Bachelor Thesis at the
Chair for Quantum Information Systems

Predicate Transformers for Nondeterministic Quantum Programs

by
Xi Wang

This written work was submitted to
Lehrstuhl für Informatik 15, RWTH Aachen University.

Submission Date:	September 2, 2026
First examiner:	Prof. Dominique Unruh
Second examiner:	Prof. Joost-Pieter Katoen
Thesis advisor:	Christina Gehnen

Communicated by Dominique Unruh

Abstract

Nondeterminism has been introduced into quantum programming languages to model, for example, unspecified behavior. Weakest precondition transformers provide a formal framework for reasoning about program correctness with respect to a given postcondition. This thesis combines these ideas by introducing demonic and angelic interpretations of nondeterminism for quantum programs, together with corresponding weakest liberal precondition transformers. To capture angelic nondeterminism in a qualitative setting, we introduce predicates represented by sets of subspaces, where each subspace is represented by a projection. Such a predicate is satisfied whenever the quantum state belongs to one of the represented subspaces. We show, however, that natural definitions of the weakest liberal precondition transformer based on these predicates do not behave as desired for measurements and loops in the demonic setting. For this reason, the demonic weakest liberal precondition transformer is restricted to singleton postconditions. We further investigate the corresponding non-liberal weakest precondition transformers using termination spaces. This yields transformer rules for all language constructs except loops, for which deriving a transformer rule remains an open problem. Finally, we show that the resulting weakest precondition variants have the same relations as in the classical case.

Acknowledgements

First, I would like to thank my thesis advisor, Christina Gehnen, for her support and supervision throughout the entire process. I am especially grateful for our regular meetings, as well as for her valuable feedback and ideas, which were very helpful. I would also like to thank Prof. Dominique Unruh for the thoughts on a possible weakest precondition rule for loops. Finally, I would like to thank Prof. Dominique Unruh and Prof. Joost-Pieter Katoen for examining my thesis.

Contents

Chapter 1

Introduction

Quantum computing offers computational advantages for certain classes of problems such as search problems [Gro96] or factorizing [Sho94], motivating the development of quantum software. When developing such quantum programs, we want to be able to verify that they actually behave as desired. As quantum programs become more complex, ensuring their correctness becomes increasingly challenging. In contrast to classical programs, this requires reasoning about quantum phenomena such as superposition, entanglement and measurements. Consequently, formal verification techniques play an important role in establishing the correctness of quantum programs. One widely used verification framework is Hoare logic [Hoa69], which has been successfully adapted from classical to quantum programs [Yin11]. Central to these approaches are predicate transformers, particularly weakest preconditions, which enable backward reasoning by characterizing the initial states from which a desired postcondition is guaranteed to hold after program execution. While the majority of existing work considers deterministic quantum programs, nondeterminism has also been introduced into the quantum setting [FX23]. It is useful for modelling underspecified programs, abstractions and alternative implementation choices during program development. Because a nondeterministic program may have multiple possible executions from the same initial state, different notions of correctness arise. In particular, one may require that all executions satisfy the desired postcondition (demonic interpretation) or that at least one execution satisfies it (angelic interpretation). These two versions motivate corresponding variants of weakest precondition transformers. In addition, we can distinguish between weakest liberal preconditions, which allow nontermination, or (non-liberal) weakest preconditions, which require termination. This thesis investigates weakest precondition and weakest liberal precondition transformers for nondeterministic quantum programs under both angelic and demonic nondeterminism and studies the relationships between the resulting weakest precondition variants.

1.1 Related Work

Existing work on quantum Hoare logic can broadly be divided into two approaches: quantitative approaches based on hermitian operators and qualitative approaches based on subspaces.

Quantitative approaches, such as [Yin11] and [DP06], represent predicates by hermitian operators and interpret correctness in terms of expectation values, i.e., a predicate is satisfied to a certain degree.

In contrast, Zhou et al. [ZYY19] introduce an applied Hoare logic, in which predicates are represented by orthogonal projections (or equivalently closed subspaces), leading to a qualitative approach, i.e., a predicate is either satisfied or not. This is the approach we will follow in this thesis. Additionally, their framework introduces termination spaces for deterministic quantum programs, which form the basis of the non-liberal predicate transformers introduced in this thesis.

Feng et al. [FZXX26] develop a refinement calculus for quantum programs featuring prescription statements, which describe pairs of predicates that specify the required pre- and postconditions of a program component without prescribing how it is implemented. They provide weakest liberal precondition transformer rules, which are the basis for the transformer rules developed in this thesis. However, their language does not include explicit nondeterministic choice.

Li et al. [FX23] introduce the nondeterministic quantum programs that we will consider in this thesis. Using quantitative predicates, they further develop weakest (liberal) precondition transformers for these nondeterministic programs, which correspond to the demonic interpretation of nondeterminism.

In the classical case, Verscht et al. [VK25] provide an overview of the four variants of weakest preconditions and their relations that we study in this thesis, in particular including the distinction between angelic and demonic nondeterminism.

Building on these works, this thesis introduces qualitative angelic and demonic weakest (liberal) preconditions for nondeterministic quantum programs. We develop weakest liberal precondition transformer rules for the angelic and demonic variants and prove their correctness. For the non-liberal variants, we define the corresponding weakest preconditions using termination spaces and derive transformer rules for all language constructs except loops. We also investigate how the four precondition variants relate to each other.

1.2 Outline

Chapter 2 introduces the mathematical background on quantum computing and the quantum programming language considered throughout the thesis. Based on the classical weakest precondition variants, Chapter 3 introduces the four weakest precondition variants for nondeterministic quantum programs that we study in this thesis. Chapter 4 defines the qualitative predicates used in this work and establishes their fundamental properties. Building on these foundations, Chapter 5 develops the angelic and demonic weakest liberal precondition transformers and proves their correctness. Chapter 6 introduces the corresponding non-liberal weakest preconditions using termination spaces and derives transformer rules for all language constructs except loops. Chapter 7 studies the relationships between the four weakest precondition variants, and Chapter 8 applies the transformers by verifying a simple three-qubit bit-flip error correction scheme. Finally, Chapter 9 concludes the thesis and presents ideas for future work.

Chapter 2

Preliminaries

This section introduces the necessary background for understanding the subsequent chapters. We start with the main concepts of quantum computing and then introduce our language for nondeterministic quantum programs.

2.1 Quantum Computing

Since the predicate transformers developed later in this thesis operate on quantum states, we first introduce the mathematical framework used to describe quantum systems. This section briefly explains Hilbert spaces, linear operators, density operators and quantum measurements. Unless stated otherwise, the definitions follow the definitions from [Yin11].

Hilbert Spaces

According to von Neumann's postulate of quantum mechanics [vN55], any isolated quantum system with finite degrees of freedom can be described by a finite-dimensional Hilbert space. We therefore begin by defining what a Hilbert space is.

Since Hilbert spaces build upon vector spaces, we first recall the definition of a vector space. For the vectors, we use the Dirac notation $|\psi\rangle$.

Definition 2.1
A *(complex) vector space* is a nonempty set $\mathcal{H}$ together with two operations:

$$\text{Vector addition } (+) : \mathcal{H} \times \mathcal{H} \rightarrow \mathcal{H}$$

and

$$\text{Scalar multiplication } (\times) : \mathbb{C} \times \mathcal{H} \rightarrow \mathcal{H}$$

satisfying:

1. $(\mathcal{H}, +)$ is an Abelian group,
2. $1|\phi\rangle = |\phi\rangle$,

3. $\lambda(\mu|\phi\rangle) = \lambda\mu|\phi\rangle$,
4. $(\lambda + \mu)|\phi\rangle = \lambda|\phi\rangle + \mu|\phi\rangle$,
5. $\lambda(|\phi\rangle + |\psi\rangle) = \lambda|\phi\rangle + \lambda|\psi\rangle$

for $\lambda, \mu \in \mathbb{C}$ and vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$.

A Hilbert space additionally requires an inner product over the vector space. We write λ^* for $\lambda \in \mathbb{C}$ to denote its complex conjugate. For a state $|\psi\rangle \in \mathcal{H}$, its conjugate transpose is denoted by $\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^*)^\top$.

Definition 2.2
An *inner product* over a vector space $\mathcal{H}$ is a mapping $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ satisfying:

1. $\langle\phi|\phi\rangle \geq 0$ with equality iff $|\phi\rangle = 0$,
2. $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$,
3. $\langle\phi|\lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1\langle\phi|\psi_1\rangle + \lambda_2\langle\phi|\psi_2\rangle$

for $|\phi\rangle, |\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ and $\lambda_1, \lambda_2 \in \mathbb{C}$.

Using the inner product, we define the length of a vector $|\psi\rangle \in \mathcal{H}$ by $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$. A vector $|\psi\rangle$ is called a *unit vector* if $\|\psi\| = 1$. A *pure state* of a quantum system is described by such a unit vector.

Another property we require for a Hilbert space is completeness. It is formulated in terms of Cauchy sequences and convergence.

Definition 2.3
Let $\{|\psi_n\rangle\}_{n\in\mathbb{N}}$ be a sequence of vectors in $\mathcal{H}$. The sequence is called a *Cauchy sequence* if for every $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that

$$\|\psi_m - \psi_n\| < \varepsilon$$

for all $m, n \geq N$.

It *converges* to $|\psi\rangle \in \mathcal{H}$ if for every $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that

$$\|\psi_n - \psi\| < \varepsilon$$

for all $n \geq N$.

Definition 2.4
A *Hilbert space* is a complete inner product space, i.e., a vector space with an inner product, in which every Cauchy sequence converges to a vector in $\mathcal{H}$.

Two vectors $|\phi\rangle$ and $|\psi\rangle$ are *orthogonal*, written $|\phi\rangle \perp |\psi\rangle$, if $\langle\phi|\psi\rangle = 0$.

Definition 2.5
A family $\{|\psi_i\rangle\}_{i\in I}$ of unit vectors is called an *orthonormal basis* of $\mathcal{H}$ if:

1. $|\psi_i\rangle \perp |\psi_j\rangle$ for all $i \neq j$,
2. for every $|\psi\rangle \in \mathcal{H}$, $|\psi\rangle = \sum_{i\in I} \langle\psi_i|\psi\rangle|\psi_i\rangle$.

The cardinality of I is called the dimension of $\mathcal{H}$. Throughout this thesis, all Hilbert spaces are assumed to be finite-dimensional.

Example 2.6
The state space of qubits is the two-dimensional Hilbert space

$$\mathcal{H}_2 = \{\alpha|0\rangle + \beta|1\rangle \mid \alpha, \beta \in \mathbb{C}\}.$$

The inner product of $\alpha|0\rangle + \beta|1\rangle$ and $\alpha'|0\rangle + \beta'|1\rangle$ in $\mathcal{H}_2$ is $\alpha^*\alpha' + \beta^*\beta'$ for $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$. The orthonormal basis $\{|0\rangle, |1\rangle\}$ is called the computational basis, where the vectors are represented in $\mathbb{C}^2$ as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Unlike classical bits, a qubit can exist in a *superposition* of basis states. A reappearing example is $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Quantum programs typically manipulate multiple quantum variables simultaneously. To describe such composite quantum systems, we use the tensor product of Hilbert spaces [Yin11]. For any two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, their tensor product is denoted as $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Linear Operators, Density Operators and Superoperators

As quantum programs manipulate quantum states, we need to formally express these operations. They are mathematically described by (linear) operators acting on Hilbert spaces. In this thesis, we only consider bounded operators:

Definition 2.7
A *bounded (linear) operator* on a Hilbert space $\mathcal{H}$ is a mapping $A : \mathcal{H} \to \mathcal{H}$ satisfying the following properties:

1. $A(|\phi\rangle + |\psi\rangle) = A\,|\phi\rangle + A\,|\psi\rangle$,
2. $A(\lambda\,|\psi\rangle) = \lambda A\,|\psi\rangle$,
3. There exists a constant $C \geq 0$ such that

$$\|A\,|\psi\rangle\| \leq C\,\|\,|\psi\rangle\,\|$$

   for all $|\psi\rangle \in \mathcal{H}$.

Let $\mathcal{L}(\mathcal{H})$ denote the set of bounded linear operators on $\mathcal{H}$. For any operator $A \in \mathcal{L}(\mathcal{H})$, there exists a unique linear operator $A^\dagger$ on $\mathcal{H}$ such that $\langle\varphi|A|\psi\rangle = \langle A^\dagger\varphi|\psi\rangle$ for all $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$. The operator $A^\dagger$ is called the adjoint of A. An operator A on $\mathcal{H}$ is called *positive* if $\langle\psi|A|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$. It is *hermitian* if $A^\dagger = A$ and *unitary* if $A^\dagger A = AA^\dagger = I_\mathcal{H}$, where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$. We use unitary operators to describe the evolution of closed quantum systems.

Example 2.8
Typical unitary operators that appear throughout this thesis are the Pauli X-gate and the controlled-X (or CX) gate. Their matrix representations with respect to the computational basis are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The X-gate exchanges the computational basis states $|0\rangle$ and $|1\rangle$. The CX-gate acts on two qubits and applies the X-gate to the second qubit iff the first qubit is in state $|1\rangle$.

While pure quantum states can be represented by unit vectors, this representation is insufficient for describing probabilistic mixtures of pure states, which can arise in our quantum programs, e.g., due to measurements as defined in the next section. For this reason, we use density operators. A quantum state is represented by a partial density operator ρ on a Hilbert space $\mathcal{H}$, which is defined as a positive operator with a trace satisfying $tr(\rho) \leq 1$. The set of all partial density operators is denoted as $\mathcal{D}(\mathcal{H})$. Every partial density operator ρ can be generated by an ensemble of pure states $\{|\psi_i\rangle\}_i$ with respective probabilities p_i (where $\sum_i p_i \leq 1$), so that $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

An evolution from one quantum state to another is described by a superoperator, i.e., a linear mapping from density operators to density operators, which will be used to describe our program semantics in Sec. 2.2.2. A superoperator $\mathcal{E}$ on $\mathcal{H}$ is completely positive if for any Hilbert space $\mathcal{K}$, the extended operator $\mathcal{E} \otimes I_{\mathcal{K}}$ maps positive operators on $\mathcal{H} \otimes \mathcal{K}$ to positive operators on $\mathcal{H} \otimes \mathcal{K}$. It is trace-nonincreasing if it does not increase the trace of density operators, i.e., $tr(\mathcal{E}(\rho)) \leq tr(\rho)$ for all $\rho \in \mathcal{D}(\mathcal{H})$ and trace-preserving if it preserves the trace of density operators, i.e., $tr(\mathcal{E}(\rho)) = tr(\rho)$ for all $\rho \in \mathcal{D}(\mathcal{H})$. Throughout this thesis, all superoperators are completely positive and trace-nonincreasing.

Quantum Measurements
Measurements in a quantum setting are probabilistic and actively change the quantum state. In this thesis, we only consider projective measurements based on (orthogonal) projections. These projections are a special type of hermitian operators that are idempotent, i.e., $P^2 = P$ for all projections P. Then a measurement on a system with state space $\mathcal{H}$ is described by a finite set of projections $\{P_m\}$ satisfying the normalization condition $\sum_m P_m^\dagger P_m = I_{\mathcal{H}}$.
If the state of a quantum system is represented by a partial density operator ρ immediately before measurement, the probability that result m occurs is $p(m) = tr(P_m^\dagger P_m \rho)$. Following the measurement, the state of the system collapses to $\rho_m = \frac{P_m \rho P_m^\dagger}{p(m)}$.

2.2 Nondeterministic Quantum Programs

Before verifying programs, we need to specify what our programs look like, i.e., the programming language. The language considered throughout this thesis is taken from [FX23] and extends the quantum while language described in [Yin11]. Similar to the classical while-language, it consists of a small collection of primitive statements together with constructs for sequential composition, conditionals and loops. In contrast to the deterministic quantum while language, it additionally includes a nondeterministic choice operator, which models situations where several program fragments may be executed without specifying which one is chosen. This section introduces the syntax and denotational semantics of this language, which will serve as the basis for the weakest precondition transformers developed in the following chapters.

2.2.1 Syntax

Let $\mathcal{V} = \{q, q_1, q_2, \dots\}$ be a finite set of quantum variables, each corresponding to a qubit. For $\mathcal{W} \subseteq \mathcal{V}$, let $\mathcal{H}_\mathcal{W} = \bigotimes_{q\in\mathcal{W}} \mathcal{H}_q$. Here, $\mathcal{H}_q$ is the two-dimensional Hilbert space associated with q and the computational basis $\{|0\rangle_q, |1\rangle_q\}$, whose order is irrelevant, as we use subscripts to distinguish Hilbert spaces with different quantum variables. We write $\overline{q}$ to denote a tuple (and sometimes a set) of distinct quantum variables from $\mathcal{V}$. The syntax of the language is defined inductively by the following grammar:

$$\begin{aligned} S ::= \; & \texttt{skip} \mid \texttt{abort} \mid \overline{q} := 0 \mid \overline{q}{*} = U \mid S_0; S_1 \mid S_0 \Box S_1 \mid \\ & \texttt{if } P[\overline{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end} \mid \texttt{while } P[\overline{q}] \texttt{ do } S_0 \texttt{ end}, \end{aligned}$$

where S, S_0, S_1 are nondeterministic quantum programs, U is a unitary operator and $P[\overline{q}] = \{P, P^\perp\}$ a projective measurement on $\mathcal{H}_{\overline{q}}$. Intuitively, `skip` does nothing, while `abort` represents nontermination. $\overline{q} := 0$ initializes the quantum variables $\overline{q}$ to the state $|0\rangle$, and $\overline{q}{*} = U$ applies the unitary operator U to the quantum variables $\overline{q}$. $S_0; S_1$ executes S_0 followed by S_1, while $S_0 \Box S_1$ represents a nondeterministic choice between executing S_0 or S_1. Finally, `if` $P[\overline{q}]$ `then` S_1 `else` S_0 `end` represents a measurement with two possible outcomes, after which, depending on the outcome, either S_0 or S_1 is executed, and `while` $P[\overline{q}]$ `do` S_0 `end` represents a loop that begins each iteration with a measurement. It executes S_0 for outcome P and terminates for outcome $P^\perp$.

One example of a nondeterministic quantum program is the three-qubit error correction scheme from [FX23], which we will revisit later. It encodes a single qubit q using two ancilla qubits q_1, q_2 and can correct a single bit-flip error on any of the three qubits.

Example 2.9

$$\begin{aligned} \text{ErrCorr} = \quad & q_1, q_2 := 0; \\ & q, q_1{*} = CX; \quad q, q_2{*} = CX; \\ & \texttt{skip} \;\Box\; q{*} = X \;\Box\; q_1{*} = X \;\Box\; q_2{*} = X; \\ & q, q_2{*} = CX; \quad q, q_1{*} = CX; \\ & \texttt{if } P^{=1}[q_2] \texttt{ then} \\ & \quad \texttt{if } P^{=1}[q_1] \texttt{ then} \\ & \quad\quad q{*} = X \\ & \quad \texttt{end} \\ & \texttt{end} \end{aligned}$$

Here, $P^{=1} = |1\rangle\langle 1|$ is the projective measurement according to the computational basis with $(P^{=1})^\perp = |0\rangle\langle 0|$, and `if` $P[q]$ `then` S `end` stands for `if` $P[q]$ `then` S `else skip end`. The nondeterministic choice adds the possibility of a bit-flip error on any of the three qubits nondeterministically.

2.2.2 Denotational Semantics

Quantum programs manipulate quantum variables whose states are represented by density operators on finite-dimensional Hilbert spaces. The semantics of a program is therefore described by completely positive trace-nonincreasing superoperators acting on these density operators. Unlike deterministic programs, a nondeterministic program may admit several possible executions. Its denotational semantics is therefore represented by a set of superoperators rather than a single superoperator, where each superoperator corresponds to one possible execution.

