Proving Quantum Programs Correct

Kesha Hietala
University of Maryland, College Park, USA

Robert Rand
University of Chicago, USA

Shih-Han Hung
University of Maryland, College Park, USA

Liyi Li
University of Maryland, College Park, USA

Michael Hicks
University of Maryland, College Park, USA

Abstract

As quantum computing steadily progresses from theory to practice, programmers are faced with a common problem: How can they be sure that their code does what they intend it to do? This paper presents encouraging results in the application of mechanized proof to the domain of quantum programming in the context of the sQIR development. It verifies the correctness of a range of a quantum algorithms including Grover's algorithm and quantum phase estimation, a key component of Shor's algorithm. In doing so, it aims to highlight both the successes and challenges of formal verification in the quantum context and motivate the theorem proving community to target quantum computing as an application domain.

2012 ACM Subject Classification Hardware → Quantum computation; Software and its engineering → Formal software verification

Keywords and phrases Formal Verification, Quantum Computing, Proof Engineering

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Supplementary Material The extended version of this paper is available at `https://www.cs.umd.edu/~mwh/papers/pqpc-extended.pdf`. The code is available at `https://github.com/inQWIRE/SQIR`.

Funding This material is based upon work supported by the U.S. Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, Quantum Testbed Pathfinder Program under Award Number DE-SC0019040.

Acknowledgements We thank Yuxiang Peng for ongoing contributions to the sQIR codebase and pointing out a bug in our original specification for QPE. We thank Xiaodi Wu for discussions about sQIR and follow-on projects.

1 Introduction

Quantum computers are fundamentally different from the "classical" computers we have been programming since the development of the ENIAC in 1945. This difference includes a layer of complexity introduced by quantum mechanics: Instead of a deterministic function from inputs to outputs, a quantum program is a function from inputs to a *superposition* of outputs, a notion that generalizes probabilities. As a result, quantum programs are strictly more expressive than probabilistic programs and even harder to get right: While we can test the output of a probabilistic program by comparing its observed distribution to the desired one, doing the same on a quantum computer can be prohibitively expensive and may not fully describe the underlying quantum state.

This challenge for quantum programming is an opportunity for formal methods: We can use formal methods to *prove*, in advance, that the code implementing a quantum algorithm does what it should for all possible inputs and configurations.

In prior work [14], we developed a formally verified optimizer for quantum programs (VOQC), implemented and proved correct in the Coq proof assistant [5]. Our optimizer transforms programs written in SQIR, a *small quantum intermediate representation*. While we designed SQIR to be a compiler intermediate representation, we quickly realized that it was not so different from languages used to write *source* quantum programs, and that the design choices that eased proving optimizations correct could ease proving source programs correct, too.

To date, we have proved the correctness of implementations of a number of quantum algorithms, including quantum teleportation, Greenberger–Horne–Zeilinger (GHZ) state preparation [12], the Deutsch-Jozsa algorithm [7], Simon's algorithm [29], the quantum Fourier transform (QFT), quantum phase estimation (QPE), and Grover's algorithm [13]. QPE is a key component of Shor's prime-factoring algorithm [28], today's best-known, most impactful quantum algorithm, with Grover's algorithm for unstructured search being the second. Our implementations can be extracted to code that can (in concept, though not in practice, due to resource constraints) be executed on quantum hardware.

While SQIR was first introduced as part of VOQC, this paper offers two new contributions. First, it presents a detailed discussion of how SQIR's design supports proofs of correctness. After presenting background on quantum computing (Section 2) and reviewing SQIR (Section 3), Section 4 discusses key elements of SQIR's design and compares and contrasts them to design decisions made in the most closely related tools, QWIRE [22], QBRICKS [4], and the Isabelle implementation of quantum Hoare logic [15]. SQIR's overall benefit over these tools is its flexibility, supporting multiple semantics and approaches to proof. As a second contribution, this paper presents the code, formal specification, and proof sketch of Grover's algorithm, QFT, and QPE (Section 5). We believe there is ripe opportunity for further application of formal methods to quantum computing and we hope this paper, and our work on SQIR, paves the way for new research; we sketch open problems in Section 6.

SQIR is implemented in just over 3500 lines of Coq, with an additional 3700 lines of example SQIR programs and proofs; it is freely available on Github.[1]

2 Background

We begin with a light background on quantum computing; for a full treatment we recommend the standard text on the subject [19].

2.1 Quantum States

A quantum state consists of one or more *quantum bits*. A quantum bit (or *qubit*) can be expressed as a two dimensional vector $\binom{\alpha}{\beta}$ such that $|\alpha|^2 + |\beta|^2 = 1$. The α and β are called *amplitudes*. We frequently write this vector as $\alpha|0\rangle + \beta|1\rangle$ where $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$ are *basis states*. When both α and β are non-zero, we can think of the qubit as being "both 0 and 1 at once," a.k.a. a *superposition*. For example, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is an equal superposition of $|0\rangle$ and $|1\rangle$ since they share coefficients.

[1] https://github.com/inQWIRE/SQIR

We can join multiple qubits together by means of the *tensor product* $\otimes$ from linear algebra. For convenience, we write $|i\rangle \otimes |j\rangle$ as $|ij\rangle$ for $i, j \in \{0, 1\}$; we may also write $|k\rangle$ where $k \in \mathbb{N}$ is the decimal interpretation of bits ij. We use $|\psi\rangle$ to refer to an arbitrary quantum state. Sometimes a multi-qubit state cannot be expressed as the tensor of individual qubits; such states are called *entangled*. One example is the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, known as a *Bell pair*.

2.2 Quantum Programs

Quantum programs are composed of a series of *quantum operations*, each of which acts on a subset of qubits in the quantum state. In the standard presentation, quantum programs are expressed as *circuits*, as shown in Figure 1(a). In these circuits, each horizontal wire represents a *qubit* and boxes on these wires indicate quantum operations, or *gates*. The circuit in Figure 1(a) uses three qubits and applies three gates: the *Hadamard* (`H`) gate and two *controlled-not* (`CNOT`) gates. The semantics of a gate is a *unitary matrix* (a matrix that preserves the unitarity invariant of quantum states); applying a gate to a state is tantamount to multiplying the state vector by the gate's matrix.

A special, non-unitary *measurement* operation is used to extract classical information from a quantum state (oftentimes at the completion of a computation). Measurement collapses the state to one of the basis states with a probability related to the state's amplitudes. For example, measuring $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ will collapse the state to $|0\rangle$ with probability $\frac{1}{2}$ and likewise for $|1\rangle$, returning classical values 0 or 1, respectively. The semantics of a program involving measurement amounts to a probability distribution over quantum states; in our example above, after the measurement we have a uniform distribution over $|0\rangle$ and $|1\rangle$. Such a distribution is called a *mixed state* (in contrast to *pure states* like $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$). We discuss the mathematical representation of non-unitary programs in Section 3.3.

3 SQIR: A Small Quantum Intermediate Representation

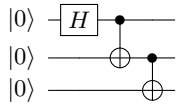
SQIR is a simple quantum language deeply embedded in the Coq proof assistant. This section presents SQIR's syntax and semantics. We defer a detailed discussion of SQIR's design rationale to the next section.

3.1 Unitary SQIR: Syntax

SQIR's *unitary fragment* is a sub-language of full SQIR that can express programs consisting of unitary gates. The full SQIR language extends unitary SQIR with measurement. A program in the unitary fragment has type `ucom` (for "unitary command"), which we define in Coq as follows:

```
Inductive ucom (U: ℕ → Set) (d : ℕ) : Set :=
| useq  : ucom U d → ucom U d → ucom U d
| uapp1 : U 1 → ℕ → ucom U d
| uapp2 : U 2 → ℕ → ℕ → ucom U d
| uapp3 : U 3 → ℕ → ℕ → ℕ → ucom U d.
```

The `useq` constructor sequences two commands; we use notational shorthand `p1 ; p2` for `useq p1 p2`. The three `uapp`i constructors indicate the application of a quantum gate to i qubits (where i is 1, 2, or 3). Qubits are identified as numbered indices into a *global qubit register* of size `d`, which stores the quantum state. Gates are drawn from parameter `U`, which



(a) Quantum circuit

```
H 0;
CNOT 0 1;
CNOT 1 2
```

(b) sQIR assembly

```
Fixpoint ghz (n : ℕ) : ucom base n :=
  match n with
  | 0 ⇒ I 0
  | 1 ⇒ H 0
  | S n' ⇒ ghz n'; CNOT (n'-1) n'
  end.
```

(c) sQIR meta-program

```
box (x,y,z) ⇒
  gate x     ← H x;
  gate (x,y) ← CNOT (x,y);
  gate (y,z) ← CNOT (y,z);
  output (x,y,z).
```

(d) QWIRE

```
SEQ(SEQ(PAR(H, PAR(I, I)),
        PAR(CNOT, I)),
    PAR(I, CNOT))
```

(e) QBRICKS-DSL

```
q1 := H q1;
q1,q2 := CNOT q1,q2;
q2,q3 := CNOT q2,q3
```

(f) QWhile

Figure 1 Example quantum program: GHZ state preparation.

is indexed by a gate's size. For writing and verifying programs, we use the following `base` set for `U`, used by IBM's OpenQASM [6]:[2]

```
Inductive base : ℕ → Set :=
  | U_R (θ ϕ λ : R) : base 1
  | U_CNOT          : base 2.
```

That is, we have a one-qubit gate `U_R` (which we write U_R when using math notation), which takes three real-valued arguments, and the standard two-qubit *controlled-not* gate, `U_CNOT` (written $CNOT$ in math notation), which negates the second qubit wherever the first qubit is $|1\rangle$, making it the quantum equivalent of a *xor* gate.

