

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

Abstract	i
Acknowledgements	ii
Table of Contents	iii
List of Tables	v
List of Figures	vi
List of Symbols	vii
1 Category theory	3
1.1 Restriction categories	3
1.1.1 Enrichment and meets	4
1.1.2 Partial monics, sections and isomorphisms	7
1.1.3 Split restriction categories	10
1.1.4 Partial Map Categories	14
1.1.5 Restriction products and Cartesian restriction categories	15
1.1.6 Graphic Categories	17
2 Reversible computation	21
2.1 Reversible Turing machines	21
2.2 Reversible automata and linear combinatory algebras	27
2.2.1 Automata	27
2.2.2 Combinatory Algebra	30
2.2.3 Linear Combinatory Algebra	32
3 Inverse categories	34
4 Quantum computation and circuits	35
4.1 Linear algebra	35
4.1.1 Basic definitions	35
4.1.2 Matrices	36
4.2 Basic quantum computation	38
4.2.1 Quantum bits	38
4.2.2 Quantum entanglement	39
4.2.3 Quantum gates	39
4.2.4 Measurement	40
4.2.5 Mixed states	41
4.2.6 Density matrix notation	41
4.2.7 Gates and density matrices	42
4.3 Quantum circuits	42
4.3.1 Contents of quantum circuits	42
4.3.2 Syntax of quantum circuits	47
4.3.3 Examples of quantum circuits	47
4.4 Extensions to quantum circuits	52
4.4.1 Renaming	52
4.4.2 Wire crossing	52
4.4.3 Scoped control	53
4.4.4 Circuit identities	54

4.5	An alternate description of quantum circuits	55
4.5.1	Base types	56
4.5.2	Types and Shapes	56
5	Transformations of Quantum Programs	58
5.1	Subroutines	58
5.1.1	Definition of a Subroutine	58
5.1.2	Subroutine Calls	60
5.1.3	High Level Structure	61
5.2	Subroutine Calls and Transformers	61
5.2.1	Iteration	62
5.2.2	Iteration transformation of a subroutine	64
5.2.3	Folding subroutines	66
5.2.4	Subroutine to folded subroutine transform	70
5.2.5	Examples of folding	74
5.3	Alternate Algorithm for Fold Transformation	78
5.3.1	Examples of folding with Alternate Algorithm	80
6	Synthesis of quantum operations	82
6.1	Introduction to synthesis	82
6.2	Exact synthesis of multi-qubit operators	82
6.2.1	Algebraic background	83
6.2.2	Decomposition into two-level matrices	88
6.2.3	Main result	93
6.2.4	The no-ancilla case	96
6.2.5	Complexity	98
7	Conclusions and future work	99
	Bibliography	100

List of Tables

4.1	Gates, circuit notation and matrices	44
4.2	Syntactic elements of quantum circuit diagrams	48
6.1	Some operations on residues	86

List of Figures and Illustrations

4.1	Simple single gate circuit	43
4.2	Entangling two qubits	43
4.3	Controlled-Not of $ 1\rangle$ and $ 1\rangle$	43
4.4	Measure notation in quantum circuits	45
4.5	Examples of multi- qubit gates and measures	45
4.6	Other forms of control for gates	46
4.7	n qubits on one line	46
4.8	Swap and controlled-Z	46
4.9	Quantum teleportation	49
4.10	Circuit for the Deutsch-Jozsa algorithm	50
4.11	Circuit for the quantum Fourier transform	51
4.12	Circuit for the inverse quantum Fourier transform	52
4.13	Renaming of a qubit and its equivalent diagram	52
4.14	Bending	53
4.15	Scope of control	53
4.16	Extensions sample	53
4.17	Swap in control vs. exchange in control	54
4.18	Measure is not affected by control	54
4.19	Control is not affected by measure	54
4.20	Zero control is syntactic sugar	55
4.21	Scoped control is parallel control	55
4.22	Scoped control is serial control	55
4.23	Multiple control	56
4.24	Control scopes commute	56
5.1	Transforming a subroutine to an iterated subroutine	66
5.2	Fold with extra in/out	74
5.3	Fold with three iterations	76
5.4	Fold of Carry	77

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition
U of C	University of Calgary
\mathbb{N}	The set of natural numbers, i.e., $\{0, 1, 2, \dots\}$
\mathbb{Z}	The ring of integers numbers, i.e., $\{0, \pm 1, \pm 2, \dots\}$
\mathbb{C}	The field of complex numbers

Overview of thesis chapters

Category Theory

This chapter will include a basic introduction to category theory. Specific areas introduced will include definitions of categories, natural transformations and functors. It will introduce limits and co-limits, focussing on products and co-products.