For a program S, let $[\![S]\!]$ denote its denotational semantics, represented as a set of superoperators. The denotational semantics are defined recursively as follows [FX23]:

$$\begin{aligned}
[\![\texttt{skip}]\!] &= \{\mathcal{I}\} \\
[\![\texttt{abort}]\!] &= \{0\} \\
[\![\overline{q} := 0]\!] &= \left\{\mathrm{Set}_{\overline{q}}^{|0\rangle}\right\} \\
[\![\overline{q} {*}= U]\!] &= \{\mathcal{U}_{\overline{q}}\} \\
[\![S_0; S_1]\!] &= [\![S_1]\!] \circ [\![S_0]\!] \\
[\![S_0 \square S_1]\!] &= [\![S_0]\!] \cup [\![S_1]\!] \\
[\![\texttt{if } P[\overline{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end}]\!] &= [\![S_1]\!] \circ \mathcal{P}_{\overline{q}} + [\![S_0]\!] \circ \mathcal{P}_{\overline{q}}^{\perp} \\
[\![\texttt{while } P[\overline{q}] \texttt{ do } S_0 \texttt{ end}]\!] &= \{\sum_{i=0}^{\infty} \mathcal{P}_{\overline{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\overline{q}} \circ \ldots \mathcal{F}_1 \circ \mathcal{P}_{\overline{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}
\end{aligned}$$

Here, $\mathcal{I}$ is the identity and 0 the zero superoperator, corresponding to nontermination. $\mathcal{U}_{\overline{q}}$ is the superoperator corresponding to the unitary operator U operating on $\overline{q}$, i.e., $\mathcal{U}_{\overline{q}}(\rho) = U_{\overline{q}} \rho U_{\overline{q}}^{\dagger}$, which applies the unitary to the quantum variables in $\overline{q}$. For singleton sets, we sometimes write $\mathcal{P}_{\overline{q}}$ instead of $\{\mathcal{P}_{\overline{q}}\}$ for readability. We use subscripts to indicate the quantum variables on which a superoperator acts. For simplicity, we do not distinguish between an operator and its cylindrical extension, which corresponds to the same operation lifted to the whole system. For example, the unitary operator $U_{\overline{q}}$ operates on the quantum variables $\overline{q}$ with the cylindrical extension $U_{\overline{q}} \otimes I_{\mathcal{V}\setminus\overline{q}}$ to $\mathcal{H}_{\mathcal{V}}$. The superoperator $\mathrm{Set}_{\overline{q}}^{|0\rangle}$ is responsible for initializing the quantum variables $\overline{q}$ and sets their state to $|0\rangle_{\overline{q}}$, i.e., $\mathrm{Set}_{\overline{q}}^{|0\rangle}(\rho) = \sum_{i=0}^{|\overline{q}|-1} |0\rangle_{\overline{q}}\langle i|\rho|i\rangle_{\overline{q}}\langle 0|$. The semantics of sequential composition is given by the composition of superoperators. Operations such as composition and addition of sets of superoperators are defined elementwise, i.e., $[\![S_1]\!] \circ [\![S_0]\!] = \{\mathcal{E} \circ \mathcal{F} \mid \mathcal{E} \in [\![S_1]\!], \mathcal{F} \in [\![S_0]\!]\}$. $\mathcal{P}_{\overline{q}}$ and $\mathcal{P}_{\overline{q}}^{\perp}$ are the superoperators corresponding to the projections P and its orthogonal complement $P^{\perp} = I - P$ acting on $\overline{q}$, respectively, for example $\mathcal{P}_{\overline{q}}(\rho) = P_{\overline{q}} \rho P_{\overline{q}}$. Therefore, our measurement corresponds to a projective measurement with two outcomes corresponding to projection P and its orthogonal complement $P^{\perp}$. The resulting state is the probabilistic mixture of the two branches. For the semantics of the loop, $\mathcal{F} = (\mathcal{F}_i)_{i \geq 1} \in [\![S_0]\!]^{\mathbb{N}}$ is a countable infinite sequence of superoperators chosen from $[\![S_0]\!]$ that acts as a scheduler, which chooses one of the superoperators in $[\![S_0]\!]$ for each iteration of the loop. We write $\mathcal{F}_i$ to represent the superoperator chosen for the i-th iteration. Then the semantics of the n-th unfolding of the loop is given by $\sum_{i=0}^{n} \mathcal{P}_{\overline{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\overline{q}} \circ \ldots \mathcal{F}_1 \circ \mathcal{P}_{\overline{q}}$, which corresponds to executing the loop body up to n times, followed by a measurement that exits the loop. This

can be alternatively characterized by nested measurements as follows, which will be useful for correctness proofs regarding the loop transformers:
Let

$$W_0 = \texttt{if } P[\bar{q}] \texttt{ then abort else skip end}$$

and for all $n \geq 0$,

$$W_{n+1} = \texttt{if } P[\bar{q}] \texttt{ then } S_0; W_n \texttt{ else skip end}.$$

Then the semantics of each W_n corresponds exactly to the semantics of the n-th unfolding of the loop, which can be used to approximate the semantics of the loop:

Lemma 2.10
For all $n \geq 0$:

$$[\![W_n]\!] = \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}.$$

Proof of Lemma 2.10.

We prove this by induction on n.

For $n = 0$, we have

$$\{\sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}\} = \{\mathcal{P}_{\bar{q}}^{\perp}\} = \{0\} \circ \{\mathcal{P}\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} = [\![\texttt{if } P[\bar{q}] \texttt{ then abort else skip end}]\!] = [\![W_0]\!].$$

For $n + 1$, we have

$$\begin{aligned}
&\{\sum_{i=0}^{n+1} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\} \\
&\overset{\text{Split}}{=} \{(\sum_{i=1}^{n+1} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}) + \mathcal{P}_{\bar{q}}^{\perp} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\} \\
&\overset{\text{Def. of }+}{=} \{\sum_{i=1}^{n+1} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} \\
&\overset{\text{Reindex}}{=} \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{G}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{G}_1 \circ \mathcal{P}_{\bar{q}} \circ \mathcal{G}_0 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}, \mathcal{F}_{i+1} = \mathcal{G}_i\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} \\
&\overset{\text{Def. of }\circ}{=} \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{G}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{G}_1 \circ \mathcal{P}_{\bar{q}} \circ \mathcal{G}_0 \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}, \mathcal{F}_{i+1} = \mathcal{G}_i\} \circ \{\mathcal{P}_{\bar{q}}\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} \\
&\overset{\text{Def. of }\circ}{=} \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{G}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{G}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{G} \in [\![S_0]\!]^{\mathbb{N}}\} \circ [\![S_0]\!] \circ \{\mathcal{P}_{\bar{q}}\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} \\
&\overset{\text{IH}}{=} [\![W_n]\!] \circ [\![S_0]\!] \circ \{\mathcal{P}_{\bar{q}}\} + \{\mathcal{P}_{\bar{q}}^{\perp}\} \\
&= [\![\texttt{if } P[\bar{q}] \texttt{ then } S_0; W_n \texttt{ else skip end}]\!] \\
&= [\![W_{n+1}]\!].
\end{aligned}$$

□

The next lemma states that the semantics are indeed well-defined, especially that the loop really yields a set of superoperators, which is proven in [FX23]:

Lemma 2.11 ([FX23])
For each program S, $[\![S]\!]$ is a set of trace-nonincreasing superoperators.

Each superoperator $\mathcal{E} \in [\![S]\!]$ represents one possible *execution* of the nondeterministic program. Executing the program on an input state ρ therefore corresponds to applying one of these superoperators to ρ.

Example 2.12
The denotational semantics for Example 2.9 are:

$$\begin{aligned}[\![\texttt{ErrCorr}]\!] = \Big\{ \Big((\mathcal{P}^{=1}_{q_2})^{\perp} + \big(\mathcal{X}_q \circ \mathcal{P}^{=1}_{q_1} + (\mathcal{P}^{=1}_{q_1})^{\perp}\big) \circ \mathcal{P}^{=1}_{q_2} \Big) \circ \mathcal{CX}_{q,q_1} \circ \mathcal{CX}_{q,q_2} \circ \mathcal{U} \\ \circ\, \mathcal{CX}_{q,q_2} \circ \mathcal{CX}_{q,q_1} \circ \mathrm{Set}^{|0\rangle}_{q_1,q_2} \,\Big|\, \mathcal{U} \in \{\mathcal{I}, \mathcal{X}_q, \mathcal{X}_{q_1}, \mathcal{X}_{q_2}\} \Big\},\end{aligned}$$

with

$$\mathcal{P}^{=1}(\rho) = |1\rangle\langle 1|\, \rho \,|1\rangle\langle 1|$$

for all $\rho \in \mathcal{D}(\mathcal{H}_2)$.

Chapter 3

Predicate Transformers

Predicate transformers, first introduced by Dijkstra in 1975 [Dij75], can be used to reason about the behavior of programs and establish correctness properties. Instead of reasoning directly about executions, they transform predicates according to the program statements. The two most common types of predicate transformers are the weakest precondition, which allows backward reasoning, and the strongest postcondition for forward reasoning. In this thesis, we develop weakest preconditions for nondeterministic quantum programs. Intuitively, a weakest precondition contains exactly the initial states from which executing a program guarantees a desired postcondition. The precise meaning of "guarantees" depends on the considered predicates and the weakest precondition variant. It is formalized using Hoare triples.

Definition 3.1
A Hoare triple is a statement of the form $\{P\}S\{Q\}$, where P and Q are predicates (the precondition and postcondition) and S is a program statement. The triple asserts that if the precondition P holds before executing S, then the postcondition Q will hold after executing S.

The exact interpretation of a Hoare triple depends on the type of weakest precondition considered and is given in Chapter 5 and Chapter 6. The weakest precondition of a program statement S with respect to a postcondition Q is the most general precondition P such that the Hoare triple $\{P\}S\{Q\}$ holds. In other words, it captures all initial states from which executing S guarantees that Q will be satisfied afterwards.

Weakest Precondition Variants

For classical nondeterministic programs, the behavior of a nondeterministic program from some initial state can be described by seven equivalence classes: For a deterministic program and a fixed initial state, exactly one of three situations can occur: the program terminates and satisfies the postcondition, the program terminates without satisfying the postcondition or the program does not terminate. The three cases are illustrated in Fig. 3.2. Nondeterminism allows several executions from the same initial state, so combinations of these three behaviors become possible. For instance, one execution may satisfy the postcondition while another fails to terminate. Altogether, this yields seven equivalence classes of behavior as shown in Fig. 3.1. Depending on which of these behaviors are considered acceptable, different types of weakest preconditions can be defined. According to [VK25], weakest preconditions for classical nondeterministic programs can be classified along two dimensions:

The first distinction concerns termination.

- The *weakest liberal precondition* characterizes partial correctness. It guarantees the postcondition whenever the program terminates, but does not require termination.
- The *weakest precondition* characterizes total correctness. Besides establishing the postcondition, it additionally guarantees that the program execution terminates.

The second distinction concerns nondeterministic programs. If a program admits several possible executions from the same initial state, correctness can be interpreted in two different ways.

- In the *demonic* case, all possible executions must satisfy the desired postcondition.
- In the *angelic* case, it is sufficient that at least one execution satisfies the postcondition.

Combining these two dimensions yields four different variants of weakest preconditions: demonic weakest preconditions (dwp), demonic weakest liberal preconditions (dwlp), angelic weakest preconditions (awp) and angelic weakest liberal preconditions (awlp). For example, the demonic weakest liberal precondition (dwlp) of a program statement S with respect to a postcondition Q is the most general precondition P such that if P holds before executing S, then whenever S terminates, Q will hold afterwards, and this must be true for all possible executions of S. The resulting classification is summarized in Fig. 3.1.

Adapting these ideas to the quantum setting, measurements additionally introduce probabilistic branching. In our case, measurement outcomes are not treated as sources of nondeterminism and have no influence on the choice. Instead, all probabilistic branches are required to satisfy the postcondition. Therefore, we can split the possible behaviors of a nondeterministic quantum program for a given initial state into seven equivalence classes again: For one execution, we either have that all branches terminate and satisfy the postcondition, all terminating branches satisfy the postcondition (but not all or even any have to terminate) or some branch terminates and does not satisfy the postcondition. These three classes mirror the three classes from the classical case, which is illustrated in Fig. 3.2. Like in the classical case, we additionally can have their combinations due to nondeterminism, which yields seven classes. The corresponding weakest precondition variants are defined analogously to the classical case. The analogous quantum classification is shown in Fig. 3.3.

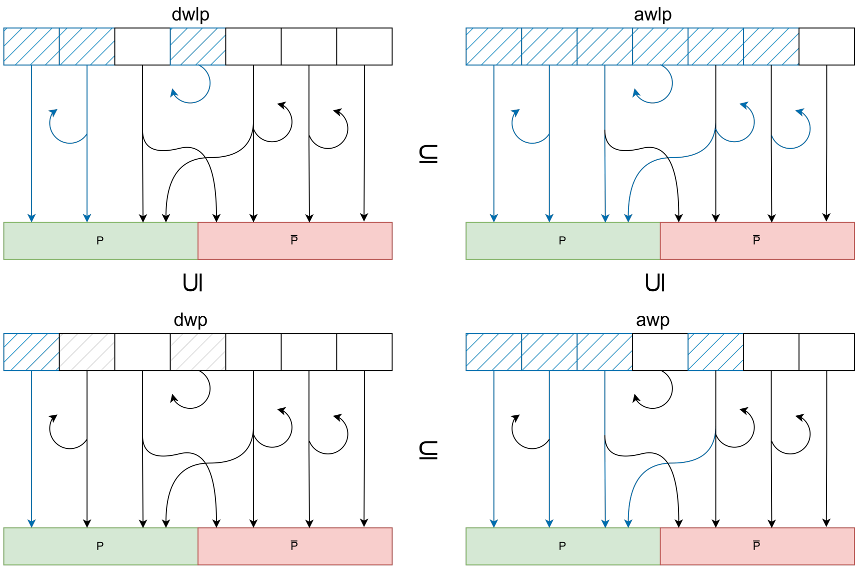

Figure 3.1: Overview of weakest precondition variants in the classical case and their relationships [VK25]. The marked boxes indicate the initial states included in the corresponding weakest precondition. The loop stands for nontermination and the branching for nondeterminism.

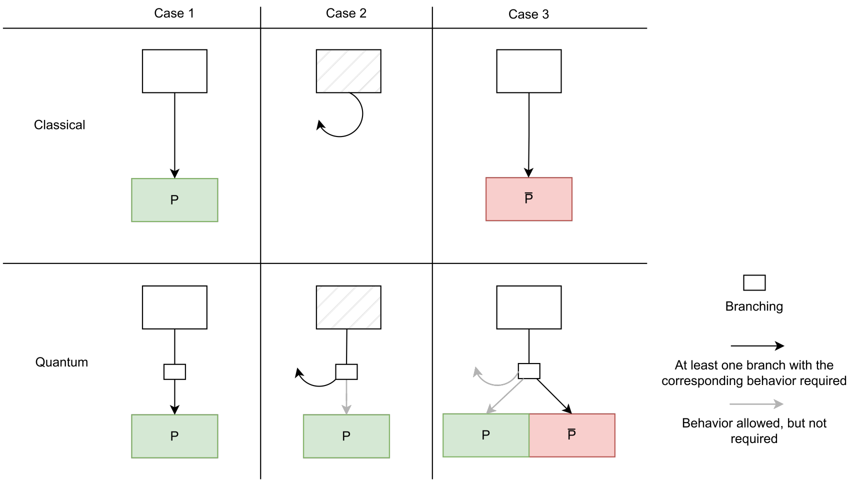

Figure 3.2: Overview of the three possible behaviors for a single execution in the classical case and the corresponding quantum case. Again, the loop stands for nontermination. The box represents probabilistic branching.

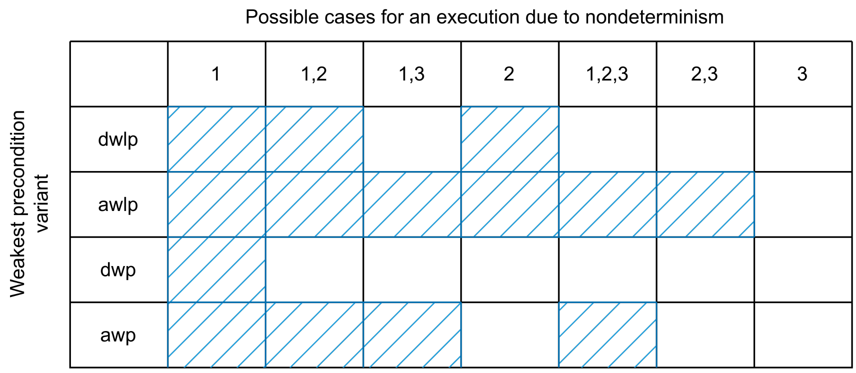

Figure 3.3: Overview of weakest precondition variants in the quantum case. The cases are illustrated in Fig. 3.2. The included initial states for each transformer, again indicated by the marked boxes, are exactly as in the classical case from Fig. 3.1.

Chapter 4

Predicates

Predicates allow us to express properties of quantum states, which can then be used to reason about quantum programs. To define predicate transformers for quantum programs, we require a formal definition of a quantum predicate. Two common types of predicates often used are *quantitative* hermitian operators [FX23] and *qualitative* projections [FZXX26], which intuitively represent sets of quantum states. Since projections naturally represent subspaces of a Hilbert space, they provide the basis for our qualitative approach. We therefore start with projections before introducing our new predicate domain based on sets of projections. For the rest of this chapter, let $\mathcal{H}$ be a fixed finite-dimensional Hilbert space, and let all projections be projections on $\mathcal{H}$ unless stated otherwise.

4.1 Projections

Projections provide a useful basis for predicates because they can be used to represent subspaces of Hilbert spaces, as there is a one-to-one correspondence between projections and closed subspaces in Hilbert spaces [FZXX26]. We first define what it means for a quantum state to satisfy a projection.

Definition 4.1
Let P be an (orthogonal) projection on $\mathcal{H}$. We write $\rho \models P$ to say that the state $\rho \in \mathcal{D}(\mathcal{H})$ satisfies P. This is defined as follows:

$$\rho \models P \text{ iff } P\rho P^\dagger = \rho.$$

Example 4.2
For state $\rho = |0\rangle\langle 0|$ and a projection $P = |0\rangle\langle 0|$, we have

$$P\rho P^\dagger = |0\rangle\langle 0|\,|0\rangle\langle 0|\,|0\rangle\langle 0| = |0\rangle\langle 0| = \rho,$$

so $\rho \models P$. The identity projection I is satisfied by all states, as $I\rho I^\dagger = \rho$ for all ρ and the zero projection 0 is only satisfied by 0, as $0\rho 0^\dagger = 0 \neq \rho$ for all $\rho \neq 0$.

The satisfaction relation also has a useful characterization in terms of the support of a quantum state. For this we define $\mathrm{supp}(\rho)$, the *support* of state ρ, which contains all pure states that ρ is a mixture of:

Definition 4.3
For a state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \in \mathcal{D}(\mathcal{H})$:

$$\mathrm{supp}(\rho) = \mathrm{span}(\{|\psi_i\rangle \mid p_i > 0\}).$$

This definition is independent of the choice of the $|\psi_i\rangle$ [Unr19].
With this, we can also characterize the satisfaction relation between states and projections by looking at the subspace represented by the projection and the support of the state. Which of these characterizations we use depends on the context and what is more convenient to use.

Lemma 4.4
For state ρ and projection P, we have

$$\rho \models P \overset{(1)}{\Longleftrightarrow} P\rho P^\dagger = \rho \overset{(2)}{\Longleftrightarrow} P\rho P = \rho \overset{(3)}{\Longleftrightarrow} P\rho = \rho \overset{(4)}{\Longleftrightarrow} \mathrm{supp}(\rho) \subseteq P.$$

Note that we write the same symbol, here P, for the projection and its corresponding subspace. While the last occurrence of P denotes the subspace, the other ones denote the projection. The intended meaning should be clear from the context.

Proof of Lemma 4.4.

The first two equivalences follow immediately from the definition of satisfaction together with the fact that orthogonal projections are hermitian. For the third equivalence, we have:

"$\Rightarrow$" Assume that $P\rho P = \rho$. Then

$$P\rho = P(P\rho P) \xRightarrow{P\cdot P = P} P\rho = P\rho P = \rho.$$

"$\Leftarrow$" Assume that $P\rho = \rho$. Since ρ is a positive operator, it is hermitian [Yin11]. As P is an orthogonal projector, it is also hermitian, so taking adjoints of both sides of $P\rho = \rho$ yields

$$(P\rho)^\dagger = \rho^\dagger P^\dagger = \rho^\dagger \Rightarrow \rho P = \rho$$

and therefore

$$P\rho P = P\rho = \rho.$$

For the last equivalence, we show $P\rho P = \rho \Leftrightarrow \mathrm{supp}(\rho) \subseteq P$.
"$\Rightarrow$" Assume that $P\rho P = \rho$ with $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ and $p_i > 0$ for all i. Take $v \in \ker(P)$, where $\ker(P)$ denotes the kernel (null space) of P, i.e., $\ker(P) = \{v \in \mathcal{H} \mid Pv = 0\}$. Since $Pv = 0$,

$$0 = \langle 0|0\rangle = \langle Pv|\rho|Pv\rangle = \langle v|P\rho P|v\rangle = \langle v|\rho|v\rangle.$$

Using $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ and $\langle v|\psi_i\rangle = \langle\psi_i|v\rangle^*$, we have

$$\begin{aligned} 0 &= \langle v|\rho|v\rangle \\ &= \left\langle v \middle| \sum_i p_i|\psi_i\rangle\langle\psi_i| \middle| v \right\rangle \\ &= \sum_i p_i\langle v|\psi_i\rangle\langle\psi_i|v\rangle \\ &= \sum_i p_i \left|\langle\psi_i|v\rangle\right|^2 . \end{aligned}$$

Because each term in the sum is non-negative and all $p_i > 0$, we have

$$\langle\psi_i|v\rangle = 0 \qquad \text{for all } i \text{ and all } v \in \ker(P).$$

So each $|\psi_i\rangle$ is orthogonal to $\ker(P)$ and thus $|\psi_i\rangle \in (\ker(P))^\perp$. Because P is an orthogonal projection, we have $(\ker(P))^\perp = P$. So $|\psi_i\rangle \in P$ for all i and

$$\mathrm{span}(\{|\psi_i\rangle\}_i) = \mathrm{supp}(\rho) \subseteq P.$$

"$\Leftarrow$" Assume that $\mathrm{supp}(\rho) \subseteq P$. Then every $|\psi_i\rangle$ with $p_i > 0$ lies in the subspace of P, so

$$P|\psi_i\rangle = |\psi_i\rangle.$$

Therefore,

$$P\rho P = \sum_i p_i\, P|\psi_i\rangle\langle\psi_i|P = \sum_i p_i\, |\psi_i\rangle\langle\psi_i| = \rho.$$

$\square$

Thus, a state satisfies a projection P if its support lies entirely inside the subspace represented by P.