Example: SWAP

The following Coq function produces a unitary sQIR program that applies three controlled-not gates in a row, with the effect of exchanging two qubits in the register. We define `CNOT` as shorthand for `uapp2 U_CNOT`.

```
Definition SWAP d a b : ucom base d :=
  CNOT a b; CNOT b a; CNOT a b.
```

Example: GHZ

Figure 1(b) is the sQIR representation of the circuit in Figure 1(a), which prepares the three-qubit GHZ state [12]. We describe *families* of sQIR circuits by meta-programming in the Coq host language. The Coq function in Figure 1(c) produces a sQIR program that prepares the n-qubit GHZ state, producing the program in Figure 1(b) when given input 3.

[2] The `U` parameter is most important when sQIR programs are subject to compiler transformations, since the compiler needs to know what gates it can include in an output program.

3.2 Unitary SQIR: Semantics

Each k-qubit quantum gate corresponds to a $2^k \times 2^k$ unitary matrix. The matrices for our `base` set are:

$$[\![U_R(\theta,\phi,\lambda)]\!] = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i(\phi+\lambda)}\cos(\theta/2) \end{pmatrix}, \qquad [\![CNOT]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Conveniently, the U_R gate can encode any single-qubit gate [19, Chapter 4]. For instance, two commonly-used single-qubit gates are X ("not") and H ("Hadamard"). The former has the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and serves to flip a qubit's α and β amplitudes; it can be encoded as $U_R(\pi/2, 0, \pi)$. The H gate has the matrix $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and is often used to put a qubit into superposition (it takes $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$); it can be encoded as $U_R(\pi, 0, \pi)$. Multi-qubit gates are easily produced by combinations of $CNOT$ and U_R; we show the definition of the three-qubit "Toffoli" gate in Section 4.6. Keeping our gate set small simplifies the language and enables easy case analysis—and does does not complicate proofs. We rarely unfold the definition of gates like X or the three-qubit Toffoli, instead providing automation to directly translate these gates to their intended denotations. Hence X is translated directly to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Users can easily extend sQIR with new gates and denotations.

A unitary sQIR program operating on a size-d register corresponds to a $2^d \times 2^d$ unitary matrix. Function `uc_eval` denotes the matrix corresponding to program `c`.

```
Fixpoint uc_eval {d} (c : ucom base d) : Matrix (2^d) (2^d) := ...
```

We write $[\![\texttt{c}]\!]_d$ for `uc_eval d c`. The denotation of composition is simple matrix multiplication: $[\![\texttt{U1; U2}]\!]_d = [\![\texttt{U2}]\!]_d \times [\![\texttt{U1}]\!]_d$. The denotation of `uapp1` is the denotation of its argument gate, but padded with the identity matrix so it has size $2^d \times 2^d$. To be precise, we have:

$$[\![\texttt{uapp1 U q}]\!]_d = \begin{cases} I_{2^q} \otimes [\![U]\!] \otimes I_{2^{d-q-1}} & q < d \\ 0_{2^d} & \text{otherwise} \end{cases}$$

where I_n is the $n \times n$ identity matrix. The denotation of any gate applied to an out-of-bounds qubit is the zero matrix, ensuring that a circuit corresponds to a zero matrix if and only if it is ill-formed. We likewise prove that every proper (well-typed) circuit corresponds to a unitary matrix.

For $[\![\texttt{CNOT q1 q2}]\!]_d$, we decompose $CNOT$ into $|0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes X$, where $|0\rangle\langle 0| = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $|1\rangle\langle 1| = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We then pad the expression appropriately, obtaining the following when $q_1 < q_2 < d$:

$$I_{2^{q_1}} \otimes |0\rangle\langle 0| \otimes I_{2^{q_2-q_1-1}} \otimes I_2 \otimes I_{2^{d-q_2-1}} \;+\; I_{2^{q_1}} \otimes |1\rangle\langle 1| \otimes I_{2^{q_2-q_1-1}} \otimes X \otimes I_{2^{d-q_2-1}}.$$

When $q_2 < q_1 < d$, we obtain a symmetric expression, and when $q_1 = q_2$ or either qubit is out of bounds, we obtain the zero matrix.

Example: Verifying SWAP

we can prove in Coq that `SWAP 2 0 1`, which swaps the first and second qubits in a two-qubit register, behaves as expected on two unentangled qubits:

```
Lemma swap2: ∀ (ϕ ψ : Vector 2), WF_Matrix ϕ → WF_Matrix ψ →
  [[SWAP 2 0 1]]_2 × (ϕ ⊗ ψ) = ψ ⊗ ϕ.
```

`WF_Matrix` says that ϕ and ψ are well-formed vectors of length 2 [26, Section 2]. This proof can be completed by simple matrix multiplication. In the full development we prove the correctness of `SWAP d a b` for arbitrary dimension `d` and qubits `a` and `b`.

3.3 Full SQIR: Adding Measurement

The full sQIR language adds a branching measurement construct inspired by Selinger's QPL [27]. This construct permits measuring a qubit, taking one of two branches based on the measurement outcome. Full sQIR defines "commands" `com` as either a unitary sub-program, a no-op `skip`, branching measurement, or a sequence of these.

```
Inductive com (U: ℕ → Set) (d : ℕ) : Set :=
| uc   : ucom U d → com U d
| skip : com U d
| meas : ℕ → com U d → com U d → com U d
| seq  : com U d → com U d → com U d.
```

The command `meas q` P_1 P_2 measures qubit `q` and performs P_1 if the outcome is 1 and P_2 if it is 0. We define non-branching measurement and resetting to a zero state in terms of branching measurement:

```
Definition measure q := meas q skip skip.
Definition reset q := meas q (X q) skip.
```

As before, we use our `base` set of unitary gates in this paper.

Example: Flipping a Coin

It is easy to generate a truly random coin flip with a quantum computer: Use the Hadamard gate to put a qubit into equal superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and then measure it.

```
Definition coin : com base 1 := H 0; measure 0.
```

Density Matrix Semantics

As discussed in Section 2.2, measurement induces a probabilistic transition, so the semantics of a program with measurement is a probability distribution over states, called a mixed state. As is standard [22, 30], we represent such a state using a *density matrix*. The density matrix of a pure state $|\psi\rangle$ is $|\psi\rangle\langle\psi|$ where $\langle\psi| = |\psi\rangle^\dagger$ is the conjugate transpose of $|\psi\rangle$. The density matrix of a mixed state is a sum over its constituent pure states. For example, the density matrix corresponding to the uniform distribution over $|0\rangle$ and $|1\rangle$ is $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.

The semantics $\{\!|\texttt{P}|\!\}_d$ of a full sQIR program `P` is a function from density matrices to density matrices. Naturally, $\{\!|\texttt{skip}|\!\}_d\ \rho = \rho$ and $\{\!|\texttt{P1 ; P2}|\!\}_d = \{\!|\texttt{P2}|\!\}_d \circ \{\!|\texttt{P1}|\!\}_d$. For unitary subroutines, we have $\{\!|\texttt{uc U}|\!\}_d\ \rho\ = [\![\texttt{U}]\!]_d \rho [\![\texttt{U}]\!]_d{}^\dagger$: Applying a unitary matrix to a state vector is equivalent to applying it to both sides of the density matrix. Finally, using $|i\rangle_q\langle j|$ for $I_{2^q} \otimes |i\rangle\langle j| \otimes I_{2^{d-q-1}}$, the semantics for $\{\!|\texttt{meas q P1 P2}|\!\}_d\ \rho$ is

$$\{\!|P_1|\!\}_d(|1\rangle_q\langle 1|\,\rho\,|1\rangle_q\langle 1|) + \{\!|P_2|\!\}_d(|0\rangle_q\langle 0|\,\rho\,|0\rangle_q\langle 0|)$$

which corresponds to probabilistically applying `P1` to ρ with the specified qubit projected to $|1\rangle\langle 1|$ or applying `P2` to a similarly altered ρ.

Example: A Provably Random Coin

We can now prove that our `coin` circuit above produces the $|1\rangle\langle 1|$ or $|0\rangle\langle 0|$ density matrix, each with probability $\frac{1}{2}$.

```
Lemma coin_dist : ⟦coin⟧1 |0⟩⟨0| = ½|1⟩⟨1| + ½|0⟩⟨0|.
```

The proof proceeds by simple matrix arithmetic. $\llbracket \texttt{H} \rrbracket\ |0\rangle\langle 0|$ is $H\,|0\rangle\langle 0|\,H^\dagger = \frac{1}{2}\left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)$. Calling this ρ_{12}, applying `measure` yields $|1\rangle\langle 1|\,\rho_{12}\,|1\rangle\langle 1| + |0\rangle\langle 0|\,\rho_{12}\,|0\rangle\langle 0|$, which can be further simplified using the fact $\langle 1|\,\rho_{12}\,|1\rangle = \langle 0|\,\rho_{12}\,|0\rangle = \left(\frac{1}{2}\right)$, yielding $\frac{1}{2}\,|1\rangle\langle 1| + \frac{1}{2}\,|0\rangle\langle 0|$ as desired.

Measurement plays a key role in many quantum algorithms; we discuss further examples and an alternative semantics in Appendix B.

4 SQIR's Design

This section describes key elements in the design of SQIR and its infrastructure for verifying quantum programs. To place those decisions in context, we introduce several related verification frameworks first, and contrast SQIR's design with theirs. In summary, SQIR benefits from the use of *concrete indices into a global register* (a common feature in the tools we looked at), support for *reasoning about unitary programs in isolation* (supported by one other tool), and the *flexibility to allow different semantics and approaches to proof* (best supported in SQIR).