This chapter will also include an introduction to restriction categories.

Reversible Computing

This will introduce the subject of reversible computing, explaining the equivalence to standard computing at the level of Turing machines and automata. (Based on work by Bennet and Abramsky respectively). It will also provide an example of a reversible language.

Inverse categories

Inverse categories will be explored, along with some basic results regarding products and splits of categories. The inverse product will be introduced, along with the concept of a discrete inverse category and the relationship to Cartesian restriction categories.

The inverse co-product and inverse categories with inverse co-products will also be addressed in this chapter.

This is based on a paper which is in preparation (joint work with R. Cockett).

Quantum Computation

The basics of quantum computation and circuits will be introduced.

Transformations of Quantum Programs

The current understanding of how to treat iteration and folding in Quantum circuits and algorithms is somewhat lacking. This chapter will present unpublished work (done under the supervision of P. Selinger) exploring this area. It will include a treatment of necessary conditions for a quantum routine, its inputs and outputs, which would allow transforming the routine into either an iterated or folded routine. Algorithms to compute this transform are also provided.

Synthesis of Quantum transformations

This chapter will discuss the issue of gate synthesis, where an arbitrary quantum transform is to be expressed in terms of a set of base gates. The histories of both approximate and exact synthesis will be reviewed.

Then, the chapter will present an algorithm for exact synthesis of single-qubit transforms over the Clifford group, together with a normal form and characterization of these. This is based on a paper that is an extension of work done by Matsumoto and Amano and is in preparation (joint work with P. Selinger.)

Finally, we will present an algorithm for exact synthesis over the Clifford group of multi-qubit transforms and characterize those transforms that may be exactly synthesized. This is based on a paper published in the journal Physical Review A (joint work with P. Selinger).

Chapter 1

Category theory

1.1 Restriction categories

Restriction categories were originally introduced in [11] as an algebraic way to formulate partial map categories:

Definition 1.1.1. A *restriction category* is a category \mathbb{X} together with a *restriction operator* on maps:

$$\frac{f : A \rightarrow B}{\bar{f} : A \rightarrow A}$$

where f is an map of \mathbb{X} and A, B are objects of \mathbb{X} , such that the following four *restriction identities* hold, whenever the compositions¹ are defined.

$$[[\mathbf{R.1}]] \quad \bar{f}f = f$$

$$[[\mathbf{R.2}]] \quad \bar{g}\bar{f} = \bar{f}\bar{g}$$

$$[[\mathbf{R.3}]] \quad \overline{\bar{f}g} = \bar{f}\bar{g}$$

$$[[\mathbf{R.4}]] \quad f\bar{g} = \bar{f}gf$$

Definition 1.1.2. A *restriction functor* is a functor which preserves the restriction. That is, given a functor $F : \mathbb{X} \rightarrow \mathbb{Y}$ with \mathbb{X} and \mathbb{Y} restriction categories, F is a restriction functor if:

$$F(\bar{f}) = \overline{F(f)}.$$

Any map such that $r = \bar{r}$ is an idempotent, as $\bar{r}r = \overline{\bar{r}r} = \bar{r}$, and is called a *restriction idempotent*. All maps \bar{f} are restriction idempotents as $\bar{f} = \overline{\bar{f}}$. Below, we record some basic facts for restriction categories shown in [11] pp 4-5:

Lemma 1.1.3. *In a restriction category \mathbb{X} ,*

¹Note that composition is written in diagrammatic order throughout this paper.

- (i) \bar{f} is idempotent;
- (ii) $\overline{fg} = \overline{fg} \bar{f}$;
- (iii) $\overline{fg} = \bar{f} \bar{g}$;
- (iv) $\overline{\bar{f}} = \bar{f}$;
- (v) $\bar{f} \bar{g} = \overline{\bar{f} \bar{g}}$;
- (vi) f monic implies $\bar{f} = 1$;
- (vii) $f = \bar{g}f \implies \bar{g} \bar{f} = \bar{f}$.

A map $f : A \rightarrow B$ in a restriction category is said to be *total* when $\bar{f} = 1_A$. The total maps in a restriction category form a subcategory $Total(\mathbb{X}) \subseteq \mathbb{X}$.

