

UNIVERSITY OF CALGARY

An investigation of the underpinnings of quantum and reversible computing

subtitle

by

Brett Gordon Giles

A DISSERTATION

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE

CALGARY, ALBERTA

August, 2013

© Brett Gordon Giles 2013

# Abstract

# Acknowledgements

# Table of Contents

|  |           |
|--|-----------|
| <b>Abstract</b>                                    | i         |
| <b>Acknowledgements</b>                            | ii        |
| Table of Contents                                  | iii       |
| List of Tables                                     | v         |
| List of Figures                                    | vi        |
| List of Symbols                                    | vii       |
| <b>1 Quantum computation and circuits</b>          | <b>1</b>  |
| 1.1 Linear algebra                                 | 1         |
| 1.1.1 Basic definitions                            | 1         |
| 1.1.2 Matrices                                     | 2         |
| 1.2 Basic quantum computation                      | 4         |
| 1.2.1 Quantum bits                                 | 4         |
| 1.2.2 Quantum entanglement                         | 5         |
| 1.2.3 Quantum gates                                | 5         |
| 1.2.4 Measurement                                  | 6         |
| 1.2.5 Mixed states                                 | 7         |
| 1.2.6 Density matrix notation                      | 7         |
| 1.3 Quantum circuits                               | 8         |
| 1.3.1 Contents of quantum circuits                 | 8         |
| 1.3.2 Syntax of quantum circuits                   | 13        |
| 1.3.3 Examples of quantum circuits                 | 13        |
| 1.4 Extensions to quantum circuits                 | 18        |
| 1.4.1 Renaming                                     | 18        |
| 1.4.2 Wire crossing                                | 19        |
| 1.4.3 Scoped control                               | 19        |
| 1.4.4 Circuit identities                           | 20        |
| <b>2 Transformations of Quantum Programs</b>       | <b>23</b> |
| 2.1 Terminology                                    | 23        |
| 2.1.1 Basic Types                                  | 23        |
| 2.1.2 Types and Shapes                             | 23        |
| 2.2 Subroutines                                    | 24        |
| 2.2.1 Definition of a Subroutine                   | 24        |
| 2.2.2 Subroutine Calls                             | 26        |
| 2.2.3 High Level Structure                         | 27        |
| 2.3 Subroutine Calls and Transformers              | 28        |
| 2.3.1 Iteration                                    | 28        |
| 2.3.2 Iteration transformation of a subroutine     | 31        |
| 2.3.3 Folding subroutines                          | 32        |
| 2.3.4 Subroutine to folded subroutine transform    | 37        |
| 2.3.5 Examples of folding                          | 41        |
| 2.4 Alternate Algorithm for Fold Transformation    | 45        |
| 2.4.1 Examples of folding with Alternate Algorithm | 47        |

|                                       |    |
|---------------------------------------|----|
| 2.5 Diagram of Folded Carry . . . . . | 48 |
| Bibliography . . . . .                | 50 |

## List of Tables

|     |  |    |
|-----|--|----|
| 1.1 | Gates, circuit notation and matrices . . . . .           | 10 |
| 1.2 | Syntactic elements of quantum circuit diagrams . . . . . | 14 |

## List of Figures and Illustrations

|      |   |    |
|------|---|----|
| 1.1  | Simple single gate circuit . . . . .                            | 9  |
| 1.2  | Entangling two <b>qubits</b> . . . . .                          | 9  |
| 1.3  | Controlled-Not of $ 1\rangle$ and $ 1\rangle$ . . . . .         | 9  |
| 1.4  | Measure notation in quantum circuits . . . . .                  | 11 |
| 1.5  | Examples of multi- <b>qubit</b> gates and measures . . . . .    | 11 |
| 1.6  | Other forms of control for gates . . . . .                      | 12 |
| 1.7  | $n$ <b>qubits</b> on one line . . . . .                         | 12 |
| 1.8  | Swap and controlled-Z . . . . .                                 | 13 |
| 1.9  | Quantum teleportation . . . . .                                 | 16 |
| 1.10 | Circuit for the Deutsch-Jozsa algorithm . . . . .               | 17 |
| 1.11 | Circuit for the quantum Fourier transform . . . . .             | 18 |
| 1.12 | Circuit for the inverse quantum Fourier transform . . . . .     | 18 |
| 1.13 | Renaming of a <b>qubit</b> and its equivalent diagram . . . . . | 18 |
| 1.14 | Bending . . . . .   | 19 |
| 1.15 | Scope of control . . . . .                                      | 19 |
| 1.16 | Extensions sample . . . . .                                     | 20 |
| 1.17 | Swap in control vs. exchange in control . . . . .               | 20 |
| 1.18 | Measure is not affected by control . . . . .                    | 20 |
| 1.19 | Control is not affected by measure . . . . .                    | 21 |
| 1.20 | Zero control is syntactic sugar . . . . .                       | 21 |
| 1.21 | Scoped control is parallel control . . . . .                    | 21 |
| 1.22 | Scoped control is serial control . . . . .                      | 22 |
| 1.23 | Multiple control . . . . .                                      | 22 |
| 1.24 | Control scopes commute . . . . .                                | 22 |
| 2.1  | Transforming a subroutine to an iterated subroutine . . . . .   | 32 |
| 2.2  | Fold with extra in/out . . . . .                                | 41 |
| 2.3  | Fold with three iterations . . . . .                            | 43 |
| 2.4  | Fold of Carry . . . . .   | 44 |
| 2.5  | Folding Carry . . . . .   | 49 |

# List of Symbols, Abbreviations and Nomenclature

|        |                       |
|--------|-----------------------|
| Symbol | Definition            |
| U of C | University of Calgary |



# Chapter 1

## Quantum computation and circuits

### 1.1 Linear algebra

Quantum computation requires familiarity with the basics of linear algebra. This section will give definitions of the terms used throughout this thesis.

#### 1.1.1 Basic definitions

The first definition needed is that of a *vector space*.

**Definition 1.1.1** (Vector Space). *Given a field  $F$ , whose elements will be referred to as scalars, a vector space over  $F$  is a non-empty set  $V$  with two operations, vector addition and scalar multiplication. Vector addition is defined as  $+$  :  $V \times V \rightarrow V$  and denoted as  $\mathbf{v} + \mathbf{w}$  where  $\mathbf{v}, \mathbf{w} \in V$ . The set  $V$  must be an abelian group under  $+$ . Scalar multiplication is defined as  $\cdot$  :  $F \times V \rightarrow V$  and denoted as  $c\mathbf{v}$  where  $c \in F, \mathbf{v} \in V$ . Scalar multiplication distributes over both vector addition and scalar addition and is associative.  $F$ 's multiplicative identity is an identity for scalar multiplication.*

The specific algebraic requirements are:

1.  $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w});$
2.  $\forall \mathbf{u}, \mathbf{v} \in V, \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u};$
3.  $\exists \mathbf{0} \in V$  such that  $\forall \mathbf{v} \in V, \mathbf{0} + \mathbf{v} = \mathbf{v};$
4.  $\forall \mathbf{u} \in V, \exists \mathbf{v} \in V$  such that  $\mathbf{u} + \mathbf{v} = \mathbf{0};$
5.  $\forall \mathbf{u}, \mathbf{v} \in V, c \in F, c(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v};$

$$6. \forall \mathbf{u} \in V, c, d \in F, (c + d)\mathbf{u} = c\mathbf{u} + d\mathbf{u};$$

$$7. \forall \mathbf{u} \in V, c, d \in F, (cd)\mathbf{u} = c(d\mathbf{u});$$

$$8. \forall \mathbf{u} \in V, 1\mathbf{u} = \mathbf{u}.$$

Examples of vector spaces over  $F$  are:  $F^{n \times m}$  – the set of  $n \times m$  matrices over  $F$ ; and  $F^n$  – the  $n$ –fold Cartesian product of  $F$ .  $F^{n \times 1}$ , the set of  $n \times 1$  matrices over  $F$  is also called the space of column vectors, while  $F^{1 \times n}$ , the set of row vectors. Often,  $F^n$  is identified with  $F^{n \times 1}$ .

This thesis shall identify  $F^n$  with the column vector space over  $F$ .

**Definition 1.1.2** (Linearly independent). *A subset of vectors  $\{\mathbf{v}_i\}$  of the vector space  $V$  is said to be linearly independent when no finite linear combination of them,  $\sum \alpha_j \mathbf{v}_j$  equals  $\mathbf{0}$  unless all the  $\alpha_j$  are zero.*

**Definition 1.1.3** (Basis). *A basis of a vector space  $V$  is a linearly independent subset of  $V$  that generates  $V$ . That is, any vector  $\mathbf{u} \in V$  is a linear combination of the basis vectors.*

### 1.1.2 Matrices

As mentioned above, the set of  $n \times m$  matrices over a field is a vector space. Additionally, matrices compose and the tensor product of matrices is defined.

Matrix composition is defined as usual. That is, for  $A = [a_{ij}] \in F^{m \times n}$ ,  $B = [b_{jk}] \in F^{n \times p}$ :

$$AB = \left[ \left( \sum_j a_{ij} b_{jk} \right) \right]_{ik} \in F^{m \times p}.$$

**Definition 1.1.4** (Diagonal matrix). *A diagonal matrix is a matrix where the only non-zero entries are those where the column index equals the row index.*

The diagonal matrix  $n \times n$  with only 1's on the diagonal is the identity for matrix multiplication, and is designated by  $I_n$ .

**Definition 1.1.5** (Transpose). The transpose of an  $n \times m$  matrix  $A = [a_{ij}]$  is an  $m \times n$  matrix  $A^t$  with the  $i, j$  entry being  $a_{ji}$ .

When the base field of a matrix is  $\mathbb{C}$ , the complex numbers, the *conjugate transpose* (also called the *adjoint*) of an  $n \times m$  matrix  $A = [a_{ij}]$  is defined as the  $m \times n$  matrix  $A^*$  with the  $i, j$  entry being  $\bar{a}_{ji}$ , where  $\bar{a}$  is the complex conjugate of  $a \in \mathbb{C}$ .

When working with column vectors over  $\mathbb{C}$ , note that  $\mathbf{u} \in \mathbb{C}^n \implies \mathbf{u}^* \in \mathbb{C}^{1 \times n}$  and that  $\mathbf{u}^* \times \mathbf{u} \in \mathbb{C}^{1 \times 1}$ . This thesis will use the usual identification of  $\mathbb{C}$  with  $\mathbb{C}^{1 \times 1}$ . A column vector  $\mathbf{u}$  is called a *unit vector* when  $\mathbf{u}^* \times \mathbf{u} = 1$ .

**Definition 1.1.6** (Trace). The trace,  $\text{Tr}(A)$  of a square matrix  $A = [a_{ij}]$  is  $\sum a_{ii}$ .

Tensor product

The tensor product of two matrices is the usual Kronecker product:

$$\mathbf{U} \otimes \mathbf{V} = \begin{bmatrix} u_{11}V & u_{12}V & \cdots & u_{1m}V \\ u_{21}V & u_{22}V & \cdots & u_{2m}V \\ \vdots & \vdots & \ddots & \\ u_{n1}V & u_{n2}V & \cdots & u_{nm}V \end{bmatrix} = \begin{bmatrix} u_{11}v_{11} & \cdots & u_{12}v_{11} & \cdots & u_{1m}v_{1q} \\ u_{11}v_{21} & \cdots & u_{12}v_{21} & \cdots & u_{1m}v_{2q} \\ \vdots & \vdots & \vdots & \ddots & \\ u_{n1}v_{p1} & \cdots & u_{n2}v_{p1} & \cdots & u_{nm}v_{pq} \end{bmatrix}$$

Special matrices

When working with quantum values certain types of matrices over the complex numbers are of special interest. These are:

**Unitary Matrix** : Any  $n \times n$  matrix  $A$  with  $AA^* = I$  ( $= A^*A$ ).

**Hermitian Matrix** : Any  $n \times n$  matrix  $A$  with  $A = A^*$ .

**Positive Matrix** : Any Hermitian matrix  $A$  in  $\mathbb{C}^{n \times n}$  where  $\mathbf{u}^*A\mathbf{u} \geq 0$  for all vectors  $\mathbf{u} \in \mathbb{C}^n$ . Note that for any Hermitian matrix  $A$  and vector  $\mathbf{u}$ ,  $\mathbf{u}^*A\mathbf{u}$  is real.

