)\end{pmatrix}$$

and so $\mathrm{Re}(\texttt{control-}U) = \texttt{control-}(\mathrm{Re}(U))$. Then (1) follows from straightforward recursion.

Similarly,

$$\frac{1}{2i}\left[\begin{pmatrix} I & 0\\ 0 & U\end{pmatrix} - \begin{pmatrix} I & 0\\ 0 & U^\dagger\end{pmatrix}\right] = \begin{pmatrix} 0 & 0\\ 0 & \frac{1}{2i}(U-U^\dagger)\end{pmatrix} = \tfrac{1}{2}(I-\sigma_z) \otimes \mathrm{Im}(U).$$

Therefore (2) also follows from recursion. □

Theorem 33. *Let U be any n-qubit unitary, and $k > 0$. Then for $j = 1, \ldots, k$, we have*

$$\begin{aligned}
&\{\mathbf{Z}_j\}\ \mathit{control}^k\text{-}U\ \{\mathbf{Z}_j\}, \text{ and} \\
&\{\mathbf{X}_j\}\ \mathit{control}^k\text{-}U\ \Big\{\mathbf{X}_j - \frac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^{j-1} \otimes \mathbf{X} \otimes (\mathbf{I}-\mathbf{Z})^{(k-j)} \otimes \mathbf{I}^n \\
&\qquad + \frac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^{j-1} \otimes \mathbf{X} \otimes (\mathbf{I}-\mathbf{Z})^{(k-j)} \otimes \mathbf{Re}(U) \\
&\qquad + \frac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^{j-1} \otimes \mathbf{Y} \otimes (\mathbf{I}-\mathbf{Z})^{(k-j)} \otimes \mathbf{Im}(U)\Big\}.
\end{aligned}$$

Moreover, for any n-qubit Pauli P with $\{\mathbf{P}\}\ U\ \{\mathbf{V}\}$ then

$$\{\mathbf{I}^k \otimes \mathbf{P}\}\ \mathit{control}^k\text{-}U\ \Big\{\mathbf{I}^k \otimes \mathbf{P} - \tfrac{1}{2^k}(\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{P}-\mathbf{V})\Big\}.$$

Proof. Clearly (1) follows immediately from Lemma 26 part (1).

For (2), we will assume $j = 1$ for clarity as the general case follows identically. From Lemma 26 part (2) we have

$$\begin{aligned}
&\{\mathbf{X} \otimes \mathbf{I}^{(k+n-1)}\} \\
&\texttt{control-(control}^{k-1}\texttt{-}U) \\
&\{\mathbf{X} \otimes \mathbf{Re}(\texttt{control}^{k-1}\texttt{-}U) + \mathbf{Y} \otimes \mathbf{Im}(\texttt{control}^{k-1}\texttt{-}U)\}.
\end{aligned}$$

From part (1) of the previous lemma we have $\mathrm{Re}(\texttt{control}^{k-1}\texttt{-}U) = \texttt{control}^{k-1}\texttt{-}(\mathrm{Re}(U))$, and so from Theorem 28

$$\mathrm{Re}(\texttt{control}^{k-1}\texttt{-}U) = I^{k+n-1} - \frac{1}{2^{k-1}}(I - \sigma_z)^{(k-1)}(I^n - \mathrm{Re}(U)).$$

Part (2) of the that lemma simply gives $\mathrm{Im}(\texttt{control}^{k-1}\texttt{-}U) = \frac{1}{2^{k-1}}(I - \sigma_z)^{(k-1)} \otimes \mathrm{Im}(U)$. Substituting these into the formula above gives the desired results.

We prove (3) inductively. For $k = 1$, Lemma 26 part (3) gives

$$\begin{aligned}
\{\mathbf{I} \otimes \mathbf{P}\}\ \texttt{control-}U\ &\{\mathbf{I} \otimes \tfrac{1}{2}(\mathbf{P}+\mathbf{V}) + \mathbf{Z} \otimes \tfrac{1}{2}(\mathbf{P}-\mathbf{V})\} \\
\rightsquigarrow\ &\{\tfrac{1}{2}\mathbf{I} \otimes \mathbf{P} + \tfrac{1}{2}\mathbf{I} \otimes \mathbf{V} + \tfrac{1}{2}\mathbf{Z} \otimes \mathbf{P} - \tfrac{1}{2}\mathbf{Z} \otimes \mathbf{V}\} \\
\rightsquigarrow\ &\{\mathbf{I} \otimes \mathbf{P} - \tfrac{1}{2}(\mathbf{I}-\mathbf{Z}) \otimes (\mathbf{P}-\mathbf{V})\}.
\end{aligned}$$

Now suppose the formula above holds for $k - 1$. Then from the typing statement we just derived,

$$\begin{aligned}
&\{\mathbf{I}^{(k-1)} \otimes (\mathbf{I} \otimes \mathbf{P})\} \\
&\texttt{control}^{k-1}\texttt{-(control-}U) \\
&\Big\{\mathbf{I}^{(k-1)} \otimes (\mathbf{I} \otimes \mathbf{P}) - \tfrac{1}{2^{k-1}}(\mathbf{I}-\mathbf{Z})^{(k-1)} \otimes \Big[(\mathbf{I} \otimes \mathbf{P}) - \Big((\mathbf{I} \otimes \mathbf{P}) - \tfrac{1}{2}(\mathbf{I}-\mathbf{Z}) \otimes (\mathbf{P}-\mathbf{V})\Big)\Big]\Big\} \\
&\quad \rightsquigarrow\ \{\mathbf{I}^k \otimes \mathbf{P} - \tfrac{1}{2^k}(\mathbf{I}-\mathbf{Z})^k \otimes (\mathbf{P}-\mathbf{V})\}.
\end{aligned}$$

□

8 Measurement for additive predicates

One missing component of additive predicates is the derivation of normal forms. As a consequence, a full formalism for measurement is incomplete. Nonetheless, we can go some distance in characterizing post-measurement conditions using the projection semantics introduced in the introduction.

8.1 Projection Semantics

Recall that our core interpretation of the predicate $\mathbf{X}$ is $\mathbf{X}(\psi)$ if and only if $\sigma_x\psi = \psi$ (that is, $|\psi\rangle = |+\rangle$ up to normalization). However, to derive postconditions of measurements in general, we need an interpretation where we associate a predicate to a projection operator, and a state satisfies the predicate precisely when it is in the image of the associated projection operator. We could interpret this as a type of semantics, where our predicates are evaluated to projections

$$[\![\mathbf{X}]\!] = |+\rangle\!\langle+| \,, \ [\![\mathbf{Y}]\!] = |i\rangle\!\langle i| \,, \text{ and } [\![\mathbf{Z}]\!] = |0\rangle\!\langle 0| \,.$$

This clarifies the behavior of negation as, for instance,

$$[\![-\mathbf{Z}]\!] = I - [\![\mathbf{Z}]\!] = I - |0\rangle\!\langle 0| = |0\rangle\!\langle 0|^{\perp} = |1\rangle\!\langle 1| \,.$$

Indeed, the negation of a predicate should behave like the orthogonal complement on the lattice of projections.

For any (multi-qubit) Pauli operator P, the projection onto its $+1$-eigenspace is precisely $\Pi_P^+ = \frac{1}{2}(I+P)$. Similarly, the projection onto its -1-eigenspace is $\Pi_P^- = \frac{1}{2}(I-P)$, illustrating the relationship between operator negation in one interpretation versus orthogonal complement in the other.

8.2 Computing post-measurement states

When studying Pauli operators, we were able to exploit standard methods from the stabilizer formalism for treating measurements in Pauli bases. However, these techniques no longer apply for general unitary Hermitian operators, even those of trace zero. Hence we need to revisit measurement from the first principles.

First, consider the problem of measuring a single qubit in the z-basis. Post measurement, we know the state would satisfy the predicate $\mathbf{Z} \uplus -\mathbf{Z}$ where the factor in this union depends on the measurement outcome. Although it is outside our logical formalism, we see the probability of these outcomes directly in any preconditions of measurement the qubit may satisfy.