4.1 Related Approaches

Our goal with SQIR has been to build a proof assistant-based framework for proving (realistic) quantum programs correct. We are not the first to have this goal. In 2010, Green [11] developed an Agda implementation of the Quantum IO Monad, and in 2015 Boender et al. [3] produced a small Coq quantum library. These were both proofs of concept, and were only capable of verifying basic protocols. There have been several more recent, substantial works on verified quantum programming, to which we can compare SQIR's design: QWIRE [24] (implemented in Coq); quantum Hoare logic (QHL) [16] (implemented in Isabelle [20]); and QBRICKS [4] (implemented in Why3 [8]). These three are the only tools aside from SQIR that have been used to verify interesting, parameterized quantum programs.

QWIRE

The QWIRE language [22, 24] originated as an embedded circuit description language in the style of Quipper [10] but with a more powerful type system. Figure 1(d) shows the QWIRE equivalent of the SQIR program in Figure 1(b). QWIRE uses variables from the host language Coq to reference qubits, an instantiation of higher-order abstract syntax [23]. In Figure 1, the QWIRE program uses variables `x`, `y`, and `z`, while the SQIR program uses indices 0, 1, and 2 to refer to the first, second, and third qubits in the global register. QWIRE does not distinguish between unitary and non-unitary programs, and thus uses density matrices for its semantics. QWIRE has been used to verify simple randomness generation circuits and a few textbook examples [25].

QBRICKS

QBRICKS [4] is a quantum proof framework implemented in Why3 [8], developed concurrently with SQIR. QBRICKS provides a domain-specific language (DSL) for constructing quantum

circuits using combinators for parallel and sequential composition (among others). Figure 1(e) presents the GHZ example written in QBRICKS' DSL. The semantics of QBRICKS are based on the *path-sums* formalism by Amy [1, 2], which can express the semantics of unitary programs in a form amenable to proof automation. QBRICKS extends path-sums to support parameterized circuits. QBRICKS has been used to verify a variety of quantum algorithms, including Grover's algorithm [13] and Quantum Phase Estimation (QPE).

Quantum Hoare logic

Quantum Hoare logic (QHL) [30] has recently been formalized in the Isabelle/HOL proof assistant [15]. QHL is built on top of the quantum while language (QWhile), which is the quantum analog of the classical while language, allowing looping and branching on measurement results. Figure 1(f) presents the GHZ example written in QHL. QWhile does not use a fixed gate set; gates are instead described directly by their unitary matrices. As such, the program in Figure 1(f) could instead be written as the application of a single gate that prepares the 3-qubit GHZ state. Given that measurement is a core part of the language, QWhile's semantics are given in terms of (partial) density matrices. A density matrix is *partial* when it may represent a sub-distribution—that is, a subset of the outcomes of measurement.

QHL has been used to verify Grover's algorithm [15]. An earlier effort by Liu et al. [17] to formalize QHL claimed to prove correctness of QPE, too. However, the approach used a combination of Isabelle/HOL and Python, calling out to Numpy to solve matrix (in)equalities; as such, we consider this only a partial verification effort. We cannot find a proof of QPE in the associated Github repository[3] and believe that this approach was abandoned in favor of Liu et al. [15].

4.2 Concrete Indices into a Global Register

The first key element of SQIR's design is its use of concrete indices into a fixed-sized global register to refer to qubits. For example, in our `SWAP` program (end of Section 3.1), `a` and `b` are natural numbers indexing into a global register of size `d`. Expressing the semantics of a program that uses concrete indices is simple because concrete indices map directly to the appropriate rows and columns in the denoted matrix. Moreover, it is easy to check relationships between operations—`X a` and `X b` act on the same qubit if and only if `a` = `b`. Keeping the register size fixed means that the denoted matrix's size is known, too.

On the other hand, concrete indices hamper programmability. The `ghz` example in Figure 1(c) only produces circuits that occupy global qubits 0...`n`; we could imagine further generalizing it to add a lower bound `m` (so the circuit uses qubits `m` ... `n`), but it is not clear how it could be generalized to use non-contiguous wires. A natural solution, employed by QWIRE (and also Quipper [10]), is to use host-level variables to refer to *abstract* qubits that can be freely introduced and discarded, simplifying circuit construction and sub-program composition. Unfortunately, abstract qubits significantly complicate formal verification. To translate circuits to operations on density matrices, variables must be mapped to concrete matrix indices. Each time a qubit is discarded, indices undergo a de Bruijn-style shifting, which immensely complicates inductive reasoning about circuits.

Similar to SQIR's use of concrete indices, QBRICKS-DSL's compositional structure makes it easy to map programs to their denotation: The "index" of a gate application can be

[3] `https://github.com/ijcar2016/propitious-barnacle`

computed by its nested position in the program. However, this syntax is even less convenient than sQIR's for programming: Although QBRICKS provides a utility function for defining `CNOT` gates between non-adjacent qubits, their underlying syntax does not support this, meaning that expressions like `CNOT 7 2` are translated into large sequences of `CNOT` gates. QHL is presented as having variables, but these variables are fixed before a program is executed and persist throughout the program. In the Isabelle formalization, these variables are represented by natural numbers, making them similar to sQIR concrete indices.

4.3 Extensible Language around a Unitary Core

Another key aspect of sQIR's design is its decomposition into a unitary sub-language and the non-unitary full language. While the full language (with measurement) is more powerful, its density matrix-based semantics adds unneeded complication to the proof of unitary programs. For example, given the program $U_1; U_2; U_3$, its unitary semantics is a matrix $U_3 \times U_2 \times U_1$ while its density matrix semantics is a function $\rho \mapsto U_3 \times U_2 \times U_1 \times \rho \times U_1^\dagger \times U_2^\dagger \times U_3^\dagger$. The latter is a larger term, with a type that is harder to work with. This added complexity, borne by QWIRE and QHL, lacks a compelling justification given that many near-term algorithms can be viewed as unitary programs with measurement occurring implicitly at their conclusion (see Section 4.7).

On the other hand, QBRICKS' semantics is based on (higher-order) path-sums, which cannot describe mixed states, and thus cannot give a semantics to measurement. sQIR's design allows for a "best of both worlds," utilizing a unitary semantics when possible, but supporting non-unitary semantics when needed. Furthermore, as we show in Section 4.6, abstractions like path-sums can be easily defined on top of sQIR's unitary semantics.

4.4 Semantics of Ill-typed Programs

We say that a sQIR program is well-typed if every gate is applied to indices within range of the global register and indices used in each multi-qubit gate are distinct. This second condition enforces linearity and thereby quantum mechanic's *no-cloning theorem*, which disallows copying an arbitrary quantum state. As an example, `SWAP d a b` is well-typed if $a < d$, $b < d$, and $a \neq b$.

QWIRE addresses this issue through its linear type system, which also guarantees that qubits are never reused. However, well-typedness is a (non-trivial) extrinsic proposition in QWIRE, meaning that many proofs require an assumption that the input program is well-typed and must manipulate this typing judgment within the proof. QBRICKS avoids the issue of well-typedness through its language design: It is not possible to construct an ill-typed circuit using sequential and parallel composition. The Isabelle implementation of QHL uses a well-typedness predicate to enforce some program restrictions (e.g. the gate in a unitary application is indeed a unitary matrix), but the issue of gate argument validity is enforced by Isabelle's type system: Gate arguments are represented as a set (disallowing duplicates) where all elements are valid variables.

In sQIR, ill-typed programs are denoted by the zero matrix. This often means that we do not need to explicitly assume or prove that a program is well-typed in order to state a property about its semantics, thereby removing clutter from theorems and proofs. For example, we can prove symmetry of `SWAP`, i.e. `SWAP d a b` $\equiv$ `SWAP d b a`, without any well-typedness constraint because either both sides of the equation are well-typed or both are ill-typed. However, we cannot always avoid well-typedness preconditions. Say we want to prove transitivity of `SWAP`, i.e. `SWAP d a c` $\equiv$ `SWAP d a b ; SWAP d b c`. In this case the left-hand side may be well-typed

while the right-hand side is ill-typed. To verify this equivalence, we (minimally) need the precondition `b` $<$ `d` $\wedge$ `b` $\neq$ `a` $\wedge$ `b` $\neq$ `c`.

4.5 Automation for Matrix Expressions

The sQIR development provides a variety of automation for dealing with matrix expressions. Most of this automation is focused on simplifying matrix terms to be easier to work with. The best example of this is our `gridify` tactic [14, Section 4.5], which rewrites terms into *grid normal form* where matrix addition is on the outside, followed by tensor product, with matrix multiplication on the inside, i.e., $((.. \times ..) \otimes (.. \times ..)) + ((.. \times ..) \otimes (.. \times ..))$. Most of the circuit equivalences available in sQIR (e.g. $\forall$ `a`, `b`, `c`. `CNOT a c ; CNOT b c` $\equiv$ `CNOT b c ; CNOT a c`) are proved using `gridify`. This style of automation is available in other verification tools too; `gridify` is similar to Liu et al.'s Isabelle tactic for matrix normalization [15, Section 5.1]. QBRICKS avoids the issue by using path-sums; they provide a matrix semantics for comparison's sake, but do not discuss automation for it.

