A programming language characterizing quantum polynomial time

Emmanuel Hainry, Romain Péchoux, Mário Silva

A programming language characterizing quantum polynomial time

Emmanuel Hainry, Romain Péchoux, and Mário Silva

Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France
{hainry,pechoux,mmachado}@loria.fr

Abstract. We introduce a first-order quantum programming language, named FOQ, whose terminating programs are reversible. We restrict FOQ to a strict and tractable subset, named PFOQ, of terminating programs with bounded width, that provides a first programming language-based characterization of the quantum complexity class FBQP. We finally present a tractable semantics-preserving algorithm compiling a PFOQ program to a quantum circuit of size polynomial in the number of input qubits.

1 Introduction

Motivations. Quantum computing is an emerging and promising computational model that has been in the scientific limelight for several decades. This phenomenon is mainly due to the advantage of quantum computers over their classical competitors, based on the use of purely quantum properties such as superposition and entanglement. The most notable example being Shor's algorithm for finding the prime factors of an integer [15], which is exponentially faster than the most efficient known classical factoring algorithm and which is expected to have implications in cryptography (RSA encryption, etc.).

Whether due to the fragility of quantum systems, namely the engineering problem of maintaining a large number of qubits in a coherent state, or by lack of reliable technological alternatives, quantum computing is typically described at a level close to hardware. Without any hope of being exhaustive, one can think to quantum circuits [9,11], to measurement-based quantum computers [4,7] or to circuit description languages [13]. This low-level machinery restricts drastically the abstraction and programming ease offered by these models and quantum programs currently suffer from the comparison with their classical competitors, which have many high-level tools and formalisms based on more than 50 years of scientific research, engineering development, and practical and industrial applications.

In order to solve these issues, a major effort is made to realize the promise of a quantum computer, which requires the development of different layers of hardware and software, together referred to as the *quantum stack*. Our paper is part of this line of research. We focus on the highest layers of the quantum stack: quantum programming languages and quantum algorithms. We seek to better understand what can be done efficiently on a quantum computer and we are

particularly interested in the development of quantum programming languages where program complexity can be certified automatically by some static analysis technique.

Contribution. Towards this end, we take the notion of polynomial time computation as our main object of study. Our contributions are the following.

- We introduce a quantum programming language, named FOQ, that includes first-order recursive procedures. The input of a FOQ program consist in a sorted set of qubits, a list of pairwise distinct qubit indexes. A FOQ program can apply to each of its qubits basic operators corresponding to unary unitary operators. The considered set of operators has been chosen in accordance with [16] to form a universal set of gates.
- After showing that terminating FOQ programs are reversible (Theorem 1), we restrict programs to a strict subset, named PFOQ, for *polynomial time* FOQ. The restrictions put on a PFOQ programs are tractable (*i.e.*, can be decided in polynomial time, see Theorem 2), ensure that programs terminate on any input (Lemma 1), and prevent programs from having any exponential blow up (Lemma 2).
- We show that the class of functions computed by PFOQ programs is *sound* and *complete* for the quantum complexity class FBQP. FBQP is the functional extension of *bounded-error quantum polynomial time*, known as BQP [2], the class of decision problems solvable by a quantum computer in polynomial time with an error probability of at most $\frac{1}{3}$ for all instances. Hence the language PFOQ is, to our knowledge, the first programming language characterizing quantum polynomial time functions. Soundness (Theorem 3) is proved by showing that any PFOQ program can be simulated by a quantum Turing machine running in polynomial time [2]. The completeness of our characterization (Theorem 6) is demonstrated by showing that PFOQ programs strictly encompass Yamakami's function algebra, known to be FBQP-complete [16].
- We also describe a polynomial-time deterministic algorithm **compile** (based on the subroutines described in Algorithms 1 and 2), that takes in a PFOQ program P and an integer n and outputs a quantum circuit of size polynomial in n that simulates P on an input size of n qubits. The existence of such circuits is not surprising, as a direct consequence of Yao's characterization of the class BQP in terms of uniform families of circuits of polynomial size [17]. However, a constructive generation based on Yao's algorithm is not satisfactory because of the use of quantum Turing machines which makes the circuits complex and not optimal (in size). We show that, in our setting, circuits can be effectively computed and that the **compile** algorithm is tractable (Theorem 9).

Our programming language FOQ and the restriction to PFOQ are illustrated throughout the paper, using the Quantum Fourier Transform QFT as a leading algorithm (Example 1).

Related work. This paper belongs to a long standing line of works trying to specify, understand, and analyze the semantics of quantum programming languages, starting with the cornerstone work of Selinger [14]. The motivations in restricting the considered programs to PFOQ were inspired by the works on *implicit computational complexity*, that seek to characterize complexity classes by putting restrictions (type systems or others) on standard programming languages and paradigms [1,5,12]. These restrictions have to be implicit (*i.e.*, not provided by the programmer) and tractable. Among all these works, we are aware of two results [16] and [6] studying polynomial time computations on quantum programming languages, works from which our paper was greatly inspired. [6] provides a characterization of BQP based on a quantum lambda-calculus. Our work is an extension to FBQP with a restriction to first-order procedures. Last but not least, [6] is based on Yao's simulation of quantum Turing machines [17] while we provide an explicit algorithm for generating circuits of polynomial size. Our work is also inspired by the function algebra of [16], that characterizes FBQP: our completeness proof shows that any function in [16] can be simulated by a PFOQ program (Theorem 6). However, we claim that FOQ is a more general language for FBQP in so far that it is much less constraining (in terms of expressive power) than the function algebra of [16]: any function of [16] can be, by design, transformed into a PFOQ program, whereas the converse is not true. We can take as example the quantum Fourier transform (QFT) which, as noted in [16], cannot be exactly computed by the function algebra without an additional initial quantum function. Furthermore, the *multi-qubit recursion* construction described in [16] is more restrictive than what we allow in PFOQ, since we may only call the same recursive function in each branch.

2 First-order quantum programming language

Syntax and well-formedness. We consider a quantum programming language, called FOQ for First-Order Quantum programming language, that includes basic data types such as Integers, Booleans, Qubits, Operators, and Sorted Sets of qubits, lists of finite length where all elements are different. A FOQ program has the ability to call first-order (recursive) procedures taking a sorted set of qubits as a parameter. Its syntax is provided in Figure 1.

Let x denote an integer variable and $\bar{\mathrm{p}}$, $\bar{\mathrm{q}}$ denote sorted sets variables. The size of the sorted set stored in $\bar{\mathrm{q}}$ will be denoted by $|\bar{\mathrm{q}}|$. We can refer to the i-th qubit in $\bar{\mathrm{q}}$ as $\bar{\mathrm{q}}[i]$, with $1 \leq i \leq |\bar{\mathrm{q}}|$. Hence, each non-empty sorted set variable $\bar{\mathrm{q}}$ can be viewed as a list $[\bar{\mathrm{q}}[1], \ldots, \bar{\mathrm{q}}[|\bar{\mathrm{q}}|]]$. The empty sorted set, of size 0, will be denoted by nil and $\bar{\mathrm{q}} \ominus [i]$ will denote the sorted set obtained by removing the qubit of index i in $\bar{\mathrm{q}}$. For notational convenience, we extend this notation by $\bar{\mathrm{q}} \ominus [i_1, \ldots, i_k]$, for the list obtained by removing the qubits of indexes $i_1, \ldots, i_k$ in the sorted set $\bar{\mathrm{q}}$.

The language also includes some constructs U^f to represent (unary) unitary operators, for some total function $f \in \mathbb{Z} \to [0, 2\pi) \cap \tilde{\mathbb{R}}$. The function f is required to be polynomial-time approximable: its output is restricted to $\tilde{\mathbb{R}}$, the set of real

numbers that can be approximated by a Turing machine for any precision 2^{-k} in time polynomial in k.

(Integers)	i	$\triangleq$	$n \mid \mathrm{x} \mid \mathrm{i}+n \mid \mathrm{i}-n \mid \lvert\mathrm{s}\rvert$, with $n \in \mathbb{N}$
(Booleans)	b	$\triangleq$	$\mathrm{i} > \mathrm{i} \mid \mathrm{i} \geq \mathrm{i} \mid \mathrm{i} = \mathrm{i} \mid \mathrm{b} \wedge \mathrm{b} \mid \mathrm{b} \vee \mathrm{b} \mid \neg \mathrm{b}$
(Sorted Sets)	s	$\triangleq$	$\mathrm{nil} \mid \bar{\mathrm{q}} \mid \mathrm{s} \ominus [\mathrm{i}]$
(Qubits)	q	$\triangleq$	$\mathrm{s}[\mathrm{i}]$
(Operators)	$\mathrm{U}^f(\mathrm{i})$	$\triangleq$	$\mathrm{NOT} \mid \mathrm{R}_Y^f(\mathrm{i}) \mid \mathrm{Ph}^f(\mathrm{i})$, with $f \in \mathbb{Z} \to [0, 2\pi) \cap \tilde{\mathbb{R}}$
(Statements)	S	$\triangleq$	**skip**; $\mid \mathrm{q}$ ***=** $\mathrm{U}^f(\mathrm{i})$; $\mid \mathrm{S}\ \mathrm{S} \mid$ **if** b **then** S **else** S $\mid$ **qcase** q **of** $\{0 \to \mathrm{S}, 1 \to \mathrm{S}\} \mid$ **call** proc[i](s);
(Procedure declarations)	D	$\triangleq$	$\varepsilon \mid$ **decl** proc[x]($\bar{\mathrm{p}}$){S}, D
(Programs)	$\mathrm{P}(\bar{\mathrm{q}})$	$\triangleq$	$\mathrm{D} :: \mathrm{S}$

Fig. 1: Syntax of FOQ programs

A FOQ *program* $\mathrm{P}(\bar{\mathrm{q}})$ consists of a sequence of *procedure declarations* D followed by a *program statement* S, ε denoting the empty sequence. In what follows, we will sometimes refer to program $\mathrm{P}(\bar{\mathrm{q}})$ simply as P. Let $var(\mathrm{S})$ be the set of variables appearing in the statement S. Let $|\mathrm{P}|$ be the size of program P, that is the total number of symbols in P.