Lemma 34. *Let $\mathbf{M} = a\mathbf{X} + b\mathbf{Y} + c\mathbf{Z}$ be an additive predicate and $\mathbf{M}(|\psi\rangle)$. Then in the z-basis,*

$$\Pr_\psi\{\mathit{meas} = +1\} = \frac{1+c}{2}, \ \mathit{and} \Pr_\psi\{\mathit{meas} = -1\} = \frac{1-c}{2}.$$

Proof. We have $\mathbf{M}(|\psi\rangle)$ when $|\psi\rangle$ is the $+1$-eigenvector of the operator $M = a\sigma_x + b\sigma_y + c\sigma_z$. As $|\psi\rangle\!\langle\psi|$ is the projector onto the $+1$-eigenspace of M, and $I - |\psi\rangle\!\langle\psi|$ is the projector onto the -1-eigenspace, we must have

$$M = |\psi\rangle\!\langle\psi| - (I - |\psi\rangle\!\langle\psi|) = 2\,|\psi\rangle\!\langle\psi| - I.$$

Let Π^Z be the projector onto the $+1$-eigenspace of Z (that is $\Pi^Z = |0\rangle\!\langle 0|$). Born's rule has

$$\begin{aligned}\Pr_\psi\{\text{meas} = +1\} &= \operatorname{tr}\Big(\Pi^Z\,|\psi\rangle\!\langle\psi|\Big) = \tfrac{1}{2}\operatorname{tr}\Big(\Pi^Z(I+M)\Big) \\ &= \frac{1}{2}\Big(1 + a\operatorname{tr}\Big(\Pi^Z X\Big) + b\operatorname{tr}\Big(\Pi^Z Y\Big) + c\operatorname{tr}\Big(\Pi^Z Z\Big)\Big) = \frac{1+c}{2}.\end{aligned}$$

Similarly, $\Pr_\psi\{\text{meas} = -1\} = \frac{1-c}{2}$ follows. □

A similar fact holds in the multi-qubit case; however, it is significantly more challenging to derive. Let us illustrate the key ideas on 2 qubits. Suppose $(\mathbf{M}_{(1)} \cap \mathbf{M}_{(2)})(|\psi\rangle)$ where $\mathbf{M}_{(1)}, \mathbf{M}_{(2)}$ are 2-qubit additive predicates. Let M_1 and M_2 be the unitary Hermitian operators associated with these. The assertion that $|\psi\rangle$ is the joint $+1$-eigenvector of M_1 and M_2 implies $M_1 M_2 = M_2 M_1$. As above, we have $|\psi\rangle\langle\psi|$ as the projector onto this space, and thus

$$|\psi\rangle\langle\psi| = \tfrac{1}{4}(I + M_1)(I + M_2) = \tfrac{1}{4}(I + M_1 + M_2 + M_1 M_2).$$

For convenience, let us write $M_0 = I$ and $M_3 = M_1 M_2$. Suppose we measure the first qubit in the z-basis. As in the lemma above, the measurement projector is $\Pi^Z \otimes I$ and Born's rule reads

$$\Pr_\psi\{\text{meas} = +1\} = \operatorname{tr}\Big((\Pi^Z \otimes I)\, |\psi\rangle\langle\psi|\Big) = \frac{1}{4}\sum_{j=0}^{3} \operatorname{tr}\Big((\Pi^Z \otimes I) M_j\Big).$$

To compute these traces, we write

$$M_j = I \otimes N_{j0} + X \otimes N_{j1} + Y \otimes N_{j2} + Z \otimes N_{j3},$$

and so

$$\begin{aligned}\operatorname{tr}\Big((\Pi^Z \otimes I) M_j\Big) &= \operatorname{tr}\Big(\Pi^Z \otimes N_{j0}\Big) + \operatorname{tr}\Big(\Pi^Z X \otimes N_{j1}\Big) + \operatorname{tr}\Big(\Pi^Z Y \otimes N_{j2}\Big) + \operatorname{tr}\Big(\Pi^Z Z \otimes N_{j3}\Big)\\ &= \operatorname{tr}(N_{j0}) + \operatorname{tr}(N_{j3}).\end{aligned}$$

Now, $M_0 = I$, and for $j > 0$ we have M_j is trace zero. Thus we may write

$$N_{00} = I \text{ and } N_{01} = N_{02} = N_{03} = 0,$$

and for $j > 0$:

$$\begin{aligned} N_{j0} &= \phantom{c_j I +{}} \tilde{x}_j X + \tilde{y}_j Y + \tilde{z}_j Z \\ N_{j3} &= c_j I + x_j X + y_j Y + z_j Z. \end{aligned} \tag{18}$$

So,

$$\begin{aligned}\Pr_\psi\{\text{meas} = +1\} &= \tfrac{1}{4}(2 + \operatorname{tr}(N_{13}) + \operatorname{tr}(N_{23}) + \operatorname{tr}(N_{33}))\\ &= \frac{1 + c_1 + c_2 + c_3}{2}\end{aligned}$$

where we extract each c_j as:

$$M_j = c_j Z \otimes I + \text{other terms}. \tag{19}$$

For c_1 and c_2 this is by direct examination of $\mathbf{M}_{(1)}$ and $\mathbf{M}_{(2)}$. However c_3 can only be obtained by computing $M_1 M_2$. A similar computation holds for the probability of measuring -1, and so we have proven the following result.

Proposition 35. *Suppose $(\mathbf{M}_{(1)} \cap \mathbf{M}_{(2)})(|\psi\rangle)$ where $\mathbf{M}_{(1)}, \mathbf{M}_{(2)}$ are 2-qubit additive predicates, and suppose we measure the first qubit in the z-basis. As above write M_1 and M_2 for the operators associated to these predicates and $M_0 = I$ and $M_3 = M_1 M_2$. For $j = 0, 1, 2, 3$ define*

$$M_j = I \otimes N_{j0} + X \otimes N_{j1} + Y \otimes N_{j2} + Z \otimes N_{j3}.$$

Then

$$\Pr_\psi\{\mathit{meas} = +1\} = p_+ = \frac{1 + c_1 + c_2 + c_3}{2}$$

and

$$\Pr_\psi\{meas = -1\} = p_- = \frac{1 - c_1 - c_2 - c_3}{2}$$

where the c_j are given in (19).

From this, we can bootstrap the full post-measurement predicates for a general 2-qubit state as follows.

Theorem 36. *On 2-qubit states, measurement in the z-basis satisfies*

$$\{\mathbf{M}_{(1)} \cap \mathbf{M}_{(2)}\}\ meas_1\ \{(\mathbf{Z}_1 \cap \mathbf{M}_+) \uplus ((-\mathbf{Z})_1 \cap \mathbf{M}_-)\}$$

where

$$\mathbf{M}_+ = \tfrac{1}{2p_+} \sum_{j=1}^{3} ((\tilde{x}_j + x_j)\mathbf{X} + (\tilde{y}_j + y_j)\mathbf{Y} + (\tilde{z}_j + z_j)\mathbf{Z}) \tag{20}$$

$$\mathbf{M}_- = \tfrac{1}{2p_-} \sum_{j=1}^{3} ((\tilde{x}_j - x_j)\mathbf{X} + (\tilde{y}_j - y_j)\mathbf{Y} + (\tilde{z}_j - z_j)\mathbf{Z}), \tag{21}$$

where $p_\pm$ are given in the proposition above, and the coefficients of $\mathbf{M}_\pm$ are in (18).

Proof. As above, write $p_+ = \frac{1+c_1+c_2+c_3}{2}$ for seeing outcome $+1$, then the post-measurement state given outcome $+1$ is

$$\begin{aligned}
\tfrac{1}{p_+}(\Pi^Z \otimes I) |\psi\rangle \langle\psi| (\Pi^Z \otimes I) &= \frac{1}{4p_+} \sum_{j=0}^{3} \Big((\Pi^Z \otimes I) M_j (\Pi^Z \otimes I)\Big) \\
&= \frac{1}{4p_+} \sum_{j=0}^{3} \Big(\Pi^Z \otimes N_{j0} + (\Pi^Z X \Pi^Z) \otimes N_{j1} + (\Pi^Z Y \Pi^Z) \otimes N_{j2} + \Pi^Z \otimes N_{j3}\Big) \\
&= \Pi^Z \otimes \frac{1}{4p_+} \left(I + \sum_{j=1}^{3} (N_{j0} + N_{j3})\right) \\
&= \Pi^Z \otimes \left(\tfrac{1}{2} I + \tfrac{1}{4p_+} \sum_{j=1}^{3} ((\tilde{x}_j + x_j)X + (\tilde{y}_j + y_j)Y + (\tilde{z}_j + z_j)Z)\right).
\end{aligned}$$

While we wrote this as a density operator, it is a pure state

$$\tfrac{1}{p_+}(\Pi^Z \otimes I) |\psi\rangle \langle\psi| (\Pi^Z \otimes I) = |0, \psi'\rangle\langle 0, \psi'|.$$

As above $|\psi'\rangle\langle\psi'| = \frac{1}{2}(I + M_+)$ so by examination the post-measurement state satisfies $\mathbf{Z}_1 \cap (\mathbf{M}_+)_2$.

For seeing outcome -1, which has probability $p_- = \frac{1-c_1-c_2-c_3}{2}$, the computation is similar:

$$\begin{aligned}
\tfrac{1}{p_-}((I - \Pi^Z) \otimes I) |\psi\rangle \langle\psi| ((I - \Pi^Z) \otimes I) &= (I - \Pi^Z) \otimes \frac{1}{4p_-} \left(I + \sum_{j=1}^{3} (N_{j0} - N_{j3})\right) \\
&= \Pi^Z \otimes \left(\tfrac{1}{2} I + \tfrac{1}{4p_-} \sum_{j=1}^{3} ((\tilde{x}_j - x_j)X + (\tilde{y}_j - y_j)Y + (\tilde{z}_j - z_j)Z)\right).
\end{aligned}$$

So the post-measurement state satisfies $(-\mathbf{Z})_1 \cap (\mathbf{M}_-)_2$ □

Example 37. *Note that in the case that $\mathbf{M}_{(1)}$ and $\mathbf{M}_{(2)}$ are derived from Pauli operators, the Proposition above recovers our measurement rules from earlier. Each additive predicate only contains one Pauli term. From (19) we see that at most one c_j can be nonzero, as otherwise two of M_1, M_2, and M_3 would equal $Z \otimes I$ contradicting independence of $\mathbf{M}_{(1)}$ and $\mathbf{M}_{(2)}$. In the case where one $c_j = \pm 1$ the measurement is deterministic (with outcome equal to this c_j) and the input state is separable. So suppose this is not the case, and the measurement is uniformly random. One of M_1, M_2, and M_3 must be of the form $\pm X \otimes P$ for some Pauli, as otherwise, one would be $Z \otimes I$ since they are independent and pairwise commuting. Without loss of generality suppose $M_1 = s_1 X \otimes P$, where $s_1 \in \{-1, +1\}$. As $M_3 = M_1 M_2$ one of M_2 or M_3 has of the form*