Some of our automation is aimed at alleviating difficulties caused by our use of *phantom types* to store the dimensions of a matrix, the rationale of which is explained in our previous work [14, Section 3.3]. In our development, matrices have the type `Matrix m n`, where `m` is the number of rows and `n` is the number of columns. One challenge with this definition is that the dimensions stored in the type may be "out of sync" with the structure of the expression itself. For example, due to simplification, rewriting, or declaration, the expression $|0\rangle \otimes |0\rangle$ may be annotated with the type `Vector` 4, although rewrite rules expect it to be of the form `Vector` $(2 * 2)$. We provide a tactic `restore_dims` that analyzes the structure of a term and rewrites its type to the desired form, allowing for more effective automated simplification.

4.6 Vector State Abstractions

To verify that the `SWAP` program has the intended semantics, we can unfold its definition (`CNOT a b`; `CNOT b a`; `CNOT a b`) and compute the associated matrix expression. However, while this proof is made simpler by automation like `gridify`, it is still fairly complicated considering that `SWAP` has a simple classical (non-quantum) purpose. In fact, this operation is much more naturally analyzed using its action on basis states. A *(computational) basis state* is any state of the form $|i_0 \dots i_d\rangle$ (so $|00\rangle$ and $|11\rangle$ are basis states, while $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is not). The set of all d-qubit basis states form a basis for the underlying d-dimensional vector space, meaning that any $2^d \times 2^d$ unitary operation can be uniquely described by its action on those basis states.

Using basis states, the reasoning for our `SWAP` example proceeds as follows, where we use $|\dots x \dots y \dots\rangle$ as informal notation to describe the state where the qubit at index a is in state x and the qubit at index b is in state y.

1. Begin with the state $|\dots x \dots y \dots\rangle$.
2. $CNOT\ a\ b$ produces $|\dots x \dots (x \oplus y) \dots\rangle$.
3. $CNOT\ b\ a$ produces $|\dots (x \oplus (x \oplus y)) \dots (x \oplus y) \dots\rangle = |\dots y \dots (x \oplus y) \dots\rangle$.
4. $CNOT\ a\ b$ produces $|\dots y \dots (y \oplus (x \oplus y)) \dots\rangle = |\dots y \dots x \dots\rangle$.

In our development, we describe basis states using `f_to_vec d f` where `d` : $\mathbb{N}$ and `f` : $\mathbb{N} \to \mathbb{B}$. This describes a d-qubit quantum state where qubit i is in the basis state $f(i)$, and `false` corresponds to 0 and `true` to 1. We also sometimes describe basis states using `basis_vector d i` where $i < 2^d$ is the index of the only 1 in the vector. We provide methods to translate between the two representations (simply converting between binary and decimal encodings).

We prove a variety of facts about the actions of gates on basis states. For example, the following succinctly describe the behavior of the $CNOT$ and $Rz(\theta)$ gates, where $Rz(\theta) = U_R(0, 0, \theta)$:

```
Lemma f_to_vec_CNOT : ∀ (d i j : ℕ) (f : ℕ → 𝔹),
  i < d → j < d → i ≠ j →
  ⟦CNOT i j⟧_d × (f_to_vec d f) = f_to_vec d (update f j (f j ⊕ f i)).

Lemma f_to_vec_Rz: ∀ (d j : ℕ) (θ : R) (f : ℕ → 𝔹),
  j < d →
  ⟦Rz θ j⟧_d × (f_to_vec d f) = e^(iθ(f j)) * f_to_vec d f.
```

There are several advantages to applying these rewrite rules instead of unfolding the definitions of $[\![\texttt{CNOT i j}]\!]_d$ and $[\![\texttt{Rz } \theta \texttt{ j}]\!]_d$. For example, these rewrite rules assume well-typedness and do not depend on the ordering of qubit arguments, avoiding the case analysis needed in `gridify` [14, Section 4.5]. In addition, the rule for $CNOT$ above is simpler to work with than the general unitary semantics ($CNOT \mapsto \_ \otimes |1\rangle\langle 1| \otimes \_ \otimes \sigma_x \otimes \_ \; + \; \_ \otimes |0\rangle\langle 0| \otimes \_ \otimes I_2 \otimes \_$).

As a concrete example of where vector-based reasoning was critical, consider the three-qubit Toffoli gate, which implements a *controlled-controlled-not*, and can be thought of as the quantum equivalent of an *and* gate. It is frequently used in algorithms, but (like all n-qubit gates with $n > 2$) rarely supported in hardware, meaning that it must be decomposed into more basic gates before execution. In practice, we found `gridify` too inefficient to verify the standard decomposition of the gate [19, Chapter 4], shown below.

```
Definition TOFF {d} a b c : ucom base d :=
  H c ; CNOT b c ; T† c ; CNOT a c ; T c ; CNOT b c ; T† c ;
  CNOT a c ; CNOT a b ; T† b ; CNOT a b ; T a ; T b ; T c ; H c.
```

However, like `SWAP`, the semantics of the Toffoli gate is naturally expressed through its action on basis states:

```
Lemma f_to_vec_TOFF : ∀ (d a b c : ℕ) (f : ℕ → 𝔹),
  a < d → b < d → c < d →
  a ≠ b → a ≠ c → b ≠ c →
 ⟦TOFF a b c⟧_d × (f_to_vec d f) = f_to_vec d (update f c (f c ⊕ (f a && f b))).
```

The proof of `f_to_vec_TOFF` is almost entirely automated using a tactic that rewrites using the `f_to_vec` lemmas shown above, since `T` and `T†` are `Rz (PI / 4)` and `Rz (−PI / 4)`, respectively.

The `f_to_vec` abstraction is simple and easy to use, but not universally applicable: Not all quantum algorithms produce basis states, or even sums over a small number of basis states, and reasoning about 2^d terms of the form $|i_1 \dots i_d\rangle$ is no easier than reasoning directly about matrices. To support more general types of quantum states we define indexed sums and tensor (Kronecker) products of vectors.

```
Fixpoint vsum {d} n (f: ℕ → Vector d) : Vector d :=
  match n with
  | 0 ⇒ Zero
  | S n' ⇒ vsum n' f + f n'
  end.
Fixpoint vkron n (f: ℕ → Vector 2) : Vector 2^n :=
  match n with
  | 0    ⇒ I 1
  | S n' ⇒ vkron n' f ⊗ f n'
  end.
```

As an example of a state that uses these constructs, the action of n parallel Hadamard gates on the state `f_to_vec n f` can be written as

$$\texttt{vkron n (fun i} \Rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(i)}\,|1\rangle)) \quad \text{or}$$
$$\tfrac{1}{\sqrt{2^n}} * (\texttt{vsum } 2^n \texttt{ (fun i} \Rightarrow (-1)^{\texttt{to\_int}(f)*i} * \texttt{basis\_vector n i})),$$

both commonly-used facts in quantum algorithms. In Section 5 we will write $|f\rangle$ for `f_to_vec n f`, $|i\rangle$ for `basis_vector n i`, $\sum_{i=0}^{n-1} f(i)$ for `vsum n (fun i ⇒ f i)`, and $\bigotimes_{i=0}^{n-1} f(i)$ for `vkron n (fun i ⇒ f i)`.

Relation with Path-sums

Our `vsum` and `vkron` definitions share similarities with the *path-sums* [1, 2] semantics used by QBRICKS [4]. In the path-sums formalism, every unitary transformation is represented as a function of the form

$$|x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{2\pi i P(x,y)/2^m}\,|f(x,y)\rangle$$

where $m \in \mathbb{N}$, P is an arithmetic function over x and y, and f is of the form $|f_1(x,y)\rangle \otimes \cdots \otimes |f_m(x,y)\rangle$ where each f_i is a Boolean function over x and y. For instance, the Hadamard gate H has the form $|x\rangle \to \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i x y/2}\,|y\rangle$. Path-sums provide a compact way to describe the behavior of unitary matrices, and are closed under matrix and tensor products, making them well-suited for automation. They can be naturally described in terms of our `vkron` and `vsum` vector-state abstractions:

```
Definition path_sum (m : ℕ) P f x :=
  vsum 2^m (fun y ⇒ e^(2*π*i*P(x,y)/2^m) * (vkron m (fun i ⇒ f i x y))).
```

As above, `P` is an arithmetic function over `x` and `y` and `f i` is a Boolean function over `x` and `y` for any `i`.

4.7 Measurement Predicates

The proofs in Section 5 do not use the non-unitary semantics directly, but describe the probability of different measurement outcomes using predicates `probability_of_outcome` and `prob_partial_meas`.

```
(* Probability of measuring φ given input ψ. *)
Definition probability_of_outcome {n} (φ ψ : Vector n) : R :=
  let c := (φ† × ψ) 0 0 in |c|².

(* Probability of measuring φ on the first n qubits given (n+m) qubit input ψ. *)
Definition prob_partial_meas {n m} (φ : Vector 2^n) (ψ : Vector 2^(n+m)) :=
  ‖ (φ† ⊗ I 2^m) × ψ ‖².
```

Above, $\|v\|$ is the 2-norm of vector v and $|c|$ is the complex norm of c. In formal terms, the "probability of measuring φ" is the probability of outcome φ when measuring a state in the basis $\{\varphi \times \varphi^\dagger, \mathtt{I}_{2^n} - \varphi \times \varphi^\dagger\}$.