A procedure declaration **decl** proc[x]($\bar{\mathrm{p}}$){S} takes a sorted set parameter $\bar{\mathrm{p}}$ and some optional integer parameter x as inputs. S is called the *procedure statement*, proc is the *procedure name* and belongs to a countable set Procedures. We will write $\mathrm{S}^{\mathrm{proc}}$ to refer to S and proc $\in$ P holds if proc is declared in D.

Statements include a no-op instruction, applications of a unitary operator to a qubit (q ***=** $\mathrm{U}^f(\mathrm{i})$;), sequences, (classical) conditionals, *quantum cases*, and *procedure calls* (**call** proc[i](s);). A quantum case **qcase** q **of** $\{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}$ provides a quantum control feature that will execute statements S_0 and S_1 in superposition. For example, the $CNOT$ gate on qubits $\bar{\mathrm{q}}[i]$ and $\bar{\mathrm{q}}[j]$, for $i, j \in \mathbb{N}$, $i \neq j$, can be simulated by the following statement:

$$\mathrm{CNOT}(\bar{\mathrm{q}}[i], \bar{\mathrm{q}}[j]) \triangleq \textbf{qcase}\ \bar{\mathrm{q}}[i]\ \textbf{of}\ \{0 \to\ \textbf{skip};, 1 \to \bar{\mathrm{q}}[j]\ \textbf{*=}\ \mathrm{NOT};\}.$$

Throughout the paper, we restrict our study to *well-formed* programs, that is, programs $\mathrm{P} = \mathrm{D} :: \mathrm{S}$ satisfying the following properties: $var(\mathrm{S}) \subseteq \{\bar{\mathrm{q}}\}$; $\forall \mathrm{proc} \in \mathrm{P}$, $var(\mathrm{S}^{\mathrm{proc}}) \subseteq \{\mathrm{x}, \bar{\mathrm{p}}\}$; procedure names declared in D are pairwise distinct; for each procedure call, the procedure name is declared in D.

Semantics. Let $\mathcal{H}_{2^n}$ be the *Hilbert space* $\mathbb{C}^{2^n}$ of n qubits. We use Dirac notation to denote a quantum state $|\psi\rangle \in \mathcal{H}_{2^n}$. Each $|\psi\rangle \in \mathcal{H}_{2^n}$ can be written as a superposition of bitstrings of size n: $|\psi\rangle = \sum_{w \in \{0,1\}^n} \alpha_w |w\rangle$, with $\alpha_w \in \mathbb{C}$ and $\sum_w |\alpha_w|^2 = 1$. The *length* $\ell(|\psi\rangle)$ of the state $|\psi\rangle$ is n. Given two matrices M, N, we denote by $M^\dagger$ the transpose conjugate of M and by $M \otimes N$ the tensor product of M by N.

$\langle\psi|$ is equal to $|\psi\rangle^\dagger$ and $|\psi\rangle\langle\phi|$ and $\langle\psi|\phi\rangle$ are respectively the inner product and outer product of $|\psi\rangle$ and $|\phi\rangle$. Let I_n be the identity matrix in $\mathbb{C}^{n\times n}$. Given $m \leq n$ and $i \in \{0,1\}$, define $|i\rangle_m \triangleq I_{2^{m-1}} \otimes |i\rangle \otimes I_{2^{n-m}}$ and $\langle i|_m \triangleq (|i\rangle_m)^\dagger$.

A function $[\![\mathrm{U}^f]\!] \in \mathbb{Z} \to \tilde{\mathbb{C}}^{2\times 2}$ is associated to each U^f as follows:

$$[\![\mathrm{NOT}]\!](n) \triangleq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ [\![\mathrm{R}_Y^f]\!](n) \triangleq \begin{pmatrix} \cos(f(n)) & -\sin(f(n)) \\ \sin(f(n)) & \cos(f(n)) \end{pmatrix},\ [\![\mathrm{Ph}^f]\!](n) \triangleq \begin{pmatrix} 1 & 0 \\ 0 & e^{if(n)} \end{pmatrix},$$

where $\tilde{\mathbb{C}}$ is the set of complex numbers whose both real and imaginary parts are in $\tilde{\mathbb{R}}$. One can check easily that each matrix $M \triangleq [\![\mathrm{U}^f]\!](n) \in \tilde{\mathbb{C}}^{2\times 2}$ is unitary, *i.e.*, it satisfies $M^\dagger M = M M^\dagger = I_2$.

Let $\mathbb{B}$ to be the set of Boolean values $b \in \{\mathbf{false}, \mathbf{true}\}$. For a given set X, let $\mathcal{L}(X)$ be the set of lists of elements in X. Let $l = [x_1, \ldots, x_m]$, with $x_1, \ldots, x_m \in X$, denote a list of m-elements in $\mathcal{L}(X)$ and $[\,]$ be the empty list (when $m = 0$). For $l, l' \in \mathcal{L}(X)$, $l@l'$ denotes the concatenation of l and l'. $hd(l)$ and $tl(l)$ represent the tail and the head of l, respectively. Lists of integers will be used to represent Sorted Sets. They contain pointers to qubits (*i.e.*, indexes) in the global memory.

We interpret each basic data type τ as follows: $[\![\mathrm{Integers}]\!] \triangleq \mathbb{Z}$, $[\![\mathrm{Booleans}]\!] \triangleq \mathbb{B}$, $[\![\mathrm{SortedSets}]\!] \triangleq \mathcal{L}(\mathbb{N})$, $[\![\mathrm{Qubits}]\!] \triangleq \mathbb{N}$, and $[\![\mathrm{Operators}]\!] \triangleq \tilde{\mathbb{C}}^{2\times 2}$. Each basic operation $\mathrm{op} \in \{+, -, >, \geq, =, \wedge, \vee, \neg\}$ of arity n, with $1 \leq n \leq 2$, has a type signature $\tau_1 \times \ldots \times \tau_n \to \tau$ fixed by the program syntax. For example, the operation + has signature Integers × Integers → Integers. A total function $[\![\mathrm{op}]\!] \in [\![\tau_1]\!] \times \ldots \times [\![\tau_n]\!] \to [\![\tau]\!]$ is associated to each op.

For each basic type τ, the reduction $\Downarrow_{[\![\tau]\!]}$ is a map in $\tau \times \mathcal{L}(\mathbb{N}) \to [\![\tau]\!]$. Intuitively, it maps an expression of type τ to its value in $[\![\tau]\!]$ for a given list l of pointers in memory. These reductions are defined in Figure 2, where e and d denote either an integer expression i or a boolean expression b.

Note that in rule ($\mathrm{Rm}_\notin$), if we try to delete an undefined index then we return the empty list, and in rule ($\mathrm{Qu}_\notin$), if we try to access an undefined qubit index then we return the value 0 (defined indexes will always be positive). The standard gates $R_Y(\pi/4)$, $P(\pi/4)$, and $CNOT$, form a universal set of gates [3], which justifies the choice of NOT, $\mathrm{R}_Y^f(\mathrm{i})$, and $\mathrm{Ph}^f(\mathrm{i})$ as basic operators. For instance, we can simulate the application of an Hadamard gate H on q by the following statement q *= $\mathrm{R}_Y^f(0)$; q *= NOT;, with the function f defined by $\forall n, f(n) = \pi/4 \in [0, 2\pi) \cap \tilde{\mathbb{R}}$. By abuse of notation, we will sometimes use q *= H; to denote this statement. Using CNOT, we can also define the SWAP operation swapping the state between two qubits $\bar{\mathrm{q}}[i]$ and $\bar{\mathrm{q}}[j]$, with $i, j \in \mathbb{N},\ i \neq j$:

$$\mathrm{SWAP}(\bar{\mathrm{q}}[i], \bar{\mathrm{q}}[j]) \triangleq \mathrm{CNOT}(\bar{\mathrm{q}}[i], \bar{\mathrm{q}}[j])\ \mathrm{CNOT}(\bar{\mathrm{q}}[j], \bar{\mathrm{q}}[i])\ \mathrm{CNOT}(\bar{\mathrm{q}}[i], \bar{\mathrm{q}}[j]).$$