Example 4.5
For state $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ and projection $P = |0\rangle\langle 0|$, we have $\rho \nvDash P$, as $\mathrm{supp}(\rho) = \mathrm{span}(\{|0\rangle, |1\rangle\}) \nsubseteq \mathrm{span}(\{|0\rangle\})$.

To construct predicate transformers, we need to combine predicates using logical operations. Two of them are $\vee$ for disjunction and $\wedge$ for conjunction from the Birkhoff-von Neumann quantum logic [BvN36][Yin22], which are defined as follows:

Definition 4.6
For two projections P and Q:

$$P \vee Q = \mathrm{span}(P \cup Q)$$

and

$$P \wedge Q = P \cap Q.$$

Example 4.7
For example, $|0\rangle\langle 0| \vee |1\rangle\langle 1| = \text{span}(\{|0\rangle, |1\rangle\}) = I$ and
$|0\rangle\langle 0| \wedge |1\rangle\langle 1| = \text{span}(\{|0\rangle\}) \cap \text{span}(\{|1\rangle\}) = 0$.

In general, $P \vee Q$ is defined as the closure of $\text{span}(P \cup Q)$. Since all subspaces of finite-dimensional Hilbert spaces are closed [Unr19], this simplifies to the above definition. Intuitively, $P \vee Q$ is the smallest subspace that contains both P and Q, while $P \wedge Q$ is the largest subspace that is contained in both P and Q.

Additionally, we want to be able to express implications in case of measurements. Ordinary implication is not suitable for reasoning about quantum measurements because a measurement splits the state into two branches. When verifying one branch, we only want the postcondition to hold for the part of the state that actually reaches this branch. The remaining part is handled separately by the other branch and should not be restricted by the postcondition of this branch. To express this, we use the Sasaki implication [GGN17] like it was done in [FZXX26].

Definition 4.8
For projections P and Q, the Sasaki implication is defined by

$$P \rightsquigarrow Q = P^{\perp} \vee (P \wedge Q).$$

Example 4.9
For example, $|0\rangle\langle 0| \rightsquigarrow |1\rangle\langle 1| = (|0\rangle\langle 0|)^{\perp} \vee (|0\rangle\langle 0| \wedge |1\rangle\langle 1|) = |1\rangle\langle 1| \vee 0 = |1\rangle\langle 1|$.

The following lemma shows that the Sasaki implications indeed behave as we intended, i.e., it only imposes the postcondition Q to the part of the state ρ that lies in P.

Lemma 4.10
For a state $\rho \in \mathcal{D}(\mathcal{H})$ and projections P and Q:

$$\rho \models P \rightsquigarrow Q \quad \text{iff} \quad P\rho P \models Q.$$

Proof of Lemma 4.10.

Let

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

be a state where $p_i > 0$ for all i. Then

$$\begin{aligned}
& \rho \models P \rightsquigarrow Q \\
\iff & \text{supp}(\rho) \subseteq \text{span}(P^{\perp} \cup (P \cap Q)) \\
\iff & \forall i: \ |\psi_i\rangle \in \text{span}(P^{\perp} \cup (P \cap Q)) \\
\overset{(*)}{\iff} & \forall i: \ P|\psi_i\rangle \in P \cap Q \\
\iff & \forall i: \ P|\psi_i\rangle \in Q \\
\iff & \text{supp}(P\rho P) \subseteq Q
\end{aligned}$$

$$\iff P\rho P \models Q.$$

(*) holds as every state can be decomposed as $|\psi_i\rangle = P|\psi_i\rangle + P^{\perp}|\psi_i\rangle$ [FZXX26]. □

Furthermore, measurements produce probabilistic mixtures of quantum states. Consequently, we would like predicates to satisfy the following property: If each branch of a measurement satisfies a predicate, then their resulting mixture should satisfy it as well. Conversely, if a mixture satisfies a predicate, then each component should also satisfy it. Projections have exactly this property because they are closed under linear combinations and decomposition. In fact, for finite-dimensional Hilbert spaces they are the only predicates with this property [Unr18].

Lemma 4.11
For states $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H})$ and a projection P:

$$\rho_1 + \rho_2 \models P \text{ iff } \rho_1 \models P \wedge \rho_2 \models P.$$

Proof of Lemma 4.11.

Let

$$\rho_1 = \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right|, \rho_2 = \sum_i q_i \left|\phi_i\right\rangle\!\left\langle\phi_i\right| \text{ with } p_i, q_i > 0 \text{ for all i.}$$

"⇒":

Assume $\rho_1 + \rho_2 \models P$.

Then

$$\begin{aligned}
& \operatorname{supp}(\rho_1 + \rho_2) \subseteq P \\
\Leftrightarrow \quad & \operatorname{supp}\left(\sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right| + \sum_i q_i \left|\phi_i\right\rangle\!\left\langle\phi_i\right|\right) \subseteq P \\
\Rightarrow \quad & \operatorname{span}\big(\{\psi_i\}_i, \{\phi_i\}_i\big) \subseteq P \\
\Rightarrow \quad & \operatorname{span}\big(\{\psi_i\}_i\big) \subseteq P \ \wedge \ \operatorname{span}\big(\{\phi_i\}_i\big) \subseteq P \\
\Rightarrow \quad & \rho_1 \models P \ \wedge \ \rho_2 \models P.
\end{aligned}$$

"⇐": Assume $\rho_1 \models P$ and $\rho_2 \models P$.

Then

$$\operatorname{span}\big(\{\psi_i\}_i\big) \subseteq P \ \wedge \ \operatorname{span}\big(\{\phi_i\}_i\big) \subseteq P$$

and thus

$$\operatorname{span}\big(\{\psi_i\}_i, \{\phi_i\}_i\big) \subseteq P$$

as P is a closed subspace.
As $\operatorname{span}\big(\{\psi_i\}_i, \{\phi_i\}_i\big)$ is the support of $\rho_1 + \rho_2$, we get $\rho_1 + \rho_2 \models P$.

□

The "$\Leftarrow$" direction of the previous lemma extends naturally to countable sums as shown in the next lemma. This extension will be needed later when reasoning about loops, since denotational semantics are defined as an infinite (but countable) sum over loop unfoldings.

Lemma 4.12
For projection P and state $\rho = \sum_{n=0}^{\infty} \rho_n \in \mathcal{D}(\mathcal{H})$, we have

$$\forall n : \rho_n \models P \implies \rho \models P.$$

Proof of Lemma 4.12.

$$\begin{aligned}
&\forall n : \rho_n \models P \\
\implies &\forall n : P\rho_n = \rho_n \\
\implies &P\rho = P\left(\sum_{n=0}^{\infty} \rho_n\right) \overset{\text{Linearity}}{=} \sum_{n=0}^{\infty} P\rho_n = \sum_{n=0}^{\infty} \rho_n = \rho \\
\implies &\rho \models P.
\end{aligned}$$

□

Lastly, to derive the weakest precondition for initialization, we need to determine the initial states of the remaining quantum variables without the initialized variables, as the initialized ones are set to $|0\rangle$. For this, we need exactly the states that, after setting the initialized variable to $|0\rangle$, still satisfy the postcondition. This leads to the following construction:

Definition 4.13
Let $\mathcal{V}$ be a finite set of quantum variables and $\bar{q} \subseteq \mathcal{V}$. Let P be a projection on $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\mathcal{V}\setminus\bar{q}}$. We define

$$\lceil P \rceil_{\bar{q}} = \left\{ |\psi\rangle \in \mathcal{H}_{\mathcal{V}\setminus\bar{q}} \;\middle|\; |0\rangle_{\bar{q}} \otimes |\psi\rangle \models P \right\}.$$

We show that this construction can be used for our predicates by showing that it is a closed subspace. As we use the same symbol for projections and their corresponding subspace, $\lceil P \rceil_{\bar{q}}$ will sometimes be used as a projection later.

Lemma 4.14
For a finite set of quantum variables $\mathcal{V}$, $\bar{q} \subseteq \mathcal{V}$ and projection P on $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\mathcal{V}\setminus\bar{q}}$, $\lceil P \rceil_{\bar{q}}$ is a closed subspace of $\mathcal{H}_{\mathcal{V}\setminus\bar{q}}$.

Proof of Lemma 4.14.

Let $|\psi_1\rangle, |\psi_2\rangle \in \lceil P \rceil_{\bar{q}}$ and let $\alpha, \beta \in \mathbb{C}$. By definition,

$$|0\rangle_{\bar{q}} \otimes |\psi_1\rangle,\ |0\rangle_{\bar{q}} \otimes |\psi_2\rangle \in P.$$

Since P is a subspace,

$$\alpha\left(|0\rangle_{\bar{q}} \otimes |\psi_1\rangle\right) + \beta\left(|0\rangle_{\bar{q}} \otimes |\psi_2\rangle\right) \in P.$$

Using the bilinearity of the tensor product,

$$\alpha\left(|0\rangle_{\bar{q}} \otimes |\psi_1\rangle\right) + \beta\left(|0\rangle_{\bar{q}} \otimes |\psi_2\rangle\right) = |0\rangle_{\bar{q}} \otimes \left(\alpha|\psi_1\rangle + \beta|\psi_2\rangle\right).$$

Hence,

$$|0\rangle_{\bar{q}} \otimes (\alpha|\psi_1\rangle + \beta|\psi_2\rangle) \in P,$$

which implies

$$\alpha|\psi_1\rangle + \beta|\psi_2\rangle \in \lceil P \rceil_{\bar{q}}.$$

Therefore, $\lceil P \rceil_{\bar{q}}$ is a linear subspace. Since all subspaces of finite-dimensional Hilbert spaces are closed [Unr19], $\lceil P \rceil_{\bar{q}}$ is closed.

$\square$

4.2 Sets of Projections as Predicates

The previous section showed that projections provide natural qualitative quantum predicates. However, they can only represent subspaces of a Hilbert space. For angelic nondeterminism, this is no longer sufficient because the set of states satisfying a weakest precondition does not have to form a subspace.

Example 4.15
Consider the quantum program $S = q{*} = I \,\square\, q{*} = X$ for one qubit q and postcondition $|0\rangle\langle 0|$.

The angelic weakest liberal precondition (formally defined in Sec. 5.1) is satisfied exactly by those states $\rho \in \mathcal{D}(\mathcal{H}_2)$ for which $\mathcal{I}(\rho) \models |0\rangle\langle 0|$ or $\mathcal{X}(\rho) \models |0\rangle\langle 0|$, which are exactly the states satisfying $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$. This set of states is not a subspace because any subspace containing $|0\rangle$ and $|1\rangle$ also contains their linear combinations, e.g. $|+\rangle$.

This is why we introduce sets of projections as predicates:

Definition 4.16
A *(quantum) predicate* is a nonempty set of projections.

The empty set is excluded because we want state $\rho = 0$ to satisfy all predicates to mirror the behavior of single projections. Thus, in this thesis, all sets of projections are assumed to be nonempty.

Example 4.17
The set of projections $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ is the predicate that describes the weakest precondition for Example 4.15.

For a set of projections Θ, we define the satisfaction relation as follows:

Definition 4.18
For a predicate Θ and a state $\rho \in \mathcal{D}(\mathcal{H})$:

$$\rho \models \Theta \text{ iff } \exists M \in \Theta : \rho \models M.$$

Thus, a state satisfies a set of projections whenever it satisfies at least one projection in that set. For singleton sets, we sometimes write M instead of $\{M\}$ for readability.

Example 4.19
For the predicate from Example 4.17, we get $|0\rangle\langle 0| \models \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, because $|0\rangle\langle 0| \models |0\rangle\langle 0|$.
However, for $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, $\rho \not\models \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ as $\rho \not\models |0\rangle\langle 0|$ and $\rho \not\models |1\rangle\langle 1|$.

Remark 4.20
Another possible definition for satisfaction would be requiring every projection in the predicate to be satisfied, i.e., $\forall M \in \Theta : \rho \models M$. However, this is equivalent to taking the conjunction $\wedge$ of every projection in that set, which will be shown in Lemma 4.23. The issue with this approach (or taking the disjunction $\vee$ of every projection in the predicate) is that it always yields a closed subspace, which is exactly what we want to avoid.

Since our predicates are now sets of projections, we also need to extend the logical operations introduced in the previous section, which is done in an element-wise way:

Definition 4.21
Let $\{\Theta_i\}_i$ be a set of predicates. Then

$$\bigwedge_i \Theta_i = \left\{ \bigwedge_i M_i \;\middle|\; M_i \in \Theta_i \text{ for all } i \right\}$$

and

$$\bigvee_i \Theta_i = \left\{ \bigvee_i M_i \;\middle|\; M_i \in \Theta_i \text{ for all } i \right\}.$$

Example 4.22
For example, we get

$$\{|0\rangle\langle 0|, |1\rangle\langle 1|\} \wedge \{I, 0\} = \{|0\rangle\langle 0| \wedge I, |0\rangle\langle 0| \wedge 0, |1\rangle\langle 1| \wedge I, |1\rangle\langle 1| \wedge 0\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|, 0\}.$$

The following lemma shows that our definition of the quantum conjunction on sets of projections behaves as a logical conjunction. In particular, a state satisfies the conjunction of a set of predicates if and only if it satisfies each predicate individually:

Lemma 4.23
Let $\{\Theta_i\}_i$ be a set of predicates. Then for every state $\rho \in \mathcal{D}(\mathcal{H})$,

$$\rho \models \bigwedge_i \Theta_i \text{ iff } \forall i : \; \rho \models \Theta_i.$$

Proof of Lemma 4.23.

$$\begin{aligned}
&\rho \models \bigwedge_i \Theta_i \\
\iff& \forall i : \exists M_i \in \Theta_i : \rho \models \bigwedge_i M_i \\
\iff& \forall i : \exists M_i \in \Theta_i : \mathrm{supp}(\rho) \subseteq \bigcap_i M_i \\
\iff& \forall i : \exists M_i \in \Theta_i : \mathrm{supp}(\rho) \subseteq M_i \\
\iff& \forall i : \exists M_i \in \Theta_i : \rho \models M_i \\
\iff& \forall i : \rho \models \Theta_i .
\end{aligned}$$

□

Remark 4.24
Note that this does not hold for the quantum disjunction, i.e., $\rho \models \bigvee_i \Theta_i$ iff $\exists i : \ \rho \models \Theta_i$ does not hold. In fact, this already fails for single projections: For example for $\rho = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$, $\rho \models |0\rangle \langle 0| \vee |1\rangle \langle 1|$, but $\rho \not\models |0\rangle \langle 0|$ and $\rho \not\models |1\rangle \langle 1|$. This is exactly the reason that the quantum disjunction fails to capture angelic nondeterminism.

Additionally, we show that the Sasaki implication preserves its intended meaning for sets of projections.

Lemma 4.25
For a state $\rho \in \mathcal{D}(\mathcal{H})$, projection P and predicate Θ:

$$\rho \models P \rightsquigarrow \Theta \quad \text{iff} \quad P\rho P \models \Theta .$$

Proof of Lemma 4.25.

$$\begin{aligned}
&\rho \models P \rightsquigarrow \Theta \\
\Leftrightarrow\ & \rho \models P^{\perp} \vee (P \wedge \Theta) \\
\Leftrightarrow\ & \exists M \in \Theta : \rho \models P^{\perp} \vee (P \wedge M) \\
\xLeftrightarrow{\textit{Lemma } 4.10}\ & \exists M \in \Theta : P\rho P \models M \\
\Leftrightarrow\ & P\rho P \models \Theta .
\end{aligned}$$

□

Up to this point, there are multiple predicates that are satisfied by exactly the same states: $\{I, |0\rangle\langle 0|\}$ and $\{I, |1\rangle\langle 1|\}$ are both satisfied by all states as all states satisfy I. Therefore we define equivalence classes:

Definition 4.26
We say two predicates Θ and Ψ are *equivalent* iff for all states $\rho \in \mathcal{D}(\mathcal{H})$:

$$\rho \models \Theta \quad \Longleftrightarrow \quad \rho \models \Psi.$$

From this definition, reflexivity, symmetry and transitivity follow directly.

Example 4.27
The predicates $\{I, |0\rangle\langle 0|\}$ and $\{I, |1\rangle\langle 1|\}$ are equivalent, as all states satisfy both predicates.

For the rest of this thesis, whenever we talk about the predicates, we always mean the corresponding equivalence class.

As the goal of this thesis is to reason about weakest preconditions, we need to be able to compare the predicates. Therefore, we define an ordering of predicates:

Definition 4.28
For predicates Θ, Ψ, we say Θ is *weaker* than Ψ (Ψ is *stronger* than Θ), written $\Psi \sqsubseteq \Theta$, iff

$$\forall \rho \in \mathcal{D}(\mathcal{H}) : \rho \models \Psi \implies \rho \models \Theta.$$

Example 4.29
A predicate can be weakened by enlarging its set of projections. As with single projections, the identity predicate $\{I\}$ is the weakest predicate. For example,

$$\{|1\rangle\langle 1|, |0\rangle\langle 0|\} \sqsubseteq \{|1\rangle\langle 1|, |0\rangle\langle 0|, |+\rangle\langle +|\} \sqsubseteq \{I\}.$$

Next, we show that this relation defines a partial order on our predicates. The antisymmetry of this order then implies that the weakest precondition, if it exists, is unique.

Theorem 4.30
$\sqsubseteq$ (as defined in Def. 4.28) is a partial order on the set of predicates.

Proof of Theorem 4.30.

Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.
1. **Reflexivity**:
For any predicate Θ, we have $\rho \models \Theta \implies \rho \models \Theta$, so $\Theta \sqsubseteq \Theta$.
2. **Antisymmetry**:
Suppose $\Theta \sqsubseteq \Psi$ and $\Psi \sqsubseteq \Theta$. Then we have $\rho \models \Theta \implies \rho \models \Psi$ and $\rho \models \Psi \implies \rho \models \Theta$. Thus, $\rho \models \Theta \iff \rho \models \Psi$, which means Θ and Ψ are equivalent, so $\Theta = \Psi$.
3. **Transitivity**:
Suppose $\Theta \sqsubseteq \Psi$ and $\Psi \sqsubseteq \Phi$. Then we have $\rho \models \Theta \implies \rho \models \Psi$ and $\rho \models \Psi \implies \rho \models \Phi$. Therefore, $\rho \models \Theta \implies \rho \models \Phi$, so $\Theta \sqsubseteq \Phi$. ∎

Furthermore, one can show that our predicate domain with respect to the partial order forms a complete lattice, which means that we can find least upper and greatest lower bounds for any subset of predicates. In our case, we can find a predicate that exactly describes all states satisfying at least one of the predicates or all of them, respectively.

Theorem 4.31
The set of all predicates with the partial order $\sqsubseteq$ forms a complete lattice. The join of a set of predicates $\{\Psi_i\}_i$ is given by $\bigcup_i \Psi_i$ and the meet by $\bigwedge_i \Psi_i$.

Proof of Theorem 4.31.

We show that $\bigcup_i \Psi_i$ and $\bigwedge_i \Psi_i$ are join and meet.