**Completely Positive Matrix** : Any positive matrix  $A$  in  $\mathbb{C}^{n \times n}$  where  $I_m \otimes A$  is positive.

The matrix

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

is an example of a matrix that is *unitary*, *Hermitian*, *positive* and *completely positive*.

Superoperators

A *Superoperator*  $S$  is a matrix over  $\mathbb{C}$  with the following restrictions:

1.  $S$  is *completely positive*. This implies that  $S$  is positive as well.
2. For all positive matrices  $A$ ,  $\text{Tr}(S A) \leq \text{Tr}(A)$ .

## 1.2 Basic quantum computation

### 1.2.1 Quantum bits

Quantum computation deals with operations on **qubits**. A **qubit** is typically represented in the literature on quantum computation as a complex linear combination of  $|0\rangle$  and  $|1\rangle$ , respectively identified with  $(1,0)$  and  $(0,1)$  in  $\mathbb{C}^2$ . Because of the identification of the basis vectors, any **qubit** can be identified with a non-zero vector in  $\mathbb{C}^2$ . In standard quantum computation, the important piece of information in a **qubit** is its direction rather than amplitude. In other words, given  $q = \alpha |0\rangle + \beta |1\rangle$  and  $q' = \alpha' |0\rangle + \beta' |1\rangle$  where  $\alpha = \gamma \alpha'$  and  $\beta = \gamma \beta'$ , then  $q$  and  $q'$  represent the same quantum state.

A **qubit** that has either  $\alpha$  or  $\beta$  zero is said to be in a *classical state*. Any other combination of values is said to be a *superposition*.

Section 1.3 on page 8 will introduce quantum circuits which act on **qubits**. This section will have some forward references to circuits to illustrate points introduced here.

### 1.2.2 Quantum entanglement

Consider what happens when working with a pair of **qubits**,  $p$  and  $q$ . This can be considered as the a vector in  $\mathbb{C}^4$  and written as

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle. \quad (1.1)$$

In the case where  $p$  and  $q$  are two independent **qubits**, with  $p = \alpha |0\rangle + \beta |1\rangle$  and  $q = \gamma |0\rangle + \delta |1\rangle$ ,

$$p \otimes q = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle \quad (1.2)$$

where  $p \otimes q$  is the standard tensor product of  $p$  and  $q$  regarded as vectors. There are states of two **qubits** that cannot be written as a tensor product. As an example, the state

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \quad (1.3)$$

is not a tensor product of two distinct **qubits**. In this case the two **qubits** are said to be *entangled*.

### 1.2.3 Quantum gates

*Quantum gates* operate on **qubits**. These gates are conceptually similar to logic gates in the classical world. In the classical world the only non-trivial single **bit** gate is the Not gate which sends 0 to 1 and 1 to 0. However, there are infinitely many non-trivial quantum gates.

An  $n$ —**qubit** quantum gate is represented by a  $2^n \times 2^n$  matrix. A necessary and sufficient condition for such a matrix to be a quantum gate is that it is *unitary*.

The entanglement of two **qubits**,  $p$  and  $q$ , is accomplished by applying a Hadamard transformation to  $p$  followed by a Not applied to  $q$  controlled by  $p$ . The circuit in figure 1.2 on page 9 shows how to entangle two **qubits** that start with an initial state of  $|00\rangle$ . See ?? on page ?? for how this can be done in L-QPL.

A list of some common gates, together with their usual quantum circuit representation is given in the next section in table 1.1 on page 10.

#### 1.2.4 Measurement

The other allowed operation on a **qubit** or group of **qubits** is measurement. When a **qubit** is measured it assumes only one of two possible values, either  $|0\rangle$  or  $|1\rangle$ . Given

$$q = \alpha |0\rangle + \beta |1\rangle \quad (1.4)$$

where  $|\alpha|^2 + |\beta|^2 = 1$ , then measuring  $q$  will result in  $|0\rangle$  with probability  $|\alpha|^2$  and  $|1\rangle$  with probability  $|\beta|^2$ . Once a **qubit** is measured, re-measuring will always produce the same value.

In multi-**qubit** systems the order of measurement does not matter. If  $p$  and  $q$  are as in equation (1.1) on the preceding page, let us suppose measuring  $p$  gives  $|0\rangle$ . The measure will result in that value with probability  $|\alpha_{00}|^2 + |\alpha_{01}|^2$ , after which the system collapses to the state:

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle \quad (1.5)$$

Measuring the second **qubit**,  $q$ , will give  $|0\rangle$  with probability  $|\alpha_{00}|^2$  or  $|1\rangle$  with probability  $|\alpha_{01}|^2$ .

Conversely, if  $q$  was measured first and gave us  $|0\rangle$  (with a probability of  $|\alpha_{00}|^2 + |\alpha_{10}|^2$ ) and then  $p$  was measured,  $p$  will give us  $|0\rangle$  with probability  $|\alpha_{00}|^2$  or  $|1\rangle$  with probability  $|\alpha_{10}|^2$ .

Thus, when measuring both  $p$  and  $q$ , the probability of getting  $|0\rangle$  from both measures is  $|\alpha_{00}|^2$ , regardless of which **qubit** is measured first.

Considering states such as in equation (1.3), measuring either **qubit** would actually force the other **qubit** to the same value. This type of entanglement is used in many quantum algorithms such as quantum teleportation.

### 1.2.5 Mixed states

The notion of *mixed states* refers to an outside observer's knowledge of the state of a quantum system. Consider a 1 **qubit** system

$$\nu = \alpha |0\rangle + \beta |1\rangle. \quad (1.6)$$

If  $\nu$  is measured but the results of the measurement are not examined, the state of the system is either  $|0\rangle$  or  $|1\rangle$  and is no longer in a superposition. This type of state is written as:

$$\nu = |\alpha|^2 \{|0\rangle\} + |\beta|^2 \{|1\rangle\}. \quad (1.7)$$

An external (to the state) observer knows that the state of  $\nu$  is as expressed in equation (1.7). Since the results of the measurement were not examined, the exact state (0 or 1) is unknown. Instead, a probability is assigned as expressed in the equation. Thus, if the **qubit**  $\nu$  is measured and the results are not examined,  $\nu$  can be treated as a probabilistic **bit** rather than a **qubit**.

### 1.2.6 Density matrix notation

The state of any quantum system of **qubits** may be represented via a *density matrix*. In this notation, given a **qubit**  $\nu$ , the coefficients of  $|0\rangle$  and  $|1\rangle$  form a column vector  $u$ . Then the density matrix corresponding to  $\nu$  is  $uu^*$ . If  $\nu = \alpha |0\rangle + \beta |1\rangle$ ,

$$\nu = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\bar{\alpha} \quad \bar{\beta}) = \begin{pmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{pmatrix}. \quad (1.8)$$

When working with mixed states the density matrix of each component of the mixed state is added. For example, the mixed state shown in equation (1.7) would be represented by the density matrix

$$|\alpha|^2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + |\beta|^2 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}. \quad (1.9)$$

Note that since the density matrix of mixed states is a linear combination of other density matrices, it is possible to have two different mixed states represented by the same density matrix.

The advantage of this notation is that it becomes much more compact for mixed state systems. Additionally, scaling issues are handled by insisting the density matrix has a trace = 1. During a general quantum computation, as we shall see, the trace can actually fall below 1 indicating that the computation is not everywhere total.

### Gates and density matrices

When considering a **qubit**  $q$  as a column vector and a unitary transform  $T$  as a matrix, the result of applying the transform  $T$  to  $q$  is the new vector  $Tq$ . The density matrix of the original **qubit** is given by  $q q^*$ , while the density matrix of the transformed **qubit** is  $(Tq)(Tq)^*$ , which equals  $T(qq^*)T^*$ . Thus, when a **qubit**  $q$  is represented by a density matrix  $A$ , the formula for applying the transform  $T$  to  $q$  is  $TAT^*$ .

## 1.3 Quantum circuits

### 1.3.1 Contents of quantum circuits

Currently a majority of quantum algorithms are defined and documented using *quantum circuits*. These are wire-type diagrams with a series of **qubits** input on the left of the diagram and output on the right. Various graphical elements are used to describe quantum gates, measurement, control and classical **bits**.

### Gates and **qubits**

The simplest circuit is a single wire with no action:

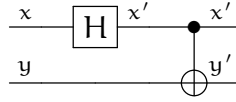
$$\text{---} \times \text{---}$$



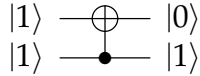
The next simplest circuit is one **qubit** and one gate. The **qubit** is represented by a single wire, while the gate is represented by a box with its name,  $G$ , inside it. This is shown in the circuit in figure 1.1. In general, the name of the wire which is input to the gate  $G$  may be different from the name of  $G$ 's output wire. Circuit diagrams may also contain constant components as input to gates as in the circuit in figure 1.3.



**Figure 1.1:** Simple single gate circuit



**Figure 1.2:** Entangling two **qubits**.


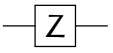
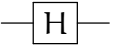





**Figure 1.3:** Controlled-Not of  $|1\rangle$  and  $|1\rangle$

Future diagrams will drop the wire labels except when they are important to the concept under discussion.

Controlled gates, where the gate action depends upon another **qubit**, are shown by attaching a wire between the wire of the control **qubit** and the controlled gate. The circuit in figure 1.2 shows two **qubits**, where a Hadamard is applied to the top **qubit**, followed by a controlled-Not applied to the second **qubit**. In circuits, the control **qubit** is on the vertical wire with the solid dot. This is then connected via a horizontal wire to the gate being controlled.

A list of common gates, their circuits and corresponding matrices is given in table 1.1 on the following page.

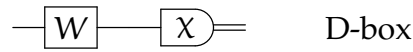
| Gate           | Circuit   | Matrix   |
|----------------|---|--|
| Not (X)        |    | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$   |
| Z              |    | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$  |
| Hadamard       |    | $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$   |
| Swap           |    | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$   |
| Controlled-Not |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$   |
| Toffoli        |  | $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ |

**Table 1.1:** Gates, circuit notation and matrices

## Measurement

Measurement is used to transform the quantum data to classical data so that it may be then used in classical computing (e.g. for output). The act of measurement is placed at the last part of the quantum algorithm in many circuit diagrams and is sometimes just implicitly considered to be there.

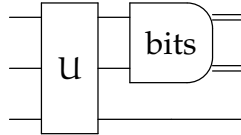
While there are multiple notations used for measurement in quantum circuit diagrams, this thesis will standardize on the *D-box* style of measurement as shown in figure 1.4.



**Figure 1.4:** Measure notation in quantum circuits

A measurement may have a double line leaving it, signifying a **bit**, or nothing, signifying a destructive measurement.

Operations affecting multiple **qubits** at the same time are shown by extending the gate or measure box to encompass all desired wires. In the circuit in figure 1.5, the gate  $U$  applies to all of the first three **qubits** and the measurement applies to the first two **qubits**.



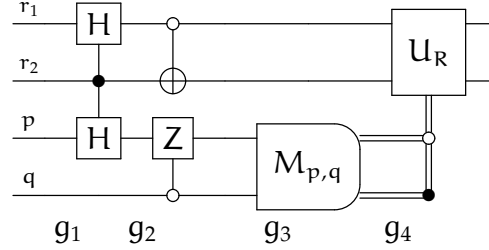
**Figure 1.5:** Examples of multi-**qubit** gates and measures

## 0-control and control by **bits**

The examples above have only shown control based upon a **qubit** being  $|1\rangle$ . Circuits also allow control on a **qubit** being  $|0\rangle$  and upon classical values. The circuit in figure 1.6 on the following page with four **qubits** ( $r_1$ ,  $r_2$ ,  $p$  and  $q$ ) illustrates all these forms of control.