An example of a restriction category is PAR, the category with objects sets and arrows the partial functions between sets. In PAR, the restriction of $f : A \rightarrow B$ is:

$$\bar{f}(x) = \begin{cases} x & \text{if } f(x) \text{ is defined,} \\ \uparrow & \text{if } f(x) \text{ is } \uparrow. \end{cases}$$

(The symbol \uparrow means that the function is undefined at that element). In PAR, the total maps correspond precisely to the functions that are defined on all elements of the domain.

1.1.1 Enrichment and meets

In any restriction category, there is a partial order on each hom-set, given by $f \leq g$ iff $\bar{f}g = f$, where $f, g : A \rightarrow B$.

Lemma 1.1.4. *In a restriction category \mathbb{X} :*

- (i) \leq as defined above is a partial order on each hom-set;
- (ii) $f \leq g \implies \bar{f} \leq \bar{g}$;
- (iii) $f \leq g \implies hf \leq hg$;

$$(iv) f \leq g \implies fh \leq gh;$$

$$(v) f \leq 1 \iff f = \bar{f}.$$

Proof.

- (i) With f, g, h parallel maps in \mathbb{X} , each of the requirements for a partial order is shown below:

Reflexivity: $\bar{f}f = f$ and therefore, $f \leq f$.

Anti-Symmetry: Given $\bar{f}g = f$ and $\bar{g}f = g$, it follows:

$$f = \bar{f}f = \overline{\bar{f}g}f = \bar{f}\bar{g}f = \bar{g}\bar{f}f = \bar{g}f = g.$$

Transitivity: Given $f \leq g$ and $g \leq h$,

$$\bar{f}h = \overline{\bar{f}g}h = \bar{f}\bar{g}h = \bar{f}g = f$$

showing that $f \leq h$.

- (ii) The premise is that $\bar{f}g = f$. From this, $\bar{f}\bar{g} = \overline{\bar{f}g} = \bar{f}$, showing $\bar{f} \leq \bar{g}$.

- (iii) $\bar{h}\bar{f}hg = h\bar{f}g = hf$ and therefore $hf \leq hg$.

- (iv) $\bar{f}g = f$, this shows $\bar{f}hgh = \overline{\bar{f}g}hgh = \bar{f}\bar{g}hgh = \bar{f}gh = fh$ and therefore $fh \leq gh$.

- (v) As $f \leq 1$ means precisely $\bar{f}1 = f$.

□

Lemma 1.1.4 shows that restriction categories are enriched in partial orders.

Definition 1.1.5. A restriction category has *meets* if there is an operation \cap on parallel maps:

$$\frac{A \begin{smallmatrix} f \\ \rightrightarrows \\ g \end{smallmatrix} B}{A \xrightarrow{f \cap g} B}$$

such that $f \cap g \leq f, f \cap g \leq g, f \cap f = f, h(f \cap g) = hf \cap hg$.

Meets were introduced in [6]. The following are basic results on meets:

Lemma 1.1.6. *In a restriction category \mathbb{X} with meets, where f, g, h are maps in \mathbb{X} , the following are true:*

- (i) $f \leq g$ and $f \leq h \iff f \leq g \cap h$;
- (ii) $f \cap g = g \cap f$;
- (iii) $\overline{f \cap 1} = f \cap 1$;
- (iv) $(f \cap g) \cap h = f \cap (g \cap h)$;
- (v) $r(f \cap g) = rf \cap g$ where $r = \bar{r}$ is a restriction idempotent;
- (vi) $(f \cap g)r = fr \cap g$ where $r = \bar{r}$ is a restriction idempotent;
- (vii) $\overline{f \cap g} \leq \bar{f}$ (and therefore $\overline{f \cap g} \leq \bar{g}$);
- (viii) $(f \cap 1)f = f \cap 1$;
- (ix) $e(e \cap 1) = e$ where e is idempotent.

Proof.

- (i) $f \leq g$ and $f \leq h$ means precisely $f = \bar{f}g$ and $f = \bar{f}h$. Therefore,

$$\bar{f}(g \cap h) = \bar{f}g \cap \bar{f}h = f \cap f = f$$

and so $f \leq g \cap h$. Conversely, given $f \leq g \cap h$, we have $f = \bar{f}(g \cap h) = \bar{f}g \cap \bar{f}h \leq \bar{f}g$. But $f \leq \bar{f}g$ means $f = \bar{f}\bar{f}g = \bar{f}g$ and therefore $f \leq g$. Similarly, $f \leq h$.

- (ii) From (i), as by definition, $f \cap g \leq g$ and $f \cap g \leq f$.

- (iii) $f \cap 1 = \overline{f \cap 1}(f \cap 1) = (\overline{f \cap 1}f) \cap (\overline{f \cap 1}) \leq \overline{f \cap 1}$ from which the result follows.