1. For a set of sets of projections $\{\Psi_i\}_i$, we have $\Psi \sqsubseteq \bigcup_i \Psi_i$ for all $\Psi \in \{\Psi_i\}_i$:

$$\rho \models \Psi \implies \exists M \in \Psi : \rho \models M \implies \exists M \in \bigcup_i \Psi_i : \rho \models M \implies \rho \models \bigcup_i \Psi_i.$$

Therefore $\bigcup_i \Psi_i$ is an upper bound of $\{\Psi_i\}_i$. If Θ is another upper bound, then $\Psi_i \sqsubseteq \Theta$ for all i and $\bigcup_i \Psi_i \sqsubseteq \Theta$: If there was a state $\rho \in \mathcal{D}(\mathcal{H})$ such that $\rho \models \bigcup_i \Psi_i$, but $\rho \not\models \Theta$, then ρ would satisfy some M in some Ψ_i, but not satisfy any M in Θ, which contradicts the assumption that $\Psi_i \sqsubseteq \Theta$ for all i. Hence, $\bigcup_i \Psi_i$ is the least upper bound, i.e., the join.

2. For a set of sets of projections $\{\Psi_i\}_i$, we have $\bigwedge_i \Psi_i \sqsubseteq \Psi$ for all $\Psi \in \{\Psi_i\}_i$:

$$\rho \models \bigwedge_i \Psi_i \xRightarrow{\textit{Lemma } 4.23} \forall i : \exists M \in \Psi_i : \rho \models M \implies \exists M \in \Psi : \rho \models M \implies \rho \models \Psi.$$

so $\bigwedge_i \Psi_i$ is a lower bound of $\{\Psi_i\}_i$. If Θ is another lower bound, then $\Theta \sqsubseteq \Psi_i$ for all i and $\Theta \sqsubseteq \bigwedge_i \Psi_i$: If there was a state $\rho \in \mathcal{D}(\mathcal{H})$ such that $\rho \models \Theta$, but $\rho \not\models \bigwedge_i \Psi_i$, then there would be some i such that ρ does not satisfy any M in Ψ_i, but satisfies some M in Θ, which contradicts the assumption that $\Theta \sqsubseteq \Psi_i$ for all i. Hence, $\bigwedge_i \Psi_i$ is the greatest lower bound, i.e., the meet. ☐

Remark 4.32
One might wonder if we can define the join as the pairwise join (the disjunction) of the projections, as we are doing in the meet. However, we then get $\{|0\rangle\langle 0|\} \vee \{|1\rangle\langle 1|\} = \{I\}$. By allowing sets of projections as predicates, we can find a stronger predicate, which is an upper bound, namely $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Using the usual intersection as the meet does not work directly either: $\{|0\rangle\langle 0|\} \cap \{I\} = \emptyset$ but $|0\rangle\langle 0| \models \{|0\rangle\langle 0|\}$ and $|0\rangle\langle 0| \models \{I\}$, so we would expect $|0\rangle\langle 0|$ to be included in their meet. This is because we are always talking about sets of quantum states and $\bigcup$ and $\bigwedge$ are how we get their intersection and union on predicate level. Of course, if we look at the corresponding subspaces, we do get their natural intersection and union. Additionally, we can see that with this definition of the meet, we can never get the empty set as a predicate, as 0 is always included in all subspaces.

Chapter 5

Weakest Liberal Precondition

With our predicate domain fixed, we can move on to the weakest precondition transformers. We begin with the weakest liberal preconditions, which means that we do not require termination. This is also referred to as *partial correctness.* This chapter develops the weakest liberal precondition transformers for nondeterministic quantum programs. We first consider the angelic interpretation of nondeterminism and then the demonic interpretation. For each transformer, we define the corresponding notion of correctness, present the inductive transformer rules and prove their correctness. For the rest of this thesis, let $\mathcal{V}$ be the finite set of quantum variables in our considered system with $\mathcal{H} = \mathcal{H}_{\mathcal{V}}$, and let all projections be projections on $\mathcal{H}$ unless specified otherwise.

5.1 Angelic Weakest Liberal Precondition

The angelic weakest liberal precondition describes the weakest precondition that guarantees that there exists at least one execution of the program such that, if that execution terminates, the postcondition holds. Unlike the demonic case, correctness only has to be established for one possible execution rather than for all executions and unlike the non-liberal case, we allow nontermination. Therefore, we define the correctness of a Hoare triple $\{\Theta\}\ S\ \{\Psi\}$ in the angelic liberal case as follows:

Definition 5.1
Let Θ, Ψ be predicates and S a program. Then

$$\models^{ang}_{par} \{\Theta\}\ S\ \{\Psi\} \text{ iff } \forall \rho \in \mathcal{D}(\mathcal{H}) : \rho \models \Theta \implies \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.$$

With this, we can define the angelic weakest liberal precondition:

Definition 5.2
Let S be a quantum program and Ψ a postcondition. The *angelic weakest liberal precondition* of Ψ with respect to S, if it exists, is the unique quantum predicate $\text{awlp}(S, \Psi)$ such that:
1. Validity:

$$\models^{ang}_{par} \{\text{awlp}(S, \Psi)\}\ S\ \{\Psi\}$$

2. Weakest: For any predicate Θ:

$$\models^{ang}_{par} \{\Theta\}\ S\ \{\Psi\} \implies \Theta \sqsubseteq \mathrm{awlp}(S, \Psi).$$

The first condition establishes that we have a valid precondition, while the second guarantees that the predicate is the weakest among all valid liberal preconditions.

Using this definition, we can now give the rules for calculating the angelic weakest liberal precondition of a quantum program S and postcondition Ψ inductively. The transformer rule for the loop is only proven for loops with finite denotational semantics for their bodies, i.e., for every loop `while` $P[\bar{q}]$ `do` S_0 `end`, $[\![S_0]\!]$ is finite. This can be guaranteed, for example, by disallowing nested loops. Whether the rule also holds for general loops remains future work.

Theorem 5.3
Assume that every loop body has finite denotational semantics. Then the angelic weakest liberal precondition of a quantum program S with respect to a postcondition Ψ is given inductively by the following equations:

1. $\mathrm{awlp}(\texttt{skip}, \Psi) = \Psi$
2. $\mathrm{awlp}(\texttt{abort}, \Psi) = \{I\}$
3. $\mathrm{awlp}(\bar{q} \mathrel{*}= U, \Psi) = \{U_{\bar{q}}^{\dagger}\, M\, U_{\bar{q}} \mid M \in \Psi\}$
4. $\mathrm{awlp}(\bar{q} := 0, \Psi) = \{I_{\bar{q}} \otimes \lceil M \rceil_{\bar{q}} \mid M \in \Psi\}$
5. $\mathrm{awlp}(S_0; S_1, \Psi) = \mathrm{awlp}\big(S_0, \mathrm{awlp}(S_1, \Psi)\big)$
6. $\mathrm{awlp}(\texttt{if}\ P[\bar{q}]\ \texttt{then}\ S_1\ \texttt{else}\ S_0\ \texttt{end}, \Psi) =$
   $\bigcup_{M\in\Psi} (P_{\bar{q}} \rightsquigarrow \mathrm{awlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{awlp}(S_0, M))$
7. $\mathrm{awlp}(S_0 \,\square\, S_1, \Psi) = \mathrm{awlp}(S_0, \Psi) \cup \mathrm{awlp}(S_1, \Psi)$
8. $\mathrm{awlp}(\texttt{while}\ P[\bar{q}]\ \texttt{do}\ S_0\ \texttt{end}, \Psi) = \bigcup_{M\in\Psi} \bigwedge_{n\geq 0} \Psi_n^M$,
   $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{awlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$,
   $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \mathrm{awlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$

The rules for `skip`, $\bar{q} \mathrel{*}= U$ and $\bar{q} := 0$ can be understood as reversing the corresponding program operations when computing the weakest liberal precondition. Since `abort` does not terminate, every initial state satisfies its weakest liberal precondition, so it is I. For measurements, the idea is to impose separate conditions on the different measurement branches. The part of the state corresponding to the outcome P must satisfy the weakest liberal precondition of S_1, expressed by $(P_{\bar{q}} \rightsquigarrow \mathrm{awlp}(S_1, M))$, and likewise the other branch must satisfy $(P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{awlp}(S_0, M))$. We have the same projection M for both branches due to Lemma 4.11 and then iterate over all projections in the postcondition. The rule for the nondeterministic choice takes the union of the initial states satisfying the weakest liberal preconditions of the individual choices, since in the angelic case, the postcondition only has to hold for one of the choices. For loops, due to Lemma 4.11 again, each terminating iteration has to satisfy the same projection. This is why we calculate the weakest liberal precondition for a fixed projection and take the union over all projections in our postcondition afterwards. For a projection M, the predicates Ψ_n^M describe the weakest liberal preconditions of the finite unfoldings of the loop, i.e., the states from which either the M is satisfied or the loop has not terminated after n iterations. Therefore, we approximate the weakest liberal precondition for the full loop and projection M from above and decrease the set of initial states in each iteration until we reach the awlp.

The correctness of the transformer rules follows immediately from the following theorem. Validity is ensured by "$\Rightarrow$" and the weakest property by "$\Leftarrow$".

Theorem 5.4
For all programs S and states $\rho \in \mathcal{D}(\mathcal{H})$, $\rho \models \text{awlp}(S, \Psi) \Leftrightarrow \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi$.

Proof of Theorem 5.4.

We prove this by induction over the structure of S. Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.

Case skip: For $S = \texttt{skip}$, we have $[\![S]\!] = \{\mathcal{E}\}$ with $\mathcal{E}(\rho) = \rho$ and $\text{awlp}(S, \Psi) = \Psi$:

$$\rho \models \text{awlp}(S, \Psi) \Leftrightarrow \rho \models \Psi \Leftrightarrow \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.$$

Case abort: For $S = \texttt{abort}$, we have $[\![S]\!] = \{\mathcal{E}\}$ with $\mathcal{E}(\rho) = 0$ and $\text{awlp}(S, \Psi) = \{I\}$:

$$\begin{aligned} & \rho \models \text{awlp}(S, \Psi) \\ \Leftrightarrow\ & \rho \models \{I\} \quad (I \cdot \rho = \rho \text{ for all } \rho \in \mathcal{D}(\mathcal{H}).) \\ \Leftrightarrow\ & 0 \models \Psi \quad (M \cdot 0 = 0 \text{ for all projections } M \text{ and } \Psi \text{ is nonempty.}) \\ \Leftrightarrow\ & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi. \end{aligned}$$

Case unitary: For $S = \bar{q} *= U$, we have $[\![S]\!] = \{\mathcal{E}\}$ with $\mathcal{E}(\rho) = U_{\bar{q}} \rho U_{\bar{q}}^\dagger$ and $\text{awlp}(S, \Psi) = \{U_{\bar{q}}^\dagger \, M \, U_{\bar{q}} \mid M \in \Psi\}$:

$$\begin{aligned} & \rho \models \text{awlp}(S, \Psi) \\ \Leftrightarrow\ & \rho \models \{U_{\bar{q}}^\dagger \, M \, U_{\bar{q}} \mid M \in \Psi\} \\ \Leftrightarrow\ & \exists M \in \Psi : \rho \models U_{\bar{q}}^\dagger \, M \, U_{\bar{q}} \\ \Leftrightarrow\ & \exists M \in \Psi : U_{\bar{q}}^\dagger \, M \, U_{\bar{q}} \rho (U_{\bar{q}}^\dagger \, M \, U_{\bar{q}})^\dagger = \rho \\ \Leftrightarrow\ & \exists M \in \Psi : U_{\bar{q}}^\dagger \, M \, U_{\bar{q}} \rho U_{\bar{q}}^\dagger \, M^\dagger \, U_{\bar{q}} = \rho \\ \Leftrightarrow\ & \exists M \in \Psi : M U_{\bar{q}} \rho U_{\bar{q}}^\dagger M^\dagger = U_{\bar{q}} \rho U_{\bar{q}}^\dagger \\ \Leftrightarrow\ & U_{\bar{q}} \rho U_{\bar{q}}^\dagger \models \Psi \\ \Leftrightarrow\ & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi. \end{aligned}$$

Case initialization: Let $\bar{q} \subseteq \mathcal{V}$ and state

$$\rho = \sum_j p_j |\phi_j\rangle\langle\phi_j|$$

with $p_j > 0$.

Since

$$\left\{ |i\rangle_{\bar{q}} \right\}_{i=0}^{2^{|\bar{q}|}-1}$$

forms an orthonormal basis of $\mathcal{H}_{\bar{q}}$, every vector in $\mathcal{H}_{\bar{q}} \otimes \mathcal{H}_{\mathcal{V}\setminus\bar{q}}$ has a unique decomposition of the form

$$|\phi_j\rangle = \sum_{i=0}^{2^{|\bar{q}|}-1} |i\rangle_{\bar{q}} \otimes |\phi_{ji}\rangle\,,$$

for suitable vectors $|\phi_{ji}\rangle \in \mathcal{H}_{\mathcal{V}\setminus\bar{q}}$.

Then for S $= \bar{q} := 0$, we have $[\![S]\!] = \{\mathcal{E}\}$ with $\mathcal{E}(\rho) = \sum_{i=0}^{|\bar{q}|-1} |0\rangle_{\bar{q}}\langle i|\rho|i\rangle_{\bar{q}}\langle 0|$ and $\operatorname{awlp}(\bar{q} := 0, \Psi) = \{I_{\bar{q}} \otimes \lceil M\rceil_{\bar{q}} \mid M \in \Psi\}$:

$$\begin{aligned}
& \rho \models \operatorname{awlp}(S, \Psi) \\
\iff & \rho \models \{I_{\bar{q}} \otimes \lceil M\rceil_{\bar{q}} \mid M \in \Psi\} \\
\iff & \exists M \in \Psi : \rho \models I_{\bar{q}} \otimes \lceil M\rceil_{\bar{q}} \\
\iff & \exists M \in \Psi : \operatorname{supp}(\rho) \subseteq I_{\bar{q}} \otimes \lceil M\rceil_{\bar{q}} \\
\iff & \exists M \in \Psi : \left\{|\phi_{ji}\rangle \mid i \in \{0,\dots,2^{|\bar{q}|}-1\}, j\right\} \subseteq \lceil M\rceil_{\bar{q}} \\
\iff & \exists M \in \Psi : \forall i \in \{0,\dots,2^{|\bar{q}|}-1\}, j : |\phi_{ji}\rangle \in \lceil M\rceil_{\bar{q}} \\
\iff & \exists M \in \Psi : \forall i \in \{0,\dots,2^{|\bar{q}|}-1\}, j : |0\rangle_{\bar{q}} \otimes |\phi_{ji}\rangle \in M \\
\iff & \exists M \in \Psi : \operatorname{span}\left\{|0\rangle_{\bar{q}} \otimes |\phi_{ji}\rangle \mid i \in \{0,\dots,2^{|\bar{q}|}-1\}, j\right\} \subseteq M \\
\iff & \exists M \in \Psi : \operatorname{supp}\left(\sum_{i=0}^{2^{|\bar{q}|}-1} \sum_j p_j\big(|0\rangle_{\bar{q}} \otimes |\phi_{ji}\rangle\big)\big(\langle 0|_{\bar{q}} \otimes \langle\phi_{ji}|\big)\right) \subseteq M \\
\overset{|0\rangle_{\bar{q}}\langle i||\phi_j\rangle = |0\rangle_{\bar{q}}\otimes|\phi_{ji}\rangle}{\iff} & \exists M \in \Psi : \operatorname{supp}\left(\sum_{i=0}^{2^{|\bar{q}|}-1} \sum_j p_j\big(|0\rangle_{\bar{q}}\langle i||\phi_j\rangle\big)\big(\langle\phi_j||i\rangle_{\bar{q}}\langle 0|\big)\right) \subseteq M \\
\iff & \exists M \in \Psi : \operatorname{supp}\left(\sum_{i=0}^{2^{|\bar{q}|}-1} |0\rangle_{\bar{q}}\langle i| \left(\sum_j p_j|\phi_j\rangle\langle\phi_j|\right) |i\rangle_{\bar{q}}\langle 0|\right) \subseteq M \\
\iff & \exists M \in \Psi : \operatorname{supp}\left(\sum_{i=0}^{2^{|\bar{q}|}-1} |0\rangle_{\bar{q}}\langle i|\rho|i\rangle_{\bar{q}}\langle 0|\right) \subseteq M \\
\iff & \exists M \in \Psi : \sum_{i=0}^{2^{|\bar{q}|}-1} |0\rangle_{\bar{q}}\langle i|\rho|i\rangle_{\bar{q}}\langle 0| \models M \\
\iff & \mathcal{E}(\rho) \models \Psi.
\end{aligned}$$

Case sequence: For S $= S_0; S_1$, we have $[\![S]\!] = [\![S_1]\!] \circ [\![S_0]\!]$ and $\operatorname{awlp}(S, \Psi) = \operatorname{awlp}\big(S_0, \operatorname{awlp}(S_1, \Psi)\big)$:

$$\begin{aligned}
& \rho \models \operatorname{awlp}(S, \Psi) \\
\iff & \rho \models \operatorname{awlp}\big(S_0, \operatorname{awlp}(S_1, \Psi)\big) \\
\overset{IH}{\iff} & \exists \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \operatorname{awlp}(S_1, \Psi) \\
\overset{IH}{\iff} & \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \\
\iff & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}$$

Case measurement: For S = `if` $P[\bar{q}]$ `then` S_1 `else` S_0 `end`, we have $[\![S]\!] = [\![S_1]\!] \circ \mathcal{P}_{\bar{q}} + [\![S_0]\!] \circ \mathcal{P}_{\bar{q}}^{\perp}$ and $\operatorname{awlp}(S, \Psi) = \bigcup_{M \in \Psi} (P_{\bar{q}} \rightsquigarrow \operatorname{awlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \operatorname{awlp}(S_0, M))$:

$$
\begin{aligned}
& \rho \models \operatorname{awlp}(S, \Psi) \\
\iff\ & \rho \models \bigcup_{M \in \Psi} \Big((P_{\bar{q}} \rightsquigarrow \operatorname{awlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \operatorname{awlp}(S_0, M)) \Big) \\
\xLeftrightarrow{\textit{Lemma 4.23}}\ & \exists M \in \Psi : \rho \models (P_{\bar{q}} \rightsquigarrow \operatorname{awlp}(S_1, M)) \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow \operatorname{awlp}(S_0, M)) \\
\xLeftrightarrow{\textit{Lemma 4.25}}\ & \exists M \in \Psi : P_{\bar{q}} \rho P_{\bar{q}} \models \operatorname{awlp}(S_1, M) \wedge P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp} \models \operatorname{awlp}(S_0, M) \\
\xLeftrightarrow{\text{IH}}\ & \exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}}) \models M \wedge \mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp}) \models M \\
\xLeftrightarrow{\textit{Lemma 4.11}}\ & \exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}}) + \mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp}) \models M \\
\iff\ & \exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \\
\xLeftrightarrow{\text{Def. + of operators}}\ & \exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \\
\iff\ & \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \exists M \in \Psi : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \\
\iff\ & \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models \Psi \\
\iff\ & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}
$$

Case nondeterministic choice: For $S = S_0 \,\square\, S_1$, we have $[\![S]\!] = [\![S_0]\!] \cup [\![S_1]\!]$ and $\operatorname{awlp}(S, \Psi) = \operatorname{awlp}(S_0, \Psi) \cup \operatorname{awlp}(S_1, \Psi)$:

$$
\begin{aligned}
& \rho \models \operatorname{awlp}(S, \Psi) \\
\iff\ & \rho \models \operatorname{awlp}(S_0, \Psi) \cup \operatorname{awlp}(S_1, \Psi) \\
\iff\ & \exists M \in \operatorname{awlp}(S_0, \Psi) : \rho \models M \vee \exists M \in \operatorname{awlp}(S_1, \Psi) : \rho \models M \\
\iff\ & \rho \models \operatorname{awlp}(S_0, \Psi) \vee \rho \models \operatorname{awlp}(S_1, \Psi) \\
\xLeftrightarrow{\textit{IH}}\ & \exists \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \Psi \vee \exists \mathcal{E}_1 \in [\![S_1]\!] : \mathcal{E}_1(\rho) \models \Psi \\
\iff\ & \exists \mathcal{E} \in [\![S_0]\!] \cup [\![S_1]\!] : \mathcal{E}(\rho) \models \Psi \\
\iff\ & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}
$$

Case loop: We first show that the recursively defined predicate Ψ_n^M is precisely the awlp of the finite unfolding W_n of the loop for a projection M.

Lemma 5.5
For $[\![W_n]\!] = \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$, $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \operatorname{awlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$ and $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \operatorname{awlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$, we have for all $n \geq 0$ and all $M \in \Psi$:

$$\operatorname{awlp}(W_n, M) = \Psi_n^M.$$

Proof of Lemma 5.5.

We show this by induction on n.