We find these predicates sufficient for our use cases, since the programs we verify are purely quantum. That is, they do not use classical subroutines, so we can analyze their outcome purely in terms of the state vector produced. In fact, the *principle of deferred measurement* [19, Chapter 4] says that measurement can always be deferred until the end of

```
(* Controlled-X with target (n-1) and controls 0, 1, ..., n-2. *)
Fixpoint generalized_Toffoli' n0 : ucom base n :=
  match n0 with
  | 0 | S 0 ⇒ X (n - 1)
  | S n0' ⇒ control (n - n0) (generalized_Toffoli' n0')
  end.
Definition generalized_Toffoli := generalized_Toffoli' n.

(* Diffusion operator. *)
Definition diff : ucom base n :=
  npar n H; npar n X ;
  H (n - 1) ; generalized_Toffoli ; H (n - 1) ;
  npar n X; npar n H.

(* Main program (iterates applying U_f and diff). *)
Definition body := U_f ; cast diff (S n).
Definition grover i := X n ; npar (S n) H ; niter i body.
```

Figure 2 Grover's algorithm in sQIR. `control` performs a unitary program conditioned on an input qubit, `npar` performs copies of a unitary program in parallel, `cast` is a no-op that changes the dimension in a `ucom`'s type, and `niter` iterates a unitary program.

a quantum computation without changing the result. However, we included measurement in Section 3.3 because it is a standard feature of quantum programming languages and used in a variety of constructs like repeat-until-success loops [21] and error-correcting codes [9]. QBRICKS also uses measurement predicates, but unlike sQIR does not support a general measurement construct.

5 Proofs of Quantum Algorithms

In this section we discuss the formal verification of two classic quantum algorithms: Grover's algorithm [19, Chapter 6] and quantum phase estimation [19, Chapter 5]. We present several additional examples in Appendices B and C. All proofs follow the corresponding textbook argument.

5.1 Grover's Algorithm

Overview

Given a circuit implementing Boolean oracle $f : \{0,1\}^n \to \{0,1\}$, the goal of Grover's algorithm is to find an input x satisfying $f(x) = 1$. Suppose that $n \geq 2$. In the classical (worst-)case, the solution requires $O(2^n)$ queries to the oracle. However, the quantum algorithm finds a solution with high probability using only $O(\sqrt{2^n})$ queries.

The algorithm alternates between applying the oracle and a "diffusion operator." Individually, these operations each perform a reflection in the two-dimensional space spanned by the input vector (a uniform superposition) and a uniform superposition over the solutions to f. Together, they perform a rotation in the same space. By choosing an appropriate number of iterations i, the algorithm will rotate the input state to be suitably close to the solution vector. The sQIR definition of Grover's algorithm is shown in Figure 2.

The sQIR version of Grover's algorithm is 15 lines, excluding utility definitions like `control`

and `npar`. The specification and proof are around 770 lines. The proof took approximately one person-week.

Proof Details

The statement of correctness says that after i iterations, the probability of measuring a solution is $\sin^2((2i+1)\theta)$ where $\theta = \arcsin(\sqrt{k/2^n})$ and k is the number of satisfying solutions to f. Note that this implies that the optimal number of iterations is $\frac{\pi}{4}\sqrt{\frac{2^n}{k}}$.

We begin the proof by showing that the uniform superposition can be rewritten as a sum of "good" states (ψ`g`) that satisfy f and "bad" states (ψ`b`) that do not satisfy f.

```
Definition ψ := 1/√(2^n) * Σ_{k=0}^{2^n-1} |k⟩.
Definition θ := asin (√(k/2^n)).
Lemma decompose_ψ : ψ = (sin θ) ψg + (cos θ) ψb.
```

We then prove that `U`$_{\texttt{f}}$ and `diff` perform the expected reflections (e.g. $[\![\texttt{diff}]\!]_n = -2\left|\psi\right\rangle\left\langle\psi\right| + I_{2^n}$) and the following key lemma, which shows the output state after i iterations of `body`.

```
Lemma loop_body_action_on_unif_superpos : ∀ i,
  [[body]]^i_{n+1} (ψ ⊗ |-⟩) =
    (-1)^i (sin ((2 * i + 1) * θ) ψg + cos ((2 * i + 1) * θ) ψb) ⊗ |-⟩.
```

This property is straightforward to prove by induction on `i`, and implies the desired result, which specifies the probability of measuring any solution to f.

```
Lemma grover_correct : ∀ i,
  Rsum 2^n (fun z ⇒  if f z
                     then prob_partial_meas |z⟩ ([[grover i]]_{n+1} × |0⟩^{n+1})
                     else 0) =
  (sin ((2 * i + 1) * θ))^2.
```

Above, `Rsum` is a sum over real numbers.

5.2 Quantum Phase Estimation

Overview

Given a unitary matrix U and eigenvector $\left|\psi\right\rangle$ such that $U\left|\psi\right\rangle = e^{2\pi i\theta}\left|\psi\right\rangle$, the goal of quantum phase estimation (QPE) is to find a k-bit representation of θ. In the case where θ can be exactly represented using k bits (i.e. $\theta = z/2^k$ for some $z \in \mathbb{Z}$), QPE recovers θ exactly. Otherwise, the algorithm finds a good k-bit approximation with high probability. QPE is often used as a subroutine in quantum algorithms, most famously Shor's factoring algorithm [28].

The full sQIR definition of QPE is given in Appendix A. The sQIR definition of the quantum Fourier transform (QFT), which is used as a subroutine in QPE, is given in Figure 3.

The sQIR version of QPE is around 40 lines and the specification and proof in the simple case ($\theta = z/2^k$) is around 800 lines. The fully general case ($\theta \neq z/2^k$) adds about 250 lines. The proof of the simple case was completed in about two person-weeks. When working out the proof of the general case, we found that we needed some non-trivial bounds on trigonometric functions (for $x \in \mathbb{R}$, $|\sin(x)| \leq |x|$ and if $|x| \leq \frac{1}{2}$ then $|2 * x| \leq |\sin(\pi x)|$). Laurent Théry kindly provided proofs of these facts using the Coq Interval package [18].

```
(* Controlled rotation cascade on n qubits. *)
Fixpoint controlled_rotations n : ucom base n :=
  match n with
  | 0 | 1 ⇒ SKIP
  | S n'  ⇒ controlled_rotations n' ; control n' (Rz (2π / 2^n) 0)
  end.

(* Quantum Fourier transform on n qubits. *)
Fixpoint QFT n : ucom base n :=
  match n with
  | 0    ⇒ SKIP
  | 1    ⇒ H 0
  | S n' ⇒ H 0 ; controlled_rotations n ; map_qubits (fun q ⇒ q + 1) (QFT n')
  end.
```

Figure 3 sQIR definition of QFT. Here, `map_qubits` increments the qubit indices.

Proof Details

The correctness property for QPE in the case where θ can be described exactly using k bits ($\theta = z/2^k$) says that the QPE program will exactly recover z. It can be stated in sQIR's development as follows.

```
Lemma QPE_correct_simplified: ∀ k n (u : ucom base n)
  z (ψ : Vector 2^n), n > 0 →
  k > 1 → uc_well_typed u → WF_Matrix ψ →
  let θ := z / 2^k in
  ⟦u⟧_n × ψ = e^{2πiθ} * ψ →
  ⟦QPE k n u⟧_{k+n} × (|0⟩^k ⊗ ψ) = |z⟩ ⊗ ψ.
```

The first four conditions ensure well-formedness of the inputs. The fifth condition enforces that input ψ is an eigenvector of c. The conclusion says that running the `QPE` program computes the value z, as desired.

In the general case where θ cannot be exactly described using k bits, we instead prove that `QPE` recovers the best k-bit approximation with high probability (in particular, with probability $\geq 4/\pi^2$).

```
Lemma QPE_semantics_full : ∀ k n (u : ucom base n) z
      (ψ : Vector 2^n) (δ : R),
  n > 0 → k > 1 → uc_well_typed u →
  Pure_State_Vector ψ →
  -1 / 2^{k+1} ≤ δ < 1 / 2^{k+1} → δ ≠ 0 →
  let θ := z / 2^k + δ in
  ⟦u⟧_n × ψ = e^{2πiθ} * ψ →
  prob_partial_meas |z⟩ (⟦QPE k n u⟧_{k+n} × (|0⟩^k ⊗ ψ)) ≥ 4 / π^2.
```

`Pure_State_Vector` is a restricted form of `WF_Matrix` that requires a vector to have norm 1.

As an example of the reasoning that goes into proving these properties, consider the QFT subroutine of QPE (Figure 3). The correctness property for `controlled_rotations` says that evaluating the program on input $|x\rangle$ will produce the state $e^{2\pi i(x_0 \cdot x_1x_2...x_{n-1})/2^n}|x\rangle$ where x_0 is the highest-order bit of x represented as a binary string and $x_1x_2...x_{n-1}$ are the lower-order $n-1$ bits.

$$
\begin{aligned}
&[\![\texttt{controlled\_rotations (n+1)}]\!]_{n+1} \times |x\rangle \\
&\quad = [\![\texttt{control } x_n \ (\texttt{Rz } (2\pi/2^{n+1})\ 0]\!]_{n+1} \times [\![\texttt{controlled\_rotations n}]\!]_{n+1} \times |x\rangle \\
&\quad = [\![\texttt{control } x_n \ (\texttt{Rz } (2\pi/2^{n+1})\ 0]\!]_{n+1} \times e^{2\pi i(x_0 \,\cdot\, x_1x_2...x_{n-1})/2^n} |x_1x_2...x_{n-1}x_n\rangle \\
&\quad = e^{2\pi i(x_0 \,\cdot\, x_n)/2^{n+1}} e^{2\pi i(x_0 \,\cdot\, x_1x_2...x_{n-1})/2^n} |x_1x_2...x_{n-1}x_n\rangle \\
&\quad = e^{2\pi i(x_0 \,\cdot\, x_1x_2...x_n)/2^{n+1}} |x_1x_2...x_{n-1}x_n\rangle
\end{aligned}
$$

Figure 4 Reasoning used in the proof of `controlled_rotations`. The first step unfolds the definition of `controlled_rotations`; the second step applies the inductive hypothesis; the third step evaluates the semantics of `control`; and the fourth step combines the exponential terms.

```
Lemma controlled_rotations_correct : ∀ n x,
  n > 1 → ⟦controlled_rotations n⟧n × |x⟩ = e^{2πi(x0 · x1x2...xn−1)/2^n} |x⟩.
```

We can prove this property via induction on n. In the base case ($n = 2$) we have that x is a 2-bit string x_0x_1. In this case, the output of the program is $e^{2\pi i(x_0 \cdot x_1)/2^2} |x_0x_1\rangle$, as desired. In the inductive step, we assume that:

$$[\![\texttt{controlled\_rotations n}]\!]_n \times |x_1x_2...x_{n-1}\rangle = e^{2\pi i(x_0 \,\cdot\, x_1x_2...x_{n-1})/2^n} |x_1x_2...x_{n-1}\rangle.$$

We then perform the simplifications shown in Figure 4, which complete the proof.