1. *$\pm I \otimes Q$ where Q commutes with P, or*
2. *$\pm Z \otimes Q$ where Q anti-commutes with P.*

Again without loss of generality, we can assume M_2 takes one of these forms. Therefore either:

1. *$M_2 = s_2 I \otimes Q$ and $M_3 = s_1 s_2 X \otimes Q$, and so in (18) the only nonvanishing coefficient is one of $\tilde{x}_2$, $\tilde{y}_2$, or $\tilde{z}_2$ (according to Q) and we obtain the postcondition $\mathbf{M}_+ = \mathbf{M}_- = s_2 \mathbf{Q}$; or,*
2. *$M_2 = s_2 Z \otimes Q$ and $M_3 = -s_1 s_2 Y \otimes iPQ$, and so in (18) the only nonvanishing coefficient is one of x_j, y_j, or z_k (again according to Q) and we have postcondtions $\mathbf{M}_+ = s_2 \mathbf{Q}$ and $\mathbf{M}_- = -s_2 \mathbf{Q}$.*

Example 38. *If we have a single T-gate, what other sort of gates can we synthesize using it, Clifford gates, and measurement in the computational basis? We will focus only on synthesizing another one-qubit gate using a single ancillary qubit that will be measured, and so this example parallels gate injection, which we will study in the next section. By Proposition 17, prior to measurement, we can assume our state $|\psi\rangle$ satisfies a predicate of the form*

$$\tfrac{1}{\sqrt{2}}(\mathbf{P}_{(0)} + \mathbf{P}_{(1)}) \cap \mathbf{P}_{(2)}$$

where the 2-qubit Pauli operators P_0 and P_1 anticommute, and P_2 commutes with both P_0 and P_1. Without loss of generality, we can assume the first qubit is measured in the z-basis. Using the notation above $M_1 = \frac{1}{\sqrt{2}}(P_0 + P_1)$, $M_2 = P_2$, and $M_3 = \frac{1}{\sqrt{2}}(P_0 P_2 + P_1 P_2)$. As in the previous example, we focus on cases involving $\mathbf{Z} \otimes \mathbf{I}$.

Case 1: $\mathbf{P}_{(2)} = \pm \mathbf{Z} \otimes \mathbf{I}$ *In the notation above, $c_1 = c_3 = 0$ while $c_2 = \pm 1$, and hence the probability of measuring $Z = +1$ is 0 or 1 depending on the sign in $\mathbf{P}_{(2)}$. Specializing (18) to this case, we must have*

$$M_1 = \tfrac{1}{\sqrt{2}} \mathbf{I} \otimes (\tilde{x}\mathbf{X} + \tilde{y}\mathbf{Y} + \tilde{z}\mathbf{Z}) + \tfrac{1}{\sqrt{2}} \mathbf{Z} \otimes (x\mathbf{X} + y\mathbf{Y} + z\mathbf{Z})$$
$$M_3 = \pm(\tfrac{1}{\sqrt{2}} \mathbf{I} \otimes (x\mathbf{X} + y\mathbf{Y} + z\mathbf{Z}) + \tfrac{1}{\sqrt{2}} \mathbf{Z} \otimes (\tilde{x}\mathbf{X} + \tilde{y}\mathbf{Y} + \tilde{z}\mathbf{Z}))$$

Hence post measurement, our state satisfies

$$\mathbf{M}'_\pm = \pm \tfrac{1}{\sqrt{2}}((\tilde{x} \pm x)\mathbf{X} + (\tilde{y} \pm y)\mathbf{Y} + (\tilde{z} \pm z)\mathbf{Z}).$$

As P_0 and P_1 anticommute, precisely one of x, y, z is nonzero and precisely one of $\tilde{x}, \tilde{y}, \tilde{z}$ is nonzero, and these cannot both be $x, \tilde{x}$ or $y, \tilde{y}$ or $z, \tilde{z}$. So by Proposition 17, this circuit is equivalent to one that uses Clifford plus one T-gate (without measurement).

Case 2: $\mathbf{P}_{(0)} = \pm\mathbf{Z}\otimes\mathbf{I}$ *Note this case also covers when P_1, P_0P_2, or P_1P_2 is $\pm\sigma_z\otimes I$, after relabeling terms as needed. As P_0 and P_1 anticommute we must have $P_1 = \pm\sigma_x\otimes Q$ or $P_1 = \pm\sigma_y\otimes Q$ for some Pauli operator Q (that may be I). Hence M_1 does not contribute to a post-measurement predicate. Yet, P_2 must commute with both P_0 and P_1, and hence $P_2 = I\otimes Q'$ where $Q'\in\{\sigma_x,\sigma_y,\sigma_z\}$. But then M_3 will not contribute to a post-measurement predicate either, and hence $\mathbf{M}'_\pm = \mathbf{P}_{(2)}$ and the circuit is equivalent to a Clifford gate.*

Case 3: None of $\mathbf{P}_{(0)}, \mathbf{P}_{(1)}, \mathbf{P}_{(2)}$ is $\pm\mathbf{Z}\otimes\mathbf{I}$ *This case is somewhat tedious, and so we let the reader verify the details. Regardless, the measurement has probability $\frac{1}{2}$ of obtaining $z=+1$ or $z=-1$. In the subcase where $P_2 = \sigma_x\otimes Q$ or $P_2 = \sigma_y\otimes Q$, then the result is similar to Case 1 above in that between M_1 and M_3 precisely two of $x, y, z, \tilde{x}, \tilde{y}, \tilde{z}$ contribute to the output predicate, and so the circuit is equivalent to a Clifford with one T-gate circuit (without measurement). In the subcase $P_2 = I\otimes Q$, then the result is similar to Case 2 above in that the state is separable, and hence the post-measurement predicate is Q, and the circuit is equivalent to a Clifford gate. Finally in the subcase $P_2 = \sigma_z\otimes Q$, we must have $M_1 = \sigma_x\otimes N_1 + \sigma_y\otimes N_2$ (as otherwise either M_1 or M_3 would have a $\sigma_z\otimes I$ term); then just as above neither M_1 or M_3 contribute a post-measurement predicate, which is Q, and so the circuit is equivalent to a Clifford gate.*

The n-qubit analysis follows in a similar way as with two qubits; however, we do not have such a concrete result. Suppose $(\mathbf{M}_{(1)}\cap\cdots\cap\mathbf{M}_{(n)})(|\psi\rangle)$. Continuing our notation from above, let M_j be the unitary Hermitian operator associated with $\mathbf{M}_{(j)}$. Then

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\prod_{j=1}^{n}(I+M_j) = \frac{1}{2^n}\sum_{J\subseteq\{1,\cdots,n\}} M_J$$

where the "multi-index" J selects a subset of $\{1,\cdots,n\}$ over which $M_J = \prod_{j\in J} M_j$. Here we adopt the convention $M_\emptyset = I$ similar to $M_0 = I$ in the 2-qubit case. Then Born's rule for measuring the first qubit reads

$$\Pr\{\text{meas} = +1\} = \frac{1}{2^n}\sum_{J\subseteq\{1,\ldots,n\}} \operatorname{tr}\left((\Pi^Z\otimes I^{(n-1)})M_J\right).$$

Again we write

$$M_J = I\otimes N_{J0} + X\otimes N_{J1} + Y\otimes N_{J2} + Z\otimes N_{J3}$$

and just as in the 2-qubit case, have

$$\operatorname{tr}\left((\Pi^Z\otimes I^{(n-1)})M_J\right) = \operatorname{tr}(N_{J0}+N_{J3}).$$

Now, $N_{\emptyset 0} = I$ and $N_{\emptyset K} = 0$. For $J\neq\emptyset$, we expand

$$N_{J0} = \sum_{K\neq\mathbf{0}} q_{JK}P_K \text{ and } N_{J3} = c_J I^{(n-1)} + \sum_{K\neq\mathbf{0}} r_{JK}P_K,$$

where here $K\in\{0,1,2,3\}^{n-1}$ and for $K=(k_1,\ldots,k_{n-1})$ we write $P_K = P_{k_1}\otimes\cdots\otimes P_{k_{n-1}}$. Then for measuring the first qubit to be state $+1$, we have

$$p_+ = \Pr\{\text{meas} = +1\} = \frac{1}{2}\left(1+\frac{1}{2^{n-1}}\sum_{J\neq\emptyset} c_J\right)$$

and the post-measurement state will be

$$\begin{aligned}&\tfrac{1}{p_+}(\Pi^Z \otimes I^{(n-1)})\,|\psi\rangle\,\langle\psi|\,(\Pi^Z \otimes I^{(n-1)})\\ &= \ \Pi^Z \otimes \frac{1}{2^{n-1}}\left(I^{(n-1)} + \frac{1}{2p_+}\sum_{J\neq\emptyset}\sum_{K\neq\mathbf{0}}(q_{JK}+r_{JK})P_K\right).\end{aligned}$$

Now, however, we face a challenge. The post-measurement state is a pure state $|\psi'\rangle$ and

$$|\psi'\rangle\!\langle\psi'| = \frac{1}{2^{n-1}}\left(I^{(n-1)} + \frac{1}{2p_+}\sum_{J\neq\emptyset}\sum_{K\neq\mathbf{0}}(q_{JK}+r_{JK})P_K\right). \tag{22}$$

But to find the predicates it satisfies, we need to find $(n-1)$-qubit additive predicates $\mathbf{M}'_1,\ldots,\mathbf{M}'_{n-1}$ such that the associated operators satisfy

$$\prod_{j=1}^{n-1}(I^{(n-1)} + M'_j) = I^{(n-1)} + \frac{1}{2p_+}\sum_{J\neq\emptyset}\sum_{K\neq\mathbf{0}}(q_{JK}+r_{JK})P_K.$$

While this does not seem immediately tractable, we can prove a lemma that shows that one feature of measurement from Pauli predicates carries over to general additive predicates: if a term in the intersection involves only I and Z in the measured qubit, then it becomes a term in the post-measurement predicate (possibly with a different sign).