(iv) By definition and transitivity, $(f \cap g) \cap h \leq f, g, h$ therefore by (i) $(f \cap g) \cap h \leq f \cap (g \cap h)$. Similarly, $f \cap (g \cap h) \leq (f \cap g) \cap h$ giving the equality.

(v) Given $rf \cap g \leq rf$, calculate:

$$rf \cap g = \overline{rf \cap g} rf = \overline{r(rf \cap g)} f = \overline{rrf \cap rgf} = \overline{r(f \cap g)} f = \overline{rf \cap gf} = r(f \cap g).$$

(vi) Using the previous point with the restriction idempotent \overline{fr} ,

$$\begin{aligned} fr \cap g &= f\overline{r} \cap g = \overline{fr} f \cap g = \overline{fr}(f \cap g) = \overline{fr} \overline{f \cap gf} \\ &= \overline{f \cap g} \overline{fr} f = \overline{f \cap g} f \overline{r} = (f \cap g)r. \end{aligned}$$

(vii) For the first claim,

$$\overline{f \cap g} \overline{f} = \overline{\overline{f}(f \cap g)} = \overline{(\overline{f}f) \cap g} = \overline{f \cap g}.$$

The second claim then follows by (ii).

(viii) Given $f \cap 1 \leq f$:

$$f \cap 1 \leq f \iff \overline{f \cap 1} f = f \cap 1 \iff (f \cap 1)f = f \cap 1$$

where the last step is by item (iii) of this lemma.

(ix) As e is idempotent, $e(e \cap 1) = (ee \cap e) = e$.

□

1.1.2 Partial monics, sections and isomorphisms

Partial isomorphisms play a central role in this paper and below we develop some their basic properties.

Definition 1.1.7. A map f in a restriction category \mathbb{X} is said:

- To be a *partial isomorphism* when there is a *partial inverse*, written $f^{(-1)}$ with $ff^{(-1)} = \overline{f}$ and $f^{(-1)}f = \overline{f^{(-1)}}$;

- To be a *partial monic* if $hf = kf \implies h\bar{f} = k\bar{f}$;
- To be a *partial section* if there exists an h such that $fh = \bar{f}$;
- To be a *restriction monic* if it is a section s with a retraction r such that $rs = \overline{rs}$.

Lemma 1.1.8. *In a restriction category:*

- (i) *f, g partial monic implies fg is partial monic;*
- (ii) *f a partial section implies f is partial monic;*
- (iii) *f, g partial sections implies fg is a partial section;*
- (iv) *The partial inverse of f , when it exists, is unique;*
- (v) *If f, g have partial inverses and fg exists, then fg has a partial inverse;*
- (vi) *A restriction monic s is a partial isomorphism.*

Proof.

- (i) Suppose $hfg = kfg$. As g is partial monic, $hf\bar{g} = kf\bar{g}$. Therefore:

$$hf\bar{g}f = kf\bar{g}f \quad [\mathbf{R.4}]$$

$$hf\bar{g}\bar{f} = kf\bar{g}\bar{f} \quad f \text{ partial monic}$$

$$hf\bar{g} = kf\bar{g} \quad \text{Lemma 1.1.3, (ii)}$$

- (ii) Suppose $gf = kf$. Then, $g\bar{f} = gfh = kfh = k\bar{f}$.

(iii) We have $fh = \overline{f}$ and $gh' = \overline{g}$. Therefore,

$$\begin{aligned}
fgh'h &= f\overline{g}h && g \text{ partial section} \\
&= \overline{f}gfh && [\mathbf{R.4}] \\
&= \overline{f}g\overline{f} && f \text{ partial section} \\
&= \overline{f}\overline{f}g && [\mathbf{R.2}] \\
&= \overline{\overline{f}fg} && [\mathbf{R.3}] \\
&= \overline{fg} && [\mathbf{R.1}]
\end{aligned}$$

(iv) Suppose both $f^{(-1)}$ and f^* are partial inverses of f . Then,

$$\begin{aligned}
f^{(-1)} &= \overline{f^{(-1)}}f^{(-1)} = f^{(-1)}ff^{(-1)} = f^{(-1)}\overline{f} = f^{(-1)}ff^* = f^{(-1)}f\overline{f^*}f^* \\
&= \overline{f^{(-1)}f^*}f^* = \overline{f^*f^{(-1)}}f^* = f^*f\overline{f^{(-1)}}f^* = f^*ff^{(-1)}ff^* = f^*ff^* = f^*
\end{aligned}$$