Our correctness property for `QFT n` (shown below) can similarly be proved by induction on n, and relies on the lemma `controlled_rotations_correct`.

```
Lemma QFT_semantics : ∀ n x, n>0 → ⟦QFT n⟧n × |x⟩ = 1/√2^n ⨂_{j=0}^{n−1} (|0⟩ + e^{2πix/2^{n−j}} |1⟩).
```

6 Open Problems and Future Work

We previously presented sQIR as the intermediate representation in a verified circuit optimizer [14]. In this paper, we presented sQIR as a source language for quantum programming and discussed how our design choices (e.g. concrete indices, unitary core, vector state abstractions) ease proofs about sQIR programs. But there is still work to be done.

So far, work on formally verified quantum computation has been limited to textbook quantum algorithms like QPE and Grover's. Although these algorithms are a useful stress-test for tools, they do not accurately reflect the types of quantum programs that are expected to run on near-term machines. Near-term algorithms are usually *approximate*. They do not implement the desired operation exactly, but rather perform an operation "close" to what was intended. Our `probability_of_outcome` and `prob_partial_meas` predicates can be used to express distance between vector states, but we currently do not have support for reasoning about distance between general quantum operations.

A related point is that near-term algorithms often need to account for hardware errors. Thus, verifying these algorithms may require considering their behavior in the presence of errors. So far, most of our work in sQIR has revolved around the unitary semantics and vector-based state abstractions because we find these simpler to work with. However, it is more natural to describe states subject to error using density matrices, since noisy states are mixtures of pure states [19].

sQIR's extensible design and flexible semantics, developed while verifying a range of quantum programs, should serve as a solid foundation for the proposed verification efforts above and those to come.

References

1 Matt Amy. *Formal Methods in Quantum Circuit Design*. PhD thesis, University of Waterloo, 2019.

2 Matthew Amy. Towards large-scale functional verification of universal quantum circuits. In *Proceedings of the 15th International Conference on Quantum Physics and Logic, QPL 2018*, June 2018.

3 Jaap Boender, Florian Kammüller, and Rajagopal Nagarajan. Formalization of quantum protocols using coq. In Chris Heunen, Peter Selinger, and Jamie Vicary, editors, *Proceedings of the 12th International Workshop on Quantum Physics and Logic, Oxford, U.K., July 15-17, 2015*, volume 195 of *Electronic Proceedings in Theoretical Computer Science*, pages 71–83. Open Publishing Association, 2015. doi:10.4204/EPTCS.195.6.

4 Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perrelle, and Benoit Valiron. Toward certified quantum programming. *arXiv e-prints*, 2020. arXiv:2003.05841.

5 The Coq Development Team. The coq proof assistant, version 8.10.0, October 2019. doi:10.5281/zenodo.3476303.

6 Andrew W. Cross, Lev S. Bishop, John A. Smolin, and Jay M. Gambetta. Open Quantum Assembly Language. *arXiv e-prints*, Jul 2017. arXiv:1707.03429.

7 David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.

8 Jean-Christophe Filliâtre and Andrei Paskevich. Why3 — where programs meet provers. In *Proceedings of the 22nd European Symposium on Programming*, Lecture Notes in Computer Science, 2013.

9 Daniel Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. In *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, volume 68, pages 13–58, 2010.

10 Alexander Green, Peter LeFanu Lumsdaine, Neil J. Ross, Peter Selinger, and Benoît Valiron. Quipper: A scalable quantum programming language. In *Proceedings of the 34th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI 2013, pages 333–342, 2013.

11 Alexander S Green. *Towards a formally verified functional quantum programming language*. PhD thesis, University of Nottingham, 2010.

12 Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. doi:10.1007/978-94-017-0849-4_10.

13 Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM Symposium on Theory of Computing*, pages 212–219, 1996.

14 Kesha Hietala, Robert Rand, Shih-Han Hung, Xiaodi Wu, and Michael Hicks. A verified optimizer for quantum circuits. *Proceedings of the ACM on Programming Languages*, 5(37), 2021.

15 Junyi Liu, Bohua Zhan, Shuling Wang, Shenggang Ying, Tao Liu, Yangjia Li, Mingsheng Ying, and Naijun Zhan. Formal verification of quantum algorithms using quantum hoare logic. In *Computer Aided Verification - 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part II*, pages 187–207, 2019. doi:10.1007/978-3-030-25543-5_12.

16 Junyi Liu, Bohua Zhan, Shuling Wang, Shenggang Ying, Tao Liu, Yangjia Li, Mingsheng Ying, and Naijun Zhan. Quantum hoare logic. *Archive of Formal Proofs*, March 2019. http://isa-afp.org/entries/QHLProver.html, Formal proof development.

17 Tao Liu, Yangjia Li, Shuling Wang, Mingsheng Ying, and Naijun Zhan. A theorem prover for quantum hoare logic and its applications. *arXiv preprint arXiv:1601.03835*, 2016.

18 Guillaume Melquiond. Interval package for coq, March 2020. URL: https://gitlab.inria.fr/coqinterval/interval.

19 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

20 Tobias Nipkow, Markus Wenzel, and Lawrence C. Paulson. *Isabelle/HOL: A Proof Assistant for Higher-order Logic*. Springer-Verlag, Berlin, Heidelberg, 2002.

21 Adam Paetznick and Krysta M Svore. Repeat-until-success: non-deterministic decomposition of single-qubit unitaries. *Quantum Information & Computation*, 14(15-16):1277–1301, 2014.

22 Jennifer Paykin, Robert Rand, and Steve Zdancewic. QWIRE: A core language for quantum circuits. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, POPL 2017, pages 846–858, New York, NY, USA, 2017. ACM. doi:10.1145/3009837.3009894.

23 Frank Pfenning and Conal Elliott. Higher-order abstract syntax. In *Proceedings of the ACM SIGPLAN 1988 Conference on Programming Language Design and Implementation*, PLDI '88, pages 199–208, New York, NY, USA, 1988. ACM. doi:10.1145/53990.54010.

24 Robert Rand. *Formally Verified Quantum Programming*. PhD thesis, University of Pennsylvania, 2018.

25 Robert Rand, Jennifer Paykin, and Steve Zdancewic. QWIRE practice: Formal verification of quantum circuits in Coq. In *Proceedings 14th International Conference on Quantum Physics and Logic, QPL 2017, Nijmegen, The Netherlands, 3-7 July 2017.*, pages 119–132, 2017. doi:10.4204/EPTCS.266.8.

26 Robert Rand, Jennifer Paykin, and Steve Zdancewic. Phantom types for quantum programs. The Fourth International Workshop on Coq for Programming Languages, January 2018.

27 Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, August 2004.

28 P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, FOCS '94, 1994.

29 DR Simon. On the power of quantum computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, 1994.

30 Mingsheng Ying. Floyd–hoare logic for quantum programs. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 33(6):19, 2011.

A Full QPE Program

The sQIR program for quantum phase estimation (QPE) is given in Figure 5. For comparison, the standard circuit diagrams for QPE and the quantum Fourier transform (QFT) are shown in Figure 6. Note that the circuits for QPE and QFT both have a recursive structure, making them simple to encode in a functional language (like Coq/Gallina).

```
(* Controlled rotation cascade on n qubits. *)
Fixpoint controlled_rotations n : ucom base n :=
  match n with
  | 0 | 1 ⇒ SKIP
  | S n'  ⇒ controlled_rotations n' ; control n' (Rz (2π / 2^n) 0)
  end.

(* Quantum Fourier transform on n qubits. *)
Fixpoint QFT n : ucom base n :=
  match n with
  | 0    ⇒ SKIP
  | 1    ⇒ H 0
  | S n' ⇒ H 0 ; controlled_rotations n ; map_qubits (fun q ⇒ q + 1) (QFT n')
  end.

(* QFT outputs qubits in the wrong order, so the qubits need to be reversed before
   further processing. This can be handled by the classical control hardware or on
   the quantum machine with SWAPs, as done here. *)
Fixpoint reverse_qubits' dim n : ucom base dim :=
  match n with
  | 0    ⇒ SKIP
  | S n' ⇒ reverse_qubits' dim n' ; SWAP n' (dim - n' - 1)
  end.
Definition reverse_qubits n := reverse_qubits' n (n/2).
Definition QFT_w_reverse n := QFT n ; reverse_qubits n.

(* Controlled powers of u. *)
Fixpoint controlled_powers' {n} (u : ucom base n) k kmax : ucom base (kmax+n) :=
  match k with
  | 0    ⇒ SKIP
  | S k' ⇒ controlled_powers' u k' kmax ; niter 2^k' (control (kmax - k' - 1) u)
  end.
Definition controlled_powers {n} (u : ucom base n) k := controlled_powers' u k k.

(* QPE circuit for program u.
   k = number of bits in resulting estimate
   n = number of qubits in input state *)
Definition QPE k n (u : ucom base n) : ucom base (k + n) :=
  npar k H ;
  controlled_powers (map_qubits (fun q ⇒ k + q) u) k;
  invert (QFT_w_reverse k).
```

Figure 5 sQIR definition of QPE. Some type annotations and calls to `cast` have been removed for clarity. `control`, `map_qubits`, `niter`, `npar`, and `invert` are Coq functions that transform sQIR programs; we have proved that they have the expected behavior (e.g. $\forall\ u.\ [\![\text{invert } u]\!]_n = [\![u]\!]_n^\dagger$).