Lemma 39. *Suppose $M = I\otimes N_0 + Z\otimes N_3$. Then*

- $(\Pi^Z \otimes I^{(n-1)})M = (\Pi^Z\otimes(N_0+N_3))(\Pi^Z\otimes I^{(n-1)})$*, and*
- $((I-\Pi^Z)\otimes I^{(n-1)})M = ((I-\Pi^Z)\otimes(N_0-N_3))((I-\Pi^Z)\otimes I^{(n-1)})$*.*

Proof. Direct computation. □

To apply this lemma, without loss of generality suppose $(\mathbf{M}_{(1)}\cap\cdots\cap\mathbf{M}_{(n)})(|\psi\rangle)$ with $M_1 = I\otimes N_{1,0} + Z\otimes N_{1,3}$, and suppose the first qubit is measured (in the z-basis) with outcome $+1$. Then the post-measurement state is

$$\begin{aligned}&\tfrac{1}{p_+}(\Pi^Z \otimes I^{(n-1)})\,|\psi\rangle\,\langle\psi|\,(\Pi^Z \otimes I^{(n-1)})\\ &= \ \tfrac{1}{2^n p_+}(\Pi^Z \otimes I^{(n-1)})\cdot\prod_{j=1}^{n}(I^n + M_j)\cdot(\Pi^Z \otimes I^{(n-1)})\\ &= \ \tfrac{1}{2}(\Pi^Z\otimes(I^{(n-1)}+N_{1,0}+N_{1,3}))\cdot\tfrac{1}{2^{n-1}p_+}(\Pi^Z \otimes I^{(n-1)})\cdot\prod_{j=2}^{n}(I^n + M_j)\cdot(\Pi^Z \otimes I^{(n-1)}).\end{aligned}$$

Hence the output state has $\mathbf{M}'_{(1)}(|0,\psi'\rangle)$ where $M'_1 = N_{1,0}+N_{1,3}$ (up to a normalization term contained in p_+). The second conclusion in the lemma handles the case for outcome -1, where the post-measurement state has $\mathbf{M}'_{(1)}(|1,\psi'\rangle)$ where $M'_1 = N_{1,0}-N_{1,3}$ (again up to normalization).

8.3 Application: Gate Injection

A standard approach to fault-tolerant universal quantum computation is through implementing non-Clifford gates on codes through gate injection using associated "magic" states. While we can be explicit about the structure of the unitary gate we wish to inject, let us

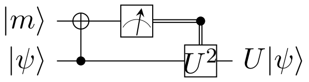

Figure 3: Gate injection circuit for U.

see what we can prove by simply appealing to Hoare-style judgments. For concreteness, we focus on single-qubit unitaries and assume the two judgments

$$\{\mathbf{X}\}\ U\ \{\mathbf{M}\} \text{ and } \{\mathbf{Z}\}\ U\ \{\mathbf{Z}\}. \tag{23}$$

The additive predicate $\mathbf{M}$ cannot be arbitrary. These assumptions imply $U\sigma_z U^\dagger = \sigma_z$ and $U\sigma_x U^\dagger = M$. Since σ_x and σ_z anti-commute, so must M and σ_z and therefore $M = a\sigma_x + b\sigma_y$ where $a^2 + b^2 = 1$. We will parametrize $a = \cos\theta$ and $b = \sin\theta$. Naturally T fits this mold with $\theta = \frac{\pi}{4}$. It is straightforward to deduce

$$\{\mathbf{Y}\}\ U\ \{i\cdot(\cos\theta\cdot\mathbf{X} + \sin\theta\cdot\mathbf{Y})\mathbf{Z}\} \rightsquigarrow \{-\sin\theta\cdot\mathbf{X} + \cos\theta\cdot\mathbf{Y}\},$$

and so we see U acts as a Bloch sphere rotation in the $\mathbf{X}/\mathbf{Y}$-plane by an angle θ.

We claim that we can synthesize U using the state $|m\rangle$ that satisfies the predicate $\mathbf{M}$ in the circuit of Figure 3. That is, we aim to show that this circuit C satisfies the triples

$$\{\mathbf{M}_1 \cap \mathbf{Z}_2\}\ C\ \{(\mathbf{Z}_1 \uplus -\mathbf{Z}_1) \cap \mathbf{Z}_2\} \text{ and } \{\mathbf{M}_1 \cap \mathbf{X}_2\}\ C\ \{(\mathbf{Z}_1 \uplus -\mathbf{Z}_1) \cap \mathbf{M}_2\}$$

hence recovering (23) in the separable second factor.

Beginning with $\mathbf{M}_1 \cap \mathbf{Z}_2 = (\mathbf{M} \otimes \mathbf{I}) \cap (\mathbf{I} \otimes \mathbf{Z})$ we evaluate the effect of the circuit on each term of the intersection:

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

Our post-measurement predicate is then

$$((\mathbf{Z}_1 \cap \mathbf{I}_2) \uplus (-\mathbf{Z}_1 \cap \mathbf{I}_2)) \cap ((\mathbf{Z}_1 \cap \mathbf{Z}_2) \uplus (-\mathbf{Z}_1 \cap \mathbf{Z}_2)) \Rightarrow (\mathbf{Z}_1 \cap \mathbf{Z}_2) \uplus (-\mathbf{Z}_1 \cap \mathbf{Z}_2),$$

as the second term on the left side can be obtained using an implication rule on the first.

Now turning to the case $\mathbf{M}_1 \cap \mathbf{X}_2 = \mathbf{M}\otimes\mathbf{I} \cap \mathbf{I}\otimes\mathbf{X}$ we again evaluate the effect of the circuit:

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

Now, however, our precondition to the measurement

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

has too many terms with an $\mathbf{X}$ in the first factor. So we use the $\cap$-MUL-R rule to multiply the second term into the first, yielding

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

Now we apply the discussions from the previous section to write the post-measurement condition as

$$(\mathbf{Z}_1 \cap (\cos\theta\cdot\mathbf{X} + \sin\theta\cdot\mathbf{Y})_2) \uplus ((-\mathbf{Z})_1 \cap (\cos\theta\cdot\mathbf{X} - \sin\theta\cdot\mathbf{Y})_2).$$

So we see that upon measuring 0, the resulting state satisfies $\mathbf{Z}_1 \cap \mathbf{M}_2$ as desired. But upon measuring 1 we have the resulting predicate $(-\mathbf{Z})_1 \cap (\cos(-\theta)\mathbf{X} + \sin(-\theta)\mathbf{Y})_2$, and so have accomplished the rotation in the opposite direction. That is, we have implemented $U^\dagger$ and so doing a post-selected correction of U^2 as in Figure 3 produces the output predicate $(-\mathbf{Z})_1 \cap \mathbf{M}_2$ as desired.

	$\mathbf{X}$	$\mathbf{Y}$	$\mathbf{Z}$
X	$\mathbf{X}$	$-\mathbf{Y}$	$-\mathbf{Z}$
Y	$-\mathbf{X}$	$\mathbf{Y}$	$-\mathbf{Z}$
Z	$-\mathbf{X}$	$-\mathbf{Y}$	$\mathbf{Z}$
H	$\mathbf{Z}$	$-\mathbf{Y}$	$\mathbf{X}$
S	$\mathbf{Y}$	$-\mathbf{X}$	$\mathbf{Z}$
T	$\mathbf{X}+\mathbf{Y}$	$\mathbf{Y}-\mathbf{X}$	$\mathbf{Z}$
$T^\dagger$	$\mathbf{X}-\mathbf{Y}$	$\mathbf{X}+\mathbf{Y}$	$\mathbf{Z}$

Table 1: Axiomatized and derived behavior of common one-qubit gates.