At  $g_1$ , a Hadamard is 1-controlled by  $r_2$  and is applied to each of  $r_1$  and  $p$ . This is followed in column  $g_2$  with the Not transform applied to  $r_2$  being 0-controlled by  $r_1$ .

In the same column, a Z gate is 0-controlled by q and applied to p. p and q are then measured in column  $g_3$  and their corresponding classical values are used for control in  $g_4$ . In  $g_4$ , the  $U_R$  gate is applied to both  $r_1$  and  $r_2$ , but only when the measure result of p is 0 and the measure result of q is 1.



**Figure 1.6:** Other forms of control for gates

### Multi-qubit lines

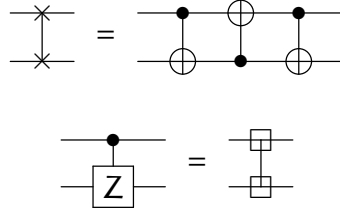
It is common to represent multiple **qubits** on one line. A gate applied to a multi-qubit line must be a tensor product of gates of the correct dimensions. The circuit in figure 1.7 shows  $n$  **qubits** on one line with the Hadamard gate (tensored with itself  $n$  times) applied to all of them. That is followed by a unary gate  $U_R$  tensored with  $I^{\otimes(n-2)}$  and tensored with itself again. This will have the effect of applying an  $U_R$  gate to the first and last **qubits** on the line.



**Figure 1.7:**  $n$  **qubits** on one line

### Other common circuit symbols

Two other symbols that are regularly used are the swap and controlled- $\mathbb{Z}$ , shown in the circuit in figure 1.8 on the following page. Note that swap is just shorthand for a series of three controlled-Not gates with the control **qubit** changing. This can also be seen directly by multiplying the matrices for the controlled-Not gates as shown in equation (1.10) on the next page.



**Figure 1.8:** Swap and controlled-Z

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (1.10)$$

### 1.3.2 Syntax of quantum circuits

Quantum circuits were originally introduced by David Deutsch in [1]. He extended the idea of standard classical based gate diagrams to encompass the quantum cases. In his paper, he introduced the concepts of quantum gates, sources of **bits**, sinks and universal gates. One interesting point of the original definition is that it *does* allow loops. Currently, the general practice is not to allow loops of **qubits**. The commonly used elements of a circuit are summarized in table 1.2 on the following page.

A valid quantum circuit must follow certain restrictions. As physics requires **qubits** must not be duplicated, circuits must enforce this rule. Therefore, three restrictions in circuits are the *no fan-out*, *no fan-in* and *no loops* rules. These conditions are a way to express the *linearity* of quantum algorithms. Variables (wires) may not be duplicated, may not be destroyed without a specific operation and may not be amalgamated.

### 1.3.3 Examples of quantum circuits

This section will present three quantum algorithms and the associated circuits. Each of these circuits presented may be found in [2].

| Desired element               | Element in a quantum circuit diagram.  | Example |
|-------------------------------|--|---------|
| <b>qubit</b>                  | A single horizontal line.  | —       |
| Classical <b>bit</b>          | A double horizontal line.  | ==      |
| Single- <b>qubit</b> gates    | A box with the gate name (G) inside it, one wire attached on its left and one wire attached on the right.  |         |
| Multi- <b>qubit</b> gates     | A box with the gate name (R) inside it, n wires on the left side and the same number of wires on the right.  |         |
| Controlled <b>qubit</b> gates | A box with the gate name (H, W) inside, with a solid (1-control) or open (0-control) dot on the control wire with a vertical wire between the dot and the second gate.   |         |
| Controlled-Not gates          | A <i>target</i> $\oplus$ , with a solid (1-control) or open (0-control) dot on the control wire with a vertical wire between the dot and the gate.   |         |
| Measurement                   | A <i>D-box</i> shaped node with optional names or comments inside. One to n single wires are attached on the left ( <b>qubits</b> coming in) and 0 to n classical <b>bit</b> wires on the left. Classical <b>bits</b> may be dropped as desired. |         |
| Classical control             | Control bullets attached to horizontal classical wires, with vertical classical wires attached to the controlled gate.   |         |
| Multiple <b>qubits</b>        | Annotate the line with the number of <b>qubits</b> and use tensors on gates.   |         |

**Table 1.2:** Syntactic elements of quantum circuit diagrams

First, *quantum teleportation*, an algorithm which sends a quantum bit across a distance via the exchange of two classical bits. This is followed by the *Deutsch-Jozsa algorithm*, which provides information about the global nature of a function with less work than a classical deterministic algorithm can. The third example is circuits for the *quantum Fourier transformation* and its inverse.

## Quantum teleportation

The standard presentation of this algorithm involves two participants A and B. (Henceforth known as Alice and Bob). Alice and Bob first initialize two **qubits** to  $|00\rangle$ , then place them into what is known as an *EPR* (for Einstein, Podolsky and Rosen) state. This is accomplished by first applying the Hadamard gate to Alice's **qubit**, followed by a controlled-Not to the pair of **qubits** controlled by Alice's **qubit**.

Then, Bob travels somewhere distant from Alice, taking his **qubit** with him<sup>1</sup>.

At this point, Alice receives a **qubit**,  $v$ , in an unknown state and has to pass  $v$  on to Bob. She then uses  $v$  as the control and applies a controlled-Not transform to this new pair. Alice then applies a Hadamard transform applied to  $v$ .

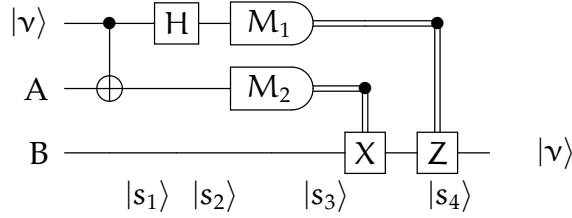
Alice now measures the two **qubits** and sends the resulting two **bits** of classical information to Bob.

Bob then examines the two **bits** that he receives from Alice. If the **bit** resulting from measuring Alice's original bit is 1, he applies the Not (also referred to as X) gate ( $= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ) to his **qubit**. If the measurement result of  $v$  is one, he applies the Z gate ( $= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ ). Bob's **qubit** is now in the same state as the **qubit** Alice wanted to send. The circuit for this is shown in figure 1.9 on the next page.

For comparison, see ?? on page ?? showing how this would be implemented in L-QPL.

---

<sup>1</sup>Notice that all other physical constraints are ignored in this algorithm. There is no concern about how one separates the **qubits**, transports the **qubit** or potential decoherence of the **qubits**.



**Figure 1.9:** Quantum teleportation

### Deutsch-Jozsa algorithm

The Deutsch-Jozsa algorithm describes a way of determining whether a function  $f^2$  is *constant* (i.e. always 0 or 1) or *balanced* (i.e. produces an equal number of 0 or 1 results) based on applying it to one quantum bit. The function takes  $n$  **bits** as input and produces a single **bit**.

$f$  is assumed to be an expensive function, therefore, a desired effect is to evaluate  $f$  as few times as possible before determining if  $f$  is balanced or constant. The worst case scenario when evaluating  $f$  classically is that determining the result requires  $2^{n-1} + 1$  invocations of the function. The best possible case is 2 invocations, which occurs when  $f$  is balanced and the first two inputs chosen produce different results.

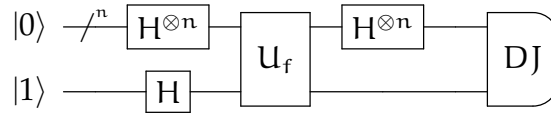
The quantum circuit requires only one application of the function to  $n+1$  **qubits** which have been suitably prepared to make the decision.

The algorithm relies on being able to construct an  $n + 1$  order unitary operator based upon  $f$ . In general, a unitary operator like this may be constructed by mapping the state  $|a, b\rangle$  to  $|a, b \oplus f(a)\rangle$  where  $\oplus$  is the exclusive-or operator and  $a$  is  $n$  **bit** values. If we name this operator  $U_f$ , the circuit in figure 1.10 on the next page will solve the problem with just one application. See the appendix, ?? on page ?? for how this would be done in L-QPL.

The idea of quantum parallelism is what makes this and many other quantum algorithms work. The initial state of the system is set to  $|0^{\otimes n} \otimes 1\rangle$  after which the Hadamard

<sup>2</sup>The obvious pre-condition for the Deutsch-Jozsa algorithm is that the function  $f$  is *either* balanced or constant and not some general function. The results are not well-defined if  $f$  does not fit into one of the two possible categories.





**Figure 1.10:** Circuit for the Deutsch-Jozsa algorithm

gate is applied to all of the **qubits**. This places the input **qubits** into a superposition of all possible input values and the answer **qubit** is a superposition of 0 and 1. At this point, the unitary transformation  $U_f$  is applied to the **qubits**. Then the Hadamard transform is applied again to the input **qubits**.

To complete the algorithm, measure *all* the **qubits**. It can be shown that if  $f$  is constant, the input **qubits** will all measure to 0, while if it is balanced, at least one of those **qubits** will be 1.

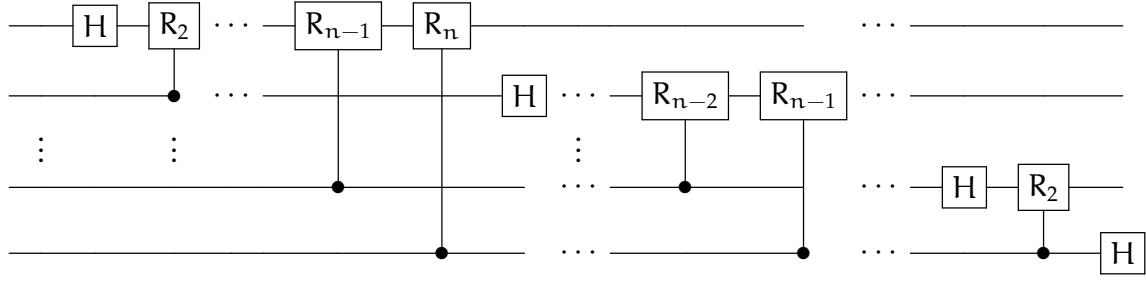
### Quantum Fourier transform

The circuits for the quantum Fourier transformation and its inverse are in figure 1.11 and figure 1.12 respectively. These transforms are used extensively in many quantum algorithms, including Shor's factoring algorithm.

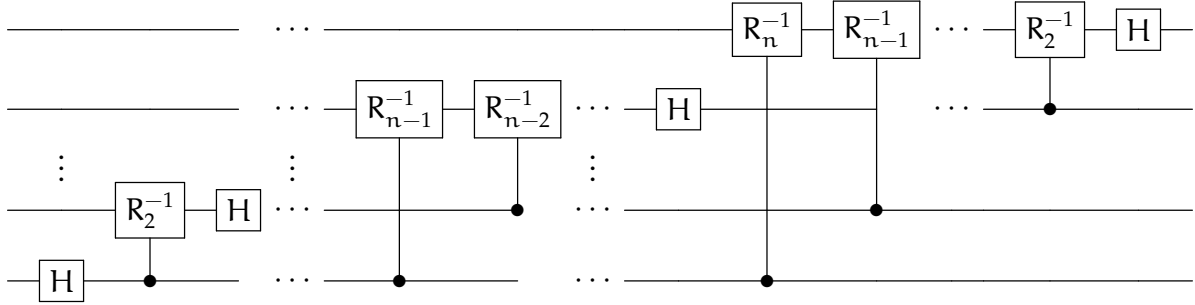
The quantum Fourier transform is definable on an arbitrary number of **qubits**. This is typically presented by eliding the 3<sup>rd</sup> to the  $n - 3^{\text{rd}}$  lines and interior processing. The L-QPL code for the quantum Fourier transform is in the appendix, ?? on page ?. In this circuit, the parametrized transform  $R_n$  is the rotation transform, given by:

$$R_n = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{bmatrix}$$

The inverse of a circuit is determined by traversing the circuit from right to left. This process changes the original quantum Fourier circuit to its inverse as shown in figure 1.12 on the following page. The L-QPL code for the inverse quantum Fourier transform is in the appendix, ?? to ?? on page ?.