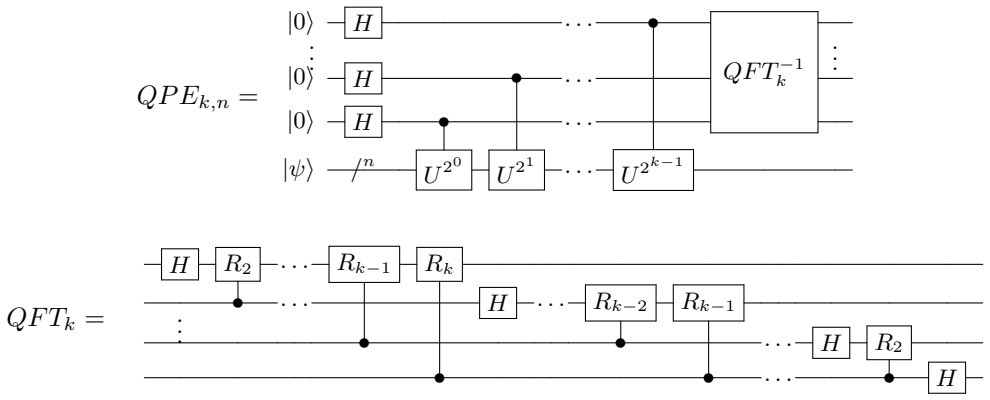


Figure 6 Circuit for quantum phase estimation (QPE) with k bits of precision and an n-qubit input state (top) and quantum Fourier transform (QFT) on k qubits (bottom). $|\psi\rangle$ and U are inputs to QPE. R_m is a z-axis rotation by $2\pi/2^m$.

B SQIR with Measurement

Full SQIR extends the unitary fragment with support for measurement. The syntax for full SQIR and its density matrix-based semantics were discussed in Section 3.3. Here we present an alternative, *nondeterministic* semantics and an example SQIR program with measurement.

B.1 Nondeterministic Semantics

In addition to the density matrix-based semantics described in Section 3.3, SQIR also supports a *nondeterministic semantics* in which evaluation is expressed as a relation. Given a state $|\psi\rangle$, a unitary program `u` will (deterministically) evaluate to $[\![\texttt{u}]\!]_d \times |\psi\rangle$. However, `meas q p1 p2` may evaluate to either `p1` applied to $|1\rangle\langle 1| \times |\psi\rangle$ or `p2` applied to $|0\rangle\langle 0| \times |\psi\rangle$. We use notation `p` / $\psi \Downarrow \psi'$ to say that on input ψ program `p` nondeterministically evaluates to ψ'.

The advantage of the nondeterministic semantics is that state is represented using a vector $|\psi\rangle$ rather than a density matrix ρ, which makes proof writing easier and allows us to use the variety of tactics proposed for dealing with unitary programs. However, because the nondeterministic semantics only describes one possible measurement outcome, it is only useful for proving certain types of properties. For example, it can be used to prove the existence of a possible output state or to show that all execution paths result in the same outcome. The following examples share the latter property, allowing us to compare the density matrix and nondeterministic semantics.

Example: Resetting a Qubit

To illustrate the difference between the nondeterministic and density matrix-based semantics, consider the following SQIR program, which resets qubit `q` to the $|0\rangle$ state.

```
Definition reset q := meas q (X q) skip.
```

Using our density matrix-based semantics, we can prove the following, which says that for any valid density matrix ρ, applying `reset` to ρ will produce the density matrix corresponding to the $|0\rangle$ state.

```
Lemma reset_to_zero: ∀ (ρ : Density 2),
```

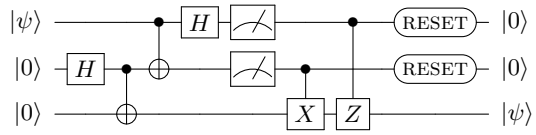


Figure 7 Circuit for quantum teleportation following the presentation in prior work [14, Sec. 5].

```
Mixed_State ρ → {|reset|}₁ ρ = |0⟩⟨0|.
```

The proof is straightforward:

$$\begin{aligned}[\![\texttt{reset}]\!]\,\rho &= X(|1\rangle\langle 1|\,\rho\,|1\rangle\langle 1|)X + I_2(|0\rangle\langle 0|\,\rho\,|0\rangle\langle 0|)I_2\\ &= |0\rangle\langle 1|\,\rho\,|1\rangle\langle 0| + |0\rangle\langle 0|\,\rho\,|0\rangle\langle 0|\\ &= |0\rangle\left(\langle 1|\,\rho\,|1\rangle + \langle 0|\,\rho\,|0\rangle\right)\langle 0|\\ &= |0\rangle\,(I_1)\,\langle 0| = |0\rangle\langle 0|\end{aligned}$$

The fourth line follows from the third on account of ρ being a valid density matrix: The numbers along the diagonal sum to 1.

Although the proof above is straightforward, it does not give a clear intuition for *why* the program is correct. The simple explanation for why this program is correct goes as follows: There are two cases, depending on the result of `meas`. In the case where measurement outputs 0, the remainder of the program is the no-op `skip`, so the output state is $|0\rangle$. In the case where measurement outputs 1, the program applies an X gate, which flips the qubit's value, leaving it in final state $|0\rangle$.

The proof using the nondeterministic semantics closely follows this argument: It considers both possible measurement transitions and inspects the output state. The correctness property for the nondeterministic semantics is stated as follows.

```
Lemma reset_to_zero: ∀ (ψ ψ' : Vector 2),
  WF_Matrix ψ → reset / ψ ⇓ ψ' → ψ' ∝ |0⟩
```

This says that *any* output state ψ' is proportional ($\propto$) to $|0\rangle$. We could instead prove `reset / ψ ⇓` $\frac{1}{\sqrt{2}} * |0\rangle$, where the $\frac{1}{\sqrt{2}}$ factor reflects the probability of each measurement outcome $((\frac{1}{\sqrt{2}})^2 = 1/2)$, but this would only be stating that *some* output is proportional to $|0\rangle$.

B.2 Quantum Teleportation

The goal of quantum teleportation is to transmit a state $|\psi\rangle$ from one party (Alice) to another (Bob) using a shared entangled state. The circuit for quantum teleportation is shown in Figure 7 and the corresponding sQIR program is given below.

```
Definition bell : ucom base 3 := H 1; CNOT 1 2.
Definition alice : com base 3 := CNOT 0 1 ; H 0; measure 0; measure 1.
Definition bob : com base 3 := CNOT 1 2; CZ 0 2; reset 0; reset 1.
Definition teleport : com base 3 := bell; alice; bob.
```

The `bell` circuit prepares a Bell pair on qubits 1 and 2, which are respectively sent to Alice and Bob. Alice applies `CNOT` from qubit 0 to qubit 1 and then measures both qubits and (implicitly) sends them to Bob. Finally, Bob performs operations controlled by the (now classical) values on qubits 0 and 1 and then resets them to the zero state.

Density Matrix-Based Semantics

The correctness property for this program says that for any (well-formed) density matrix ρ, `teleport` takes the state $\rho \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|$ to the state $|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes \rho$.

```
Lemma teleport_correct : ∀ (ρ : Density 2),
 WF_Matrix ρ →
 ⦇teleport⦈₃ (ρ ⊗ |0⟩⟨0| ⊗ |0⟩⟨0|) = |0⟩⟨0| ⊗ |0⟩⟨0| ⊗ ρ
```

The proof is simple: We perform (automated) arithmetic to show that the output matrix has the desired form.

Nondeterministic Semantics

Under the nondeterministic semantics, we aim to prove the following, which says that on input $|\psi\rangle \otimes |0,0\rangle$, `teleport` will produce a state that is proportional to $|0,0\rangle \otimes |\psi\rangle$.

```
Lemma teleport_correct : ∀ (ψ : Vector (2^1)) (ψ' : Vector (2^3)),
  WF_Matrix ψ → teleport / (ψ  ⊗ |0,0⟩) ⇓ ψ' →
  ψ' ∝ |0,0⟩ ⊗ ψ.
```

The first half of the circuit is unitary, so the proof simply computes the effect of applying a H gate, two $CNOT$ gates and another H gate to the input vector state. The two measurement steps then leave four different cases to consider. In each of the four cases, we can use the outcomes of measurement to correct the final qubit, putting it into the state $|\psi\rangle$. Finally, resetting the already-measured qubits is deterministic and leaves us with the desired state.

C Additional Examples

Here we present three additional examples of quantum algorithms we have verified in sQIR. We begin with *superdense coding*, a simple algorithm whose proof is almost entirely automated. We then analyze the *Deutsch-Jozsa algorithm*, the first algorithm we verified that is parameterized by an input oracle (Grover's algorithm and QPE both share this property). We conclude with *Simon's algorithm*.