	$\mathbf{X}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{X}$	$\mathbf{Y}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{Y}$	$\mathbf{Z}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{Z}$
$CNOT$	$\mathbf{X}\otimes\mathbf{X}$	$\mathbf{I}\otimes\mathbf{X}$	$\mathbf{Y}\otimes\mathbf{X}$	$\mathbf{Z}\otimes\mathbf{Y}$	$\mathbf{Z}\otimes\mathbf{I}$	$\mathbf{Z}\otimes\mathbf{Z}$
CZ	$\mathbf{X}\otimes\mathbf{Z}$	$\mathbf{Z}\otimes\mathbf{X}$	$\mathbf{Y}\otimes\mathbf{Z}$	$\mathbf{Z}\otimes\mathbf{Y}$	$\mathbf{Z}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{Z}$

	$\mathbf{X}{\otimes}\mathbf{X}$	$\mathbf{X}{\otimes}\mathbf{Y}$	$\mathbf{X}{\otimes}\mathbf{Z}$	$\mathbf{Y}{\otimes}\mathbf{X}$	$\mathbf{Y}{\otimes}\mathbf{Y}$	$\mathbf{Y}{\otimes}\mathbf{Z}$	$\mathbf{Z}{\otimes}\mathbf{X}$	$\mathbf{Z}{\otimes}\mathbf{Y}$	$\mathbf{Z}{\otimes}\mathbf{Z}$
$CNOT$	$\mathbf{X}{\otimes}\mathbf{I}$	$\mathbf{Y}{\otimes}\mathbf{Z}$	$-\mathbf{Y}{\otimes}\mathbf{Y}$	$\mathbf{Y}{\otimes}\mathbf{I}$	$-\mathbf{X}{\otimes}\mathbf{Z}$	$\mathbf{X}{\otimes}\mathbf{Y}$	$\mathbf{Z}{\otimes}\mathbf{X}$	$\mathbf{I}{\otimes}\mathbf{Y}$	$\mathbf{I}{\otimes}\mathbf{Z}$
CZ	$\mathbf{Y}{\otimes}\mathbf{Y}$	$-\mathbf{Y}{\otimes}\mathbf{X}$	$\mathbf{X}{\otimes}\mathbf{I}$	$-\mathbf{X}{\otimes}\mathbf{Y}$	$\mathbf{X}{\otimes}\mathbf{X}$	$\mathbf{Y}{\otimes}\mathbf{I}$	$\mathbf{I}{\otimes}\mathbf{X}$	$\mathbf{I}{\otimes}\mathbf{Y}$	$\mathbf{Z}{\otimes}\mathbf{Z}$

Table 2: Behavior of common two-qubit gates over all Pauli pairs.

9 Complexity of program verification

We can now present the algorithm for inferring postconditions and validating triples on quantum circuits. These are noticeably different procedures: validating triples ensures that a program has a given user-specified type, while postcondition inference attempts to derive a valid triple for a program. Given that our logic is rich enough to give infinitely many predicated to any circuit (though many will be equivalent), we will not perform full postcondition inference on a circuit. Instead, we can ask the user to specify the input, i.e., a precondition, and derive the output or postcondition through our inference rules. Alternatively, if the user has a specific postcondition in mind, we can do the same inference procedure and normalize both the pre- and postconditions (applying weakening rules as needed) and check that they are equivalent. Hence, in this section, we will focus on postcondition inference given a variety of programs and preconditions.

Inference on tensor preconditions Given a Clifford circuit and a predicate $\mathbf{P}_1 \otimes \mathbf{P}_2 \otimes \cdots \otimes \mathbf{P}_n$ (consisting of no intersections or additive terms), we can derive the corresponding postcondition on applying the circuit in $O(m)$ time, where m is the number of gates. This follows from the fact that we can update the postcondition on each gate application in constant time. In practice, this only takes a single lookup since it proves convenient to add a number of derived triples to the system (Tables 1 and 2). Note that we assume tensors are implemented by arrays, saving us the time of iterating through an n qubit list.

Inference on intersection predicates Restricting to just Pauli predicates, we can fully describe the semantics of a Clifford circuit (though we rarely will). Doing so requires determining the postcondition for $I^{k-1} \otimes \mathbf{X}_k \otimes I^{n-k}$ and $I^{k-1} \otimes \mathbf{Z}_k \otimes I^{n-k}$, for every $1 \leq k \leq n$ where n is the number of qubits. There are precisely $2n$ terms in this intersection, so the time to infer the fully descriptive output predicate is $O(mn)$.

Inference on fully separable preconditions When we get to separable preconditions, we have to start doing normalization (§3). The normalization procedure iterates over each tensor in an intersection and then multiplies it by potentially all the remaining tensors. Since there are at most $2n$ elements in the intersection and each tensor is of length n, this winds up being an $O(n^3)$ operation. Once the normalization is done, applying the separability rules is straightforward. This gives us a complexity of $O(mn + n^3)$, which we can simplify to $O(mn)$ (our previous result) when $m \gg n^2$.

Post-measurement inference on Pauli predicates Measurement is where some complexity can start to appear, especially with it being a non-unitary operation. In general, we want to use the *principle of deferred measurement* [22, §4.4] to push off measurements until the end of the circuit, allowing us to perform normalization only once. A single-qubit post-measurement predicate doubles in size when a random outcome is expected due to the use of unions. Then, performing m measurements could potentially add a 2^m factor increase in the number of terms. This is in line with the fact that there could be 2^m possible outcomes to track.

In practice, however, it is more common for us to post-select on certain measurement outcomes or perform subsequent operations conditioned on certain outcomes (e.g., error correction). In such cases, it will be possible to simplify the expression or focus only on a pre-determined set of postconditions to understand the measurement behavior. The cost for computing the post-measurement predicate for a single Pauli measurement on an n-qubit system with ℓ terms in the union is $O(2\ell n^3)$.

The Clifford+T set and exponential blowup Naturally, universal quantum computing is the real test case for our logic. We know that our system is capable of fully describing arbitrary quantum computations, so unless quantum computing is efficiently simulable, we cannot efficiently validate the action of arbitrary quantum circuits. This is clear in the case of Toffoli. As we saw in §7.2, despite having seven T gates, checking the Toffoli circuit only involves additive predicates with at most 4 terms (in the worst case). So in some sense, Toffoli only has an "effective" T-depth of 2 (which is essentially the content of Theorem 21).

Nevertheless, in the worst case, the running time of our validation and inference procedures is $O(2^t)$, where t is the number of T-gates, illustrating that our system cannot be efficiently applied to arbitrary circuits.

Post-measurement inference on additive predicates At this time, we refrain from providing any asymptotic expressions for the complexity of measuring additive predicates as we only consider very restricted cases of measuring single and 2-qubit systems. These are performed in an ad-hoc way by manipulating the underlying matrix corresponding to the given predicates. Hence, even generalizing the current process may not provide any non-trivial insights into asymptotic complexities beyond taking $O(2^n)$ time for an n-qubit system.

10 Related Work

A variety of Hoare logics for quantum programs already exist. These logics use a variety of predicates, including quantum observables [35], subspaces [33], and projections [38], going from most general to least. Notably, each assertion style is more expressive than our stabilizer predicates. This is both an advantage and a limitation. The combination of highly expressive predicates and a fully general consequence rule allows the user to prove arbitrary properties of programs, but this requires significant manual effort. In particular, in the rule for unitary application $\left\{\mathbf{U}^\dagger\mathbf{P}\mathbf{U}\right\}\ U\ \{\mathbf{P}\}$, some variant of which is present in almost every Hoare logic, $U^\dagger PU$ is almost never explicitly computed: Doing so would make using the logic as complex as simulating the program. Instead, such expressions tend to be left symbolic and are simplified by the liberal application of the consequence rule.

By contrast, the logic presented here is designed to be fully automated and efficient at the cost of expressiveness. When a unitary gate is applied to a qubit, the corresponding predicate changes, and this change is efficient, modulo the effect of non-Clifford gates. This allows us to efficiently characterize properties like separability, provided that the T count is low. However, we cannot prove the correctness of Grover's algorithm or Harrow-Hassidim-Lloyd algorithm, as in prior logics [35, 38].

Prior work on lightweight static analysis of quantum programs used the lens of *abstract interpretation*. Abstract interpretation was developed by Cousot and Cousot [8] in order to show useful properties of programs at low cost. Abstract interpretation necessarily sacrifices fidelity (being able to perfectly describe a program) in favor of efficiency. Perdrix [23] was the first to apply abstract interpretation to quantum programs (expanding on earlier work [24] that used a type system), but his system was quite limited: It could only precisely characterize a qubit as being in the z or x basis, and *conservatively* tracked entanglement, meaning that it would err on the side of saying qubits were entangled if it could not rule that out. Building on Perdix's work, Prose and Zerrari [25] developed a Hoare-like logic for conservatively tracking entanglement, applied to Selinger and Valiron's quantum lambda calculus [28].

More recently, Yu and Palsberg [36] developed an approach to quantum abstract interpretation based on *reduced density matrices*, specifically 4×4 partial traces of the full system. The expressiveness of such an approach is unclear and is mostly used to check that qubits are in $|0\rangle$ or $|1\rangle$ states in practice. However, it does demonstrate remarkable performance in assertion checking and admits the possibility of using larger, more informative, reduced density matrices.

Honda [17] presented a more powerful system based, like ours, on the stabilizer formalism. It represented states using stabilizer arrays, which can be translated to our logic but are rather less useful than human-readable predicates. It dealt with non-stabilizer states simply by treating them as black boxes (literally represented as ■), which could propagate throughout the program. This could be useful in a few cases, such as where a non-stabilizer state was quickly discarded, but generally meant the system could not meaningfully speak about non-Clifford circuits.