**Figure 1.11:** Circuit for the quantum Fourier transform



**Figure 1.12:** Circuit for the inverse quantum Fourier transform

## 1.4 Extensions to quantum circuits

To facilitate the transition to the programming language L-QPL, this section introduces three extensions to quantum circuits. The extensions are *renaming*, *wire bending* and *crossing*, and *scoped control*. Each extension adds expressive power to quantum circuits but does not change the semantic power. For each of the extensions, examples of how to re-write the extension in standard quantum circuit terminology will be provided.

### 1.4.1 Renaming

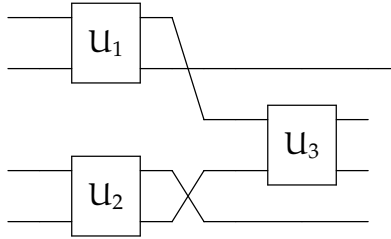
Quantum circuits currently allow renaming to be an implicit part of any gate. The circuit in figure 1.13 gives an operation to explicitly do this and its rewriting in standard circuit notation.

$$\text{y} \text{---} \boxed{x := y} \text{---} x \equiv \text{y} \text{---} \boxed{I} \text{---} x$$

**Figure 1.13:** Renaming of a **qubit** and its equivalent diagram

### 1.4.2 Wire crossing

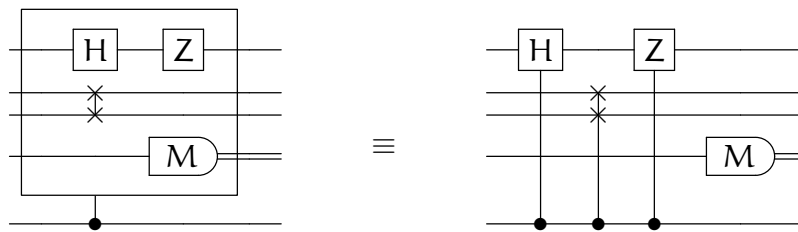
Crossing and bending of wires in a circuit diagram is added to allow a simpler presentation of algorithms. The circuit in figure 1.14 illustrates the concept of re-organizing and bending of wires.



**Figure 1.14:** Bending

### 1.4.3 Scoped control

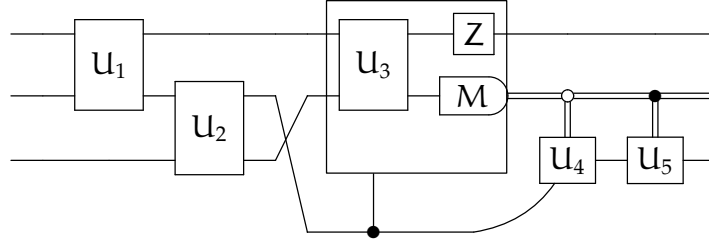
This extension allows us to group different operations in a circuit and show that all of them are controlled by a particular **qubit**. This is the same as attaching separate control wires to each of the gates in the grouped operations. Measurements are not affected by control. Figure 1.15 shows a scoped control box on the left which includes a measure. The right hand side of the same figure shows the circuit translated back to standard circuit notation, with the measure not being affected by the control.



**Figure 1.15:** Scope of control

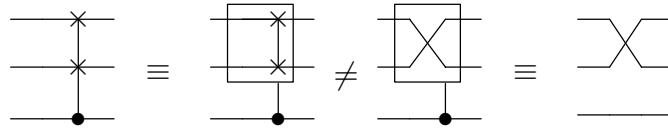
Scoping boxes correspond to procedures and blocks in L-QPL.

Naturally, both scoping and bending may be combined as in figure 1.16.



**Figure 1.16:** Extensions sample

However, note that exchanging wires is not the same as swap. Exchanging a pair of wires is not affected by control, but a swap is affected by control, as shown in figure 1.17.

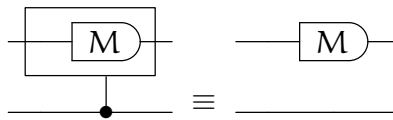


**Figure 1.17:** Swap in control vs. exchange in control

#### 1.4.4 Circuit identities

Circuits allow the writing of the same algorithm in multiple ways. This sub-section will list some of the circuit identities that hold with the extended notation.

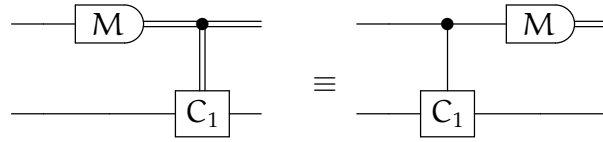
First, note that although a measure may appear inside a control box, it is not affected by the control, as in figure 1.18. Conversely, a measurement commutes with control of a circuit as in figure 1.18.



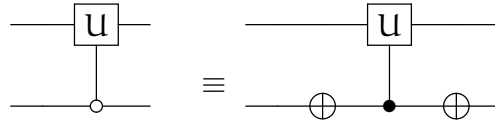
**Figure 1.18:** Measure is not affected by control

One of the notations introduced earlier was that of *0-control*. This type of control is the same as applying a Not transform before and after a *1-control*, as shown in figure 1.20 on the following page.

Figure 1.21 on the next page shows that scoped control of multiple transforms is the same as controlling those transforms individually. Figure 1.22 similarly shows that



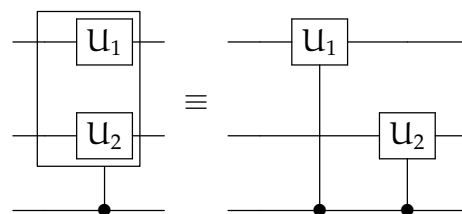
**Figure 1.19:** Control is not affected by measure



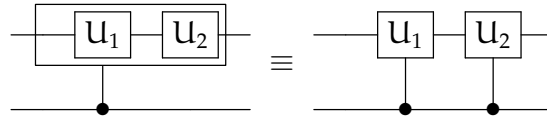
**Figure 1.20:** Zero control is syntactic sugar

scoped control of multiple transforms of the same **qubit** is the same as controlling those transforms serially.

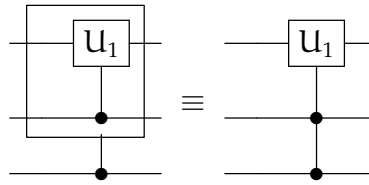
Multiple control commutes with scoping as shown in figure 1.23 to figure 1.24 on the following page.



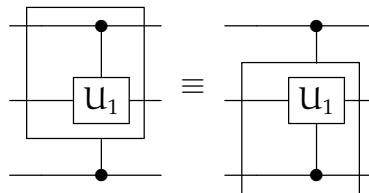
**Figure 1.21:** Scoped control is parallel control



**Figure 1.22:** Scoped control is serial control



**Figure 1.23:** Multiple control



**Figure 1.24:** Control scopes commute

# Chapter 2

## Transformations of Quantum Programs

### 2.1 Terminology

#### 2.1.1 Basic Types

Throughout this note, the types **bit** and **qubit** will be taken as given. These are intended to correspond to the classical notions of “bit” (i.e., 0 or 1) and “qubit” (i.e.,  $\alpha|0\rangle + \beta|1\rangle$ ).

**Definition 2.1.1.** *An **Endpoint** is either **bit** or **qubit**.*

**Definition 2.1.2.** *An **Arity** is a partial map from  $W \subset \mathcal{N}$  to **Endpoint**.*

**Definition 2.1.3.** *A wire is an element of  $W \subset \mathcal{N}$ . A typed wire is a wire together with a specified **Arity**.*

**Definition 2.1.4.** *A control wire is a pair  $(w, b)$  where  $w$  is a typed wire and  $b :: \mathbf{Bool}$ .*

A quantum program uses *typed wires* as its data.

**Definition 2.1.5.** *A gate is a function from  $W_1$ , a set of typed wires, to  $W_2$ , another set of typed wires. The gate function must be a superoperator as defined in [3].*

#### 2.1.2 Types and Shapes

Although circuits, gates and low level subroutines are defined at the level of wires, programmatically, we would like to refer to groupings of wires. For example, a list of **qubit** or a register (tuple) of **qubit**. These groupings may have a required leaf type (e.g., **qubit** or **bit**) or it may be considered polymorphic. Additionally, the leaf type may be mixed or homogenous.

**TODO:** Read and work on definitions of shapes and QCData

**Definition 2.1.6.** The singleton type **B** is defined as having the instance  $B_{()}$  and the singleton type **Q** is defined as having the singleton instance  $Q_{()}$ .

**Definition 2.1.7.** The type family **QCData** consists of algebraic data types built up from **bit** or **qubit**.

Examples of **QCData** include (**bit**, **qubit**, [**qubit**]) and **bit**.

**Definition 2.1.8.** Given an instance  $I$  of a type **T** in **QCData**, the shape of  $I$  is the instance  $I_s$  obtained from  $I$  by replacing all terms of type **bit** by  $B_{()}$  and all terms of type **qubit** by  $Q_{()}$ .

For example, a 2 element list of **qubit** has shape  $[Q_{()}, Q_{()}]$  while a pair of a **qubit** and **bit** has shape  $(Q_{()}, B_{()})$

The concepts of shape and the type **QCData** allow us to group the wires of a quantum circuit into higher order types.

## 2.2 Subroutines

In the following, we will assume *gate* as above is a given and that  $W \subset \mathcal{N}$  is fixed and finite. We will use typing notation to show membership in  $W$  —  $w \in W$  is equivalent to  $w :: W$ .

### 2.2.1 Definition of a Subroutine

The concept of *subroutine* as defined below is intended to capture the essence of a describable computation in a quantum language. The low level subroutine is considered in isolation, meaning that it contains no information regarding how it fits into a larger circuit.

**Definition 2.2.1.** A bare subroutine is defined as a list of gates, written as  $[g_0, g_1, \dots, g_n]$ . The list of gates must satisfy the following:



- $\text{range } g_i = \text{dom } g_{i+1}$  for  $i \in \{0, 1, \dots, n-1\}$ .

A bare subroutine  $B$  can then be viewed as a function from  $\text{dom } g_0$  to  $\text{range } g_n$  by applying each gate in order to  $\text{dom } g_0$ .

**Definition 2.2.2.** A low level subroutine is a bare subroutine with a triple  $(C, I, O)$  where each of  $C, I, O$  are of type **Arity** and

$$\text{dom } C \cap \text{dom } I = \phi \quad (2.1)$$

$$\text{dom } C \cap \text{dom } O = \phi \quad (2.2)$$

In the definition of the low level subroutine, the triple  $(C, I, O)$  describes the inputs and outputs of the subroutine.  $C$  describes the control wires, which are inputs and outputs without change,  $I$  the input wires and  $O$  the output wires.

The above data together with three additional flags provides everything we need to know regarding a subroutine:

**Definition 2.2.3.** A subroutine is a low level subroutine together with a tripartite flag  $c$  with values in  $\{N, B, Q\}$ , and two boolean flags,  $r$  and  $n$ .

The three flags describe the ways this subroutine may be used. Each of these flags provide information that the calling quantum program uses to determine the ways the subroutine may be called:

- *Controllable:* When  $c$  is  $B$ , a calling program may make this subroutine the target of one or more *control wires* with type **bit**. When  $c$  is  $Q$ , the control wires may be of type **bit** or **qubit**. When  $c$  is  $N$ , no control wires may be used. Note this is separate from the  $C$  wires of the subroutine, which may be used for internally controlling portions of the subroutine.
- *Reversible:* A calling program may specify the subroutine run normally or reversed.

- *No-controllable*: In the case where this subroutine is part of a preparation / unpreparation in a (prep, transform, unprep) sequence and that sequence is controlled, then the control wires may be ignored for this subroutine.

Noting that the domains of C and I and the domains of C and O do not overlap, we can also provide an ordering of the inputs and outputs for a low level subroutine. This ordering is used for display purposes and has no additional semantic content.