Let $\top$ and $\bot$ be two special symbols for termination and error, respectively, and let $\diamond$ stand for a symbol in $\{\top, \bot\}$. The set of *configurations* of dimension 2^n, denoted Conf_n, is defined by

$$\mathrm{Conf}_n \triangleq (\mathrm{Statements} \cup \{\top, \bot\}) \times \mathcal{H}_{2^n} \times \mathcal{P}(\mathbb{N}) \times \mathcal{L}(\mathbb{N}),$$

with $\mathcal{P}(\mathbb{N})$ being the powerset over $\mathbb{N}$. A configuration $c = (\mathrm{S}, |\psi\rangle, A, l) \in \mathrm{Conf}_n$ contains a statement S to be executed (provided that $\mathrm{S} \notin \{\top, \bot\}$), a quantum

$$\frac{(\mathrm{e}, l) \Downarrow_{[\![\tau_1]\!]} m \qquad (\mathrm{d}, l) \Downarrow_{[\![\tau_2]\!]} n}{(\mathrm{e}\ \mathrm{op}\ \mathrm{d}, l) \Downarrow_{[\![\mathrm{op}]\!]([\![\tau_1]\!],[\![\tau_2]\!])} [\![\mathrm{op}]\!](m,n)}\ (\mathrm{Op}) \qquad \frac{(\mathrm{i}, l) \Downarrow_{\mathbb{Z}} n}{(\mathrm{U}^f(\mathrm{i}), l) \Downarrow_{\mathbb{C}^{2\times 2}} [\![\mathrm{U}^f]\!](n)}\ (\mathrm{Unit})$$

$$\frac{}{(n, l) \Downarrow_{\mathbb{Z}} n}\ (\mathrm{Cst}) \qquad \frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_m] \qquad (\mathrm{i}, l) \Downarrow_{\mathbb{Z}} k \in [1, m]}{(\mathrm{s} \ominus [\mathrm{i}], l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_m]}\ (\mathrm{Rm}_\in)$$

$$\frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_n]}{(|\mathrm{s}|, l) \Downarrow_{\mathbb{Z}} n}\ (\mathrm{Size}) \qquad \frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_m] \qquad (\mathrm{i}, l) \Downarrow_{\mathbb{Z}} k \notin [1, m]}{(\mathrm{s} \ominus [\mathrm{i}], l) \Downarrow_{\mathcal{L}(\mathbb{N})} [\,]}\ (\mathrm{Rm}_\notin)$$

$$\frac{}{(\mathrm{nil}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [\,]}\ (\mathrm{Nil}) \qquad \frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_m] \qquad (\mathrm{i}, l) \Downarrow_{\mathbb{Z}} k \in [1, m]}{(\mathrm{s}[\mathrm{i}], l) \Downarrow_{\mathbb{N}} x_k}\ (\mathrm{Qu}_\in)$$

$$\frac{}{(\bar{\mathrm{q}}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} l}\ (\mathrm{Var}) \qquad \frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [x_1, \ldots, x_m] \qquad (\mathrm{i}, l) \Downarrow_{\mathbb{Z}} k \notin [1, m]}{(\mathrm{s}[\mathrm{i}], l) \Downarrow_{\mathbb{N}} 0}\ (\mathrm{Qu}_\notin)$$

Fig. 2: Semantics of expressions

state $|\psi\rangle$ of length n, a set A containing the indexes of qubits that are allowed to be accessed by statement S, and a list l of qubit pointers.

The program big-step semantics $\longrightarrow$, described in Figure 3, is defined as a relation in $\bigcup_{n\in\mathbb{N}} \mathrm{Conf}_n \times \mathrm{Conf}_n$. In the rules of Figure 3, $\longrightarrow$ is annotated by an integer, called *level*. For example, the level of the conclusion in the $(\mathrm{Call}_{[\,]})$ rule is 1. The level is used to count the total number of procedure calls that are not in superposition (*i.e.*, in distinct branches of a quantum case).

We now give a brief intuition on the rules of Figure 3. Rules $(\mathrm{Asg}_\perp)$ and $(\mathrm{Asg}_\top)$ evaluate the application of a unitary operator, corresponding to $\mathrm{U}^f(\mathrm{j})$, to a qubit s[i]. For that purpose, they evaluate the index n of s[i] in the global memory. Rule $(\mathrm{Asg}_\perp)$ deals with the error case, where the corresponding qubit is not allowed to be accessed. Rule $(\mathrm{Asg}_\top)$ deals with the success case: the new quantum state is obtained by applying the result of tensoring the evaluation of $\mathrm{U}^f(\mathrm{j})$ to the right index. Rules $(\mathrm{Seq}_\diamond)$ and $(\mathrm{Seq}_\perp)$ evaluate the sequence of statements, depending on whether an error occurs or not. The (If) rule deals with classical conditionals in a standard way. The three rules $(\mathrm{Case}_\top)$, $(\mathrm{Case}_\perp)$, and $(\mathrm{Case}_\notin)$ evaluate the qubit index n of the control qubit s[i]. Then they check whether this index belongs to the set of accessible qubits (is n in A?). If so, the two statements S_0 and S_1 are intuitively evaluated in superposition, on the projected state $\langle 0|_n|\psi\rangle$ and $\langle 1|_n|\psi\rangle$, respectively. During these evaluations, the index n cannot be accessed anymore. The rule $(\mathrm{Call}_{[\,]})$ treats the base case of a procedure call when the sorted set parameter is empty. In the non-empty case, rule $(\mathrm{Call}_\diamond)$ evaluates the sorted set parameter s to l' and the integer parameter

$$\frac{}{(\mathbf{skip}, |\psi\rangle, A, l) \xrightarrow{0} (\top, |\psi\rangle, A, l)} \text{ (Skip)}$$

$$\frac{(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n \notin A}{(\mathrm{s[i]}\ \texttt{*=}\ \mathrm{U}^f(\mathrm{j});, |\psi\rangle, A, l) \xrightarrow{0} (\bot, |\psi\rangle, A, l)} \text{ ($\mathrm{Asg}_\bot$)}$$

$$\frac{(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n \in A \qquad (\mathrm{U}^f(\mathrm{j}), l) \Downarrow_{\mathbb{C}^{2\times 2}} M}{(\mathrm{s[i]}\ \texttt{*=}\ \mathrm{U}^f(\mathrm{j});, |\psi\rangle, A, l) \xrightarrow{0} (\top, I_{2^{n-1}} \otimes M \otimes I_{2^{l(|\psi\rangle)-n}} |\psi\rangle, A, l)} \text{ ($\mathrm{Asg}_\top$)}$$

$$\frac{(\mathrm{S}_1, |\psi\rangle, A, l) \xrightarrow{m_1} (\top, |\psi'\rangle, A, l) \qquad (\mathrm{S}_2, |\psi'\rangle, A, l) \xrightarrow{m_2} (\diamond, |\psi''\rangle, A, l)}{(\mathrm{S}_1\ \mathrm{S}_2, |\psi\rangle, A, l) \xrightarrow{m_1+m_2} (\diamond, |\psi''\rangle, A, l)} \text{ ($\mathrm{Seq}_\diamond$)}$$

$$\frac{(\mathrm{S}_1, |\psi\rangle, A, l) \xrightarrow{m} (\bot, |\psi\rangle, A, l)}{(\mathrm{S}_1\ \mathrm{S}_2, |\psi\rangle, A, l) \xrightarrow{m} (\bot, |\psi\rangle, A, l)} \text{ ($\mathrm{Seq}_\bot$)}$$

$$\frac{(\mathrm{b}, l) \Downarrow_{\mathbb{B}} b \in \mathbb{B} \qquad (\mathrm{S}_b, |\psi\rangle, A, l) \xrightarrow{m_b} (\diamond, |\psi'\rangle, A, l)}{(\mathbf{if}\ \mathrm{b}\ \mathbf{then}\ \mathrm{S}_{\mathbf{true}}\ \mathbf{else}\ \mathrm{S}_{\mathbf{false}}, |\psi\rangle, A, l) \xrightarrow{m_b} (\diamond, |\psi'\rangle, A, l)} \text{ (If)}$$

$$\frac{(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n \in A \qquad (\mathrm{S}_k, |\psi\rangle, A\backslash\{n\}, l) \xrightarrow{m_k} (\top, |\psi_k\rangle, A\backslash\{n\}, l)}{(\mathbf{qcase}\ \mathrm{s[i]}\ \mathbf{of}\ \{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}, |\psi\rangle, A, l) \xrightarrow{\max_k m_k} (\top, \sum_k |k\rangle_n\langle k|_n |\psi_k\rangle, A, l)} \text{ ($\mathrm{Case}_\top$)}$$

$$\frac{(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n \in A \qquad (\mathrm{S}_k, |\psi\rangle, A\backslash\{n\}, l) \xrightarrow{m_k} (\diamond_k, |\psi_k\rangle, A\backslash\{n\}, l) \qquad \bot \in \{\diamond_0, \diamond_1\}}{(\mathbf{qcase}\ \mathrm{s[i]}\ \mathbf{of}\ \{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}, |\psi\rangle, A, l) \xrightarrow{\max_k m_k} (\bot, |\psi\rangle, A, l)} \text{ ($\mathrm{Case}_\bot$)}$$

$$\frac{(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n \notin A}{(\mathbf{qcase}\ \mathrm{s[i]}\ \mathbf{of}\ \{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}, |\psi\rangle, A, l) \xrightarrow{0} (\bot, |\psi\rangle, A, l)} \text{ ($\mathrm{Case}_\notin$)}$$

$$\frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} l' \neq [\,] \qquad (\mathrm{i}, l) \Downarrow_{\mathbb{Z}} n \qquad (\mathrm{S}^{\mathrm{proc}}\{n/\mathrm{x}\}, |\psi\rangle, A, l') \xrightarrow{m} (\diamond, |\psi'\rangle, A, l')}{(\mathbf{call}\ \mathrm{proc[i](s)};, |\psi\rangle, A, l) \xrightarrow{m+1} (\diamond, |\psi'\rangle, A, l)} \text{ ($\mathrm{Call}_\diamond$)}$$

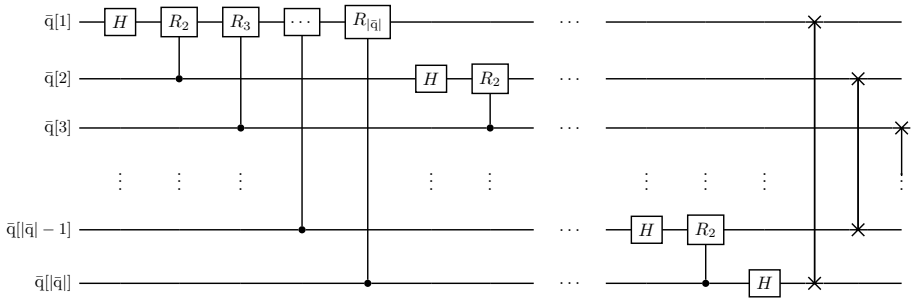
$$\frac{(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [\,]}{(\mathbf{call}\ \mathrm{proc[i](s)};, |\psi\rangle, A, l) \xrightarrow{1} (\top, |\psi\rangle, A, l)} \text{ ($\mathrm{Call}_{[\,]}$)}$$

Fig. 3: Semantics of statements

x to n. It returns the result of evaluating the procedure statement $\mathrm{S}^{\mathrm{proc}}\{n/\mathrm{x}\}$, where n has been substituted to x, w.r.t. the updated qubit pointers list l'.