Prior versions of this work [27, 31] presented the logic as a lightweight type system for quantum programs. While there is a rich literature on semantic subtyping and set-theoretic types [11, 4], in which types can convey rich information about a program, as our logic became more complex, using types came to feel less natural. In particular, typing derivations, which tend to be expressed in the form of trees, grew unwieldy, and it became clear that we would need a notion of subtyping corresponding to Hoare logic's consequence rule. Our lightweight consequence rule ($\Rrightarrow$) proved to be the right middle ground, allowing us to simplify assertions without allowing arbitrary mathematical derivations. However, the switch is not without cost: A type system allows us to fully characterize the behavior of H with the type $(\mathbf{X} \to \mathbf{Z}) \cap (\mathbf{Z} \to \mathbf{X})$, while in Hoare logic we had to introduce the somewhat artificial judgment $\{\{\mathbf{X} \parallel \mathbf{Z}\}\}\ \ H\ \ \{\{\mathbf{Z} \parallel \mathbf{X}\}\}$, which is external to the core logic. Note that $U : (\mathbf{A} \to \mathbf{B}) \cap (\mathbf{A}' \to \mathbf{B}')$ implies $U : (\mathbf{A} \cap \mathbf{A}') \to (\mathbf{B} \cap \mathbf{B}')$ via standard subtyping rules. We could add a corresponding rule for $\{\{\mathbf{A} \parallel \mathbf{A}'\}\}\ \ U\ \ \{\{\mathbf{B} \parallel \mathbf{B}'\}\}$, but this would add unnecessary complications to the logic.

Yuan et al. [37], introduce a type system for conservatively tracking entanglement, with an interesting twist: Qubits can be cast to unentangled ("Pure", in the paper's terminology) at the cost of a runtime check. This is a surprisingly lightweight and readable approach to tracking entanglement. However, the runtime check is potentially costly (whether the program is simulated or executed on a quantum computer) and it is not clear how this type system could be extended to express additional properties.

Concurrently with this work, Wu et al. [34] developed QECV, a quantum Hoare logic based on stabilizers for verifying error-correcting codes. This approach is largely complementary to our own (save for our comparatively small steps towards verifying stabilizer codes) but suggests a variety of new possible directions. Their language, as well as their logic, references predicates, allowing for measurement that branches on those predicates and a custom measurement that reflects that. The language also includes loops, which we do not address in this work. Adapting QECV's language and logic to verifying attributes like separability seems like a promising future direction for this work. It also seems likely that we could build a verified tool that can check program properties using a generalization of QECV that captures properties like separability.

Finally, there are two approaches to quantum program verification that are adjacent to our own but worth addressing. Quantum assertions [18, 21, 20] allow one to embed assertions inside programs that will check that a given property holds. While prior work was limited to checking simple assertions, Li et al. [20] treats arbitrary projections as assertions. However, these systems can fail at runtime (e.g., if the measured state has some probability of being in the desired state) and also require us to check a program's behavior on a quantum device or sufficiently powerful simulator. At the other end of the spectrum are sophisticated logical systems for quantum programs [35, 33] and powerful tools to formally verify quantum program behavior [5, 16]. However, even with an assist from automation, these tools tend to require substantial effort on the part of the programmer. We refer the reader to two recent surveys [6, 19] for an in-depth analysis of the advantages and disadvantages of these approaches.

11 Future work

There are still various ways to further enrich our program logic, providing many promising avenues for us to explore.

Inference on Quantum Channels Other than measurement, all the operations whose behavior we infer are unitary circuits. More general quantum operations are given by completely positive trace-preserving maps, i.e., quantum channels. Extending our logic to handle quantum channels could potentially allow us to perform inference on or validate quantum cryptography and communication protocols. A starting point for this would be to use additive predicates and unions to characterize partial traces and post-selection.

Applications for error-correcting codes Implementing a fault-tolerant universal set of gates transversally will reduce the overall cost of error correction. However, as this cannot be achieved using just one code, a common method used switches between two sets of codes, each having a different set of transversal gates [2]. Extending our logic to either infer the structure of or even validate the code-switching circuit given the predicates describing two codes would prove to be fruitful. Similarly, validating the encoding and decoding circuits for a code given its predicate could also be of value in verifying the implementation of error-correcting codes.

Normalization for additive predicates Finding a canonical representation for additive predicates is imperative to effectively validate additive postconditions. A big roadblock to it is that, unlike with Pauli predicates, additive predicates (especially multi-qubit ones) could have terms that neither commute nor anticommute. This makes it hard to find a normalization procedure for them similar to that in §3. Additionally, this also limits our ability to make multi-qubit separability judgments in the additive case.

General measurement for additive predicates Although we have outlined some cases in §8 where we can infer the post-measurement states, this is limited to performing σ_z-basis measurement on single and two-qubit systems. In order to fully exploit the power of additive predicates, it is essential that we have a full characterization for post-measurement states. An immediate consequence of this could be a deeper analysis of predicates for multi-qubit magic states and applications associated with them.

A logic for quantum programs with classical control A key component of quantum error correction and many quantum algorithms in practice (whether intermediate or large scale) is that they are interspersed with classical processing. This includes the use of classical control to decide which quantum operations to apply along with any pre- or post-processing. To account for this, we would need to formally extend our logic to explicitly handle classical data types as well as other program elements such as conditional statements, loops and recursions.

Acknowledgments

This material is based upon work supported by EPiQC, an NSF Expedition in Computing, under Grant No. 1730449 and the Air Force Office of Scientific Research under Grant No. FA95502110051.

References

[1] Scott Aaronson and Daniel Gottesman. “Improved Simulation of Stabilizer Circuits”. In: *Physical Review A* 70.5 (2004), p. 052328. DOI: 10.1103/physreva.70.052328. arXiv: quant-ph/0406196.

[2] Jonas T. Anderson, Guillaume Duclos-Cianci, and David Poulin. “Fault-Tolerant Conversion between the Steane and Reed-Muller Quantum Codes”. In: *Phys. Rev. Lett.* 113 (8 2014), p. 080501. DOI: 10.1103/PhysRevLett.113.080501. arXiv: 1403.2734.

[3] Benjamin Bichsel, Maximilian Baader, Timon Gehr, and Martin Vechev. “Silq: A High-Level Quantum Language with Safe Uncomputation and Intuitive Semantics”. In: *Proc. PLDI ’20.* ACM, 2020, pp. 286–300. DOI: 10.1145/3385412.3386007. URL: https://files.sri.inf.ethz.ch/website/papers/pldi20-silq.pdf.

[4] Giuseppe Castagna. *Programming with Union, Intersection, and Negation Types.* 2022. arXiv: 2111.03354.

[5] Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perrelle, and Benoît Valiron. “An Automated Deductive Verification Framework for Circuit-Building Quantum Programs”. In: *Programming Languages and Systems, ESOP 2021*. Ed. by Nobuko Yoshida. Vol. 12648. Lecture Notes in Computer Science. Springer International Publishing, 2021, pp. 148–177. DOI: 10.1007/978-3-030-72019-3_6.

[6] Christophe Chareton, Sébastien Bardin, Dongho Lee, Benoît Valiron, Renaud Vilmart, and Zhaowei Xu. *Formal Methods for Quantum Programs: A Survey*. To appear as Chapter “Formal methods for Quantum Algorithms” in “Handbook of Formal Analysis and Verification in Cryptography”, CRC. 2022. arXiv: 2109.06493.

[7] Richard Cleve and Daniel Gottesman. “Efficient Computations of Encodings for Quantum Error Correction”. In: *Phys. Rev. A* 56 (1 1997), pp. 76–82. DOI: 10.1103/PhysRevA.56.76. arXiv: quant-ph/9607030.

[8] Patrick Cousot and Radhia Cousot. “Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints”. In: *Conference Record of the Fourth ACM Symposium on Principles of Programming Languages, Los Angeles, California, USA, January 1977*. ACM, 1977, pp. 238–252. DOI: 10.1145/512950.512973. URL: https://courses.cs.washington.edu/courses/cse503/10wi/readings/p238-cousot.pdf.

[9] David Deutsch. “Quantum theory, the Church–Turing principle and the universal quantum computer”. In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117. DOI: 10.1098/rspa.1985.0070.

[10] David Deutsch and Richard Jozsa. “Rapid solution of problems by quantum computation”. In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558. DOI: 10.1098/rspa.1992.0167.

[11] Alain Frisch, Giuseppe Castagna, and Véronique Benzaken. “Semantic Subtyping: Dealing Set-Theoretically with Function, Union, Intersection, and Negation Types”. In: *J. ACM* 55.4 (2008). DOI: 10.1145/1391289.1391293.

[12] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. “An Algorithm for the T-Count”. In: *Quantum Info. Comput.* 14.15–16 (2014), pp. 1261–1276. DOI: 10.26421/QIC14.15-16-1. arXiv: 1308.4134.

[13] Daniel Gottesman. “Class of quantum error-correcting codes saturating the quantum Hamming bound”. In: *Phys. Rev. A* 54.3 (1996), pp. 1862–1868. DOI: 10.1103/physreva.54.1862. arXiv: quant-ph/9604038.

[14] Daniel Gottesman. “The Heisenberg Representation of Quantum Computers”. In: *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*. LA-UR-98-2848. International Press, 1998, pp. 32–43. arXiv: quant-ph/9807006.

[15] Alexander S. Green, Peter LeFanu Lumsdaine, Neil J. Ross, Peter Selinger, and Benoît Valiron. “Quipper: A Scalable Quantum Programming Language”. In: *Proc. PLDI ’13*. ACM, 2013, pp. 333–342. DOI: 10.1145/2491956.2462177. arXiv: 1304.3390.

[16] Kesha Hietala, Robert Rand, Shih-Han Hung, Liyi Li, and Michael Hicks. “Proving Quantum Programs Correct”. In: *12th International Conference on Interactive Theorem Proving (ITP 2021)*. Vol. 193. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 21. DOI: 10.4230/LIPIcs.ITP.2021.21. CODE: https://github.com/inQWIRE/SQIR.