**Definition 2.2.4.** *An ordering of a low level subroutine is a pair of bijections,  $(i, o)$  such that:*

$$i : \text{dom } C \cup \text{dom } I \leftrightarrow \{0, 1, \dots, n - 1\} \quad (2.3)$$

$$o : \text{dom } C \cup \text{dom } O \leftrightarrow \{0, 1, \dots, m - 1\} \quad (2.4)$$

where  $|\text{dom } C \cup \text{dom } I| = n$  and  $|\text{dom } C \cup \text{dom } O| = m$ .

### 2.2.2 Subroutine Calls

In this section, we describe the permissible bindings given two sets of wires, where the first set will be considered as control wires and the second as either input or output wires.

**Definition 2.2.5.** *Given C and K are **Arity** functions over the same set of typed wires  $V$ , then  $f$  is a permissible binding to a set of typed wires  $W$  with **Arity**  $T_w$  when:*

- $f : \text{dom } C + \text{dom } K \rightarrow W$ ,
- $\forall x, y \in \text{dom } f, f(x) = f(y) \implies x = y \vee x, y \in \text{dom } C$ ,
- $x \in \text{dom } C \wedge C(x) = \mathbf{qubit} \implies T_w(f(x)) = \mathbf{bit} \vee T_w(f(x)) = \mathbf{qubit}$ ,
- $x \in \text{dom } C \wedge C(x) = \mathbf{bit} \implies T_w(f(x)) = \mathbf{bit}$ ,
- $x \in \text{dom } K \implies T_w(f(x)) = K(x)$ .

We denote the permissible bindings to  $W$  of  $C$  and  $K$  by  $F(C, K, W)$ .

**Definition 2.2.6.** *In a context of typed wires  $W_1$ , a subroutine call, resulting in the typed wires  $W_2$ , of the subroutine  $([gates], C, I, O, r, c, n)$  is a tuple  $(f, g, h, i, ncf, ctrls)$  consisting of three functions, two boolean flags and a list of control wires. The functions  $f, g, h$  must satisfy:*

- $f : \text{dom } C \rightarrow W_1 \cap W_2$
- $g : \text{dom } I \rightarrow W_1$
- $h : \text{dom } O \rightarrow W_2$
- $f + g \in F(C, I, W_1)$
- $f + h \in F(C, O, W_2)$ .

*The two flags must satisfy:*

- $i \implies r$
- $ncf \implies n$ .

*The control list must satisfy:*

- $\forall w_c \in \text{ctrls}, \text{fst}(w_c) \in W_1 \cap W_2,$
- $N = c \implies \text{length}(\text{ctrls}) = 0,$
- $B = c \implies \forall w_c \in \text{ctrls}, T_1(\text{fst}(w_c)) = \mathbf{bit}.$

### 2.2.3 High Level Structure

Let  $s, t$  be of type of the family **QCData** and  $a$  be of shape  $s$ ,  $b$  be of shape  $t$ . Further, let  $A = \{qt | qt :: a, qt \text{ has shape } s\}$  and  $B = \{qt | qt :: b, qt \text{ has shape } t\}$ , that is,  $A$  and  $B$  are the sets of quantum terms of shape  $s$  (respectively  $t$ ) and type  $a$  (respectively  $b$ ).

**Definition 2.2.7.** *A high level structure for a call to the subroutine  $([gates], C, I, O, r, c, n)$  starting in context  $W_1$  and ending in context  $W_2$  is a pair of maps  $(i_s, o_s)$  with  $i_s : A \rightarrow F(C, I, W_1)$  and  $o_s : F(C, O, W_2) \rightarrow B$ .*

**Definition 2.2.8.** *Given the data for a subroutine call as above in definition 2.2.6, a structured subroutine call is a high level structure as in definition 2.2.7 and a pair of quantum terms  $(a, b)$  such that:*

- $i_s(a) = f + g$  and
- $o_s(f + h) = b$ .

## 2.3 Subroutine Calls and Transformers

We are interested in two transformed calls of subroutines. Iteration and folding. We provide the necessary information for creating either a transformed call or first transforming the subroutine and then doing a standard call as in subsection sub-section 2.2.2.

### 2.3.1 Iteration

Iteration of subroutines means to call the same subroutine within a quantum circuit some positive number of times. Discussion points:

- Can we handle the case of zero iterations? Would this just mean doing a direct mapping of the I to the O in numerical sequence?
- Can we handle the case of negative iterations? This could mean calling the inverse of the subroutine in the case where it is reversible and then iterating.
- Does iteration affect the no-control or other flags?
- The analysis below assumes that “non-linear safety” is an important property to preserve during iteration. If we remove that requirement, iteration becomes more flexible, e.g., the bijections  $c_b$  and  $io_b$  could be replaced with a single bijection  $cio_b : C \cup O \leftrightarrow C \cup I$ . This would allow a **qubit** that was affected by the subroutine on one iteration to be used as the control on the next iteration. (Or is this the simple case that has already been handled?)

**Definition 2.3.1.** *Given a subroutine as in subsection sub-section 2.2.2 on page 26, and a subroutine call  $(f, g, h, i, \text{ncf}, \text{ctrls})$  an iterated call of the subroutine  $S = ([\text{gates}], C, I, O, r, c, n)$  consists of all elements of a subroutine call excepting  $f$  plus another tuple of five elements  $(f_{\text{in}}, f_{\text{out}}, c_b, i_{\text{ob}}, i_{\text{count}})$  where:*

- $f_{\text{in}} : \text{dom } C \rightarrow W_1 \cap W_2$
- $f_{\text{out}} : \text{dom } C \rightarrow W_1 \cap W_2$
- $i_{\text{count}}$  is a positive integer,
- $c_b$  is a bijection (permutation) of  $C$  to  $C$ ,
- $i_{\text{ob}}$  is a bijection between  $I$  and  $O$ .
- $f_{\text{in}} + g \in F(C, I, W_1)$
- $f_{\text{out}} + h \in F(C, O, W_2)$
- The relation  $f_{\text{out}} \circ c_b^{i_{\text{count}}} \circ f_{\text{in}}^{-1}$  is a function.

Note these requirements mean that  $|I| = |O|$ .

**Definition 2.3.2.** *Given the data for an iterated call, a structured iterated call is a high level structure as in definition 2.2.7 and a pair of quantum terms  $(a, b)$  such that:*

- $i_s(a) = f_{\text{in}} + g$  and
- $o_s(f_{\text{out}} + h) = b$ .

From the definition, note the  $C$  wires may be permuted as desired, but the combination of the  $f_{\text{in}}^{-1}$  and the permutation must leave the wires in a state where  $f_{\text{out}}$  is well-defined. See below for an example. Note the disposition of the wires due to calling the iterated subroutine is given by:

- Control mapping:  $f_{\text{out}} \circ c_b^{i_{\text{count}}} \circ f_{\text{in}}^{-1}$ ,
- In-out mapping:  $h \circ i_{\text{ob}}^{i_{\text{count}}} \circ g^{-1}$ .

**Example 1 (Single call).**

For this example, we will elide the details relating to high level structure, invertability, control wires and the no-control flag.

Suppose  $C = [c_1, c_2, c_3]$ ,  $I = [i_1, i_2]$  and  $O = [o_1, o_2]$ . For the first part of the example, assume we are calling  $S$  from a context of  $W_1 = [w_1, w_2, w_3, w_4]$ , resulting in the same context (i.e.,  $W_1 = W_2$ ). In this case, the call of  $S$  can be given by:

- $f = \{c_1 \mapsto w_1, c_2 \mapsto w_1, c_3 \mapsto w_4\},$
- $g = \{i_1 \mapsto w_2, i_2 \mapsto w_3\}$
- $h = \{o_1 \mapsto w_3, o_2 \mapsto w_2\}$

Hence we are calling  $S$  which will use  $w_1$  as its first two control inputs and  $w_4$  as the third. The inputs will use  $w_2$  and  $w_3$ , while the output will “switch” those to  $w_3$  and  $w_2$ .

**Example 2 (Iterated call).**

Assume  $S$  is as above and we are using the call as above. To aid in distinguishing input and output wires of the calling circuit, we will use  $w'$  for naming the output wires, so we may write  $W_1 = [w_1, w_2, w_3, w_4]$  and  $W_2 = [w'_1, w'_2, w'_3, w'_4]$ , noting that  $w_i = w'_i$  for  $i \in \{1, 2, 3, 4\}$ . A call iterated 5 times of  $S$  is  $(g, h, i, ncf, ctrl_s)$  plus the tuple  $(f_{in}, f_{out}, c_b, io_b, 5)$  where

- $f_{in} = \{c_1 \mapsto w_1, c_2 \mapsto w_1, c_3 \mapsto w_4\},$
- $f_{out} = \{c_1 \mapsto w'_4, c_2 \mapsto w'_1, c_3 \mapsto w'_1\},$
- $c_b = (c_1, c_2, c_3),$
- $io_b = \{o_1 \mapsto i_2, o_2 \mapsto i_1\}$

If we calculate the movement of the wires for this iterated call, we see

$$(w_1, w_4) \xrightarrow{f_{in}^{-1}} C = (w_1, w_1, w_4) \xrightarrow{(1,2,3)^5} C = (w_4, w_1, w_1) \xrightarrow{f_{out}} (w'_1(=w_1), w'_4(=w_4)) \quad (2.5)$$

$$(w_2, w_3) \xrightarrow{g^{-1}} I = (w_2, w_3) \xrightarrow{io_b^5 \circ S} O = (w_3, w_2) \xrightarrow{h} (w'_3(=w_3), w'_3(=w_3)) \quad (2.6)$$

In this above example, the choice of  $f_{in}$  and  $f_{out}$  worked correctly with  $c_b$  such that the mappings were well defined. Consider however, if  $f_{out}$  were defined as  $\{c_1 \mapsto w'_1, c_2 \mapsto w'_1, c_3 \mapsto w'_4\}$ . We would then be expected to map / combine  $w_1$  and  $w_4$  into  $w'_1$  and duplicate  $w_1$  into both  $w'_1$  and  $w'_4$ .

### 2.3.2 Iteration transformation of a subroutine

The data required to transform a subroutine is similar to that of an iterated subroutine call.

**Definition 2.3.3.** *The iteration transform of a subroutine is a function  $S_i$  with parameters  $(n, c_p, io_b)$  which takes the subroutine  $(gates, C, I, O, r, c, n)$  to the subroutine  $(gates', C', I', O', r, c, n)$ . The parameters have the following types:*

$n :: \mathbf{Int}, n > 0;$

$c_p :: \mathbf{Perm}_C, \text{Permutations of the elements of } C$

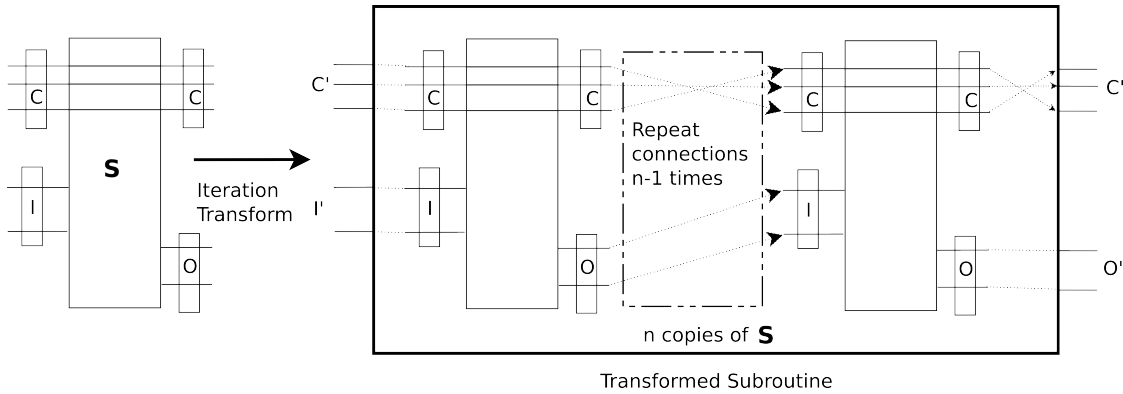
$io_b :: \mathbf{bijection}(I \leftrightarrow O)$

The function  $S_i$  performs the following actions:

- Type checking:
  - Ensure  $c_p$  is a permutation of the appropriate number of wires.
  - Ensure  $n$  is a positive number greater than 0.
  - Ensure  $io_b$  is a bijection between the  $O$  and  $I$  wires.
- Create  $n$  copies of gates.