For a given program $\mathrm{P} = \mathrm{D} :: \mathrm{S}$ and a given quantum state $|\psi\rangle \in \mathcal{H}_{2^n}$, the *initial configuration* for input $|\psi\rangle$ is $c_{init}(|\psi\rangle) \triangleq (\mathrm{S}, |\psi\rangle, \{1, \ldots, n\}, [1, \ldots, n]) \in \mathrm{Conf}_n$. A program is *error-free* if there is no initial configuration $c_{init}(|\psi\rangle)$ such that $c_{init}(|\psi\rangle) \longrightarrow (\bot, |\psi'\rangle, A, l)$. We write $[\![\mathrm{P}]\!](|\psi\rangle) = |\psi'\rangle$, whenever $c_{init}(|\psi\rangle) \xrightarrow{m} (\top, |\psi'\rangle, A, l)$ holds for some m. $(\top, |\psi'\rangle, A, l)$ is called a *terminal configuration*. Let $\mathcal{H} = \bigcup_n \mathcal{H}_{2^n}$, a program *terminates* if $[\![\mathrm{P}]\!]$ is a total function in $\mathcal{H} \to \mathcal{H}$. Note that if a program terminates then it is obviously error-free but the converse property does not hold. Every program P can be efficiently transformed into an error-free program $\mathrm{P}_{\neg\bot}$ such that $\forall |\psi\rangle$, if $[\![\mathrm{P}]\!](|\psi\rangle)$ is defined then $[\![\mathrm{P}]\!](|\psi\rangle) = [\![\mathrm{P}_{\neg\bot}]\!](|\psi\rangle)$. For example, an assignment $\mathrm{s[i]} \mathrel{*}= \mathrm{U}^f(\mathrm{j})$; can be transformed into the conditional statement **if** $((0 < \mathrm{i}) \wedge (\mathrm{i} \leq |\mathrm{s}|))$ **then** $\mathrm{s[i]} \mathrel{*}= \mathrm{U}^f(\mathrm{j})$; **else skip**;.

Example 1. A notable example of quantum algorithm is the Quantum Fourier Transform (QFT), used as a subroutine in Shor's algorithm [15], and whose quantum circuit is provided below, with $R_n \triangleq [\![\mathrm{Ph}^{\lambda x.\pi/2^{x-1}}]\!](n)$, for $n \geq 2$. After applying Hadamard and controlled R_n gates, the circuit performs a permutation of qubits using swap gates.



Note that $\lambda x.\pi/2^{x-1}$ is a total function in $\mathbb{Z} \to [0, 2\pi) \cap \tilde{\mathbb{R}}$. Hence, it is polynomial time approximable. The above circuit can be simulated for any number of qubits $|\mathrm{q}|$ by the following FOQ program QFT.

---

decl rec($\bar{\mathrm{p}}$){
  $\bar{\mathrm{p}}$[1] *= H;
  call rot[2]($\bar{\mathrm{p}}$);
  call rec($\bar{\mathrm{p}} \ominus [1]$);},

decl rot[x]($\bar{\mathrm{p}}$){
  if $|\bar{\mathrm{p}}| > 1$ **then**
    qcase $\bar{\mathrm{p}}$[2] **of** {
      $0 \to$ **skip**;
      $1 \to \bar{\mathrm{p}}$[1] *= $\mathrm{Ph}^{\lambda x.\pi/2^{x-1}}$(x);
    }
    call rot[x + 1]($\bar{\mathrm{p}} \ominus [2]$);
  else skip;},

decl inv($\bar{\mathrm{p}}$){
  if $|\bar{\mathrm{p}}| > 1$ **then**
    SWAP($\bar{\mathrm{p}}[1], \bar{\mathrm{p}}[|\bar{\mathrm{p}}|]$);
    call inv($\bar{\mathrm{p}} \ominus [1, |\bar{\mathrm{p}}|]$);
  else skip;} ::

call rec($\bar{\mathrm{q}}$); **call** inv($\bar{\mathrm{q}}$);

Derivation tree and level. Given a configuration c wrt a fixed program P, $\pi_{\mathrm{P}} \rhd c$ denotes the *derivation tree* of P, the tree of root c whose children are obtained

by applying the rules of Figures 2 and 3 on configuration c with respect to P. We write π instead of $\pi_{\mathrm{P}} \rhd c$ when P and c are clear from the context. Note that a derivation tree π can be infinite in the particular case of a non-terminating computation. When π' is finite, $\pi \trianglelefteq \pi'$ denotes that π is a subtree of π'.

In the case of a terminating computation $\pi \rhd c$, there exists a terminal configuration c' and a level $m \in \mathbb{N}$ such that $c \xrightarrow{m} c'$ holds. In this case, the level of π is defined as $\mathrm{lv}_\pi \triangleq m$. Given a FOQ program P that terminates, $\mathrm{level}_{\mathrm{P}}$ is a total function in $\mathbb{N} \to \mathbb{N}$ defined as $\mathrm{level}_{\mathrm{P}}(n) \triangleq \max_{|\psi\rangle \in \mathcal{H}_{2^n}} \mathrm{lv}_{\pi_{\mathrm{P}} \rhd c_{init}(|\psi\rangle)}$.

Intuitively, $\mathrm{level}_{\mathrm{P}}(n)$ corresponds to the maximal number of non-superposed procedure calls in any program execution on an input of length n.

Example 2. Consider the program QFT of example 1. Assume temporarily that QFT terminates (this will be shown in Example 3). For all $n \in \mathbb{N}$, $\mathrm{level}_{\mathrm{QFT}}(n) = \frac{(n+1)(n+2)}{2} + \lfloor \frac{n}{2} \rfloor + 1$. Indeed, on sorted sets of size n, procedure rec is called recursively $n+1$ times and makes $n+1$ calls to procedure rot on sorted sets of size n, $n-1$, ..., and 1. On sorted sets of size n, rot performs n recursive calls. Hence the total number of calls to rot is equal to $\sum_{i=1}^{n} i$. Finally, on a sorted set of size n, procedure inv does $\lfloor \frac{n}{2} \rfloor + 1$ recursive call.

A program P is reversible if it terminates and there exists a program P^{-1} such that $[\![\mathrm{P}^{-1}]\!] \circ [\![\mathrm{P}]\!] = Id$.

Theorem 1. *All terminating* FOQ *programs are reversible.*

3 Polynomial time soundness

In this section, we restrict the set of FOQ programs to a strict subset, named PFOQ, that is sound for the quantum complexity class FBQP. For this, we define two criteria: a criterion ensuring that a program terminates and a criterion preventing a terminating program from having an exponential runtime.

Polynomial-time FOQ. Given two statements S, S', we write $\mathrm{S} \in \mathrm{S}'$ to mean that S is a substatement of S' and $\mathrm{proc} \in \mathrm{S}$ holds if there are i and s such that **call** proc[i](s);$\in$ S. Given a program P = D :: S, we define the relation $>_{\mathrm{P}} \subseteq$ Procedures $\times$ Procedures by $\mathrm{proc}_1 >_{\mathrm{P}} \mathrm{proc}_2$ if $\mathrm{proc}_2 \in \mathrm{S}^{\mathrm{proc}_1}$, for any two procedures $\mathrm{proc}_1, \mathrm{proc}_2 \in$ S. Let the partial order $\geq_{\mathrm{P}}$ be the transitive and reflexive closure of $>_{\mathrm{P}}$ and define the equivalence relation $\sim_{\mathrm{P}}$ by $\mathrm{proc}_1 \sim_{\mathrm{P}} \mathrm{proc}_2$ if $\mathrm{proc}_1 \geq_{\mathrm{P}} \mathrm{proc}_2$ and $\mathrm{proc}_2 \geq_{\mathrm{P}} \mathrm{proc}_1$ both hold. Define also the strict order $>_{\mathrm{P}}$ by $\mathrm{proc}_1 >_{\mathrm{P}} \mathrm{proc}_2$ if $\mathrm{proc}_1 \geq_{\mathrm{P}} \mathrm{proc}_2$ and $\mathrm{proc}_1 \not\sim_{\mathrm{P}} \mathrm{proc}_2$ both hold.

Definition 1. *Let* WF *be the set of* FOQ *programs* P *that are error-free and satisfy the well-foundedness constraint:* $\forall \mathrm{proc} \in \mathrm{P},\ \forall$**call** $\mathrm{proc}'[\mathrm{i}](\mathrm{s});\in \mathrm{S}^{\mathrm{proc}}$,

$$\mathrm{proc} \sim_{\mathrm{P}} \mathrm{proc}' \Rightarrow \exists k > 0, \exists \mathrm{i}_1, \ldots, \mathrm{i}_k,\ s = \bar{\mathrm{p}} \ominus [\mathrm{i}_1, \ldots, \mathrm{i}_k].$$

Lemma 1 *If* $\mathrm{P} \in$ WF*, then* P *terminates.*

Example 3. Consider the program QFT of Example 1. The statements of the procedure declarations define the following relation: rec $>_{\mathrm{QFT}}$ rec, rec $>_{\mathrm{QFT}}$ rot, rot $>_{\mathrm{QFT}}$ rot, and inv $>_{\mathrm{QFT}}$ inv. Consequently, rec $\sim_{\mathrm{QFT}}$ rec, rot $\sim_{\mathrm{QFT}}$ rot, inv $\sim_{\mathrm{QFT}}$ inv, and rec $>_{\mathrm{QFT}}$ rot hold. For each call to an equivalent procedure, we check that the argument decreases: $\bar{\mathrm{p}} \ominus [1]$ in rec, $\bar{\mathrm{p}} \ominus [2]$ in rot, and $\bar{\mathrm{p}} \ominus [1, |\bar{\mathrm{p}}|]$ in inv. Consequently, QFT $\in$ WF. We deduce from Theorem 1 that QFT terminates.