[17] Kentaro Honda. “Analysis of Quantum Entanglement in Quantum Programs using Stabilizer Formalism”. In: *Proc. QPL ’15*. Vol. 195. Open Publishing Association, 2015, pp. 262–272. DOI: 10.4204/EPTCS.195.19.

[18] Yipeng Huang and Margaret Martonosi. “Statistical Assertions for Validating Patterns and Finding Bugs in Quantum Programs”. In: *Proceedings of the 46th International Symposium on Computer Architecture*. ISCA ’19. ACM, 2019, pp. 541–553. DOI: 10.1145/3307650.3322213.

[19] Marco Lewis, Sadegh Soudjani, and Paolo Zuliani. *Formal Verification of Quantum Programs: Theory, Tools and Challenges*. 2021. arXiv: `2110.01320`.

[20] Gushu Li, Li Zhou, Nengkun Yu, Yufei Ding, Mingsheng Ying, and Yuan Xie. “Projection-Based Runtime Assertions for Testing and Debugging Quantum Programs”. In: *Proc. ACM Program. Lang.* 4.OOPSLA, 150 (2020). DOI: 10.1145/3428218.

[21] Ji Liu, Gregory T. Byrd, and Huiyang Zhou. “Quantum Circuits for Dynamic Runtime Assertions in Quantum Computation”. In: *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*. ASPLOS ’20. ACM, 2020, pp. 1017–1030. DOI: 10.1145/3373376.3378488.

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

[23] Simon Perdrix. “Quantum Entanglement Analysis Based on Abstract Interpretation”. In: *Static Analysis*. Springer, 2008, pp. 270–282. DOI: 10.1007/978-3-540-69166-2_18. arXiv: `0801.4230`.

[24] Simon Perdrix. “Quantum Patterns and Types for Entanglement and Separability”. In: *Electron. Notes Theor. Comput. Sci.* 170 (2007). Proc. QPL ’05, pp. 125–138. DOI: 10.1016/j.entcs.2006.12.015.

[25] Frédéric Prost and Chaouki Zerrari. “Reasoning about entanglement and separability in quantum higher-order functions”. In: *International Conference on Unconventional Computation*. Springer. 2009, pp. 219–235. DOI: 10.1007/978-3-642-03745-0_25.

[26] Robert Rand, Jennifer Paykin, Dong-Ho Lee, and Steve Zdancewic. “ReQWIRE: Reasoning about Reversible Quantum Circuits”. In: *Proc. QPL ’18*. 2018, pp. 299–312. DOI: 10.4204/EPTCS.287.17.

[27] Robert Rand, Aarthi Sundaram, Kartik Singhal, and Brad Lackey. “Gottesman Types for Quantum Programs”. In: *Proceedings of the 17th International Conference on Quantum Physics and Logic (QPL), Paris, France, June 2–6, 2020*. Vol. 340. Electronic Proceedings in Theoretical Computer Science. Waterloo, NSW, Australia: Open Publishing Association, 2021, pp. 279–290. DOI: 10.4204/EPTCS.340.14.

[28] Peter Selinger and Benoît Valiron. “A lambda calculus for quantum computation with classical control”. In: *Mathematical Structures in Computer Science* 16.3 (2006), pp. 527–552. DOI: 10.1017/S0960129506005238.

[29] Andrew Steane. “Multiple-particle interference and quantum error correction”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 452.1954 (1996), pp. 2551–2577. DOI: 10.1098/rspa.1996.0136.

[30] Andrew M. Steane. “Active Stabilization, Quantum Computation, and Quantum State Synthesis”. In: *Phys. Rev. Lett.* 78 (11 1997), pp. 2252–2255. DOI: 10.1103/PhysRevLett.78.2252. arXiv: `quant-ph/9611027`.

[31] Aarthi Sundaram, Robert Rand, Kartik Singhal, and Brad Lackey. *A Rich Type System for Quantum Programs*. 2021. arXiv: 2101.08939v3.

[32] Krysta Svore, Alan Geller, Matthias Troyer, John Azariah, Christopher Granade, Bettina Heim, Vadym Kliuchnikov, Mariia Mykhailova, Andres Paz, and Martin Roetteler. "Q#: Enabling Scalable Quantum Computing and Development with a High-level DSL". In: *Proc. Real World Domain Specific Languages Workshop (RWDSL) 2018*. ACM, 2018, 7:1–7:10. DOI: 10.1145/3183895.3183901. arXiv: 1803.00652.

[33] Dominique Unruh. "Quantum Hoare Logic with Ghost Variables". In: *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science*. LICS '19. IEEE Computer Society, 2019, pp. 1–13. DOI: 10.1109/LICS.2019.8785779. arXiv: 1902.00325.

[34] Anbang Wu, Gushu Li, Hezi Zhang, Gian Giacomo Guerreschi, Yuan Xie, and Yufei Ding. *QECV: Quantum Error Correction Verification*. 2021. arXiv: 2111.13728.

[35] Mingsheng Ying. "Floyd–Hoare Logic for Quantum Programs". In: *ACM Trans. Program. Lang. Syst.* 33.6, 19 (2012). DOI: 10.1145/2049706.2049708.

[36] Nengkun Yu and Jens Palsberg. "Quantum Abstract Interpretation". In: *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*. PLDI '21. ACM, 2021, pp. 542–558. DOI: 10.1145/3453483.3454061. URL: http://web.cs.ucla.edu/~palsberg/paper/pldi21-quantum.pdf.

[37] Charles Yuan, Christopher McNally, and Michael Carbin. "Twist: Sound Reasoning for Purity and Entanglement in Quantum Programs". In: *Proc. ACM Program. Lang.* 6.POPL, 30 (2022). DOI: 10.1145/3498691. arXiv: 2205.02287. CODE: https://github.com/psg-mit/twist-popl22.

[38] Li Zhou, Nengkun Yu, and Mingsheng Ying. "An Applied Quantum Hoare Logic". In: *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation*. PLDI '19. ACM, 2019, pp. 1149–1162. DOI: 10.1145/3314221.3314584. URL: https://opus.lib.uts.edu.au/bitstream/10453/140615/2/3314221.3314584.pdf.

A Full Grammar and Rules

1. Predicates:

$$\begin{aligned} \mathbf{G} &:= \mathbf{I} \mid \mathbf{X} \mid \mathbf{Y} \mid \mathbf{Z} \\ \mathbf{T} &:= \mathbf{G} \mid \mathbf{cT} \mid \mathbf{T} \otimes \mathbf{T} \mid \mathbf{T} + \mathbf{T} \\ \mathbf{P} &:= \mathbf{T} \mid \mathbf{P} \cap \mathbf{P} \mid \mathbf{P} \uplus \mathbf{P} \mid \mathbf{P_S} \end{aligned}$$

2. Core Rules:

$$\begin{array}{cc} \{\mathbf{X}\}\ H\ \{\mathbf{Z}\} & \{\mathbf{X} \otimes \mathbf{I}\}\ CNOT\ \{\mathbf{X} \otimes \mathbf{X}\} \\ \{\mathbf{Z}\}\ H\ \{\mathbf{X}\} & \{\mathbf{I} \otimes \mathbf{X}\}\ CNOT\ \{\mathbf{I} \otimes \mathbf{X}\} \\ \{\mathbf{X}\}\ S\ \{\mathbf{Y}\} & \{\mathbf{Z} \otimes \mathbf{I}\}\ CNOT\ \{\mathbf{Z} \otimes \mathbf{I}\} \\ \{\mathbf{Z}\}\ S\ \{\mathbf{Z}\} & \{\mathbf{I} \otimes \mathbf{Z}\}\ CNOT\ \{\mathbf{Z} \otimes \mathbf{Z}\} \\ \{\mathbf{Z}\}\ T\ \{\mathbf{Z}\} & \{\mathbf{X}\}\ T\ \left\{\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X} + \mathbf{Y})\right\} \end{array}$$

3. Tensor Rules:

$$\frac{\mathbf{T}[i] = \mathbf{A} \qquad \{\mathbf{A}\}\ U\ \{\mathbf{B}\}}{\{\mathbf{T}\}\ U\ i\ \{\mathbf{T}[\mathbf{i} \mapsto \mathbf{B}]\}}\ \otimes_1 \qquad \frac{\mathbf{T}[i] = \mathbf{A} \qquad \mathbf{T}[j] = \mathbf{B} \qquad \{\mathbf{A} \otimes \mathbf{B}\}\ U\ \{\mathbf{C} \otimes \mathbf{D}\}}{\{\mathbf{T}\}\ U\ i\ j\ \{\mathbf{T}[\mathbf{i} \mapsto \mathbf{C}; \mathbf{j} \mapsto \mathbf{D}]\}}\ \otimes_2$$

4. Arithmetic Rules:

$$\frac{\{\mathbf{A}\}\ g\ \{\mathbf{A'}\} \qquad \{\mathbf{B}\}\ g\ \{\mathbf{B'}\}}{\{\mathbf{AB}\}\ g\ \{\mathbf{A'B'}\}}\ \textsc{mul} \qquad \frac{\{\mathbf{A}\}\ g\ \{\mathbf{A'}\}}{\{\mathbf{cA}\}\ g\ \{\mathbf{cA'}\}}\ \textsc{scale}$$

5. Sequence Rule:

$$\frac{\{\mathbf{A}\}\ g_1\ \{\mathbf{B}\} \qquad \{\mathbf{B}\}\ g_2\ \{\mathbf{C}\}}{\{\mathbf{A}\}\ g_1; g_2\ \{\mathbf{C}\}}\ \textsc{seq}$$