- Connect the O wires of copy  $i - 1$  to the I wires of copy  $i$ , using the bijection  $io_b$ .
- Apply the permutation  $c_p$  to the C out wires of copy  $i - 1$  and connect to the input C wires of copy  $i$ .
- Apply the permutation  $c_p^k$  to the C out wires of copy  $n$  where  $c_p^{n-1+k} = \text{Id}$ . Connect those wires to the  $C'$  output.
- Connect the  $C'$  input wires to the C input wires of copy 1.
- Connect the  $I'$  wires to the I wires of copy 1.
- Connect the O wires of copy  $n$  to the  $O'$  wires.

The intended effect of this transform may be seen in figure figure 2.1



**Figure 2.1:** Transforming a subroutine to an iterated subroutine

### 2.3.3 Folding subroutines

In addition to the concept of iteration the ability to fold subroutines over data structures could also be useful. A folded call of a subroutine is similar to an iteration, in that controls and possibly some of the inputs and outputs are iterated. The difference occurs in that we expect to take some of the inputs from a data structure and return some of the outputs



to a data structure. An example of this would be folding over a list of **qubits** where each qubit is taken as a input for each iteration.

First, we will examine the requirements for a non-linear safe fold, that is, where no input duplication on the control wires is allow

**Definition 2.3.4.** *Given a subroutine  $S = ([\text{gate}], C, I, O, c, r, n)$ , a starting context of typed wires  $W_1$  and a data structure on wires  $D \subset W_1$ , a linear-only folded call of  $S$  over  $D$  resulting in the context of typed wires  $W_2$  and the data structure  $E \subset W_2$  consists of the tuple  $(CI_f, CO_f, g, h, \text{ciof}_b, s_{\text{in}}, s_{\text{out}})$  where*

- $CI_f :: \mathbf{Arity}, \text{dom } CI_f \subset \text{dom } C \cup \text{dom } I,$
- $CO_f :: \mathbf{Arity}, \text{dom } CO_f \subset \text{dom } C \cup \text{dom } O,$
- $g : \text{dom } C \cup \text{dom } I / \text{dom } CI_f \rightarrow W_1$  and  $g$  is injective,
- $h : \text{dom } C \cup \text{dom } O / \text{dom } CO_f \rightarrow W_2$  and  $h$  is injective
- $\text{ciof}_b$  is a bijection between  $(\text{dom } C \cup \text{dom } O) / \text{dom } CO_f$  and  $(\text{dom } C \cup \text{dom } I) / \text{dom } CI_f,$
- $s_{\text{in}} : \text{dom } CI_f \rightarrow W_1$  (pulls from  $D$ ),
- $s_{\text{out}} : \text{dom } CO_f \rightarrow W_2$  (pushes to  $E$ ),
- $g + s_{\text{in}} \in F(\phi, I, W_1),$
- $\text{ciof}_b^{-1} + s_{\text{in}} \in F(\phi, I, W_1),$
- $\text{ciof}_b + s_{\text{out}} \in F(\phi, O, W_2),$
- $h + s_{\text{out}} \in F(\phi, O, W_2),$
- $|\text{dom } CI_f| = \text{leafsize}(D),$
- $\text{leafsize}(E) = |\text{dom } CO_f|.$

**Definition 2.3.5.** *Given the data for an linear-only folded call, a structured linear-only folded call is a pair of high level structures  $(i_s, o_s)$  and  $(i_{fs}, o_{fs})$  and a pair of quantum terms  $(a, b)$  such that:*

- $i_s(a) = g + s_{in}$ ,
- $o_s(h + s_{out}) = b$ ,
- $i_{fs}(a) = s_{in}$ , *and*
- $o_{fs}(s_{out}) = b$ .

Discussion points:

- Does the structured call get rid of the last two items regarding leafsize?  
Same issue with non-linear safe call.
- For the structured call, it appears to me that there is only one pair of terms  $a, b$  with two different (de)structuring morphisms.

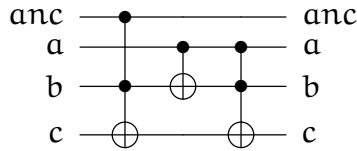
The action on the wires of the calling program will be given by this relation:

$$s_{out} + h \circ (s_{out} + c i o_f + s_{in})^{\text{len}(D)} \circ (g + s_{in})^{-1}.$$

**Example 3 (Fold over Carry).**

For this example, we use the carry portion of the addition algorithm found in [4]. (See Appendix section 2.5 for full diagram.)

The carry circuit is shown below:



The intent of this circuit is to compute the final carry when adding the quregisters  $A$  and  $B$ . The input prepares the  $anc$  in state  $|0\rangle$  and an auxiliary register  $R$ , the same size as  $A$  and  $B$  as  $|00\dots 0\rangle$ . Assume that  $A = [w_1, w_2, w_3]$ ,  $B = [w_4, w_5, w_6]$ ,  $anc = w_7$  and  $R = [w_8, w_9, w_{10}]$ .  $(A, B, R)$ , a tuple of three registers forms our  $D$  — the input to the fold. Then, we may perform a folded call of carry as follows:

- $\text{dom } C = \{\text{anc}, a\}$ ,  $\text{dom } I = \{b, c\} = \text{dom } O$ ;
- $\text{dom } CI_f = \{a, b, c\}$  and  $\text{dom } CO_f = \{\text{anc}, a, b\}$ ;
- $g = \{\text{anc} \mapsto w_6\}$ ,  $h = \{c \mapsto w_{10}\}$
- $\text{ciof}_b = \{c \mapsto \text{anc}\}$
- $s_{\text{in}} = \{a \mapsto D[0], b \mapsto D[1], c \mapsto D[2]\}$
- $s_{\text{out}} = \{\text{anc} \mapsto E[2], a \mapsto E[0], b \mapsto E[1]\}$ .

From the mapping  $s_{\text{out}}$ , we set  $E = (A, B, R')$  where  $R' = [w_7, w_8, w_9]$ .

Discussion points:

- Is there a non-linear safe use case? Carry seemed quite simple, but it required linear safe inputs when folded.
- Each fold iteration input might be multiple **qubits**, combined into a single data structure, as in example 3 on the preceding page.
- The number of inputs and outputs no longer need to agree as they did in iteration. An example would be a subroutine that applied a two **qubit** gate and then discarded one of the **qubits**. The fold would be expected to convert a list of pairs of **qubits** to a list of **qubits**. (Note this subroutine would not be reversible or controllable).
- The shape of the foldable in and out as well as the number of **qubits** at each leaf would need to be known.
- The  $F(C, K, W)$  permissible functions are not quite right for linear-only folds — we do not want to allow duplication of any of the inputs, so  $F(C, K, W)$  becomes  $F(\phi, C + K, W)$ .

**Definition 2.3.6.** Given a subroutine  $S = ([\text{gate}], C, I, O, c, r, n)$ , a starting context of typed wires  $W_1$  and a data structure on wires  $D \subset W_1$ , a folded call of  $S$  over  $D$  resulting in the context of typed wires  $W_2$  and the data structure  $E \subset W_2$  consists of the tuple  $(I_f, O_f, f_{\text{in}}, f_{\text{out}}, g, h, c_b, \text{iof}_b, s_{\text{in}}, s_{\text{out}})$  where

- $I_f :: \mathbf{Arity}, \text{dom } I_f \subset \text{dom } I,$
- $O_f :: \mathbf{Arity}, \text{dom } O_f \subset \text{dom } O,$
- $f_{\text{in}} : \text{dom } C \rightarrow W_1 \cup W_2$
- $f_{\text{out}} : \text{dom } C \rightarrow W_1 \cup W_2$
- $g : \text{dom } I / \text{dom } I_f \rightarrow W_1$
- $h : \text{dom } O / \text{dom } O_f \rightarrow W_2$
- $c_b$  is a bijection (permutation) of  $C,$
- $\text{iof}_b$  is a bijection between  $\text{dom } O / \text{dom } O_f$  and  $\text{dom } I / \text{dom } I_f,$
- $s_{\text{in}} : \text{dom } I_f \rightarrow W_1$  (pulls from  $D$ )
- $s_{\text{out}} : \text{dom } O_f \rightarrow W_2$  (pushes to  $E$ )
- $f_{\text{in}} + g + s_{\text{in}} \in F(C, I, W_1),$
- $f_{\text{out}} + h + s_{\text{out}} \in F(C, O, W_2),$
- $\text{iof}_b + s_{\text{in}} \in F(\phi, I, W_1),$
- $\text{iof}_b + s_{\text{out}} \in F(\phi, O, W_2),$
- $|\text{dom } I_f| = \text{leafsize}(D)$
- $\text{leafsize}(E) = |\text{dom } O_f|$

**Definition 2.3.7.** Given the data for an folded call, a structured folded call is a pair of high level structures  $(i_s, o_s)$  and  $(i_{fs}, o_{fs})$  and a pair of quantum terms  $(a, b)$  such that:

- $i_s(a) = f_{\text{in}} + g + s_{\text{in}},$

- $o_s(f_{out} + h + s_{out}) = b$ ,
- $i_{fs}(a) = s_{in}$ , and
- $o_{fs}(s_{out}) = b$ .

#### 2.3.4 Subroutine to folded subroutine transform

In order to transform a given subroutine, we require the following data:

- A bijection from some subset of the control and output wires to some subset of the control and input wires;
- a count of the number of iterations.

This allows us to derive a new  $C, I, O$  for the fold subroutine. We proceed with the formal definition.

**Definition 2.3.8.** *The fold transform of a subroutine is a function  $S_f$  with parameters  $(n, b_{cio})$  which takes the subroutine  $(gates, C, I, O, r, c, n)$  to the subroutine  $(gates', C', I', O', r, c, n)$ . The parameters have the following types:*

$$n :: \mathbf{Int}, n > 0;$$

$$b_{cio} :: \mathbf{bijection}(CI \leftrightarrow CO)$$

$$\text{where } CI \subseteq C \cup I \text{ and } CO \subseteq C \cup O.$$

Note that  $b_{cio}$  may be defined as a set of ordered pairs

$$\{(f, t) | f \in C \cup I, t \in C \cup O, \text{ and } f, t \text{ appear at most once}\}. \quad (2.7)$$

The data we need to create for the end result are the set of control wires, the input and output wires and the new gates sequence. We proceed with presenting the algorithm for the control wires.

When considering which inputs (and hence outputs) are control wires in the transformed subroutine, we must follow the path of a control input. A control input to the base subroutine will remain a control input to the transformed subroutine only if its full folded path contains only control wires before exiting. Depending upon the structure of  $b_{cio}$  it is possible all, none or some finite subset of specific control wires become controls for the transformed routine.

To determine if a wire is a control, we will calculate a characteristic of the wire and show that it requires at most  $k$  iterations to calculate, where  $k$  is the number of control wires of the original subroutine.

First, define:

$$\Omega :: C \rightarrow C \cup \{*, @\}$$

$$\Omega(c) = \begin{cases} c' & \text{if } b_{cio}(c) = c' \text{ and } c' \in C, \\ * & \text{if } c \text{ is not the first element of any pair in } b_{cio}, \\ @ & \text{if } b_{cio}(c) = j \text{ and } j \in I. \end{cases}$$

Then, noting that  $k = |C|$ , define:

$$\Gamma :: C \rightarrow \mathcal{N} \cup \{\infty\}$$

$$\Gamma(c) = \begin{cases} \infty & \Omega(c) = *, \\ 0 & \Omega(c) = @, \\ 1 + \Gamma(\Omega(c)) & \Gamma(\Omega(c)) < k, \\ \infty & \Gamma(\Omega(c)) \geq k. \end{cases}$$

Dually, we may define functions  $\Theta(c)$  and  $\Delta(c)$ :

$$\begin{aligned}\Theta &:: C \rightarrow C \cup \{*, @\} \\ \Theta(c) &= \begin{cases} c' & \text{if } b_{cio}(c') = c \text{ and } c' \in C, \\ * & \text{if } c \text{ is not the second element of any pair in } b_{cio}, \\ @ & \text{if } b_{cio}(o) = c \text{ and } o \in O. \end{cases} \\ \Delta &:: C \rightarrow \mathcal{N} \cup \{\infty\} \\ \Delta(c) &= \begin{cases} \infty & \Theta(c) = *, \\ 0 & \Theta(c) = @, \\ 1 + \Delta(\Theta(c)) & \Delta(\Theta(c)) < k, \\ \infty & \Delta(\Theta(c)) \geq k. \end{cases}\end{aligned}$$

Note that in the case of cycles among control wires, the cycle *must* be of size  $k$  or less. As such, at most  $k$  iterations of  $\Gamma$  are required before confirming a value for  $\Gamma(c)$ . The same argument applies to computing  $\Theta$ .