For $n = 0$, we show

$$\rho \models \text{awlp}(W_0, M) \Leftrightarrow \exists \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M$$

for all states ρ.
We have $[\![W_0]\!] = \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}$ and $\text{awlp}(W_0, M) = \Psi_0^M = (P_{\bar{q}} \rightsquigarrow \text{awlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$:

$$\begin{aligned}
& \rho \models \text{awlp}(W_0, M) \\
\Longleftrightarrow\ & \rho \models (P_{\bar{q}} \rightsquigarrow \text{awlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\overset{(*)}{\Longleftrightarrow}\ & \rho \models (P_{\bar{q}} \rightsquigarrow I) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\Longleftrightarrow\ & \rho \models P_{\bar{q}}^{\perp} \rightsquigarrow M \\
\xLeftrightarrow{\textit{Lemma 4.25}}\ & \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \\
\Longleftrightarrow\ & \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \\
\Longleftrightarrow\ & \exists \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M.
\end{aligned}$$

(*) holds as $\rho \models I \iff \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models I$ and thus $\text{awlp}(S, I) = I$ for all programs S.

For $n + 1$:
Using $[\![W_{n+1}]\!] = [\![\texttt{if}\ P\ \texttt{then}\ S_0; W_n\ \texttt{else skip end}]\!]$ from Lemma 2.10, we obtain

$$\begin{aligned}
\text{awlp}(W_{n+1}, M) &= \text{awlp}(\texttt{if}\ P\ \texttt{then}\ S_0; W_n\ \texttt{else skip end}, M) \\
&= (P_{\bar{q}} \rightsquigarrow \text{awlp}(S_0; W_n, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M).
\end{aligned} \tag{5.1}$$

Using the rule for sequential composition, we get $\text{awlp}(S_0; W_n, M) = \text{awlp}(S_0, \text{awlp}(W_n, M))$ and together with the induction hypothesis $\text{awlp}(S_0; W_n, M) = \text{awlp}(S_0, \Psi_n^M)$. Replacing this in Eq. (5.1) gives us

$$\text{awlp}(W_{n+1}, M) = (P_{\bar{q}} \rightsquigarrow \text{awlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) = \Psi_{n+1}^M.$$

□

Next, we show that $\bigwedge_{n \geq 0} \Psi_n^M$ is the angelic weakest liberal precondition for a single projection M, which we will generalize for sets of projections later.

Lemma 5.6
For S = $\texttt{while}\ P[\bar{q}]\ \texttt{do}\ S_0\ \texttt{end}$, projection M and state $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$\rho \models \bigwedge_{n \geq 0} \Psi_n^M \iff \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M.$$

Proof of Lemma 5.6.

"⇒":
Assume $\rho \models \bigwedge_{n\geq 0} \Psi_n^M$. It is

$$\begin{aligned}\rho \models \bigwedge_{n\geq 0} \Psi_n^M &\xLeftrightarrow{\textit{Lemma 4.23}} \forall n \geq 0 : \rho \models \Psi_n^M \\ &\xLeftrightarrow{\textit{Lemma 5.5}} \forall n \geq 0\ \exists \mathcal{G} \in [\![W_n]\!] : \mathcal{G}(\rho) \models M.\end{aligned} \tag{5.2}$$

We show that this implies $\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M$, i.e., we can find $(\mathcal{F}_i)_{i\geq 1} \in [\![S_0]\!]^{\mathbb{N}}$ such that

$$\mathcal{E} = \sum_{i=0}^{\infty} \mathcal{E}_i,$$

where $\mathcal{E}_i = \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}$ with $\mathcal{E}_0 = \mathcal{P}_{\bar{q}}^{\perp}$. For each $n \geq 0$, let T_n denote the set of all finite sequences $(\mathcal{F}_1, \ldots, \mathcal{F}_n) \in [\![S_0]\!]^n$ such that

$$\left(\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}\right)(\rho) \models M.$$

We then call $(\mathcal{F}_1, \ldots, \mathcal{F}_n) \in [\![S_0]\!]^n$ successful. By Equivalence 5.2, every T_n is nonempty. Furthermore, if $\left(\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}\right)(\rho) \models M$, then, by Lemma 4.11, $\left(\sum_{i=0}^{n-1} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}\right)(\rho) \models M$. So if $(\mathcal{F}_1, \ldots, \mathcal{F}_n) \in T_n$, then we have $(\mathcal{F}_1, \ldots, \mathcal{F}_{n-1}) \in T_{n-1}$ for its prefix.

As we restrict the program to loops where $[\![S_0]\!]$ is finite, there are only finitely many possible choices for the first superoperator, which means at least one $\mathcal{F}_1 \in [\![S_0]\!]$ occurs as the first element of successful sequences of arbitrarily large length: Otherwise every possible first choice would only occur in successful sequences up to some finite length. Taking the maximum of these finitely many bounds would imply that there exists a maximal length of a successful sequence, contradicting the fact that $T_n \neq \emptyset$ for every n.

Having fixed $\mathcal{F}_1$, consider only successful sequences beginning with $\mathcal{F}_1$. Again, since $[\![S_0]\!]$ is finite, there exists a choice of $\mathcal{F}_2$ such that $(\mathcal{F}_1, \mathcal{F}_2)$ is the prefix of successful sequences of arbitrarily large length.

Proceeding inductively, we obtain an infinite sequence $(\mathcal{F}_i)_{i\geq 1} \in [\![S_0]\!]^{\mathbb{N}}$ such that every finite prefix $(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ belongs to T_n. Consider

$$\mathcal{E} = \sum_{i=0}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}.$$

Since every terminating finite unfolding of the loop satisfies M, it follows from Lemma 4.12 that $\mathcal{E}(\rho) \models M$. Hence, $\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M$.

"⇐":
Assume $\exists \mathcal{E} \in [\![S]\!] : \ \mathcal{E}(\rho) \models M$. Then there exists $\mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}$ such that

$$\mathcal{E} = \sum_{i=0}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \in [\![S]\!].$$

For $n \geq 0$, let $\mathcal{E}_n \in [\![W_n]\!]$ be

$$\mathcal{E}_n = \sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}.$$

By assumption, $\mathcal{E}(\rho) \models M$. Hence, by Lemma 4.11 and $\mathcal{E}(\rho) = \mathcal{E}_n + \sum_{i=n+1}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}(\rho)$, we get $\mathcal{E}_n(\rho) \models M$ and therefore

$$\forall n \geq 0 \, \exists \mathcal{E}_n \in [\![W_n]\!] : \mathcal{E}_n(\rho) \models M.$$

Therefore

$$\begin{aligned} & \forall n \geq 0 : \exists \mathcal{E}_n \in [\![W_n]\!] : \mathcal{E}_n(\rho) \models M \\ \xLeftrightarrow{\textit{Lemma 5.5}} \; & \forall n \geq 0 : \rho \models \Psi_n^M \\ \xLeftrightarrow{\textit{Lemma 4.23}} \; & \rho \models \bigwedge_{n \geq 0} \Psi_n^M. \end{aligned}$$

□

From this, the correctness of the whole loop rule follows directly: For S = `while` $P[\bar{q}]$ `do` S_0 `end`, we have $[\![S]\!] = \{\sum_{i=0}^{\infty} P_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ P_{\bar{q}} \circ \ldots \mathcal{F}_1 \circ P_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$ and $\mathrm{awlp}(S, \Psi) = \bigcup_{M \in \Psi} \bigwedge_{n \geq 0} \Psi_n^M$:

$$\begin{aligned} & \rho \models \mathrm{awlp}(S, \Psi) \\ \iff \; & \rho \models \bigcup_{M \in \Psi} \bigwedge_{n \geq 0} \Psi_n^M \\ \iff \; & \exists M \in \Psi : \rho \models \bigwedge_{n \geq 0} \Psi_n^M \\ \xLeftrightarrow{\textit{Lemma 5.6}} \; & \exists M \in \Psi : \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M \\ \iff \; & \exists \mathcal{E} \in [\![S]\!] : \exists M \in \Psi : \mathcal{E}(\rho) \models M \\ \iff \; & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi. \end{aligned}$$

□

5.2 Demonic Weakest Liberal Precondition

The demonic weakest liberal precondition describes the weakest precondition that guarantees for *all* possible executions that all terminating branches satisfy the postcondition. In contrast to the angelic case, we have to look at all executions of a program and in contrast to the non-liberal case, the demonic weakest liberal precondition allows the program to not terminate. Therefore, we define the correctness of a Hoare triple $\{\Theta\}\ S\ \{\Psi\}$ in the demonic liberal case as follows:

Definition 5.7
Let Θ, Ψ be predicates and S a program. Then

$$\models^{dem}_{par} \{\Theta\}\ S\ \{\Psi\} \text{ iff } \forall \rho \in \mathcal{D}(\mathcal{H}) : \rho \models \Theta \implies \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.$$

With this, we can define the demonic weakest liberal precondition:

Definition 5.8
Let S be a quantum program and Ψ a postcondition. The *demonic weakest liberal precondition* of Ψ with respect to S, if it exists, is the unique quantum predicate $\mathrm{dwlp}(S, \Psi)$ such that:
1. Validity:
$$\models^{dem}_{par} \{\mathrm{dwlp}(S, \Psi)\}\ S\ \{\Psi\}$$
2. Weakest: For any predicate Θ:
$$\models^{dem}_{par} \{\Theta\}\ S\ \{\Psi\} \implies \Theta \sqsubseteq \mathrm{dwlp}(S, \Psi).$$

Using this definition, we can now give the rules for calculating the demonic weakest liberal precondition of a quantum program S and postcondition Ψ with one element $\Psi = \{M\}$ inductively. The transformer is only defined for singleton postconditions because measurements introduce difficulties when predicates contain several projections, which is explained further at the end of Sec. 5.2.

Theorem 5.9
The demonic weakest liberal precondition of a quantum program S and singleton postcondition $\Psi = \{M\}$ can be given inductively by the following equations:

1. $\mathrm{dwlp}(\texttt{skip}, \Psi) = \Psi$
2. $\mathrm{dwlp}(\texttt{abort}, \Psi) = \{I\}$
3. $\mathrm{dwlp}(\bar{q} *= U, \Psi) = \{U_{\bar{q}}^{\dagger}\, M\, U_{\bar{q}} \mid M \in \Psi\}$
4. $\mathrm{dwlp}(\bar{q} := 0, \Psi) = \{I_{\bar{q}} \otimes \lceil M \rceil_{\bar{q}} \mid M \in \Psi\}$
5. $\mathrm{dwlp}(S_0; S_1, \Psi) = \mathrm{dwlp}\big(S_0, \mathrm{dwlp}(S_1, \Psi)\big)$
6. $\mathrm{dwlp}(\texttt{if } P[\bar{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end}, \Psi) =$
   $(P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, M))$
7. $\mathrm{dwlp}(S_0 \,\square\, S_1, \Psi) = \mathrm{dwlp}(S_0, \Psi) \wedge \mathrm{dwlp}(S_1, \Psi)$

8. $\mathrm{dwlp}(\texttt{while}\ P[\bar{q}]\ \texttt{do}\ S_0\ \texttt{end}, \Psi) = \bigwedge_{n\geq 0} \Psi_n^M$,
   $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$,
   $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$

Remark 5.10
If we always start with only one projection in the postcondition, the transformer will always yield a singleton set again, as none of the operations increase the number of projections in the predicate. Therefore, we can use these rules to calculate the dwlp for any program as long as the postcondition is a singleton set.

Note that compared to the angelic case, the main difference is the nondeterministic choice, as this is exactly where we have to distinguish how we want to deal with nondeterministic behavior. The rule for nondeterministic choice takes the intersection of the initial states satisfying the weakest liberal preconditions of the individual choices, since we are in the demonic case, which means that the postcondition must hold for every possible choice. Additionally, the measurement and loop rules are only correct for singleton postconditions, which is why there is no union over every projection in our postcondition anymore. Similar to Sec. 5.1, we prove the correctness of the rules using the following theorem. As previously, validity is ensured by "$\Rightarrow$" and the weakest property by "$\Leftarrow$".

Theorem 5.11
For all programs S and states $\rho \in \mathcal{D}(\mathcal{H})$, $\rho \models \mathrm{dwlp}(S, \Psi) \Leftrightarrow \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi$.

Proof of Theorem 5.11.

We prove this by induction on the structure of S. Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.

Cases skip, abort, unitary, initialization: As for all four base cases, there exists exactly one superoperator $\mathcal{E} \in [\![S]\!]$, we do not have nondeterminism in these cases and the weakest liberal preconditions and proofs are the same as in the proof of Theorem 5.4.

Case sequence: For S $= S_0; S_1$, we have $[\![S]\!] = [\![S_1]\!] \circ [\![S_0]\!]$ and $\mathrm{dwlp}(S, \Psi) = \mathrm{dwlp}\big(S_0, \mathrm{dwlp}(S_1, \Psi)\big)$:

$$\begin{aligned}
&\rho \models \mathrm{dwlp}(S, \Psi) \\
\Longleftrightarrow\ &\rho \models \mathrm{dwlp}\big(S_0, \mathrm{dwlp}(S_1, \Psi)\big) \\
\overset{IH}{\Longleftrightarrow}\ &\forall \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \mathrm{dwlp}(S_1, \Psi) \\
\overset{IH}{\Longleftrightarrow}\ &\forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \\
\Longleftrightarrow\ &\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}$$

Case measurement: For S $= \texttt{if}\ P[\bar{q}]\ \texttt{then}\ S_1\ \texttt{else}\ S_0\ \texttt{end}$, we have $[\![S]\!] = [\![S_1]\!] \circ \mathcal{P}_{\bar{q}} + [\![S_0]\!] \circ \mathcal{P}_{\bar{q}}^{\perp}$ and $\mathrm{dwlp}(S, \Psi) = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, M))$:

$$\begin{aligned}
&\rho \models \mathrm{dwlp}(S, \Psi) \\
\Longleftrightarrow\ &\rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, M)) \\
\overset{Lemma\ 4.23}{\Longleftrightarrow}\ &\rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, M)) \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, M))
\end{aligned}$$

$$
\begin{aligned}
&\xLeftrightarrow{\textit{Lemma } 4.25} P_{\bar{q}}\rho P_{\bar{q}} \models \mathrm{dwlp}(S_1, M) \wedge P_{\bar{q}}^{\perp}\rho P_{\bar{q}}^{\perp} \models \mathrm{dwlp}(S_0, M) \\
&\xLeftrightarrow{\text{IH}} \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}}) \models M \wedge \mathcal{E}_0(P_{\bar{q}}^{\perp}\rho P_{\bar{q}}^{\perp}) \models M \\
&\xLeftrightarrow{\textit{Lemma } 4.11} \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}}) + \mathcal{E}_0(P_{\bar{q}}^{\perp}\rho P_{\bar{q}}^{\perp}) \models M \\
&\iff \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \\
&\xLeftrightarrow{\text{Def. } + \text{ of operators}} \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \\
&\iff \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \{M\} \\
&\iff \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}
$$

Case nondeterministic choice: For $S = S_0 \,\square\, S_1$, we have $[\![S]\!] = [\![S_0]\!] \cup [\![S_1]\!]$ and $\mathrm{dwlp}(S, \Psi) = \mathrm{dwlp}(S_0, \Psi) \wedge \mathrm{dwlp}(S_1, \Psi)$:

$$
\begin{aligned}
&\rho \models \mathrm{dwlp}(S, \Psi) \\
\iff\ &\rho \models \mathrm{dwlp}(S_0, \Psi) \wedge \mathrm{dwlp}(S_1, \Psi) \\
\xLeftrightarrow{\textit{Lemma } 4.23}\ &\rho \models \mathrm{dwlp}(S_0, \Psi) \wedge \rho \models \mathrm{dwlp}(S_1, \Psi) \\
\xLeftrightarrow{\textit{IH}}\ &\forall \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \Psi \wedge \forall \mathcal{E}_1 \in [\![S_1]\!] : \mathcal{E}_1(\rho) \models \Psi \\
\iff\ &\forall \mathcal{E} \in [\![S_0]\!] \cup [\![S_1]\!] : \mathcal{E}(\rho) \models \Psi \\
\iff\ &\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.
\end{aligned}
$$

Case loop: We start by showing that the recursively defined predicates Ψ_n^M are precisely the demonic weakest liberal preconditions of the finite unfoldings W_n of the loop.

Lemma 5.12
Let $[\![W_n]\!] = \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$, $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$ and $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$. For all $n \geq 0$,

$$\mathrm{dwlp}(W_n, M) = \Psi_n^M$$

holds.

Proof of Lemma 5.12.

The proof is analogous to the one for the angelic transformer in the proof of Lemma 5.5. We again proceed by induction on n.

For $n = 0$, we show

$$\rho \models \mathrm{dwlp}(W_0, M) \Leftrightarrow \forall \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M$$

for all states ρ.
We have $[\![W_0]\!] = \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}$ and $\mathrm{dwlp}(W_0, \Psi) = \Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$:

$$
\begin{aligned}
&\rho \models \mathrm{dwlp}(W_0, M) \\
\iff\ &\rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, I)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(*)}{\iff} \rho \models P_{\bar{q}} \rightsquigarrow I \wedge P_{\bar{q}}^{\perp} \rightsquigarrow M \\
&\iff \rho \models P_{\bar{q}}^{\perp} \rightsquigarrow M \\
&\overset{\textit{Lemma 4.25}}{\iff} \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \\
&\iff \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \\
&\iff \forall \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M.
\end{aligned}
$$

(*) holds as $\rho \models I \iff \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models I$ and thus $\mathrm{dwlp}(S, I) = I$ for all programs S.

For $n+1$:
Using $[\![W_{n+1}]\!] = [\![\texttt{if } P[\bar{q}] \texttt{ then } S_0; W_n \texttt{ else skip end}]\!]$ from Lemma 2.10, we obtain

$$
\begin{aligned}
\mathrm{dwlp}(W_{n+1}, M) &= \mathrm{dwlp}(\texttt{if } P[\bar{q}] \texttt{ then } S_0; W_n \texttt{ else skip end}, M) \\
&= (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0; W_n, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M).
\end{aligned}
\tag{5.3}
$$

Using the rule for sequential composition, we get $\mathrm{dwlp}(S_0; W_n, M) = \mathrm{dwlp}(S_0, \mathrm{dwlp}(W_n, M))$ and together with the induction hypothesis $\mathrm{dwlp}(S_0; W_n, M) = \mathrm{dwlp}(S_0, \Psi_n^M)$. Replacing this in Eq. (5.3) gives us

$$\mathrm{dwlp}(W_{n+1}, M) = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) = \Psi_{n+1}^M.$$

□

For the correctness of the whole loop rule, we have S = $\texttt{while } P[\bar{q}] \texttt{ do } S_0 \texttt{ end}$, $[\![S]\!] = \{\sum_{i=0}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \dots \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$ and $\mathrm{dwlp}(S, \Psi) = \bigwedge_{n \geq 0} \Psi_n^M$: We show

$$\rho \models \bigwedge_{n \geq 0} \Psi_n^M \iff \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi.$$

"$\Rightarrow$":
Assume $\rho \models \bigwedge_{n \geq 0} \Psi_n^M$. For an arbitrary $\mathcal{E} \in [\![S]\!]$, we show that $\mathcal{E}(\rho) \models M$:
Let $\mathcal{E} \in [\![S]\!]$, then there exists a sequence $(\mathcal{F}_i)_{i \geq 1} \in [\![S_0]\!]^{\mathbb{N}}$ such that

$$\mathcal{E} = \sum_{i=0}^{\infty} \mathcal{E}_i,$$

where

$$\mathcal{E}_i = \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \dots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}.$$

For every $n \geq 0$,

$$\sum_{i=0}^{n} \mathcal{E}_i \in [\![W_n]\!] = \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \dots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$$

and using

$$\begin{aligned}
&\rho \models \bigwedge_{n\geq 0} \Psi_n^M \\
\xLeftrightarrow{\textit{Lemma 4.23}}\ &\forall n \geq 0 : \rho \models \Psi_n^M \\
\xLeftrightarrow{\textit{Lemma 5.12}}\ &\forall n \geq 0 : \forall \mathcal{G} \in [\![W_n]\!] : \mathcal{G}(\rho) \models M,
\end{aligned}$$

we have

$$\left(\sum_{i=0}^{n} \mathcal{E}_i\right)(\rho) \models M,$$

By repeated application of Lemma 4.11, we get for all $i \geq 0$

$$\mathcal{E}_i(\rho) \models M.$$

Thus, by Lemma 4.12

$$\mathcal{E}(\rho) = \sum_{i=0}^{\infty} \mathcal{E}_i(\rho) \models M.$$

Since $\mathcal{E} \in [\![S]\!]$ was arbitrary, we have $\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M$ and therefore $\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi$.