We now add a further restriction on mutually recursive procedure calls for guaranteeing polynomial time using a notion of width.

Definition 2. *Given a program* P *and a procedure* $\mathrm{proc} \in \mathrm{P}$*, the* width *of* proc *in* P*, noted* $\mathrm{width}_{\mathrm{P}}(\mathrm{proc})$*, and the* width *of* proc *in* P relatively to statement S*, noted* $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S})$*, are two positive integers in* $\mathbb{N}$*. They are defined inductively by:*

$$\mathrm{width}_{\mathrm{P}}(\mathrm{proc}) \triangleq w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}^{\mathrm{proc}}),$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\textbf{skip};) \triangleq 0,$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{q} \mathrel{*}= \mathrm{U}^{f}(\mathrm{i});) \triangleq 0,$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1\ \mathrm{S}_2) \triangleq w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1) + w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_2),$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\textbf{if}\ \mathrm{b}\ \textbf{then}\ \mathrm{S}_{\textbf{true}}\ \textbf{else}\ \mathrm{S}_{\textbf{false}}) \triangleq \max(w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_{\textbf{true}}), w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_{\textbf{false}})),$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\textbf{qcase}\ \mathrm{q}\ \textbf{of}\ \{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}) \triangleq \max(w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_0), w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1)),$$
$$w_{\mathrm{P}}^{\mathrm{proc}}(\textbf{call}\ \mathrm{proc}'[\mathrm{i}](\mathrm{s});) \triangleq \begin{cases} 1 & \textit{if } \mathrm{proc} \sim_{\mathrm{P}} \mathrm{proc}', \\ 0 & \textit{otherwise.} \end{cases}$$

Definition 3 (PFOQ). *Let* PFOQ *be the set of programs* P *in* WF *that satisfy the following constraint:* $\forall \mathrm{proc} \in \mathrm{P}, \mathrm{width}_{\mathrm{P}}(\mathrm{proc}) \leq 1$.

Example 4. In the program of Example 1, $\mathrm{width}_{\mathrm{QFT}}(\mathrm{rec}) = \mathrm{width}_{\mathrm{QFT}}(\mathrm{rot}) = \mathrm{width}_{\mathrm{QFT}}(\mathrm{inv}) = 1$, since rec $>_{\mathrm{QFT}}$ rot holds. Since QFT $\in$ WF, by Example 3, we conclude that QFT is a PFOQ program.

We now show that the level of a PFOQ program is bounded by a polynomial in the length of its input.

Lemma 2 *For each* PFOQ *program* P*, there exists a polynomial* $Q \in \mathbb{N}[X]$ *such that* $\forall n \in \mathbb{N},\ \mathrm{level}_{\mathrm{P}}(n) \leq Q(n)$.

Moreover, checking whether a program is PFOQ is tractable.

Theorem 2. *For each* FOQ *program* P*, it can be decided in time* $O(|\mathrm{P}|^2)$ *whether* $\mathrm{P}_{\neg\perp} \in$ PFOQ.

Quantum Turing machines and FBQP. Following Bernstein and Vazirani [2], a k-tape *Quantum Turing Machine* (QTM), with $k \geq 1$, is defined by a triplet (Σ, Q, δ) where Σ is a finite alphabet including a blank symbol $\#$, Q is a finite set of states with an initial state s_0 and a final state $s_{\mathrm{T}} \neq s_0$, and δ is the quantum transition function in $Q \times \Sigma^k \to \tilde{\mathbb{C}}^{Q \times \Sigma^k \times \{L,N,R\}^k}$; $\{L, N, R\}$ being the

set of possible movements of a head on a tape. Each tape of the QTM is two-way infinite and contains cells indexed by $\mathbb{Z}$. A QTM successfully terminates if it reaches a superposition of only the final state $s_\top$. A QTM is said to be *well-formed* if the transition function δ preserves the norm of the superposition (or, equivalently, if the time evolution of the machine is unitary). The starting position of the tape heads is the *start cell*, the cell indexed by 0. If the machine terminates with all of its tape heads back on the start cells, it is called *stationary*. We will use *stationary* in the case where the machine terminates with its input tape head in the first cell, and all other tape heads in the last non-blank cell. We will further refer to a QTM as being *in normal form* if the only transitions from the final state $s_\top$ are towards the initial state s_0. These will be important conditions for the composition and branching constructions of QTMs. If a QTM is well-formed, stationary, and in normal form, we will call it *conservative* [16] (N.B.: our notion of stationary QTM differs but can be shown to be equivalent to the definition of stationary QTM in [16]).

A configuration γ of a k-tape QTM is a tuple $(s, \overline{w}, \overline{n})$, where s is a state in Q, $\overline{w}$ is a k-tuple of words in Σ^*, and $\overline{n}$ is a k-tuple of indexes (head positions) in $\mathbb{Z}$. An initial (final) configuration γ_{init} (resp. γ_{fin}) is a configuration of the shape $(s_0, \overline{w}, \overline{0})$ (resp. $(s_\top, \overline{w}, \overline{0})$). We use $\gamma(w)$ to denote a configuration γ where the word w is written on the input/output tape. Following [2], we write $\mathcal{S}$ to represent the inner-product space of finite complex linear combinations of configurations of the QTM M with the Euclidean norm. A QTM M defines a linear time operator $U_M : \mathcal{S} \to \mathcal{S}$, that outputs a superposition of configurations $\sum_i \alpha_i |\gamma_i\rangle$ obtained by applying a single-step transition of M to a configuration $|\gamma\rangle$ (*i.e.*, $U_M|\gamma\rangle = \sum_i \alpha_i |\gamma_i\rangle$). Let U_M^t, for $t \geq 1$, be the t-steps transition obtained from U_M as follows: $U_M^1 \triangleq U_M$ and $U_M^{t+1} \triangleq U_M \circ U_M^t$. Given a quantum state $|\psi\rangle = \sum_{w \in \{0,1\}^n} \alpha_w |w\rangle$ and a configuration γ, let $\gamma(|\psi\rangle) \in \mathcal{S}$ be the quantum configuration defined by $\gamma(|\psi\rangle) \triangleq \sum_{w \in \{0,1\}^n} \alpha_w |\gamma(w)\rangle$.

A quantum function $f : \mathcal{H} \to \mathcal{H}$ is computed by the QTM M in time t if for any $|\psi\rangle \in \mathcal{H}$, $U_M^t(\gamma_{init}(|\psi\rangle)) = \gamma_{fin}(f(|\psi'\rangle))$. Given $T : \mathbb{N} \to \mathbb{N}$ and a quantum function f, we say that the QTM M computes f in time T if for inputs of length n, M computes f in time $T(n)$.

Definition 4. *Given two functions $f : \{0,1\}^\star \to \{0,1\}^\star$, $F : \mathcal{H} \to \mathcal{H}$, and a value $p \in [0,1]$, we say that f is computed by F with probability p if $\forall x \in \{0,1\}^\star,\ |\langle f(x)|F(|x\rangle)|^2 \geq p$.*

The class FBQP is the functional extension of the complexity class BQP.

Definition 5 ([2]). *A function $f \in \{0,1\}^\star \to \{0,1\}^\star$ is in FBQP iff there exist a QTM M and a polynomial $P \in \mathbb{N}[X]$ s.t. M computes f in time P with probability $\frac{2}{3}$.*

A function $f \in \{0,1\}^\star \to \{0,1\}^\star$ has a *polynomial bound* $P \in \mathbb{N}[X]$ if $\forall n \in \mathbb{N}, \forall x \in \{0,1\}^n, \exists k \leq P(n),\ f(x) \in \{0,1\}^k$. Functions in FBQP have a polynomial bound as the size of their output is smaller than the polynomial time bound.

Soundness. We show that QTMs can simulate the function computed by any terminating FOQ program. The time complexity of this simulation depends on the length of the input quantum state and on the level of the considered program.

Lemma 3 *For any terminating* FOQ *program* P*, there exists a conservative QTM* M *that computes* $[\![\mathrm{P}]\!]$ *in time* $O(n + n \times \mathrm{level}_{\mathrm{P}}(n))$.

Now we show that any PFOQ program computes a FBQP function.

Theorem 3. *Given a* PFOQ *program* P*, a function* $f : \{0,1\}^\star \to \{0,1\}^\star$*, and a value* $p \in (\frac{1}{2}, 1]$*. If* f *is computed by* $[\![\mathrm{P}]\!]$ *with probability* p *then* $f \in$ FBQP.

Proof. Using Lemma 2 and Lemma 3. □

4 FBQP completeness

In this section we show that any function in FBQP can be faithfully approximated by a PFOQ program. Toward this end, we show that Yamakami's [16] FBQP-complete function algebra can be exactly simulated in PFOQ.

Yamakami's function algebra. A characterization of FBQP was provided in [16] using a function algebra, named $\widehat{\Box_1^{\mathrm{QP}}}$. Given a quantum state $|\psi\rangle$ and a word $w \in \{0,1\}^n$, with $n \leq l(|\psi\rangle)$. $|\psi\rangle$ can be written as $|\psi\rangle = \sum_i \alpha_i |w_i z_i\rangle$, with $w_i \in \{0,1\}^n$ and $z_i \in \{0,1\}^{l(|\psi\rangle)-n}$. We write $\langle w|\psi\rangle$ as an abuse of notation for the quantum state defined by $\langle w|\psi\rangle \triangleq \sum_i \alpha_i \langle w|w_i\rangle |z_i\rangle$.