6. Consequence Rule:

$$\frac{\mathbf{A'} \Rightarrow \mathbf{A} \qquad \{\mathbf{A}\}\ g\ \{\mathbf{B}\} \qquad \mathbf{B} \Rightarrow \mathbf{B'}}{\{\mathbf{A'}\}\ g\ \{\mathbf{B'}\}}\ \textsc{cons}$$

7. Intersection and Disjoint Union Rules:

$$\frac{\{\mathbf{A}\}\ g\ \{\mathbf{A'}\} \qquad \{\mathbf{B}\}\ g\ \{\mathbf{B'}\}}{\{\mathbf{A} \cap \mathbf{B}\}\ g\ \{\mathbf{A'} \cap \mathbf{B'}\}}\ \cap \qquad \frac{\{\mathbf{A}\}\ g\ \{\mathbf{A'}\} \qquad \{\mathbf{B}\}\ g\ \{\mathbf{B'}\}}{\{\mathbf{A} \uplus \mathbf{B}\}\ g\ \{\mathbf{A'} \uplus \mathbf{B'}\}}\ \uplus$$

8. Addition Rules:

$$\frac{\{\mathbf{A}\}\ g\ \{\mathbf{C}\} \qquad \{\mathbf{B}\}\ g\ \{\mathbf{D}\}}{\{\mathbf{A} + \mathbf{B}\}\ g\ \{\mathbf{C} + \mathbf{D}\}}\ \textsc{add} \qquad \frac{\{\mathbf{A}\}\ U\ \{\mathbf{B} + \mathbf{C}\} \qquad \mathbf{T}[i] = \mathbf{A}}{\{\mathbf{T}\}\ U\ i\ \{\mathbf{T}[\mathbf{i} \mapsto \mathbf{B}] + \mathbf{T}[\mathbf{i} \mapsto \mathbf{C}]\}}\ \otimes\text{-}\textsc{add}$$

Figure 4: The basic predicates, Hoare triples, and deductive rules for our stabilizer logic. The grammar allows us to describe ill-formed predicates, such as $\mathbf{X} \cap (\mathbf{I} \otimes \mathbf{Z})$, but these are never satisfied.

1. Simplification rules:

$$\begin{array}{ccc} \mathbf{GG} \rightsquigarrow \mathbf{I} & \mathbf{IG} \rightsquigarrow \mathbf{G} & \mathbf{GI} \rightsquigarrow \mathbf{G} \\ \mathbf{ZX} \rightsquigarrow i\mathbf{Y} & \mathbf{XY} \rightsquigarrow i\mathbf{Z} & \mathbf{YZ} \rightsquigarrow i\mathbf{X} \\ \mathbf{XZ} \rightsquigarrow -i\mathbf{Y} & \mathbf{YX} \rightsquigarrow -i\mathbf{Z} & \mathbf{ZY} \rightsquigarrow -i\mathbf{X} \end{array}$$

$$c\mathbf{A} \otimes \mathbf{B} \rightsquigarrow c(\mathbf{A} \otimes \mathbf{B}) \qquad \mathbf{A} \otimes c\mathbf{B} \rightsquigarrow c(\mathbf{A} \otimes \mathbf{B})$$

2. Implication rules:

$$\begin{array}{ll} \mathbf{A} \cap \mathbf{B} \Rightarrow \mathbf{A} & \\ \mathbf{A} \cap \mathbf{B} \Rightarrow \mathbf{B} \cap \mathbf{A} & \\ \mathbf{A} \cap (\mathbf{B} \cap \mathbf{C}) \Leftrightarrow (\mathbf{A} \cap \mathbf{B}) \cap \mathbf{C} & \\ \mathbf{A} \Rightarrow \mathbf{A} \uplus \mathbf{B} & \\ \mathbf{A} \uplus \mathbf{B} \Rightarrow \mathbf{B} \uplus \mathbf{A} & \\ \mathbf{A} \uplus (\mathbf{B} \uplus \mathbf{C}) \Leftrightarrow (\mathbf{A} \uplus \mathbf{B}) \uplus \mathbf{C} & \\ \mathbf{A} \cap \mathbf{B} \Leftrightarrow \mathbf{A} \cap \mathbf{AB} & \text{(for Pauli Predicates } \mathbf{A}, \mathbf{B}) \\ \mathbf{A} + \mathbf{B} \Rightarrow \mathbf{B} + \mathbf{A} & \\ (\mathbf{A} + \mathbf{B}) + \mathbf{C} \Leftrightarrow \mathbf{A} + (\mathbf{B} + \mathbf{C}) & \\ \mathbf{A} + 0\mathbf{B} \Rightarrow \mathbf{A} & \end{array}$$

3. Single-qubit Separability Rules:

$$\begin{array}{ll} \mathbf{I}^{k-1} \otimes \mathbf{B} \otimes \mathbf{I}^{n-k} \Leftrightarrow \mathbf{B}_k & \\ \mathbf{B}_k \cap \mathbf{T} \Leftrightarrow \mathbf{B}_k \cap \mathbf{T}_{[n]\setminus\{k\}} & \text{where } \mathbf{T}[k] \in \{\mathbf{B}, \mathbf{I}\} \end{array}$$

4. Multi-qubit separability rules for Pauli predicates when $S = \{j_1, \ldots, j_k\} \subset [n]$:

$$\begin{array}{l} \mathbf{B} \cap \mathbf{T}_{(1)} \cap \ldots \cap \mathbf{T}_{(k)} \Leftrightarrow \mathbf{B}_{\overline{S}} \cap \left(\mathbf{C}_{(1)} \cap \ldots \cap \mathbf{C}_{(k)}\right)_S, \\ \text{where } \forall_{j\in[k]}\ \mathbf{T}_{(j)}[S] = \mathbf{C}_{(j)} \forall_{j\in[k]}\ \mathbf{T}_{(j)}[\overline{S}] = \mathbf{I}^{n-k}\mathbf{B}[S] = \mathbf{I}^k \end{array}$$

Figure 5: Simplification and implication rules for our predicates. These cover our applications for normalization and separability judgments. Let $[n] = \{1, \ldots, n\}$ and $S \subset [n]$. The conditions that $\mathbf{C}_{(1)}, \ldots, \mathbf{C}_{(k)}$ need to satisfy to achieve multi-qubit separability are described in §4.2.

B Transitivity of Clifford groups

Recall that a group G acting on a set Ω is *transitive* if for any $x, y \in \Omega$ there exists a $g \in G$ with $g \cdot x = y$. Since Clifford operators act on Pauli operators by conjugation, the Clifford group can never be transitive as $C \cdot I = CIC^\dagger = I$. However, for nontrivial Paulis, it is.

Proposition 40. *Let $P, Q \in \mathcal{P}_n \backslash \{\pm I\}$. Then there exists a $C \in C\ell_n$ such that $CPC^\dagger = Q$.*

More generally, a group is m-transitive if given tuples $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in \Omega^m$ with each $x_i \neq x_j$ and $y_i \neq y_j$, then there exists a $g \in G$ with $g \cdot x_i = y_i$ for $i = 1, \ldots, m$. Again, since the Clifford group acts by conjugation $C \cdot (-P) = -CPC^\dagger = -C \cdot P$ and so the Clifford group cannot be even 2-transitive. However, we modify the definition to require our Pauli elements to be distinct up to sign; then, we do obtain a higher transitivity result in the one-qubit, which follows from simply counting the number of one-qubit Clifford operators.

Lemma 41. *Given $P_1, P_2, Q_1, Q_2 \in \mathcal{P}_1 \setminus \{\pm I\}$ with $P_1 \neq \pm P_2$ and $Q_1 \neq \pm Q_2$, then there exists a $C \in C\ell_1$ with $CP_1C^\dagger = Q_1$ and $CP_2C^\dagger = Q_2$.*

Note that from the conditions in the lemma above, we must have P_1 and P_2 (and respectively Q_1 and Q_2) anticommute. But for higher qubit Paulis, this is not the case: even if $P_1 \neq \pm P_2$ we could have P_1 and P_2 commute. Since conjugation preserves commutativity, again, the Clifford group cannot be 2-transitive. However, it is on pairs of commuting/anticommuting Paulis.

Theorem 42. *Given $P_1, P_2, Q_1, Q_2 \in \mathcal{P}_n \setminus \{\pm I\}$ with $P_1 \neq \pm P_2$ and $Q_1 \neq \pm Q_2$ and either both P_1, P_2 and Q_1, Q_2 commute or both anticommute. Then then there exists a $C \in C\ell_n$ with $CP_1C^\dagger = Q_1$ and $CP_2C^\dagger = Q_2$.*

The proof of this theorem follows from the 2-qubit case (much like building a general Clifford operator out of CNOT and one-qubit Cliffords). For two commuting 2-qubit Cliffords P, Q, using the lemma above (and CNOT if necessary) one can easily produce a C with $CPC^\dagger = \sigma_y \otimes \sigma_y$ and $CQC^\dagger = \sigma_z \otimes \sigma_z$. Similarly, for two anticommuting 2-qubit Cliffords P, Q, one gets a C with $CPC^\dagger = I \otimes \sigma_y$ and $CQC^\dagger = I \otimes \sigma_z$. Then the theorem follows from chaining each of P_1, Q_1 and P_2, Q_2 through the appropriate normal form.