C.1 Superdense Coding

Superdense coding is a protocol that allows a sender to transmit two classical bits, b_1 and b_2, to a receiver using a single quantum bit. Initially, the sender and receiver share an entangled pair of qubits called a *Bell pair*. To start, the sender conditionally applies X and Z to their qubit, contingent on the values of b_1 and b_2, and then transmit their qubit to the receiver. The receiver then applies a *Bell measurement* (reversed entangling operation followed by measure) to recover the bits. The circuit for superdense coding and the sQIR program corresponding to the unitary part of this circuit are shown in Figure 8.

We can prove that the result of evaluating the program `superdense b1 b2` on an input state consisting of two qubits initialized to zero is the state $|b_1, b_2\rangle$.

```
Lemma superdense_correct : ∀ b1 b2, ⟦superdense b1 b2⟧₂ × | 0,0 ⟩ = | b1,b2 ⟩.
```

The proof simply destructs `b1` and `b2` and applies matrix simplification tactics.

```
Definition bell00 := H 0; CNOT 0 1.
Definition encode (b1 b2 : 𝔹) :=
  (if b2 then X 0 else I 0);
  (if b1 then Z 0 else I 0).
Definition decode := CNOT 0 1; H 0.
Definition superdense (b1 b2 : 𝔹) :=
  bell00 ; encode b1 b2 ; decode.
```

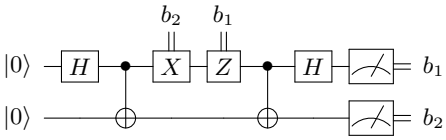


Figure 8 Superdense coding in sQIR and as a circuit. Each definition in the sQIR program has type `ucom base 2`.

```
Definition deutsch_jozsa n (u : ucom base n) :=
  X (n-1) ; npar n H ; u ; npar n H.
```

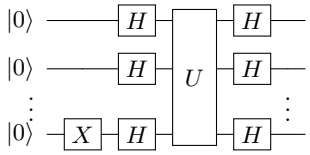


Figure 9 The Deutsch-Jozsa algorithm in sQIR and as a circuit. The Coq function `npar` constructs a sQIR program that applies the same operation to every qubit.

C.2 Deutsch-Jozsa Algorithm

In the Deutsch-Jozsa problem [7], the goal is to determine whether a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is *constant* (always returns the same value) or *balanced* (returns 0 and 1 equally often), given that one is the case. The function f is encoded in an "oracle" $U : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$, which is a linear operator over a 2^{n+1} dimensional Hilbert space. In sQIR, we express the requirement that program u encodes the function f as follows.

```
Definition boolean_oracle {n} (u : ucom (n + 1)) f :=
  ∀ x y, ⟦u⟧_{n+1} × |x⟩ ⊗ |y⟩ = |x⟩ ⊗ |y ⊕ (f x)⟩.
```

To express that a function is constant or balanced, we can define a function `count f n` that counts all inputs on which function `f` (with domain size 2^n) evaluates to true. Then we have:

```
Definition balanced f n := n > 0 ∧ count f n = 2^{n-1}.
Definition constant f n := count f n = 0 ∨  count f n = 2^n.
```

As shown in Figure 9, the Deutsch-Jozsa algorithm begins with an all $|0\rangle$ state and prepares the input state $|+\rangle^{\otimes n} \otimes |-\rangle$ by applying an X gate on the last qubit followed by a H gate on every qubit. Next the oracle U is queried, and a H gate is again applied to every qubit in the program. Finally, all qubits are measured in the standard basis. If measuring all qubits but the last yields an all-zero string (the last qubit is guaranteed to be in the $|1\rangle$ state) then the algorithm outputs "accept," indicating that the function is constant. Otherwise the algorithm outputs "reject."

The probability of measuring $|0\rangle$ in the first n qubits is given by

`prob_partial_meas` $|0\rangle^n$ (⟦`deutsch_jozsa n u`⟧$_{n+1}$ × $|0\rangle^{n+1}$).

We define an `accept` predicate that states that this expression is 1 and a `reject` predicate that states that it is 0. The correctness property is then stated as follows.

```
Lemma deutsch_jozsa_correct :
  ∀ (n : ℕ) (f : ℕ → 𝔹) (u : ucom base (n + 1)),
  n > 0 → boolean_oracle u f →
  (constant f n → accept u) ∧ (balanced f n → reject u).
```

The key lemma in our proof states that the probability of accepting depends on the number of inputs on which `f` evaluates to 1, i.e., `count f n`. In particular, the probability is $Pr_{accept} = |1 - \frac{2*(\texttt{count f n})}{2^n}|^2$. We prove this using matrix simplification and induction on n. Correctness of the Deutsch-Jozsa algorithm follows directly from this lemma: For a constant function, `count f n` $= 0$ or `count f n` $= 2^n$ so $Pr_{accept} = 1$. For a balanced function, `count f n` $= 2^{n-1}$ so $Pr_{accept} = 0$.

C.3 Simon's Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that for all $x, y \in \{0,1\}^n$, $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0, s\}$ for unknown $s \in \{0,1\}^n$, the goal of Simon's algorithm is to find s. The inputs to the algorithm are the input size n and a program (oracle) U_f with the property that $U_f |x\rangle |y\rangle = |x\rangle |f(x) \oplus y\rangle$. If $s = 0$, then the output of Simon's algorithm is a uniform superposition over all n-bit strings (meaning that any string is measured with equal probability). If $s \neq 0$, then the output is a uniform distribution over strings y such that $s \cdot y = 0$, where $x \cdot y$ is the bitwise dot product of x and y modulo 2. The value of s can be determined by $O(n)$ iterations of the algorithm.

The `simon` function, shown below, produces the sQIR circuit for the algorithm, which has a simple structure. First, a layer of Hadamard gates prepares a uniform superposition on the first n inputs. Next, U_f encodes information about f in the phase, in essence evaluating the oracle on all possible inputs at once. Finally, another layer of Hadamard gates brings information in the phase back to the state where it can be measured. The circuit is run on input $|0\rangle^{2*n}$ ($= |00...0\rangle$ with $2 * n$ entries).

```
Definition simon {n} (Uf : ucom base (2 * n)) := npar n H ; Uf ; npar n H.
```

Our statements of correctness for Simon's algorithm say that (1) if s is zero then the probability of measuring any particular output is $1/2^n$, (2) if s is nonzero then the probability of measuring y such that $s \cdot y = 0$ is $1/2^{n-1}$, and (3) if s is nonzero then the probability of measuring y such that $s \cdot y \neq 0$ is 0. We show the full statement of correctness for property (2) below.

```
Lemma simon_nonzero_A : ∀ {n : ℕ} (Uf : ucom base (2 * n)) f y s,
  n > 0 → y < 2^n → s < 2^n →
  integer_oracle Uf f →
  (∀ x, x < 2^n → f x < 2^n) →
  (∀ x y, x < 2^n → y < 2^n → f x = f y ↔ x ⊕ y = s ∨ x = y)) →
  s ≠ 0 →
  s · y = 0 →
  prob_partial_meas |y⟩ (⟦simon Uf⟧_2*n × |0⟩^2*n) = 1/2^(n-1).
```

The first three conditions ensure well-formedness of the inputs; the next three describe constraints on f and state that `Uf` implements f. We call `Uf` an *integer oracle* because it maps an n-bit number to another n-bit number. The conclusion states that after running the program `simon Uf` on $|0\rangle^{2*n}$, the probability of measuring y such that $s \cdot y = 0$ is $\frac{1}{2^{n-1}}$.

We begin by showing that for any (well-formed) s and y, `prob_partial_meas` $|y\rangle$ (⟦`simon Uf`⟧$_{2*n} \times |0\rangle^{2*n}$) is equal to

$$\| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |f(x)\rangle \|^2.$$

The proofs of the three properties listed above then amount to showing properties about this norm-sum term.

In the case where $s \neq 0$, f is a two-to-one function, which means that the expression above can be rewritten as a sum over elements in the range of f. In the standard presentation, this expression is simplified as follows.

$$\begin{aligned}
&\Big\| \frac{1}{2^n} \sum_{z \in \text{range}(f)} ((-1)^{x_1 \cdot y} + (-1)^{x_2 \cdot y}) \, |z\rangle \Big\|^2, \qquad f(x_1) = f(x_2) = z \\
&= \Big\| \frac{1}{2^n} \sum_{z \in \text{range}(f)} ((-1)^{x_1 \cdot y} + (-1)^{(x_1 \oplus s) \cdot y}) \, |z\rangle \Big\|^2 \\
&= \Big\| \frac{1}{2^n} \sum_{z \in \text{range}(f)} ((-1)^{x_1 \cdot y}(1 + (-1)^{s \cdot y}) \, |z\rangle \Big\|^2
\end{aligned}$$

From this rewritten form, it is clear that the probability of measuring y such that $s \cdot y = 0$ is $2 * 1/2^n = 1/2^{n-1}$ and the probability of measuring y such that $s \cdot y \neq 0$ is 0.

Our Coq proof essentially follows this structure, although we found it easier to define a function `to_injective` that takes the two-to-one function f and makes it one-to-one.

```
Definition to_injective n s f x :=
  let y := x ⊕ s in
  if (x <? y) then f x else (2^n + f x).
```

Using this function, we can rewrite the norm-sum term as a sum over vectors of size 2^{n+1}.

$$\Big\| \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} \, |f(x)\rangle \Big\| = \frac{1}{\sqrt{2}} \Big\| \sum_{x=0}^{2^n-1} ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) \, |(\texttt{to\_injective n s f})(x)\rangle \Big\|$$