Assuming that  $C$  is ordered, the data for  $b_{cio}$  may be stored such that computing  $b_{cio}(c)$  and therefore  $\Omega(c)$  is of  $\mathcal{O}(\log k)$ . Therefore,  $\Gamma$  is of complexity  $\mathcal{O}(k \log k)$  and computing  $\Gamma$  for all of  $C$  will then be of  $\mathcal{O}(k^2 \log k)$ . Computing  $\Delta$  will have the same complexity.

We may now describe the algorithm for determining control wires,  $C'$  input wires,  $I'$  and output wires,  $O'$  of the transformed subroutine. In the algorithm,  $n$  is the number of iterations,  $k$  is the cardinality of  $C$ . Additionally, we compute a *rank* of each  $c$  in  $C'$ . The *rank* of  $c$  is the number of iterations that  $c$  will go through.

1. Add all members of  $I$  to  $I'$ , subscripting with 1.
2. For all  $i \in I$  where  $i \notin \text{range } b_{cio}$ , add  $i_2, i_3, \dots, i_n$  to  $I'$ .

3. Add all members of  $O$  to  $O'$ , subscripting with  $n$ .
4. For all  $o \in O$  where  $o \notin \text{dom } b_{cio}$ , add  $o_1, o_2, \dots, o_{n-1}$  to  $O'$ .
5. Partition  $C$  into four subsets:

$$C_* = \{c | c \notin \text{dom } b_{cio} \text{ and } c \notin \text{range } b_{cio}\},$$

$$C_d = \{c | c \in \text{dom } b_{cio} \text{ and } c \notin \text{range } b_{cio}\},$$

$$C_r = \{c | c \notin \text{dom } b_{cio} \text{ and } c \in \text{range } b_{cio}\},$$

$$C_{dr} = \{c | c \in \text{dom } b_{cio} \text{ and } c \in \text{range } b_{cio}\}.$$

6. For each  $c \in C_*$ , add  $c_1, c_2, \dots, c_n$  to  $C'$ . Set the rank of each of these to 0.
7. For each  $c \in C_d$ , compute  $j = \Gamma(c)$ . If  $j \geq n$ , add  $c_1, c_2, \dots, c_n$  to  $C'$ . If not, then:

- Add  $c_{n-j}, c_{n-j+1}, \dots, c_n$  to  $C'$ , setting the rank of  $c_\ell$  to  $n - \ell$ .
- Add  $c_1, c_2, \dots, c_{n-j-1}$  to  $I'$ .

8. For each  $c \in C_r$ , compute  $m = \Delta(c)$ . If  $m \geq n$ , add  $c_1, c_2, \dots, c_n$  to  $C'$ , setting each item to rank 0. If not, then:

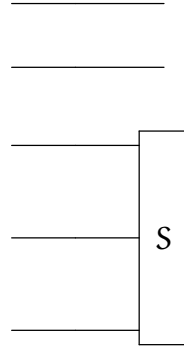
- Add  $c_1, c_2, \dots, c_{j+1}$  to  $C'$ , setting each rank to 0.
- Add  $c_{j+2}, c_{j+3}, \dots, c_n$  to  $I'$ .

9. For each  $c \in C_{dr}$ , compute  $j = \Gamma(c)$ ,  $m = \Delta(c)$ . Then if  $j > n - 1$ , add  $c_1$  to  $C'$ , setting its rank to  $n - 1$ , otherwise add it to  $I'$ . Conversely, if  $m > n - 1$ , add  $c_n$  to  $C'$ , setting its rank to 0, otherwise add it to  $O'$ . In the case where both  $c_1$  and  $c_n$  are added to  $C'$ , we have actually added one too many items to  $C'$  as there will be a duplication. This is addressed in the final step, where the in-out names of the control wires are reconciled.

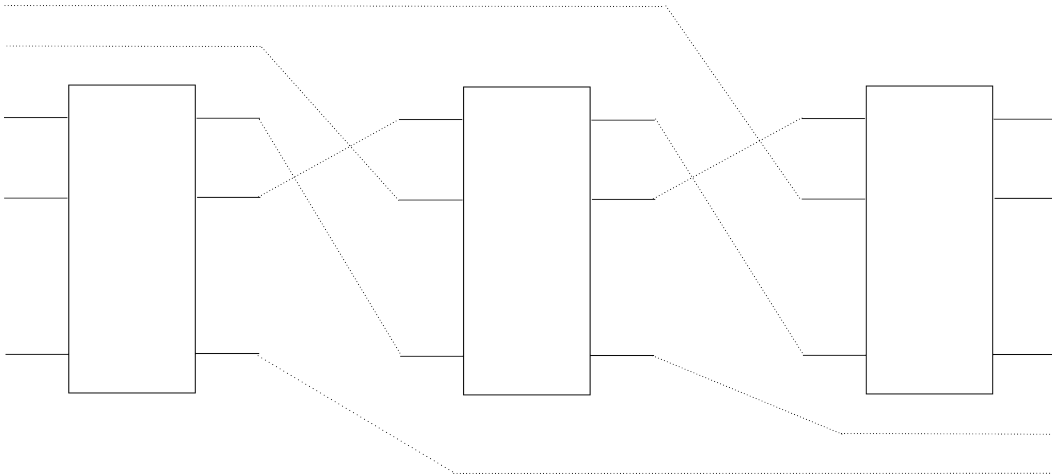


10. Reconcile the  $C'$  names: For each  $c_h \in C'$ , compute  $x = b_{\text{cio}}^{\text{Rank}(c)}(c)$ . In  $C'$ , replace  $x_n$  with  $c_h$ . After completing this computation, remove any duplicates.

### 2.3.5 Examples of folding



**Example 4.** Consider  $S = (\_, \{a, b\}, \{c\}, \{d\}, \_, \_, \_)$  and  $b_{\text{cio}} = \{(a, c), (b, a)\}$  and an iteration count of 3. See figure figure 2.2.



**Figure 2.2:** Fold with extra in/out

From the data, we compute:

$$\Omega(a) = @ \text{ and } \Omega(b) = a,$$

$$\Gamma(a) = 0 \text{ and } \Gamma(b) = 1,$$

$$\Theta(b) = * \text{ and } \Delta(b) = \infty,$$

$$\Theta(a) = b \text{ and } \Delta(a) = \infty.$$

Now, following the steps of the algorithm,

1.  $I' \mapsto \{c_1\}$ .
2. No change to  $I'$ .
3.  $O' \mapsto \{d_3\}$ .
4.  $O' \mapsto \{d_1, d_2, d_3\}$ .
5.  $C_* = \phi, C_d = \{b\}, C_r = \phi, C_{dr} = \{a\}$ .
6. For  $C_d$ , As  $\Gamma(b) = 1$ , we have  $C' \mapsto \{b_2, b_3\}$  and  $I' \mapsto \{c_1, b_1\}$ . The rank of  $b_2$  is 1 and the rank of  $b_3$  is 0.
7. For  $C_{dr} = \{a\}$ ,  $\Gamma(a) = 0$  and  $\Delta(a) = \infty$ , therefore we add  $a_1$  to  $I'$  and  $a_3$  to  $C'$ . The rank of  $a_3$  is zero. At this stage, we now have  $I' = \{c_1, b_1, a_1\}$ ,  $O' = \{d_1, d_2, d_3\}$  and  $C' = \{b_2, b_3, a_3\}$ .
8. Reconcile  $C'$ :  $b_{cio}(b) = a$  and  $b_{cio}(a) = c$ , therefore  $b_{cio}^1(b_2) = a_3$ ,  $b_{cio}^0(b_3) = b_3$ , and  $b_{cio}^0(a_3) = a_3$ . Following our replacement scheme,  $C' = \{b_2, b_3\}$ .

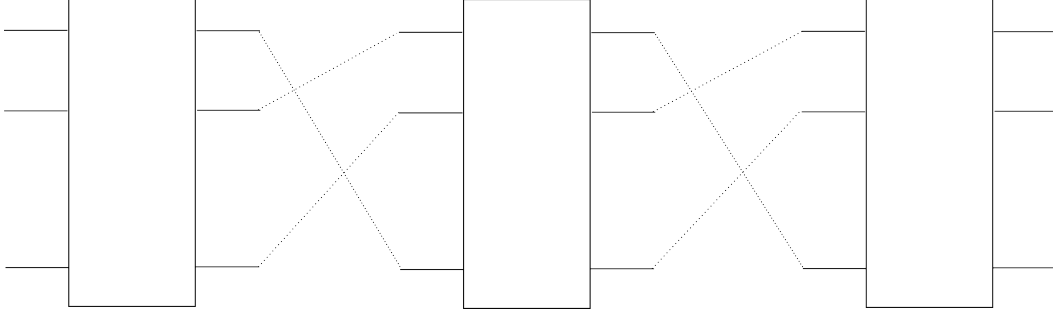
Hence our final result is:

$$I' = \{c_1, b_1, a_1\},$$

$$O' = \{d_1, d_2, d_3\} \text{ and}$$

$$C' = \{b_2, b_3\}.$$

**Example 5.** Consider  $S = (\_, \{a, b\}, \{c\}, \{d\}, \_, \_, \_)$  as in Example 4 and  $b_{cio} = \{(a, c), (b, a), (d, b)\}$  and an iteration count of 3. See figure figure 2.3.



**Figure 2.3:** Fold with three iterations

From the data, we have:

$$\Omega(a) = @ \text{ and}$$

$$\Gamma(a) = 0,$$

$$\Omega(b) = a \text{ and}$$

$$\Gamma(b) = 1,$$

$$\Theta(b) = @ \text{ and}$$

$$\Delta(b) = 0,$$

$$\Theta(a) = b \text{ and}$$

$$\Delta(a) = 1.$$

Now, following the steps of the algorithm,

1.  $I' \mapsto \{c_1\}$ .
2. No change to  $I'$ .
3.  $O' \mapsto \{d_3\}$ .
4. All o are in the range of  $b_{cio}$ , therefore no further change to  $O'$ .
5.  $C_* = C_d = C_r = \phi, C_{dr} = \{a, b\}$ .
6. As  $n - 1 = 2 > \Gamma(a), \Gamma(b)$ , we have  $I' \mapsto \{c_1, a_1, b_1\}$ . Similarly, since  $n - 1 = 2 > \Delta(a), \Delta(b)$ ,  $O' \mapsto \{a_3, b_3, d_3\}$
7. With  $C'$  empty, there are no further steps.