"$\Leftarrow$":
Assume $\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi$ and thus $\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M$. Let $n \geq 0$ and $\mathcal{E}_n \in [\![W_n]\!]$. Then there exists a sequence $(\mathcal{F}_i)_{i\geq 1} \in [\![S_0]\!]^{\mathbb{N}}$ such that

$$\mathcal{E}_n = \sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}.$$

Consider

$$\mathcal{E} = \sum_{i=0}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \in [\![S]\!].$$

By assumption,

$$\mathcal{E}(\rho) \models M.$$

Hence, by Lemma 4.11 and $\mathcal{E}(\rho) = \mathcal{E}_n(\rho) + \sum_{i=n+1}^{\infty} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}(\rho)$, we get

$$\mathcal{E}_n(\rho) \models M.$$

Since n and $\mathcal{E}_n$ were arbitrary,

$$\forall n \geq 0\ \forall \mathcal{E}_n \in [\![W_n]\!] : \mathcal{E}_n(\rho) \models M.$$

Therefore

$$\begin{aligned}
&\forall n \geq 0 : \forall \mathcal{E}_n \in [\![W_n]\!] : \mathcal{E}_n(\rho) \models M \\
\xLeftrightarrow{\textit{Lemma 5.12}}\ &\forall n \geq 0 : \rho \models \Psi_n^M \\
\xLeftrightarrow{\textit{Lemma 4.23}}\ &\rho \models \bigwedge_{n\geq 0} \Psi_n^M.
\end{aligned}$$

$\square$

On Dwlp Transformer for Sets of Projections

Naturally, one might ask whether the restriction to singleton sets is necessary, or whether the transformer can be extended to arbitrary predicates. For every construct apart from loops and measurements, we can apply the same rules, as the proofs never require Ψ to be a singleton set. For the measurement, however, we run into problems. To see this, let us look at two ideas to adapt our transformer to arbitrary predicates: A natural first attempt is to replace the singleton postcondition by an arbitrary predicate Ψ to get

$$\mathrm{dwlp}(\texttt{if } P[\bar{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end}, \Psi) = (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, \Psi)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, \Psi)).$$

However, this does not give us a valid precondition, which can be seen from the following example:

Consider the program

$$\texttt{if } P^{=1}[q] \texttt{ then skip else skip end}$$

with one qubit q, $P^{=1} = |1\rangle\langle 1|$ and postcondition $\Psi = \{|0\rangle\!\langle 0|, |1\rangle\!\langle 1|\}$.

Applying the above rule yields $\{I\}$ as the dwlp, but running the program on initial state $|+\rangle\!\langle +|$ yields

$$\tfrac{1}{2}|0\rangle\!\langle 0| + \tfrac{1}{2}|1\rangle\!\langle 1| \not\models \Psi.$$

Hence, the proposed rule is not correct. Intuitively, this approach fails because the $\Leftarrow$ direction of Lemma 4.11 does not hold for sets of projections, e.g., $\frac{1}{2}|0\rangle\!\langle 0| \models \Psi$ and $\frac{1}{2}|1\rangle\!\langle 1| \models \Psi$, but their sum does not satisfy Ψ.

The next possibility would be to choose a single projection $M \in \Psi$ before reasoning about both branches and get

$$\mathrm{dwlp}(\texttt{if } P[\bar{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end}, \Psi) = \bigcup_{M \in \Psi} (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(S_0, M)).$$

This is essentially the approach from the angelic transformer in Sec. 5.1. But this approach is too restrictive, as the following example demonstrates:

Consider the program

$$\texttt{if } I[q] \texttt{ then } (q{*} = I \square q{*} = X) \texttt{ else abort}$$

for one qubit q and postcondition $\Psi = \{|0\rangle\!\langle 0|, |1\rangle\!\langle 1|\}$.

Using the new rule, we get $\{0\}$ as the dwlp, which is only satisfied by $\rho = 0$. However, for initial state $|0\rangle\langle 0|$ with choice I, the resulting state $\mathcal{I}(|0\rangle\langle 0|) = |0\rangle\langle 0|$ satisfies $|0\rangle\!\langle 0|$, whereas for the execution with choice X, the resulting state $\mathcal{X}(|0\rangle\langle 0|) = |1\rangle\langle 1|$ satisfies $|1\rangle\!\langle 1|$. Thus, every execution from initial state $|0\rangle\langle 0|$ satisfies the postcondition and $|0\rangle\langle 0|$ should satisfy the dwlp as well. The problem here is that no single projection in Ψ is satisfied by both executions. Intuitively, this approach fails because it requires both choices I and X to satisfy the same projection $M \in \Psi$.

The difficulty is the following: For every pair of executions $\mathcal{E}_0 \in [\![S_0]\!]$ and $\mathcal{E}_1 \in [\![S_1]\!]$, the resulting state

$$\mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}}) + \mathcal{E}_0(P_{\bar{q}}^{\perp}\rho P_{\bar{q}}^{\perp})$$

must satisfy a projection contained in Ψ. From Lemma 4.11, this means that $\mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}})$ and $\mathcal{E}_0(P_{\bar{q}}^{\perp}\rho P_{\bar{q}}^{\perp})$ both need to satisfy the same projection. However, a different pair of executions

$\mathcal{E}_0' \in [\![S_0]\!]$ and $\mathcal{E}_1' \in [\![S_1]\!]$ may satisfy a different projection from Ψ. Consequently, no single projection can be fixed globally for all branches, as although we want a fixed projection for each pair of executions from different branches, we still need to allow different ones within one branch.

Therefore, we need some forward calculation to decide which subspace each nondeterministic choice results in, which could look like

$$\begin{aligned}&\mathrm{dwlp}(\texttt{if } P[\bar{q}] \texttt{ then } S_1 \texttt{ else } S_0 \texttt{ end}, \Psi) = \\ &\bigwedge_{\mathcal{E}_0 \in [\![S_0]\!], \mathcal{E}_1 \in [\![S_1]\!]} \bigcup_{M \in \Psi} (P_{\bar{q}} \rightsquigarrow \mathrm{dwlp}(\mathcal{E}_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwlp}(\mathcal{E}_0, M)).\end{aligned}$$

But this is no longer a genuine weakest precondition transformer rule: It requires the transformer to access the denotational semantics of a program, and evaluating it requires the explicit (forward) denotational semantics of S_0 and S_1, since the set of possible executions must first be computed. Consequently, it does not admit a purely backward inductive computation.

The same difficulty appears in the loop rule, where the semantics is likewise defined as a sum of states. Therefore, we restrict our backward transformer to singleton postconditions in the demonic setting.

Chapter 6

Weakest Precondition

Unlike weakest liberal preconditions, non-liberal weakest preconditions characterize *total correctness*, which means that they additionally require program termination. We therefore first introduce the notion of termination in our quantum setting [ZYY19].

Definition 6.1
For a superoperator $\mathcal{E}$, we say that the execution of $\mathcal{E}$ on input state $\rho \in \mathcal{D}(\mathcal{H})$ *terminates almost surely* if

$$tr(\mathcal{E}(\rho)) = tr(\rho).$$

To define weakest preconditions for total correctness, we introduce a predicate that characterizes exactly those input states from which a given execution terminates almost surely. For this purpose, we use the termination subspace derived by Zhou et al. [ZYY19], which is defined as follows:

Definition 6.2
For a superoperator $\mathcal{E}$, the termination space $T^{\mathcal{E}}$ is
$\left(I_H - \sum_i \mathcal{E}_i^\dagger \mathcal{E}_i\right)^\perp = \{|\psi\rangle \mid \left(I_H - \sum_i \mathcal{E}_i^\dagger \mathcal{E}_i\right)|\psi\rangle = 0\}$, where $\mathcal{E}(\rho) = \sum_i \mathcal{E}_i \rho \mathcal{E}_i^\dagger$ is a Kraus operator-sum representation [KBDW83] of $\mathcal{E}$.

Note that in our setting, the termination space is associated with an individual superoperator rather than an entire nondeterministic program. This distinction is necessary because different notions of termination for nondeterministic programs are considered in the angelic and demonic settings.

We further get that this termination space $T^{\mathcal{E}}$ is a closed subspace [ZYY19]. The singleton set containing the corresponding projection $\{T^{\mathcal{E}}\}$ is the predicate that expresses for a state ρ that the execution terminates. [ZYY19] shows that this predicate exactly describes the initial states that almost surely terminate under execution of superoperator $\mathcal{E}$.

Lemma 6.3 ([ZYY19])
Let $\mathcal{E}$ be a (trace-nonincreasing) superoperator. Then for every state $\rho \in \mathcal{D}(\mathcal{H})$,

$$\rho \models T^{\mathcal{E}} \text{ iff } tr(\mathcal{E}(\rho)) = tr(\rho).$$

Additionally, this gives us an alternative characterization to express that a state lies in the termination space of a given superoperator, which lets us reason about the termination space without explicitly calculating the Kraus representation.

The following lemma shows that projective measurements themselves do not introduce nontermination. This property will be needed when proving the correctness of the measurement rule of the transformer.

Lemma 6.4
For projection P and state ρ,

$$tr(\rho) = tr(P\rho P) + tr(P^\perp \rho P^\perp).$$

Proof of Lemma 6.4.

Since $P^\perp = I - P$, we have $I = P + P^\perp$. Therefore,

$$\begin{aligned}
&tr(\rho)\\
=&tr(I\rho I)\\
=&tr\Big((P+P^\perp)\rho(P+P^\perp)\Big)\\
\overset{\text{Linearity of } tr}{=}&tr(P\rho P) + tr(P\rho P^\perp) + tr(P^\perp\rho P) + tr(P^\perp \rho P^\perp)\\
=&tr(P\rho P) + tr(P^\perp\rho P^\perp), \text{ as } tr(P\rho P^\perp) = tr(P^\perp \rho P) = 0.
\end{aligned}$$

□

In the next two sections, we define the non-liberal versions of angelic and demonic weakest preconditions, derive transformer rules for every construct except loops and prove their correctness. The reason that there is no rule for loops in either case is that almost sure termination is difficult to capture with our predicates, which is explained further in Sec. 6.3.

6.1 Angelic Weakest Precondition

The angelic weakest precondition describes the weakest precondition that guarantees for *some* possible execution that it terminates and the postcondition holds. In contrast to the demonic case, we only have to consider some execution of a program, and in contrast to the liberal case, the angelic weakest precondition does not allow nontermination. Therefore, we define the total correctness of a Hoare triple $\{\Theta\}\ S\ \{\Psi\}$ in the angelic case as follows:

Definition 6.5
Let Θ, Ψ be predicates and S a program. Then

$$\models_{tot}^{ang} \{\Theta\}\ S\ \{\Psi\} \text{ iff } \forall \rho \in \mathcal{D}(\mathcal{H}) : \rho \models \Theta \implies \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.$$

With this, we can define the angelic weakest precondition:

Definition 6.6
Let S be a quantum program and Ψ a postcondition. The *angelic weakest precondition* of Ψ with respect to S, if it exists, is the unique quantum predicate $\text{awp}(S, \Psi)$ such that:
1. Validity:
$$\models_{tot}^{ang} \{\text{awp}(S, \Psi)\}\ S\ \{\Psi\}$$
2. Weakest: For any predicate Θ:
$$\models_{tot}^{ang} \{\Theta\}\ S\ \{\Psi\} \implies \Theta \sqsubseteq \text{awp}(S, \Psi).$$

Using this definition, we give the rules for calculating the angelic weakest precondition of a loopfree quantum program S and postcondition Ψ inductively:

Theorem 6.7
The angelic weakest precondition of a quantum program S without loops and postcondition Ψ can be given inductively by the following equations:

1. $\text{awp}(\texttt{skip}, \Psi) = \Psi$
2. $\text{awp}(\texttt{abort}, \Psi) = \{0\}$
3. $\text{awp}(\bar{q} *= U, \Psi) = \{U_{\bar{q}}^{\dagger}\, M\, U_{\bar{q}} \mid M \in \Psi\}$
4. $\text{awp}(\bar{q} := 0, \Psi) = \{I_{\bar{q}} \otimes \lceil M \rceil_{\bar{q}} \mid M \in \Psi\}$
5. $\text{awp}(S_0; S_1, \Psi) = \text{awp}\big(S_0, \text{awp}(S_1, \Psi)\big)$
6. $\text{awp}(\texttt{if}\ \ P[\bar{q}]\ \ \texttt{then}\ \ S_1\ \ \texttt{else}\ \ S_0\ \ \texttt{end}, \Psi) =$
$\bigcup_{M \in \Psi} (P_{\bar{q}} \rightsquigarrow \text{awp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \text{awp}(S_0, M))$
7. $\text{awp}(S_0 \,\square\, S_1, \Psi) = \text{awp}(S_0, \Psi) \cup \text{awp}(S_1, \Psi)$

In contrast to the liberal case, only the transformer rule for `abort` changes because that is the only construct (except for loops) that introduces nonterminating behavior.

We show the following theorem to prove the correctness of the rules, which ensures validity by "$\Rightarrow$" and the weakest property by "$\Leftarrow$":

Theorem 6.8
For all programs S and states $\rho \in \mathcal{D}(\mathcal{H})$, $\rho \models \text{awp}(S, \Psi) \Leftrightarrow \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}$.

Proof of Theorem 6.8.

Again, we prove this by induction on the structure of program S. Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.

Cases skip, unitary, initialization: In all three cases, we only have one superoperator in $[\![S]\!]$, for which we have $T^{\mathcal{E}} = \{I\}$: For the respective Kraus operators, $I^\dagger \cdot I$, $U^\dagger \cdot U$ and $\sum_{i=0}^{2^n-1} |i\rangle_{\bar{q}}\langle 0||0\rangle_{\bar{q}}\langle i|$ are all equal to I, so $(I-I)^\perp = I$. Therefore, $\rho \models T^{\mathcal{E}} = I$ is trivially true for all $\rho \in \mathcal{D}(\mathcal{H})$ and $\mathrm{awp}(S,\Psi) = \mathrm{awlp}(S,\Psi)$.

Case abort: For $\{\mathcal{E}\} = \{0\} = [\![S]\!]$, we have $T^{\mathcal{E}} = (I-0)^\perp = 0$, so $\rho \models T^{\mathcal{E}}$ is only true iff $\rho = 0$ and thus $\mathrm{awp}(\texttt{abort}, \Psi) = \{0\}$.

Case sequence: For S $= S_0; S_1$, we have $[\![S]\!] = [\![S_1]\!] \circ [\![S_0]\!]$ and $\mathrm{awp}(S,\Psi) = \mathrm{awp}\big(S_0, \mathrm{awp}(S_1,\Psi)\big)$:

$$
\begin{aligned}
&\rho \models \mathrm{awp}(S,\Psi)\\
\iff\ &\rho \models \mathrm{awp}\big(S_0, \mathrm{awp}(S_1,\Psi)\big)\\
\xLeftrightarrow{IH,\text{Lemma } 6.3}\ &\exists \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \mathrm{awp}(S_1,\Psi) \wedge tr(\rho) = tr(\mathcal{E}_0(\rho))\\
\xLeftrightarrow{IH,\text{Lemma } 6.3}\ &\exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \wedge\\
&\quad tr(\mathcal{E}_0(\rho)) = tr(\mathcal{E}_1(\mathcal{E}_0(\rho))) \wedge tr(\rho) = tr(\mathcal{E}_0(\rho))\\
\iff\ &\exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_1(\mathcal{E}_0(\rho)))\\
&\quad (\Leftarrow \text{ as we deal with trace-nonincreasing superoperators.})\\
\iff\ &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}
$$

Case measurement: For S $=$ $\texttt{if}\ P[\bar{q}]\ \texttt{then}\ S_1\ \texttt{else}\ S_0\ \texttt{end}$, we have $[\![S]\!] = [\![S_1]\!] \circ \mathcal{P}_{\bar{q}} + [\![S_0]\!] \circ \mathcal{P}_{\bar{q}}^\perp$ and $\mathrm{awp}(S,\Psi) = \bigcup_{M\in\Psi} (P_{\bar{q}} \rightsquigarrow \mathrm{awp}(S_1,M)) \wedge (P_{\bar{q}}^\perp \rightsquigarrow \mathrm{awp}(S_0,M))$:

$$
\begin{aligned}
&\rho \models \mathrm{awp}(S,\Psi)\\
\iff\ &\rho \models \bigcup_{M\in\Psi} (P_{\bar{q}} \rightsquigarrow \mathrm{awp}(S_1,M)) \wedge (P_{\bar{q}}^\perp \rightsquigarrow \mathrm{awp}(S_0,M))\\
\xLeftrightarrow{\text{Lemma } 4.23}\ &\exists M \in \Psi : \rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{awp}(S_1,M)) \wedge \rho \models (P_{\bar{q}}^\perp \rightsquigarrow \mathrm{awp}(S_0,M))\\
\xLeftrightarrow{\text{Lemma } 4.25}\ &\exists M \in \Psi : P_{\bar{q}}\rho P_{\bar{q}} \models \mathrm{awp}(S_1,M) \wedge P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp \models \mathrm{awp}(S_0,M)\\
\xLeftrightarrow{IH,\text{Lemma } 6.3}\ &\exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}}) \models M \wedge tr(P_{\bar{q}}\rho P_{\bar{q}}) = tr(\mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}})) \wedge\\
&\quad \mathcal{E}_0(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp) \models M \wedge tr(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp) = tr(\mathcal{E}_0(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp))\\
\xLeftrightarrow{\text{Lemma } 4.11}\ &\exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}}) + \mathcal{E}_0(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp) \models M \wedge\\
&\quad tr(P_{\bar{q}}\rho P_{\bar{q}}) + tr(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp) = tr(\mathcal{E}_1(P_{\bar{q}}\rho P_{\bar{q}})) + tr(\mathcal{E}_0(P_{\bar{q}}^\perp \rho P_{\bar{q}}^\perp))\\
&\quad (\Leftarrow \text{ as we deal with trace-nonincreasing superoperators.})\\
\xLeftrightarrow{\text{Lemma } 6.4}\ &\exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^\perp)(\rho) \models M \wedge\\
&\quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^\perp)(\rho))\\
\xLeftrightarrow{\text{Def. + of operators}}\ &\exists M \in \Psi : \exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^\perp)(\rho) \models M \wedge
\end{aligned}
$$

$$
\begin{aligned}
&\quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\overline{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\overline{q}}^{\perp})(\rho)) \\
\iff &\exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \exists M \in \Psi : (\mathcal{E}_1 \circ \mathcal{P}_{\overline{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\overline{q}}^{\perp})(\rho) \models M \wedge \\
&\quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\overline{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\overline{q}}^{\perp})(\rho)) \\
\iff &\exists \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\overline{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\overline{q}}^{\perp})(\rho) \models \Psi \wedge \\
&\quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\overline{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\overline{q}}^{\perp})(\rho)) \\
\iff &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}
$$

Case nondeterministic choice: For $S = S_0 \,\Box\, S_1$, we have $[\![S]\!] = [\![S_0]\!] \cup [\![S_1]\!]$ and $\mathrm{awp}(S, \Psi) = \mathrm{awp}(S_0, \Psi) \cup \mathrm{awp}(S_1, \Psi)$.

$$
\begin{aligned}
&\rho \models \mathrm{awp}(S, \Psi) \\
\iff &\rho \models \mathrm{awp}(S_0, \Psi) \cup \mathrm{awp}(S_1, \Psi) \\
\iff &\rho \models \mathrm{awp}(S_0, \Psi) \vee \rho \models \mathrm{awp}(S_1, \Psi) \\
\xLeftrightarrow{IH, Lemma\ 6.3} &(\exists \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_0(\rho))) \vee \\
&\quad (\exists \mathcal{E}_1 \in [\![S_1]\!] : \mathcal{E}_1(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_1(\rho))) \\
\iff &\exists \mathcal{E} \in [\![S_0]\!] \cup [\![S_1]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\iff &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}
$$

□

6.2 Demonic Weakest Precondition

The demonic weakest precondition characterizes the weakest predicate that guarantees both almost sure termination and satisfaction of the postcondition for every possible execution of the program. Therefore, we define the total correctness of a Hoare triple $\{\Theta\}\ S\ \{\Psi\}$ in the demonic case as follows:

Definition 6.9
Let Θ, Ψ be predicates and S a program. Then

$$\models^{dem}_{tot} \{\Theta\}\ S\ \{\Psi\} \text{ iff } \forall \rho \in \mathcal{D}(\mathcal{H}) : \rho \models \Theta \implies \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.$$

With this, we can define the demonic weakest precondition:

Definition 6.10
Let S be a quantum program and Ψ a postcondition. The *demonic weakest precondition* of Ψ with respect to S, if it exists, is the unique quantum predicate $\mathrm{dwp}(S, \Psi)$ such that:
1. Validity:
$$\models^{dem}_{tot} \{\mathrm{dwp}(S, \Psi)\}\ S\ \{\Psi\}$$
2. Weakest: For any predicate Θ:
$$\models^{dem}_{tot} \{\Theta\}\ S\ \{\Psi\} \implies \Theta \sqsubseteq \mathrm{dwp}(S, \Psi).$$

Using this definition, we give the rules for calculating the demonic weakest precondition of a loopfree quantum program S and postcondition Ψ with one element $\Psi = \{M\}$ inductively:

Theorem 6.11
The demonic weakest precondition of a quantum program S without loops and a singleton postcondition $\Psi = \{M\}$ can be given inductively by the following equations:

1. $\mathrm{dwp}(\texttt{skip}, \Psi) = \Psi$
2. $\mathrm{dwp}(\texttt{abort}, \Psi) = \{0\}$
3. $\mathrm{dwp}(\bar{q} *{=} U, \Psi) = \{U_{\bar{q}}^{\dagger}\, M\, U_{\bar{q}} \mid M \in \Psi\}$
4. $\mathrm{dwp}(\bar{q} := 0, \Psi) = \{I_{\bar{q}} \otimes \lceil M \rceil_{\bar{q}} \mid M \in \Psi\}$
5. $\mathrm{dwp}(S_0; S_1, \Psi) = \mathrm{dwp}\big(S_0, \mathrm{dwp}(S_1, \Psi)\big)$
6. $\mathrm{dwp}(\texttt{if}\ \ P[\bar{q}]\ \ \texttt{then}\ \ S_1\ \ \texttt{else}\ \ S_0\ \ \texttt{end}, \Psi) =$
   $(P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwp}(S_0, M))$
7. $\mathrm{dwp}(S_0 \,\Box\, S_1, \Psi) = \mathrm{dwp}(S_0, \Psi) \wedge \mathrm{dwp}(S_1, \Psi)$

As in the angelic case, the transformer rules for every construct except for `abort` are the same as in Theorem 5.9 because nothing else introduces nontermination.