Definition 6. $\widehat{\Box_1^{\mathrm{QP}}}$ *is the smallest class of functions including the basic initial functions* $\{I, Ph_\theta, Rot_\theta, NOT, SWAP\}$*, with* $\theta \in [0, 2\pi) \cap \tilde{\mathbb{C}}$*,*

- $I(|\psi\rangle) \triangleq |\psi\rangle$
- $Ph_\theta(|\psi\rangle) \triangleq |0\rangle\langle 0|\psi\rangle + e^{i\theta}|1\rangle\langle 1|\psi\rangle$
- $Rot_\theta(|\psi\rangle) \triangleq \cos\theta|\psi\rangle + \sin\theta(|1\rangle\langle 0|\psi\rangle - |0\rangle\langle 1|\psi\rangle)$
- $NOT(|\psi\rangle) \triangleq |0\rangle\langle 1|\psi\rangle + |1\rangle\langle 0|\psi\rangle$
- $SWAP(|\psi\rangle) \triangleq \begin{cases} |\psi\rangle & \text{if } l(|\psi\rangle) \leq 1 \\ \sum_{a,b\in\{0,1\}} |ba\rangle\langle ab|\psi\rangle & \text{otherwise} \end{cases}$

and closed under schemes Comp, Branch, and $kQRec_t$*, for* $k, t \in \mathbb{N}$*,*

- $Comp[F,G](|\psi\rangle) \triangleq F(G(|\psi\rangle))$
- $Branch[F,G](|\psi\rangle) \triangleq \begin{cases} |\psi\rangle & \text{if } l(|\psi\rangle) \leq 1 \\ |0\rangle \otimes F(\langle 0|\psi\rangle) + |1\rangle \otimes G(\langle 1|\psi\rangle) & \text{otherwise} \end{cases}$
- $kQRec_t[F,G,H](|\psi\rangle) \triangleq \begin{cases} F(|\psi\rangle) & \text{if } l(|\psi\rangle) \leq t \\ G\left(\sum_{w\in\{0,1\}^k} |w\rangle \otimes F_w(\langle w|H(|\psi\rangle))\right) & \text{otherwise} \end{cases}$

  where each $F_w \in \{kQRec_t[F,G,H], I\}$.

To handle general FBQP functions, [16] defines the extended encoding of an input $x \in \{0,1\}^\star$ as $\phi_P(|x\rangle) \triangleq |0^{l(|x|)}1\rangle\!\rangle 0^{P(l(|x|))}10^{11P(l(|x|))+6}1\rangle\!\rangle |x\rangle$, for some polynomial $P \in \mathbb{N}[X]$ that is an upper bound on the output size of the desired FBQP function. ϕ_P simply consists in the quantum state $|x\rangle$ preceded by a polynomial number of ancilla qubits. These ancilla provide space for internal computations and account for the polynomial bound associated to polynomial time QTMs.

Theorem 4 ([16]). *Given $f : \{0,1\}^\star \to \{0,1\}^\star$ with polynomial bound $P \in \mathbb{N}[X]$, the following statements are equivalent.*

1. *The function f is in* FBQP.
2. *There exists $F \in \widehat{\square_1^{\mathrm{QP}}}$ such that $F \circ \phi_P$ computes f with probability $\frac{2}{3}$.*

We show the following result by structural induction on a function in $\widehat{\square_1^{\mathrm{QP}}}$.

Theorem 5. *Let F be a function in $\widehat{\square_1^{\mathrm{QP}}}$. Then there exists a* PFOQ *program* P *such that* $[\![\mathrm{P}]\!] = F$.

We are now ready to state the completeness result.

Theorem 6. *For every function f in* FBQP *with polynomial bound $Q \in \mathbb{N}[X]$, there is a* PFOQ *program* P *such that* $[\![\mathrm{P}]\!] \circ \phi_Q$ *computes f with probability $\frac{2}{3}$.*

Proof. By Theorem 4 and Theorem 5. □

5 Compilation to polynomial-size quantum circuits

In this section, we provide an algorithm that compiles a PFOQ program on a given input length $n \in \mathbb{N}$ into a quantum circuit of size polynomial in n.

Quantum circuits [8] are a well-known graphical computational model for describing quantum computations. Qubits are represented by wires. Each unitary transformation U acting on n qubits can be represented as a gate U with n inputs and n outputs. A circuit C is an element of a PROP category ([10], a symmetric strict monoidal category) whose morphisms are generated by gates G and wires. Let $\mathbb{1}$ be the identity circuit (for any length) and $\circ$ and $\otimes$ be the composition and product, respectively. By abuse of notation, given k circuits $C^1, \ldots, C^k$, $\circ_{i=1}^k C^i$ will denote the circuit $\tilde{C}^1 \circ \cdots \circ \tilde{C}^k$, where each circuit $\tilde{C}^i$ is obtained by tensoring C^i appropriately with identities so that the output of C^i matches the input of C^{i+1}. By construction, a circuit is acyclic. Each circuit C_n can be indexed by its number $n \in \mathbb{N}$ of input wires (i.e., non ancilla qubits) and computes a function $[\![C_n]\!] \in \mathcal{H}_{2^n} \to \mathcal{H}_{2^n}$. To deal with functions in $\mathcal{H} \to \mathcal{H}$, we consider families of circuits $(C_n)_{n\in\mathbb{N}}$, that are sequences of circuits such that each C_n encodes computation on quantum states of length n. Hence each circuit has n input qubits plus some extra ancilla qubits. These ancillas can be used to perform intermediate computations but also to represent functions whose output size is strictly greater than their input size. To avoid the consideration of families encoding undecidable properties, we put a uniformity restriction.

Definition 7. *A family of circuits $(C_n)_{n\in\mathbb{N}}$ is said to be* uniform *if there exists a polynomial time Turing machine that takes n as input and outputs a representation of C_n, for all $n \in \mathbb{N}$.*

In quantifying the complexity of a circuit, it is necessary to specify the considered elementary gates, and define the complexity of an operation as the number of elementary gates needed to perform it. In our setting, we consider the following set of universal elementary gates $\{R_Y(\pi/4), P(\pi/4), CNOT\}$. The size $\#C$ of a circuit C is equal to the number of its gates and wires.

Definition 8. *A family of circuits $(C_n)_{n\in\mathbb{N}}$ is said to be* polynomial-size *with $\alpha \in \mathbb{N} \to \mathbb{N}$ ancilla qubits if there exists a polynomial $P \in \mathbb{N}[X]$ such that, for each $n \in \mathbb{N}$, $\#C_n \leq P(n)$ and the number of ancilla qubits in C_n is exactly $\alpha(n)$.*

Let $\chi_m : \mathcal{H}_{2^n} \to \mathcal{H}_{2^{n+m}}$ be defined by $\chi_m(|\psi\rangle) \triangleq |\psi\rangle \otimes |0^m\rangle$, for a state $|\psi\rangle$ of size n. Let $\xi_m : \mathcal{H}_{2^n} \to \mathcal{H}_{2^m}$, with $m \leq n$, be defined by $\xi_m(|\psi\rangle) \triangleq \sum_{w\in\{0,1\}^m} \sum_{z\in\{0,1\}^{n-m}} \langle wz|\psi\rangle\, |w\rangle$. Finally, let $|w|$, for $w \in \{0,1\}^\star$, be the size of the word w.

Theorem 7. (Adapted from [17] and [11]) *A function $f : \{0,1\}^\star \to \{0,1\}^\star$ is in* FBQP *iff there exists a uniform polynomial-size family of circuits $(C_n)_{n\in\mathbb{N}}$ with α ancilla qubits s.t. $\forall x \in \{0,1\}^\star$, $\left|\left\langle f(x)\middle|\xi_{|f(x)|} \circ [\![C_{|x|}]\!] \circ \chi_{\alpha(|x|)}(|x\rangle)\right\rangle\right|^2 \geq \frac{2}{3}$.*

In Theorem 7, $[\![C_{|x|}]\!]$ is a function in $\mathcal{H}_{2^{|x|+\alpha(|x|)}} \to \mathcal{H}_{2^{|x|+\alpha(|x|)}}$ The function $\chi_{\alpha(|x|)}$ pads the input with ancilla in state $|0\rangle$ to match the circuit dimension. The function $\xi_{|f(x)|}$ projects the output of the circuit to match the length of the function output $|f(x)|$. Hence, for $|x\rangle \in \mathcal{H}_{2^{|x|}}$, $\xi_{|f(x)|} \circ [\![C_{|x|}]\!] \circ \chi_{\alpha(|x|)}(|x\rangle) \in \mathcal{H}_{2^{|f(x)|}}$.

Compilation to circuits. For each PFOQ program P, the existence of a polynomial-size uniform family of circuits $(C_n)_{n\in\mathbb{N}}$ that computes $[\![\mathrm{P}]\!]$ is entailed by the combination of Lemma 2 and Theorem 7. However, due to the complex machinery of QTM, the constructions of both proofs cannot be used in practice to generate a circuit. In this section, we exhibit an algorithm that compiles directly a PFOQ program to a polynomial-size circuit. Note that this compilation process requires some care since recursive procedure calls in quantum cases may yield an exponential number of calls. The remainder of this section will be devoted to presenting an algorithm, named **compile**, which, for a given PFOQ program P and a given integer n produces a circuit C_n such that $\forall |\psi\rangle \in \mathcal{H}_{2^n}$, $[\![\mathrm{P}]\!](|\psi\rangle) = \xi_n \circ [\![C_n]\!] \circ \chi_{\alpha(n)}(|\psi\rangle)$.

The **compile** algorithm uses two subroutines, named **compr** and **optimize**, and is defined by $\mathbf{compile}(\mathrm{P}, n) \triangleq \mathbf{compr}(\mathrm{P}, [1, \ldots, n], \cdot)$.