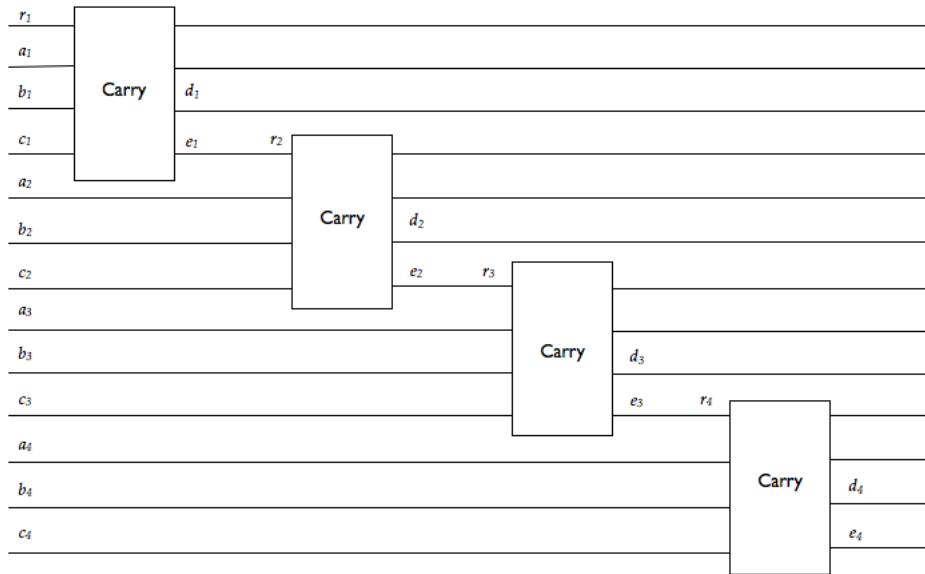
Hence our final result is:

$$I' = \{c_1, b_1, a_1\},$$

$$O' = \{a_3, b_3, d_3\} \text{ and}$$

$$C' = \phi.$$

**Example 6.** Consider  $\text{Carry} = (\_, \{r, a\}, \{b, c\}, \{d, e\}, \_, \_, \_)$ ,  $b_{\text{cio}} = \{(e, r)\}$  and an iteration count of 4. See figure figure 2.4.



**Figure 2.4:** Fold of Carry

From the data, we have:

$$\Omega(r) = *$$

$$\Omega(a) = *,$$

$$\Gamma(r) = \infty$$

$$\Gamma(a) = \infty,$$

$$\Theta(r) = @$$

$$\Delta(r) = 0,$$

$$\Theta(a) = * \text{ and } \Delta(a) = \infty.$$

Now, following the steps of the algorithm,

1.  $I' \mapsto \{b_1, c_1\}$ .
2. No element of  $I$  appears in  $b_{cio}$ , therefore we now have  $I' \mapsto \{b_1, c_1, b_2, c_2, b_3, c_3, b_4, c_4\}$
3.  $O' \mapsto \{d_4, e_4\}$ .
4. Only  $e$  is in the range of  $b_{cio}$ , therefore we add  $d_1, d_2, d_3$  to  $O'$ , giving us  $\{d_1, d_2, d_3, d_4, e_4\}$ .
5.  $C_* = \{a\}$ ,  $C_d = \phi$ ,  $C_r = \{r\}$ ,  $C_{dr} = \phi$ .
6. Considering  $C_*$ , we add  $\{a_1, a_2, a_3, a_4\}$  to  $C'$ , each with rank 0.
7. Next considering  $C_r$ , as  $\Delta(r) = 0$ , we add  $r_1$  to  $C'$  with rank 0 and then add  $r_2, r_3, r_4$  to  $O'$ .
8. As each element of  $C'$  is of rank 0, there is no changes to the names.

Hence our final result is:

$$I' = \{b_1, c_1, b_2, c_2, b_3, c_3, b_4, c_4\},$$

$$O' = \{d_1, d_2, d_3, d_4, e_4, r_2, r_3, r_4\} \text{ and}$$

$$C' = \{r_1, a_1, a_2, a_3, a_4\}.$$

## 2.4 Alternate Algorithm for Fold Transformation

In this section, we present an alternate algorithm for calculating the type and names of control, input and output wires for a folded subroutine. The starting point is Definition 2.3.8 and the ordered pairs of  $b_{cio}$ : A set of ordered pairs  $\{(f, t) | f \in C \cup I, t \in C \cup O\}$ .

To implement the algorithm of calculating the folded subroutines  $C, I$  and  $O$ , we need the following:

- $I \cap O = \phi$ , which may be accomplished by renaming if needed.
- We create the sets  $C_j, I_j, O_j$  for  $j = 1 \dots n$  where the members of  $X_j$  are the elements of  $X$  together with the subscript  $j$  where  $X$  is one of  $C, I, O$ .

The algorithm proceeds by creating a set of “type” constraints for each of the elements of the new sets, based upon  $b_{cio}$  and membership in a  $C, I$  or  $O$  set.

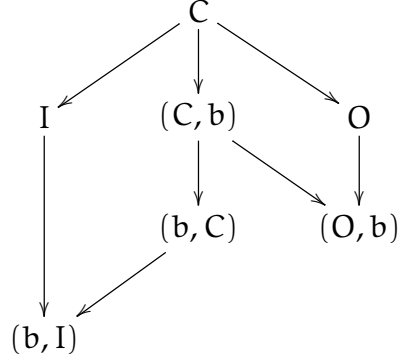
The algorithm steps are:

1. Create a set  $\mathcal{C}$  of pairs  $(a_j, b_{j+1})$  for  $j$  ranging from 0 to  $n - 1$  based upon the bijection  $b_{cio}$ .
2. For each  $j = 0 \dots n - 1$ ,
  - (a) For all  $c \in C_j$ , if  $(c, \_) \notin \mathcal{C}$ , add the pair  $(c, \phi)$
  - (b) For all  $c \in C_j$ , if  $(\_, c) \notin \mathcal{C}$ , add the pair  $(\phi, c)$
  - (c) For all  $o \in O_j$ , if  $(o, \_) \notin \mathcal{C}$ , add the pair  $(o, \phi)$
  - (d) For all  $i \in I_j$ , if  $(\_, i) \notin \mathcal{C}$ , add the pair  $(\phi, i)$
3. Convert the pairs in  $\mathcal{C}$  to equations and constraints as follows for each pair  $(a, b)$ :

$$\begin{aligned}
 \text{(a) } a = \phi &\implies \begin{cases} b :: (b, C) & \text{when } b \in C_j \text{ for some } j, \\ b :: (b, I) & \text{when } b \in I_j \text{ for some } j. \end{cases} \\
 \text{(b) } a \in C_{j-1} &\implies \begin{cases} b = a & \text{when } b \in C_j, \\ b = a, b :: I & \text{when } b \in I_j, \\ a :: (C, a) & \text{when } b = \phi. \end{cases}
 \end{aligned}$$

$$(c) \ a \in O_{j-1} \implies \begin{cases} b = a, b :: O & \text{when } b \in C_j, \\ \text{no equation} & \text{when } b \in I_j, \\ a :: (O, a) & \text{when } b = \phi. \end{cases}$$

4. Solve the equations with the constraints, with the assumption that



For example,

- $a :: O, a :: C$  is solvable with  $a :: O$ ;
- $a = b, b :: (b, C), a :: I$  is solved by  $b, a :: (b, I)$ ;
- $a = b, b = d, a :: (a, C), d :: (C, d)$  is solved by  $a, b, d :: (a, C)$ .

5. For the folded subroutine, X will be all items of “type” X, where X is any of C, I, O, the names of each entry will be the companion name with the “type”.

**(Internal Note):** The algorithm above works correctly, but likely has too high of a complexity, depending on the number of iterations. Need to revise in the next version to see if we can make the complexity proportional to the number of wires in/out.

#### 2.4.1 Examples of folding with Alternate Algorithm

**Example 7.** We repeat Example 4, that is,  $S = (\_, \{a, b\}, \{c\}, \{d\}, \_, \_, \_)$  and  $b_{cio} = \{(a, c), (b, a), (d, b)\}$  and an iteration count of 3. See figure figure 2.3.

There are two control wires  $a, b$ , an input wire  $d$  and one output wire  $d$ . We will do three iterations. Our set  $\mathcal{C}$  of pairs becomes:

$$\begin{aligned} & \{(\phi, a), (\phi, b), (\phi, c), \\ & (b, a_1), (d, b_1), (a, c_1), \\ & (b_1, a_2), (d_1, b_2), (a_1, c_2), \\ & (a_2, \phi), (b_2, \phi), (c_2, \phi)\}. \end{aligned}$$

Translating each of these to equations and constraints, we get:

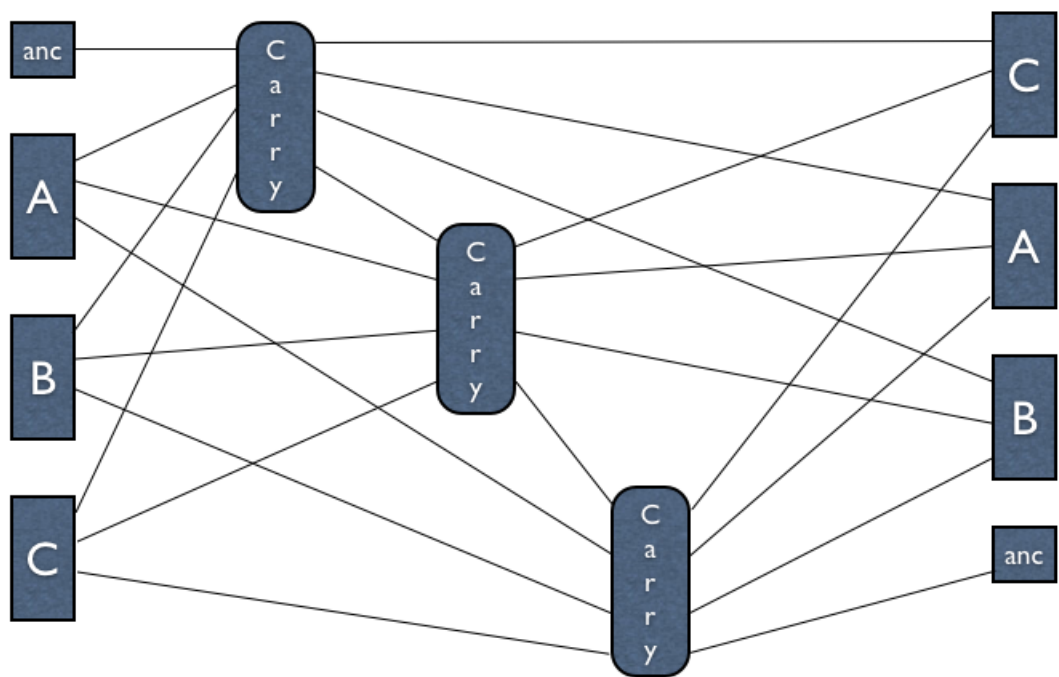
$$\begin{aligned} a &:: (a, C), b:: (b, C), c:: (c, I) \\ b &= a_1, b_1 = d \quad b_1:: O, a = c_1 \quad c_1:: I \\ b_1 &= a_2, b_2 = d_1 \quad b_2:: O, a_1 = c_2 \quad c_2:: I \\ a_2 &:: (C, a_2), b_2:: (C, b_2), d_2:: (O, d_2) \end{aligned}$$

As we have three wires in and three wires out, we expect to see six separate groupings in the solution to the above equations. We will proceed by starting from the top left.

$$\begin{array}{ll} \text{start: } a & a = c_1, :: I, :: (a, C) \quad \Longrightarrow \quad a:: (a, I) \\ \text{start: } b & b = a_1, a_1 = c_2, :: I, :: (b, C) \quad \Longrightarrow \quad b:: (b, I) \\ \text{start: } c & :: (c, I) \quad \Longrightarrow \quad c:: (c, I) \\ \text{start: } b_1 & b_1 = d, b_1 = a_2, :: O, :: (C, a_2) \quad \Longrightarrow \quad a_2:: (O, a_2) \\ \text{start: } b_2 & b_2 = d_1, :: O, :: (C, b_2) \quad \Longrightarrow \quad b_2:: (O, b_2) \\ \text{start: } d_2 & :: (O, d_2) \quad \Longrightarrow \quad d_2:: (O, d_2) \end{array}$$

## 2.5 Diagram of Folded Carry





**Figure 2.5:** Folding Carry

## Bibliography

- [1] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London Ser. A*, A425:73–90, 1989.
- [2] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, The Edinburgh Building, Cambridge CB2 2RU, UK, 2000. ISBN 0 521 63235 8.
- [3] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.
- [4] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Physical Review A*, 54:147, 1995.