For the non-liberal case, we additionally need to show that all states satisfying the precondition terminate. Thus, the correctness of the rules follows from the following theorem. Again, validity is ensured by "$\Rightarrow$", and the weakest property is ensured by "$\Leftarrow$".

Theorem 6.12
For all programs S and states $\rho \in \mathcal{D}(\mathcal{H})$, $\rho \models \mathrm{dwp}(S, \Psi) \Leftrightarrow \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}$.

Proof of Theorem 6.12.

Again, we prove this by induction on the structure of program S. Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.

Cases skip, abort, unitary, initialization: Again, the demonic weakest precondition for the base cases is the same as for the angelic weakest precondition from Sec. 6.1 with almost identical proofs, as for all four operations, there exists exactly one superoperator $\mathcal{E} \in [\![S]\!]$.

Case sequence: For S $= S_0; S_1$, we have $[\![S]\!] = [\![S_1]\!] \circ [\![S_0]\!]$ and $\mathrm{dwp}(S, \Psi) = \mathrm{dwp}\big(S_0, \mathrm{dwp}(S_1, \Psi)\big)$:

$$\begin{aligned}
& \rho \models \mathrm{dwp}(S, \Psi) \\
\Longleftrightarrow\ & \rho \models \mathrm{dwp}\big(S_0, \mathrm{dwp}(S_1, \Psi)\big) \\
\xLeftrightarrow{IH, Lemma\ 6.3}\ & \forall \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \mathrm{dwp}(S_1, \Psi) \wedge tr(\rho) = tr(\mathcal{E}_0(\rho)) \\
\xLeftrightarrow{IH, Lemma\ 6.3}\ & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \wedge tr(\mathcal{E}_0(\rho)) = tr(\mathcal{E}_1(\mathcal{E}_0(\rho))) \wedge tr(\rho) = tr(\mathcal{E}_0(\rho)) \\
\Longleftrightarrow\ & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1 \circ \mathcal{E}_0(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_1(\mathcal{E}_0(\rho))) \\
& \qquad (\text{"}\Leftarrow\text{" because the superoperators are trace-nonincreasing.}) \\
\Longleftrightarrow\ & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}$$

Case measurement: For S = `if` $P[\bar{q}]$ `then` S_1 `else` S_0 `end`, we have $[\![S]\!] = [\![S_1]\!] \circ \mathcal{P}_{\bar{q}} + [\![S_0]\!] \circ \mathcal{P}_{\bar{q}}^{\perp}$ and $\mathrm{dwp}(S, \Psi) = (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwp}(S_0, M))$:

$$
\begin{aligned}
& \rho \models \mathrm{dwp}(S, \Psi) \\
\iff & \rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_1, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwp}(S_0, M)) \\
\xLeftrightarrow{\textit{Lemma 4.23}} & \rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_1, M)) \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow \mathrm{dwp}(S_0, M)) \\
\xLeftrightarrow{\textit{Lemma 4.25}} & P_{\bar{q}} \rho P_{\bar{q}} \models \mathrm{dwp}(S_1, M) \wedge P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp} \models \mathrm{dwp}(S_0, M) \\
\xLeftrightarrow{\textit{IH,Lemma 6.3}} & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}}) \models M \wedge tr(P_{\bar{q}} \rho P_{\bar{q}}) = tr(\mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}})) \wedge \\
& \quad \mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp}) \models M \wedge tr(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp}) = tr(\mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp})) \\
\xLeftrightarrow{\textit{Lemma 4.11}} & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}}) + \mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp}) \models M \wedge \\
& \quad tr(P \rho P) + tr(P^{\perp} \rho P^{\perp}) = tr(\mathcal{E}_1(P_{\bar{q}} \rho P_{\bar{q}})) + tr(\mathcal{E}_0(P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp})) \\
& \qquad (\text{"}\Leftarrow\text{" because the superoperators are trace-nonincreasing.}) \\
\xLeftrightarrow{\textit{Lemma 6.4}} & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \wedge \\
& \quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}})(\rho) + (\mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho)) \\
\xLeftrightarrow{\text{Def. + of operators}} & \forall \mathcal{E}_1 \in [\![S_1]\!], \mathcal{E}_0 \in [\![S_0]\!] : (\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho) \models M \wedge \\
& \quad tr(\rho) = tr((\mathcal{E}_1 \circ \mathcal{P}_{\bar{q}} + \mathcal{E}_0 \circ \mathcal{P}_{\bar{q}}^{\perp})(\rho)) \\
\iff & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \{M\} \wedge \rho \models T^{\mathcal{E}} \\
\iff & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}
$$

Case nondeterministic choice: For $S = S_0 \,\square\, S_1$, we have $[\![S]\!] = [\![S_0]\!] \cup [\![S_1]\!]$ and $\mathrm{dwp}(S, \Psi) = \mathrm{dwp}(S_0, \Psi) \wedge \mathrm{dwp}(S_1, \Psi)$:

$$
\begin{aligned}
& \rho \models \mathrm{dwp}(S_0, \Psi) \wedge \mathrm{dwp}(S_1, \Psi) \\
\iff & \rho \models \mathrm{dwp}(S_0, \Psi) \wedge \rho \models \mathrm{dwp}(S_1, \Psi) \\
\xLeftrightarrow{\textit{IH,Lemma 6.3}} & (\forall \mathcal{E}_0 \in [\![S_0]\!] : \mathcal{E}_0(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_0(\rho))) \wedge \\
& \quad (\forall \mathcal{E}_1 \in [\![S_1]\!] : \mathcal{E}_1(\rho) \models \Psi \wedge tr(\rho) = tr(\mathcal{E}_1(\rho))) \\
\iff & \forall \mathcal{E} \in [\![S_0]\!] \cup [\![S_1]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\iff & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}
$$

□

Just as in the liberal case in Sec. 5.2, the proposed rule for measurements is the only one that is not correct for arbitrary predicates. As we have the same problems in the non-liberal demonic case as in the liberal one, we restrict the postcondition to singleton sets again.

6.3 Weakest Precondition Transformer for Loops

The most interesting case for the non-liberal transformers is arguably the loop because, apart from `abort`, this is the only construct that introduces nonterminating behavior. The reason that loops are not included in the transformer rules is that finding a weakest precondition transformer for them is significantly more difficult than for the rest. The main challenge is capturing almost sure termination with qualitative predicates. One idea for the loop is to start by calculating the weakest precondition for each unfolding of the loop like it is done in the liberal case. For the demonic weakest liberal transformer, we would get

$$\mathrm{dwp}(\texttt{while } P[\bar{q}] \texttt{ do } S_0 \texttt{ end}, \{M\}) = \bigcup_{n \geq 0} \Psi_n^M$$

with $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, 0)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$ and $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$. However, this cannot capture the initial states that only terminate almost surely, but never for a concrete unfolding of the loop. To see this, consider the program

$$\texttt{while } P^{=0}[q] \texttt{ do } q{*}=H \texttt{ end}$$

with one qubit q, $P^{=0} = |0\rangle\langle 0|$ and its semantics $\{\sum_{i=0}^{\infty} \mathcal{P}^{=1} \circ (\mathscr{H} \circ \mathcal{P}^{=0})^i\}$. Here, H is the Hadamard gate, which maps $|0\rangle$ to $|+\rangle$, and $\mathscr{H}$ is the corresponding superoperator (as $\mathcal{H}$ already refers to the Hilbert space). Then

$$\sum_{i=0}^{\infty} \mathcal{P}^{=1} \circ (\mathscr{H} \circ \mathcal{P}^{=0})^i (|+\rangle\langle +|) = |1\rangle\langle 1|,$$

but for every finite unfolding with n iterations of the loop,

$$\left(\sum_{i=0}^{n} \mathcal{P}^{=1} \circ (\mathscr{H} \circ \mathcal{P}^{=0})^i\right)(|+\rangle\langle +|) = \sum_{i=0}^{n} \frac{1}{2^{i+1}} |1\rangle\langle 1| = \left(1 - \frac{1}{2^{n+1}}\right)|1\rangle\langle 1|,$$

whose trace is strictly smaller than that of the input state. Hence $|+\rangle\langle +|$ is not contained in the termination space of any finite approximation. The reason is that

$$\rho \models T^{\mathcal{E}} \quad \text{for every } \mathcal{E} \in [\![\texttt{while } P[\bar{q}] \texttt{ do } S_0 \texttt{ end}]\!]$$

does not imply

$$\exists n : \forall \mathcal{E} \in [\![W_n]\!] : \rho \models T^{\mathcal{E}},$$

where W_n denote the finite unfoldings of the loop. Almost sure termination is therefore not captured by finite unfoldings. Finding some way of describing almost surely terminating states in this framework remains an interesting question for future work.

Nevertheless, the unfolding construction still yields a valid (although generally not weakest) precondition, which is proven in the following. We first show that the weakest precondition of each finite unfolding of the loop is still characterized by the corresponding predicate Ψ_n^M.

Lemma 6.13
For $[\![W_n]\!] = \{\sum_{i=0}^{n} \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}} \mid \mathcal{F} \in [\![S_0]\!]^{\mathbb{N}}\}$, $\Psi_0^M = (P \rightsquigarrow \mathrm{dwp}(S_0, 0)) \wedge (P^{\perp} \rightsquigarrow M)$ and $\Psi_{n+1}^M = (P \rightsquigarrow \mathrm{dwp}(S_0, \Psi_n^M)) \wedge (P^{\perp} \rightsquigarrow M)$, we have for all $n \geq 0$ and all projections M:

$$\mathrm{dwp}(W_n, M) = \Psi_n^M.$$

Proof of Lemma 6.13.

We show this by induction on n.

For $n = 0$, we show

$$\rho \models \mathrm{dwp}(W_0, M) \Leftrightarrow \forall \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M \wedge \rho \models T^{\mathcal{E}}$$

for all $\rho \in \mathcal{D}(\mathcal{H})$. Let state ρ be arbitrary.
We have $[\![W_0]\!] = \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}$ and $\mathrm{dwp}(W_0, M) = \Psi_0^M = (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, 0)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$:

$$\begin{aligned}
& \rho \models \mathrm{dwp}(W_0, M) \\
\Longleftrightarrow\ & \rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, 0)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\overset{(*)}{\Longleftrightarrow}\ & \rho \models (P_{\bar{q}} \rightsquigarrow 0) \wedge (P^{\perp} \rightsquigarrow M) \\
\xLeftrightarrow{\textit{Lemma 4.25}}\ & P_{\bar{q}} \rho P_{\bar{q}} \models 0 \wedge P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp} \models M \\
\Longleftrightarrow\ & P_{\bar{q}} \rho P_{\bar{q}} = 0 \wedge P_{\bar{q}}^{\perp} \rho P_{\bar{q}}^{\perp} \models M \\
\Longleftrightarrow\ & \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \wedge tr(\mathcal{P}_{\bar{q}}(\rho) = 0) \\
\xLeftrightarrow{\textit{Lemma 6.4}}\ & \sum_{i=0}^{0} \mathcal{P}_{\bar{q}}^{\perp}(\rho) \models M \wedge tr(\rho) = tr(\mathcal{P}_{\bar{q}}^{\perp}(\rho)) \\
\xLeftrightarrow{\textit{Lemma 6.3}}\ & \forall \mathcal{E} \in [\![W_0]\!] : \mathcal{E}(\rho) \models M \wedge \rho \models T^{\mathcal{E}}.
\end{aligned}$$

(*) holds as $\rho \models 0 \iff \rho = 0 \iff \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models 0 \wedge tr(\rho) = tr(\mathcal{E}(\rho))$, so $\mathrm{dwp}(S, 0) = 0$ for all programs S.

For $n + 1$:
Using $[\![W_{n+1}]\!] = [\![\texttt{if } P \texttt{ then } S_0; W_n \texttt{ else skip end}]\!]$ from Lemma 2.10, we obtain

$$\begin{aligned}
\mathrm{dwp}(W_{n+1}, M) &= \mathrm{dwp}(\texttt{if } P \texttt{ then } S_0; W_n \texttt{ else skip end}, M) \\
&= (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0; W_n, M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M).
\end{aligned} \tag{6.1}$$

Using the rule for sequential composition, we get $\mathrm{dwp}(S_0; W_n, M) = \mathrm{dwp}(S_0, \mathrm{dwp}(W_n, M))$ and together with the induction hypothesis $\mathrm{dwp}(S_0; W_n, M) = \mathrm{dwp}(S_0, \Psi_n^M)$. Replacing this in Eq. (6.1) gives us

$$\mathrm{dwp}(W_{n+1}, M) = (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) = \Psi_{n+1}^M.$$

□

To relate the predicates Ψ_n^M for different unfoldings, we first need the monotonicity of the demonic weakest precondition transformer. Intuitively, this shows that weakening the postcondition cannot make its weakest precondition stronger.

Lemma 6.14
dwp is monotonic, i.e., for every program S and predicates Ψ, Φ,

$$\text{if } \Psi \sqsubseteq \Phi \text{ then } \mathrm{dwp}(S, \Psi) \sqsubseteq \mathrm{dwp}(S, \Phi) \text{ holds.}$$

Proof of Lemma 6.14.

$$\begin{aligned}
& \Psi \sqsubseteq \Phi \\
\iff & \forall \rho \in \mathcal{D}(\mathcal{H}) : (\rho \models \Psi \implies \rho \models \Phi) \\
\iff & \forall \rho \in \mathcal{D}(\mathcal{H}) : (\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \implies \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Phi) \\
\implies & \forall \rho \in \mathcal{D}(\mathcal{H}) : (\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \implies \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Phi \wedge \rho \models T^{\mathcal{E}}), \\
& \quad \text{as } T^{\mathcal{E}} \text{ is independent of the postcondition.} \\
\overset{\textit{Theorem 6.12}}{\Longleftrightarrow} & \forall \rho \in \mathcal{D}(\mathcal{H}) : (\rho \models \mathrm{dwp}(S, \Psi) \implies \rho \models \mathrm{dwp}(S, \Phi)) \\
\iff & \mathrm{dwp}(S, \Psi) \sqsubseteq \mathrm{dwp}(S, \Phi).
\end{aligned}$$

□

Using the monotonicity of dwp, we can now show that the sequence of predicates $(\Psi_n^M)_{n \geq 0}$ is increasing. Intuitively, this means that each initial state that satisfies Ψ_n^M also satisfies Ψ_{n+1}^M, and our calculation can only increase the initial states included in the dwp.

Lemma 6.15
For all $n \geq 0$ and projections M,

$$\Psi_n^M \sqsubseteq \Psi_{n+1}^M.$$

Proof of Lemma 6.15.

We prove this by induction on n. Let $\rho \in \mathcal{D}(\mathcal{H})$ be arbitrary.
For $n = 0$, we have:

$$\begin{aligned}
& \rho \models \Psi_0^M \\
\implies & \rho \models (P_{\bar{q}} \rightsquigarrow 0) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\xRightarrow{\textit{Lemma 4.23}} & \rho \models (P_{\bar{q}} \rightsquigarrow 0) \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\xRightarrow{\textit{Lemma 4.25}} & P_{\bar{q}} \rho P_{\bar{q}} \models 0 \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\Rightarrow & P_{\bar{q}} \rho P_{\bar{q}} = 0 \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\xRightarrow{0 \models \Psi \text{ for all predicates } \Psi} & P_{\bar{q}} \rho P_{\bar{q}} \models \mathrm{dwp}(S_0, \Psi_0^M) \wedge \rho \models (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\xRightarrow{\textit{Lemma 4.25}, \textit{Lemma 4.23}} & \rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, \Psi_0^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M) \\
\implies & \rho \models \Psi_1^M.
\end{aligned}$$

For $n+1$:
For all states $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$
\begin{aligned}
&\rho \models \Psi^M_{n+1} \\
\Longrightarrow\ &\rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, \Psi^M_n)) \wedge (P^\perp_{\bar{q}} \rightsquigarrow M) \\
\xRightarrow{\textit{Lemma 4.25}}\ &P_{\bar{q}}\rho P_{\bar{q}} \models \mathrm{dwp}(S_0, \Psi^M_n) \wedge P^\perp_{\bar{q}}\rho P^\perp_{\bar{q}} \models M \\
\xRightarrow{\textit{IH}}\ &P_{\bar{q}}\rho P_{\bar{q}} \models \mathrm{dwp}(S_0, \Psi^M_{n+1}) \wedge P^\perp_{\bar{q}}\rho P^\perp_{\bar{q}} \models M \\
&\qquad\text{(as by Lemma 6.14 and induction hypothesis, } \mathrm{dwp}(S_0, \Psi^M_n) \sqsubseteq \mathrm{dwp}(S_0, \Psi^M_{n+1})\text{)} \\
\xRightarrow{\textit{Lemma 4.25}}\ &\rho \models (P_{\bar{q}} \rightsquigarrow \mathrm{dwp}(S_0, \Psi^M_{n+1})) \wedge (P^\perp_{\bar{q}} \rightsquigarrow M) \\
\Longrightarrow\ &\rho \models \Psi^M_{n+2}.
\end{aligned}
$$

□

With this, we use the finite approximations to show that the unfolding construction yields a valid precondition for the full loop. In particular, if a state satisfies $\bigcup_{n\geq 0} \Psi^M_n$, then every execution of the loop terminates from that state and satisfies the postcondition M.

Theorem 6.16
For S = `while` $P[\bar{q}]$ `do` S_0 `end` and projection M, we have

$$\rho \models \bigcup_{n\geq 0} \Psi^M_n \implies \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M \wedge \rho \models T^{\mathcal{E}}$$

for all states $\rho \in \mathcal{D}(\mathcal{H})$,

Proof of Theorem 6.16.

Assume $\rho \models \bigcup_{n\geq 0} \Psi^M_n$. Then

$$
\begin{aligned}
&\rho \models \bigcup_{n\geq 0} \Psi^M_n \\
\Longleftrightarrow\ &\exists n \geq 0 : \rho \models \Psi^M_n \\
\xRightarrow{\textit{Lemma 6.15}}\ &\exists n \geq 0 : \forall N \geq n : \rho \models \Psi^M_N \\
\xRightarrow{\textit{Lemma 6.13}}\ &\exists n \geq 0 : \forall N \geq n : \rho \models \mathrm{dwp}(W_N, M) \\
\Longrightarrow\ &\exists n \geq 0 : \forall N \geq n : \forall \mathcal{E} \in [\![W_N]\!] : \mathcal{E}(\rho) \models M \wedge \rho \models T^{\mathcal{E}}, \\
&\text{with } \mathcal{E} = \sum_{i=0}^{N} \mathcal{E}_i \text{ and } \mathcal{E}_i = \mathcal{P}^\perp_{\bar{q}} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}, (\mathcal{F}_i)_{i\geq 1} \in [\![S_0]\!]^{\mathbb{N}}.
\end{aligned}
$$

Thus, there exists an n such that:

1. for all N $\geq$ n, using Lemma 4.11, $\mathcal{E}_N(\rho) \models M$ holds for all $\mathcal{E} \in [\![W_N]\!]$,
2. for all 0 $\leq$ N $\leq$ n, again using Lemma 4.11, $\mathcal{E}_N(\rho) \models M$ holds for all $\mathcal{E} \in [\![W_N]\!]$.