The subroutine **compr** (Algorithm 1) generates the circuit inductively on the program statement. It takes as inputs: a program P, a list of qubit pointers l, and a control structure cs. A *control structure* cs is a partial function in $\mathbb{N} \to \{0,1\}$, mapping a qubit pointer to a control value (of a quantum case). Let $\cdot$ be the control structure of empty domain. For $n \in \mathbb{N}$ and $k \in \{0,1\}$, $cs[n := k]$ is the control structure obtained from cs by setting $cs(n) \triangleq k$. For a given $x \in \{0,1\}^\star$,

we say that state $|x\rangle$ *satisfies* cs if, $\forall n \in dom(cs)$, $cs(n) = k \Rightarrow |\langle k|_n |x\rangle|^2 = 1$. Two control structures cs and cs' are *orthogonal* if there does not exist a state $|x\rangle$ that satisfies cs and cs'. Note that if $\exists i \in dom(cs) \cap dom(cs'),\ cs(i) + cs'(i) = 1$ then cs and cs' are orthogonal.

Algorithm 1 (**compr**)
Input: $(\mathrm{P}, l, cs) \in \mathrm{Programs} \times \mathcal{L}(\mathbb{N}) \times (\mathbb{N} \to \{0,1\})$

Let $\mathrm{D} :: \mathrm{S} = \mathrm{P}$ **in**
if $\mathrm{S} =$ **skip**; **then**
  $C \leftarrow \mathbb{1}$ ▷ Identity circuit

else if $\mathrm{S} = \mathrm{s[i]} \mathrel{*}= \mathrm{U}^f(\mathrm{j})$; **and** $(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n$ **and** $(\mathrm{U}^f(\mathrm{j}), l) \Downarrow_{\mathbb{C}^{2\times 2}} M$ **then**
  $C \leftarrow M(cs, [n])$ ▷ Controlled gate

else if $\mathrm{S} = \mathrm{S}_1\,\mathrm{S}_2$ **then**
  $C \leftarrow$ **compr**$(\mathrm{D} :: \mathrm{S}_1, l, cs) \circ$ **compr**$(\mathrm{D} :: \mathrm{S}_2, l, cs)$ ▷ Composition

else if $\mathrm{S} =$ **if** b **then** $\mathrm{S}_{\mathbf{true}}$ **else** $\mathrm{S}_{\mathbf{false}}$ **and** $(\mathrm{b}, l) \Downarrow_{\mathbb{B}} b$ **then**
  $C \leftarrow$ **compr**$(\mathrm{D} :: \mathrm{S}_b, l, cs)$ ▷ Conditional

else if $\mathrm{S} =$ **qcase** s[i] **of** $\{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}$ **and** $(\mathrm{s[i]}, l) \Downarrow_{\mathbb{N}} n$ **then**
  $C \leftarrow$ **compr**$(\mathrm{D} :: \mathrm{S}_0, l, cs[n := 0]) \circ$ **compr**$(\mathrm{D} :: \mathrm{S}_1, l, cs[n := 1])$ ▷ Quantum case

else if $\mathrm{S} =$ **call** proc[i](s) **and** $(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} [\,]$ **then**
  $C \leftarrow \mathbb{1}$ ▷ Nil call

else if $\mathrm{S} =$ **call** proc[i](s) **and** $(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} l' \neq [\,]$ **and** $(\mathrm{i}, l) \Downarrow_{\mathbb{Z}} n$ **then**
  if $\mathrm{width}_{\mathrm{P}}(\mathrm{proc}) = 0$ **then**
    $C \leftarrow$ **compr**$(\mathrm{D} :: \mathrm{S}^{\mathrm{proc}}\{n/\mathrm{x}\}, l', cs)$ ▷ Non-recursive call
  else if $\mathrm{width}_{\mathrm{P}}(\mathrm{proc}) = 1$ **then**
    $C \leftarrow$ **optimize**$(\mathrm{D}, [(cs, \mathrm{S}^{\mathrm{proc}}\{n/\mathrm{x}\})], \mathrm{proc}, l', \{\})$ ▷ Recursive call
  end if
end if
return C

Given a control structure cs and a statement S, a *controlled statement* is a pair $(cs, \mathrm{S}) \in \mathrm{Cst} \triangleq (\mathbb{N} \to \{0,1\}) \times \mathrm{Statements}$. Intuitively, a controlled statement (cs, S) denotes a statement controlled by the qubits whose indices are in $dom(cs)$. For a unitary gate $U \in \mathcal{H}_{2^n} \to \mathcal{H}_{2^n}$, a control structure cs, and a list of pointers $l = [x_1, \ldots, x_n] \in \mathcal{L}(\mathbb{N})$ such that $\{x_1, \ldots, x_n\} \cap dom(cs) = \varnothing$, $U(cs, l)$ denotes the circuit applying gate U on qubits $\bar{\mathrm{q}}[x_1], \ldots, \bar{\mathrm{q}}[x_n]$, whenever $\forall m \in dom(cs)$, $\bar{\mathrm{q}}[m]$ is in state $|cs(m)\rangle$. As demonstrated in [11], this circuit can be built with $O(card(dom(cs)))$ elementary gates and ancillas, and a single controlled-U gate.

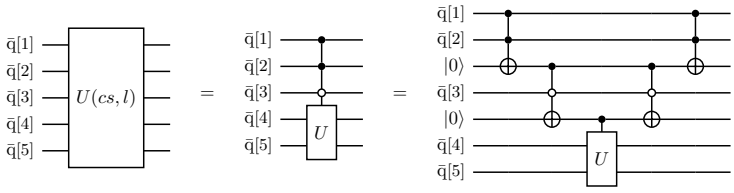


Fig. 4: Example of circuit $U(cs, l)$

Example 5. As an illustrative example, consider a binary gate U and a control structure cs such that $dom(cs) = \{1, 2, 3\}$, $cs(1) = cs(2) = 1$, and $cs(3) = 0$. Also consider a list $l = [4, 5] \in \mathcal{L}(\mathbb{N})$. The circuit $U(cs, l)$ is provided in Figure 4.

Similarly, we can define a generalized Toffoli gate as a circuit of the shape $NOT(cs, n)$. Since $card(dom(cs))$ will not scale with the size of the input, such a circuit has a constant cost in gates and ancillas and can thus be considered as an elementary gate. We will also be interested in rearranging wires under a given control structure. For two lists of qubit pointers $l_1 = [x_1, \ldots, x_n]$, $l_2 = [x'_1, \ldots, x'_n] \in \mathcal{L}(\mathbb{N})$, define $SWAP(cs, l_1, l_2)$ as the circuit that swaps the wires in l_1 with wires in l_2, controlled on cs. This circuit needs in the worst case one ancilla and $O(n)$ controlled $SWAP$ gates (also known as Fredkin gates).

Let $\mathcal{D} \triangleq \mathcal{D}(\text{Procedures} \times \mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathcal{L}(\mathbb{N}))$ be the set of dictionaries mapping keys of the shape (proc, i, j) to pairs of the shape (a, l), where i is the value of a classical parameter, j is the size of a sorted set, and a is a qubit index. We will denote the empty dictionary by $\{\}$. Let also $a \leftarrow \textbf{new}\ ancilla()$ be an instruction that sets a to a fresh qubit index.

The subroutine **optimize** (Algorithm 2) treats the complex cases where circuit optimizations (merging) are needed, that is for recursive procedure calls. It takes as input a sequence of procedure declarations D, a list of controlled statements l_{Cst}, a procedure name proc, a list of qubit pointers l, and a dictionary Anc. The subroutine iterates on list l_{Cst} of controlled statements, indicating the statements left to be treated together with their control qubits. When recursive procedure calls appear in distinct branches of a quantum case, the algorithm merges these calls together. For that purpose, it uses new ancilla qubits as control qubits. Given procedure calls of shape **call** proc[i](s);, with respect to a given list $l \in \mathcal{L}(\mathbb{N})$, such that $(\text{i}, l) \Downarrow_{\mathbb{Z}} i$, $(\text{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} l'$, and $(|\text{s}|, l) \Downarrow_{\mathbb{N}} j$. If the key (proc, i, j) already exists in the dictionary Anc, the associated ancilla is re-used, otherwise, Anc$[\text{proc}, i, j]$ is set to (a, l'). We can assume w.l.o.g. that the statement controlled on the ancilla can be treated only after all the re-uses of the ancilla. This can be done without increasing the total complexity of **optimize**.

Some extra ancillas e are also created for swapping wires and are not explicitly indexed since they are not revisited by the subroutine, and are just considered unique. Ancillas a and e are indexed and treated as input qubits, therefore they can be part of the domain of control structures.