Thus, we have for all $N \geq 0$, $\mathcal{E}_N(\rho) \models M$. With Lemma 4.12, we get

$$\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) = \sum_{i=0}^{\infty} \mathcal{E}_i(\rho) \models M.$$

We additionally have to show that $tr(\rho) = tr(\mathcal{E}(\rho))$ for every $\mathcal{E} \in [\![S]\!] = \sum_{i=0}^{\infty} \mathcal{E}_i$ with $\mathcal{E}_i = \mathcal{P}_{\bar{q}}^{\perp} \circ \mathcal{F}_i \circ \mathcal{P}_{\bar{q}} \circ \cdots \circ \mathcal{F}_1 \circ \mathcal{P}_{\bar{q}}, (\mathcal{F}_i)_{i\geq 1} \in [\![S_0]\!]^{\mathbb{N}}$.
From

$$\exists n \geq 0 : \forall \sum_{i=0}^{n} \mathcal{E}_i \in [\![W_n]\!] : \rho \models T^{\mathcal{E}},$$

we have that there exists some $n \geq 0$ such that

$$tr\left(\sum_{i=0}^{n} \mathcal{E}_i(\rho)\right) = tr(\rho).$$

Furthermore, we have

$$tr\left(\sum_{i=0}^{n+1} \mathcal{E}_i(\rho)\right) = tr\left(\sum_{i=0}^{n} \mathcal{E}_i(\rho)\right) + tr(\mathcal{E}_{n+1}(\rho)) \geq tr\left(\sum_{i=0}^{n} \mathcal{E}_i(\rho)\right),$$

since each $\mathcal{E}_{n+1}(\rho)$ is positive and thus the traces of the partial sums are monotone increasing. On the other hand, every superoperator in $[\![S]\!]$ is trace-nonincreasing and therefore

$$tr\left(\sum_{i=0}^{\infty} \mathcal{E}_i(\rho)\right) \leq tr(\rho).$$

Using the monotonicity of the traces of the partial sums, we have

$$tr(\rho) = tr\left(\sum_{i=0}^{n} \mathcal{E}_i(\rho)\right) \leq tr\left(\sum_{i=0}^{\infty} \mathcal{E}_i(\rho)\right) \leq tr(\rho)$$

and thus

$$tr\left(\sum_{i=0}^{\infty} \mathcal{E}_i(\rho)\right) = tr(\rho).$$

As $\mathcal{E}(\rho) = \sum_{i=0}^{\infty} \mathcal{E}_i(\rho)$, $tr(\mathcal{E}(\rho)) = tr(\rho)$ holds for all $\mathcal{E} \in [\![S]\!]$.

Together, we get

$$\begin{aligned} & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M \wedge tr(\mathcal{E}(\rho)) = tr(\rho) \\ \overset{\text{Lemma 6.3}}{\Longleftrightarrow} & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models M \wedge \rho \models T^{\mathcal{E}}. \end{aligned}$$

□

The same applies to the angelic weakest precondition for loops:
The rule $\text{awp}(\texttt{while } P[\bar{q}] \texttt{ do } S_0 \texttt{ end}, \Psi) = \bigcup_{M \in \Psi} \bigcup_{n \geq 0} \Psi_n^M$ with $\Psi_0^M = (P_{\bar{q}} \rightsquigarrow \text{awp}(S_0, 0)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$ and $\Psi_{n+1}^M = (P_{\bar{q}} \rightsquigarrow \text{awp}(S_0, \Psi_n^M)) \wedge (P_{\bar{q}}^{\perp} \rightsquigarrow M)$ fails for the same reason that it does not capture the initial states that only terminate almost surely, but never after finite iterations of the loop. Proving that this still yields a valid precondition works just as in the demonic case combined with the extension for arbitrary predicates, but with the restriction to finite semantics within loops from the angelic weakest liberal precondition in Sec. 5.1.

Chapter 7

Relations between Weakest Preconditions

The four weakest precondition variants differ along two independent dimensions: the distinction between demonic and angelic nondeterminism and the distinction between total and partial correctness. The next question that arises is whether we can find relationships between them. It turns out that the differences induce a natural ordering between the corresponding predicate transformers, shown in the following theorem:

Theorem 7.1
For a quantum program S and postcondition Ψ, we have the following relations:

$$\begin{array}{ccc} \mathrm{awp}(S,\Psi) & \sqsubseteq & \mathrm{awlp}(S,\Psi) \\ \sqcup\!\!\mid & & \sqcup\!\!\mid \\ \mathrm{dwp}(S,\Psi) & \sqsubseteq & \mathrm{dwlp}(S,\Psi) \end{array}$$

The vertical relations compare demonic and angelic reasoning, whereas the horizontal relations compare total and partial correctness.

Proof of Theorem 7.1.

Let $\rho \in \mathcal{D}(\mathcal{H})$ be a state. The angelic versions are weaker than the demonic ones because requiring the property to hold for at least one execution is weaker than requiring it to hold for every execution:

$$\begin{aligned} & \rho \models \mathrm{dwlp}(S,\Psi) \\ \Longleftrightarrow\ & \forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \\ \Longrightarrow\ & \exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \\ \Longleftrightarrow\ & \rho \models \mathrm{awlp}(S,\Psi) \end{aligned}$$

$$\begin{aligned}
&\rho \models \operatorname{dwp}(S, \Psi) \\
\iff &\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\implies &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\iff &\rho \models \operatorname{awp}(S, \Psi)
\end{aligned}$$

The liberal versions are weaker than the non-liberal ones because total correctness additionally requires almost sure termination:

$$\begin{aligned}
&\rho \models \operatorname{dwp}(S, \Psi) \\
\iff &\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\implies &\forall \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \\
\iff &\rho \models \operatorname{dwlp}(S, \Psi)
\end{aligned}$$

$$\begin{aligned}
&\rho \models \operatorname{awp}(S, \Psi) \\
\iff &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \wedge \rho \models T^{\mathcal{E}} \\
\implies &\exists \mathcal{E} \in [\![S]\!] : \mathcal{E}(\rho) \models \Psi \\
\iff &\rho \models \operatorname{awlp}(S, \Psi)
\end{aligned}$$

□

Thus, total correctness always yields a stronger precondition than partial correctness, while demonic reasoning yields a stronger precondition than angelic reasoning. These are the same relationships as in the classical case [VK25].

Chapter 8

Example Application

This chapter illustrates the previously developed predicate transformers by applying them to the three-qubit bit-flip error correction scheme introduced in Example 2.9. For readability, we write $[|\psi\rangle]$ for the corresponding partial density operator $|\psi\rangle\langle\psi|$ of a pure state $|\psi\rangle$ and omit the subscript $_{q,q_1,q_2}$ whenever it is clear from the context.

For the demonic case, the goal is to verify that the program preserves the qubit q for every possible bit-flip error. Therefore, we choose $\{[\alpha_0\,|0\rangle + \alpha_1\,|1\rangle]_q \otimes I_{q_1,q_2}\}$ as the postcondition. This expresses that, after executing the error correction procedure, the information stored in the qubit q has been recovered correctly, whereas the ancilla qubits q_1 and q_2 are left unspecified because these ancillas are only used to detect and correct errors and are no longer relevant after the computation. Computing the weakest precondition of this postcondition backwards through the program yields the weakest condition on the initial state that guarantees successful error correction, so we expect $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$ as the demonic weakest precondition.

The application of the demonic weakest precondition transformer is shown in the following. As the program does not include `abort` or loops, the demonic weakest precondition and demonic weakest liberal precondition coincide.

Example 8.1 (Demonic Weakest Precondition)

10 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

$q_1, q_2 := 0$

9 $\{[\alpha_0|000\rangle + \alpha_1|100\rangle]\}$

$q, q_1 * = CX; \qquad q, q_2 * = CX;$

8 $\{[\alpha_0|000\rangle + \alpha_1|111\rangle]\}$

$\texttt{skip} \,\square\, q* = X \,\square\, q_1* = X \,\square\, q_2* = X;$

7 $\{[\alpha_0|100\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle]\}$

$q, q_2 * = CX; \qquad q, q_1 * = CX;$

6 $\{[\alpha_0|111\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|101\rangle] \vee [\alpha_0|010\rangle + \alpha_1|110\rangle] \vee [\alpha_0|000\rangle + \alpha_1|100\rangle]\}$

if $P^{=1}[q_2]$ **then**

5 $\Big(\{[\alpha_0|11\rangle + \alpha_1|01\rangle]_{q,q_1} \vee [\alpha_0|00\rangle + \alpha_1|10\rangle]_{q,q_1}\}\Big) \otimes I_{q_2}$

if $P^{=1}[q_1]$ **then**

4 $\{[\alpha_0|1\rangle + \alpha_1|0\rangle]_q \otimes I_{q_1,q_2}\}$

$q* = X$

3 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

end

2 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

end

1 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

Most steps follow directly from the initialization, unitary and sequential composition rules. The only nontrivial applications are the measurement rule and the nondeterministic choice rule, which we derive below.

For step 5, we need to apply the measurement rule:

$$\begin{aligned}
&\mathrm{dwp}(\texttt{if } P^{=1}[q_1] \texttt{ then } q* = X \texttt{ else skip end}, \{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}) \\
&= ([|1\rangle]_{q_1} \otimes I_{q,q_2} \rightsquigarrow [\alpha_0|1\rangle + \alpha_1|0\rangle]_q \otimes I_{q_1,q_2}) \\
&\wedge ([|0\rangle]_{q_1} \otimes I_{q,q_2} \rightsquigarrow [\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}) \\
&= [\alpha_0|11\rangle + \alpha_1|01\rangle]_{q,q_1} \otimes I_{q_2} \vee [\alpha_0|00\rangle + \alpha_1|10\rangle]_{q,q_1} \otimes I_{q_2}.
\end{aligned}$$

Step 6 can be derived similarly.

For the nondeterministic choice in step 8, we obtain

$$\begin{aligned}
&\mathrm{dwp}(\texttt{skip}\Box q* = X\Box q_1* = X\Box q_2* = X, \Psi_7) \\
&= \mathrm{dwp}(\texttt{skip}, \Psi_7) \wedge \mathrm{dwp}(q* = X, \Psi_7) \wedge \mathrm{dwp}(q_1* = X, \Psi_7) \wedge \mathrm{dwp}(q_2* = X, \Psi_7) \\
&= \{([\alpha_0|100\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee \\
&\qquad [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle]) \wedge \\
&\quad ([\alpha_0|000\rangle + \alpha_1|111\rangle] \vee [\alpha_0|101\rangle + \alpha_1|010\rangle] \vee \\
&\qquad [\alpha_0|110\rangle + \alpha_1|001\rangle] \vee [\alpha_0|100\rangle + \alpha_1|011\rangle]) \wedge \\
&\quad ([\alpha_0|110\rangle + \alpha_1|001\rangle] \vee [\alpha_0|011\rangle + \alpha_1|100\rangle] \vee \\
&\qquad [\alpha_0|000\rangle + \alpha_1|111\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle]) \wedge \\
&\quad ([\alpha_0|101\rangle + \alpha_1|010\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle] \vee \\
&\qquad [\alpha_0|011\rangle + \alpha_1|100\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle])\} \\
&= \{[\alpha_0|000\rangle + \alpha_1|111\rangle]\},
\end{aligned}$$

with $\Psi_7 =$
$\{[\alpha_0|100\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle]\}$

Thus, we obtain

$$\mathrm{dwp}(S, \{[\alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle]_q \otimes I_{q_1,q_2}\}) = \{[\alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle]_q \otimes I_{q_1,q_2}\},$$

where S denotes the three-qubit bit-flip error correction program. This weakest precondition states that if the qubit q is in state $[\alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle]$ before the program execution, it remains in this state after program execution, showing that the qubit is recovered correctly regardless of which single bit-flip error occurs.

Next, we apply the angelic weakest precondition transformer to the same program and postcondition to illustrate the difference between the two predicate transformers. Due to the angelic interpretation of the nondeterministic choice, it is sufficient that one of the possible bit-flips establishes the postcondition, rather than requiring all possible choices to do so. As in the demonic case, the weakest precondition and weakest liberal precondition coincide because the program contains neither `abort` statements nor loops.

Example 8.2 (Angelic Weakest Precondition)

10 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

$q_1, q_2 := 0$

9 $\{([\alpha_0|111\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|100\rangle])\}\cup$
$\{([\alpha_0|000\rangle + \alpha_1|100\rangle] \vee [\alpha_0|101\rangle + \alpha_1|010\rangle] \vee [\alpha_0|101\rangle + \alpha_1|001\rangle] \vee [\alpha_0|111\rangle + \alpha_1|011\rangle])\}\cup$
$\{([\alpha_0|101\rangle + \alpha_1|001\rangle] \vee [\alpha_0|011\rangle + \alpha_1|111\rangle] \vee [\alpha_0|000\rangle + \alpha_1|100\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle])\}\cup$
$\{([\alpha_0|110\rangle + \alpha_1|010\rangle] \vee [\alpha_0|000\rangle + \alpha_1|100\rangle] \vee [\alpha_0|011\rangle + \alpha_1|111\rangle] \vee [\alpha_0|001\rangle + \alpha_1|101\rangle])\}$

$q, q_1 * = CX; \qquad q, q_2 * = CX;$

8 $\{([\alpha_0|100\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle])\}\cup$
$\{([\alpha_0|000\rangle + \alpha_1|111\rangle] \vee [\alpha_0|101\rangle + \alpha_1|010\rangle] \vee [\alpha_0|110\rangle + \alpha_1|001\rangle] \vee [\alpha_0|100\rangle + \alpha_1|011\rangle])\}\cup$
$\{([\alpha_0|110\rangle + \alpha_1|001\rangle] \vee [\alpha_0|011\rangle + \alpha_1|100\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle])\}\cup$
$\{([\alpha_0|101\rangle + \alpha_1|010\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle] \vee [\alpha_0|011\rangle + \alpha_1|100\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle])\}$

`skip` $\square \; q* = X \; \square \; q_1 * = X \; \square \; q_2 * = X;$

7 $\{[\alpha_0|100\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|110\rangle] \vee [\alpha_0|010\rangle + \alpha_1|101\rangle] \vee [\alpha_0|000\rangle + \alpha_1|111\rangle]\}$

$q, q_2 * = CX; \qquad q, q_1 * = CX;$

6 $\{[\alpha_0|111\rangle + \alpha_1|011\rangle] \vee [\alpha_0|001\rangle + \alpha_1|101\rangle] \vee [\alpha_0|010\rangle + \alpha_1|110\rangle] \vee [\alpha_0|000\rangle + \alpha_1|100\rangle]\}$

if $P^{=1}[q_2]$ **then**

5 $\Big(\{[\alpha_0|11\rangle + \alpha_1|01\rangle]_{q,q_1} \vee [\alpha_0|00\rangle + \alpha_1|10\rangle]_{q,q_1}\}\Big) \otimes I_{q_2}$

if $P^{=1}[q_1]$ **then**

4 $\{[\alpha_0|1\rangle + \alpha_1|0\rangle]_q \otimes I_{q_1,q_2}\}$

$q{*} = X$

3 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

end

2 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

end

1 $\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}$

The main difference is step 8, which yields the union of all weakest preconditions for each choice due to the angelic resolution of the nondeterminism. This is because the postcondition only constrains the qubit q, while leaving the ancilla qubits q_1, q_2 unrestricted. Under the angelic interpretation, it is sufficient that there exists a choice establishing the postcondition. Consequently, each choice may require a different ancilla state, and all such possibilities are collected in the union of weakest preconditions. In contrast, the demonic transformer requires a single precondition that is valid for every choice simultaneously. Therefore, only ancilla states common to all choices remain. The distinction disappears after step 10, since the initialization resets both ancilla qubits to $|00\rangle$, which erases the differences between the individual preconditions. After applying the initialization rule, we get

$$
\begin{aligned}
&\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}\cup\\
&\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}\cup\\
&\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}\cup\\
&\{[\alpha_0|0\rangle + \alpha_1|1\rangle]_q \otimes I_{q_1,q_2}\}.
\end{aligned}
$$

This example also illustrates the ordering established in Chapter 7: Throughout the derivation, every angelic weakest precondition is weaker than the corresponding demonic weakest precondition.

Chapter 9

Conclusion

In this thesis, we studied four variants of weakest preconditions for nondeterministic quantum programs. We introduced angelic and demonic weakest preconditions and weakest liberal preconditions and showed that the angelic variants are weaker than the corresponding demonic ones, while the liberal variants are weaker than the corresponding non-liberal ones.

When deriving the corresponding predicate transformers, we found that single projections are not expressive enough for angelic weakest preconditions, as they cannot represent arbitrary sets of states that do not form a closed subspace. To overcome this limitation, we introduced sets of projections as quantum predicates. However, these predicates turned out to be problematic in the demonic setting, where the measurement rule no longer behaves as expected. Restricting predicates to singleton sets resolves this issue. Under this restriction, we derived weakest liberal precondition transformers for both demonic and angelic nondeterminism, with the restriction to finite denotational semantics for loop bodies in the angelic case.

For the non-liberal setting, we used termination spaces to characterize almost sure termination. This allowed us to derive weakest precondition transformers for all language constructs except loops. The main obstacle is capturing almost sure termination by qualitative predicates. Consequently, we were not able to derive weakest precondition transformer rules for loops. Developing them therefore remains the main direction for future work. In particular, it would be interesting to find a qualitative predicate domain capable of expressing almost sure termination.

Another direction for future work concerns the treatment of measurements in the presence of nondeterminism. In the denotational semantics considered in this thesis, the nondeterministic choice is resolved independently of the measurement outcome. Especially for angelic nondeterminism, it would be interesting to study semantic models in which the nondeterministic choice may depend on the observed measurement result and to investigate the corresponding weakest precondition transformers.

Finally, [VK25] also introduces angelic and demonic variants of strongest postconditions and strongest liberal postconditions. Adapting these concepts to nondeterministic quantum programs and deriving corresponding predicate transformers is another promising direction for future research.

Bibliography

[BvN36] Garrett Birkhoff and John von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37(4):823–843, 1936.

[Dij75] Edsger W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Commun. ACM*, 18(8):453–457, 1975. `doi:10.1145/360933.360975`.

[DP06] Ellie D'Hondt and Prakash Panangaden. Quantum weakest preconditions. *Math. Struct. Comput. Sci.*, 16(3):429–451, 2006. `doi:10.1017/S0960129506005251`.

[FX23] Yuan Feng and Yingte Xu. Verification of nondeterministic quantum programs. In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 3, ASPLOS 2023, Vancouver, BC, Canada, March 25-29, 2023*, pages 789–805. ACM, 2023. `doi:10.1145/3582016.3582039`.

[FZXX26] Yuan Feng, Li Zhou, Yingte Xu, and Xiaoquan Xu. Refinement calculus of quantum programs with projective assertions. *ACM Trans. Softw. Eng. Methodol.*, 35(8), July 2026. `doi:10.1145/3770083`.

[GGN17] Jeannine Gabriëls, Stephen Gagola, and Mirko Navara. Sasaki projections. *Algebra Universalis*, 77, 2017. `doi:10.1007/s00012-017-0428-1`.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996. `doi:10.1145/237814.237866`.

[Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, 1969. `doi:10.1145/363235.363259`.

[KBDW83] Karl Kraus, A. Böhm, J. D. Dollard, and W. H. Wootters. *The first Representation theorem*, pages 42–61. 1983. `doi:10.1007/3540127321_24`.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, November 20-22, 1994*, pages 124–134. IEEE Computer Society, 1994. `doi:10.1109/SFCS.1994.365700`.

[Unr18] Dominique Unruh. Quantum relational hoare logic. *CoRR*, abs/1802.03188, 2018. `arXiv:1802.03188`.

[Unr19] Dominique Unruh. Quantum hoare logic with ghost variables. In *34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, June 24-27, 2019*, pages 1–13. IEEE, 2019. doi:10.1109/LICS.2019.8785779.

[VK25] Lena Verscht and Benjamin Lucien Kaminski. A taxonomy of hoare-like logics: Towards a holistic view using predicate transformers and kleene algebras with top and tests. *Proc. ACM Program. Lang.*, 9(POPL):1782–1811, 2025. doi:10.1145/3704896.

[vN55] John von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, 1955.

[Yin11] Mingsheng Ying. Floyd-hoare logic for quantum programs. *ACM Trans. Program. Lang. Syst.*, 33(6):19:1–19:49, 2011. doi:10.1145/2049706.2049708.

[Yin22] Mingsheng Ying. Birkhoff-von neumann quantum logic as an predicate language for quantum programs, 2022. arXiv:2205.01959, doi:10.48550/arXiv.2205.01959.

[ZYY19] 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 2019, Phoenix, AZ, USA, June 22-26, 2019*, pages 1149–1162. ACM, 2019. doi:10.1145/3314221.3314584.