Algorithm 2 (optimize) Build circuit for recursive procedure proc
Inputs: $(\mathrm{D}, l_{\mathrm{Cst}}, \mathrm{proc}, l, \mathrm{Anc}) \in \mathrm{Decl} \times \mathcal{L}(\mathrm{Cst}) \times \mathrm{Procedures} \times \mathcal{L}(\mathbb{N}) \times \mathcal{D}$

$C_{\mathrm{L}} \leftarrow \mathbb{1}$; $C_{\mathrm{R}} \leftarrow \mathbb{1}$; $\mathrm{P} \leftarrow \mathrm{D} :: \mathbf{skip}$;
while $l_{\mathrm{Cst}} \neq [\,]$ **do**
  $(cs, \mathrm{S}) \leftarrow hd(l_{\mathrm{Cst}})$; $l_{\mathrm{Cst}} \leftarrow tl(l_{\mathrm{Cst}})$

  if $\mathrm{S} = \mathrm{S}_1\,\mathrm{S}_2$ **then**
    if $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1) = 1$ **then**
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs, \mathrm{S}_1)]$; $C_{\mathrm{R}} \leftarrow \mathbf{compr}(\mathrm{D} :: \mathrm{S}_2, l, cs) \circ C_{\mathrm{R}}$
    else
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs, \mathrm{S}_2)]$; $C_{\mathrm{L}} \leftarrow C_{\mathrm{L}} \circ \mathbf{compr}(\mathrm{D} :: \mathrm{S}_1, l, cs)$
    end if
  end if

  if $\mathrm{S} =$ **if** b **then** $\mathrm{S}_{\mathbf{true}}$ **else** $\mathrm{S}_{\mathbf{false}}$ **and** $(\mathrm{b}, l) \Downarrow_{\mathbb{B}} b$ **then**
    if $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_b) = 1$ **then**
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs, \mathrm{S}_b)]$
    else
      $C_L \leftarrow C_L \circ \mathbf{compr}(\mathrm{D} :: \mathrm{S}_b, l, cs)$
    end if
  end if

  if $\mathrm{S} =$ **qcase** $s[\mathrm{i}]$ **of** $\{0 \to \mathrm{S}_0, 1 \to \mathrm{S}_1\}$ **and** $(s[\mathrm{i}], l) \Downarrow_{\mathbb{N}} n$ **then**
    if $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_0) = 1$ **and** $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1) = 1$ **then**
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs[n := 0], \mathrm{S}_0), (cs[n := 1], \mathrm{S}_1)]$
    else if $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_1) = 0$ **then**
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs[n := 0], \mathrm{S}_0)]$;
      $C_{\mathrm{R}} \leftarrow \mathbf{compr}(\mathrm{D} :: \mathrm{S}_1, l, cs[n := 1]) \circ C_{\mathrm{R}}$
    else if $w_{\mathrm{P}}^{\mathrm{proc}}(\mathrm{S}_0) = 0$ **then**
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(cs[n := 1], \mathrm{S}_1)]$;
      $C_{\mathrm{R}} \leftarrow \mathbf{compr}(\mathrm{D} :: \mathrm{S}_0, l, cs[n := 0]) \circ C_{\mathrm{R}}$
    end if
  end if

  if $\mathrm{S} =$ **call** $\mathrm{proc}'[\mathrm{i}](\mathrm{s})$ **and** $(\mathrm{s}, l) \Downarrow_{\mathcal{L}(\mathbb{N})} l' \neq [\,]$ **and** $(\mathrm{i}, l) \Downarrow_{\mathbb{Z}} n$ **then**
    if $(\mathrm{proc}', n, |l'|) \in \mathrm{Anc}$ **then**
      Let $(a, l'') = \mathrm{Anc}[\mathrm{proc}', n, |l'|]$ **in**
      $e \leftarrow$ **new** $ancilla()$;
      $C_{\mathrm{L}} \leftarrow C_{\mathrm{L}} \circ NOT(cs, e) \circ NOT(\cdot[e = 1], a) \circ SWAP(\cdot[e = 1], l', l'')$;
      $C_{\mathrm{R}} \leftarrow SWAP(\cdot[e = 1], l'', l') \circ NOT(\cdot[e = 1], a) \circ NOT(cs, e) \circ C_{\mathrm{R}}$
    else
      $a \leftarrow$ **new** $ancilla()$
      $\mathrm{Anc}[\mathrm{proc}', n, |l'|] \leftarrow (a, l')$;
      $C_{\mathrm{L}} \leftarrow C_{\mathrm{L}} \circ NOT(cs, a)$; $C_{\mathrm{R}} \leftarrow NOT(cs, a) \circ C_{\mathrm{R}}$;
      $l_{\mathrm{Cst}} \leftarrow l_{\mathrm{Cst}} @ [(\cdot[a = 1], \mathrm{S}^{\mathrm{proc}'}\{n/\mathrm{x}\})]$
    end if
  end if
end while
return $C_L \circ C_R$

Theorem 8. *For any* P *in* PFOQ*, there is* $Q \in \mathbb{N}[X]$*,* $\forall n \in \mathbb{N}$*,* $\forall |\psi\rangle \in \mathcal{H}_{2^n}$*,* $[\![\mathrm{P}]\!](|\psi\rangle) = \xi_n \circ [\![\mathbf{compile}(\mathrm{P}, n)]\!] \circ \chi_{\alpha(n)}(|\psi\rangle)$ *and* $\#\mathbf{compile}(\mathrm{P}, n) \leq Q(n)$*.*

Example 6. $\mathbf{compile}(\mathrm{QFT}, n)$ outputs the circuit provided in Example 1. Notice that there is no extra ancilla as no procedure call appears in the branch of a quantum case.

Polynomial-size circuits. We show Theorem 8 by exhibiting that any exponential growth of the circuit can be avoided by the **compile** algorithm using an argument based on orthogonal control structures. With a linear number of gates and a constant number of extra ancillas, we can merge calls referring to the same procedure, on different branches of a quantum case, when they are applied to sorted sets of equal size. An example of the construction is given in Figure 5 where two instances of a gate U are merged into one using $SWAP$ gates and gates controlled by orthogonal control structures.

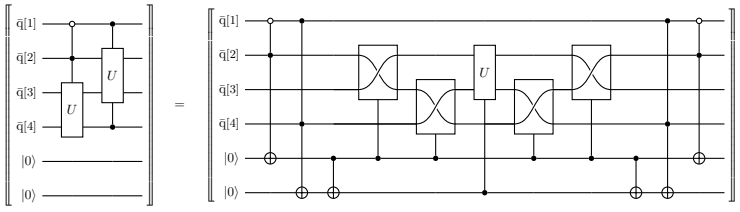


Fig. 5: Example of circuit optimization.

The following proposition shows that multiple uses of a gate can be merged in one provided they are applied to orthogonal control structures.

Lemma 4 *For any circuit* $C_n \triangleq \circ_{i=1}^{k} U(cs_i, l_i)$*, with a unitary gate* U*, pairwise orthogonal* $cs_1, \ldots, cs_k \in \mathrm{Cst}$*, and* $l_1, \ldots l_k \in \mathcal{L}(\mathbb{N})$*, there exists a circuit* C *using one controlled gate* U*,* $O(kn)$ *gates, and* $O(k)$ *ancillas, and such that* $[\![C]\!] = [\![C_n]\!]$*.*

Now we show that orthogonality is an invariant property of **compile**.

Lemma 5 *Orthogonality is an invariant property of the control structures in* l_{Cst} *of the subroutine* **optimize***. In other words, for any two distinct pairs* (cs, S)*,* (cs', S') *in* l_{Cst}*,* cs *and* cs' *are orthogonal.*

Theorem 9. *For any* P *in* PFOQ*,* $\mathbf{compile}(\mathrm{P}, n)$ *runs in time* $O(n^{2|\mathrm{P}|+1})$*.*

Proof. Using Lemma 4 and Lemma 5. □

As there is no circuit duplication in the assignments of **compile**, we can deduce from Theorem 9 that the compiled circuit is of polynomial size.

Corollary 1. *For any* P *in* PFOQ*, there exists a polynomial* $Q \in \mathbb{N}[X]$ *such that* $\#\mathbf{compile}(\mathrm{P}, n) \leq Q(n)$*.*

References

1. Bellantoni, S., Cook, S.: A new recursion-theoretic characterization of the polytime functions. computational complexity **2**(2), 97–110 (Jun 1992). https://doi.org/10.1007/BF01201998
2. Bernstein, E., Vazirani, U.: Quantum complexity theory. SIAM Journal on Computing **26**(5), 1411–1473 (1997). https://doi.org/10.1137/S0097539796300921
3. Boykin, P.O., Mor, T., Pulver, M., Roychowdhury, V., Vatan, F.: On universal and fault-tolerant quantum computing (1999). https://doi.org/10.48550/ARXIV.QUANT-PH/9906054
4. Briegel, H.J., Browne, D.E., Dür, W., Raussendorf, R., Van den Nest, M.: Measurement-based quantum computation. Nature Physics **5**(1), 19–26 (2009). https://doi.org/10.1038/nphys1157
5. Dal Lago, U.: A short introduction to implicit computational complexity. In: ESSLLI 2010. pp. 89–109 (2011). https://doi.org/10.1007/978-3-642-31485-8$_3$
6. Dal Lago, U., Masini, A., Zorzi, M.: Quantum implicit computational complexity. Theoretical Computer Science **411**(2), 377–409 (2010). https://doi.org/10.1016/j.tcs.2009.07.045
7. Danos, V., Kashefi, E.: Determinism in the one-way model. Physical Review A **74**(5), 052310 (2006). https://doi.org/10.1103/PhysRevA.74.052310
8. Deutsch, D.E.: Quantum computational networks. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **425**(1868), 73–90 (1989)
9. Feynman, R.P.: Simulating physics with computers. International Journal of Theoretical Physics **21**(6), 467–488 (Jun 1982). https://doi.org/10.1007/BF02650179
10. MacLane, S.: Categorical algebra. Bulletin of the American Mathematical Society **71**(1), 40–106 (1965). https://doi.org/10.1090/S0002-9904-1965-11234-4
11. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2011)
12. Péchoux, R.: Implicit computational complexity: past and future. Mémoire d'habilitation à diriger des recherches (2020), `https://tel.archives-ouvertes.fr/tel-02978986`, université de Lorraine
13. Ross, N.J.: Algebraic and logical methods in quantum computation. PhD thesis (2015). https://doi.org/10.48550/ARXIV.1510.02198
14. Selinger, P.: Towards a quantum programming language. Mathematical Structures in Computer Science **14**(4), 527–586 (2004). https://doi.org/10.1017/S0960129504004256
15. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124–134 (1994). https://doi.org/10.1109/SFCS.1994.365700
16. Yamakami, T.: A schematic definition of quantum polynomial time computability. J. Symb. Log. **85**(4), 1546–1587 (2020). https://doi.org/10.1017/jsl.2020.45
17. Yao, A.C.C.: Quantum circuit complexity. In: Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science. pp. 352–361 (1993). https://doi.org/10.1109/SFCS.1993.366852