(v) For $f : A \rightarrow B$, $g : B \rightarrow C$ with partial inverses $f^{(-1)}$ and $g^{(-1)}$ respectively, the partial inverse of fg is $g^{(-1)}f^{(-1)}$. Calculating $fgg^{(-1)}f^{(-1)}$ using all the restriction identities:

$$fgg^{(-1)}f^{(-1)} = f\overline{g}f^{(-1)} = \overline{f}gf^{(-1)} = \overline{f}g\overline{f} = \overline{f}\overline{f}g = \overline{\overline{f}fg} = \overline{fg}.$$

The calculation of $g^{(-1)}f^{(-1)}fg = \overline{g^{(-1)}f^{(-1)}}$ is similar.

(vi) The partial inverse of s is $\overline{rs}r$. First, note that $\overline{\overline{rs}r} = \overline{rs}\overline{r} = \overline{r}\overline{rs} = \overline{\overline{r}rs} = \overline{rs}$.

Then, it follows that $(\overline{rs}r)s = rs = \overline{rs} = \overline{\overline{rs}r}$ and $s(\overline{rs}r) = sr\overline{s} = \overline{s}$.

□

A restriction category in which every map is a partial isomorphism is called an *inverse category*.

An interesting property of inverse categories:

Lemma 1.1.9. *In an inverse category, all idempotents are restriction idempotents.*

Proof. Given an idempotent e ,

$$\bar{e} = ee^{(-1)} = eee^{(-1)} = e\bar{e} = \bar{e}ee = \bar{e}e = e.$$

□

1.1.3 Split restriction categories

The split restriction category, $K_E(\mathbb{X})$ is defined as:

Objects: (A, e) , where A is an object of \mathbb{X} , $e : A \rightarrow A$ and $e \in E$.

Maps: $f : (A, d) \rightarrow (B, e)$ is given by $f : A \rightarrow B$ in \mathbb{X} , where $f = dfe$.

Identity: The map e for (A, e) .

Composition: inherited from \mathbb{X} .

This is the standard idempotent splitting construction, also known as the Karoubi envelope.

Note that for $f : (A, d) \rightarrow (B, e)$, by definition, in \mathbb{X} we have $f = dfe$, giving

$$df = d(dfe) = ddfe = dfe = f \quad \text{and} \quad fe = (dfe)e = dfee = dfe = f.$$

When \mathbb{X} is a restriction category, there is an immediate candidate for a restriction in $K_E(\mathbb{X})$.

If $f \in K_E(\mathbb{X})$ is e_1fe_2 in \mathbb{X} , then define \bar{f} as given by $e_1\bar{f}$ in \mathbb{X} . Note that for $f : (A, d) \rightarrow (B, e)$, in \mathbb{X} we have:

$$d\bar{f} = \bar{d}\bar{f}d = \bar{f}d.$$

Proposition 1.1.10. *If \mathbb{X} is a restriction category and E is a set of idempotents, then the restriction as defined above makes $K_E(\mathbb{X})$ a restriction category.*

Proof. The restriction takes $f : (A, e_1) \rightarrow (B, e_2)$ to an endomorphism of (A, e_1) . The restriction is in $K_E(\mathbb{X})$ as

$$e_1(e_1\bar{f})e_1 = e_1\bar{f}e_1 = \bar{e}_1\bar{f}e_1e_1 = \bar{e}_1\bar{f}e_1 = e_1\bar{f}.$$

Checking the 4 restriction axioms:

$$[\mathbf{R.1}] \quad \llbracket \bar{f}f \rrbracket = e_1 \bar{f}f = e_1 f = \llbracket f \rrbracket$$

$$[\mathbf{R.2}] \quad \llbracket \bar{g}\bar{f} \rrbracket = e_1 \bar{g}e_1 \bar{f} = e_1 e_1 \bar{g}\bar{f} = e_1 e_1 \bar{f}\bar{g} = e_1 \bar{f}e_1 \bar{g} = \llbracket \bar{f}\bar{g} \rrbracket$$

$$[\mathbf{R.3}] \quad \llbracket \bar{f}g \rrbracket \equiv e_1 \overline{e_1 \bar{f}g} = \overline{e_1 e_1 \bar{f}g} = \overline{e_1 \bar{f}g} e_1 = \overline{e_1 \bar{f}g} = e_1 \bar{f}g = e_1 e_1 \bar{f}g = e_1 \bar{f}e_1 \bar{g} = \llbracket \bar{f}\bar{g} \rrbracket$$

$$[\mathbf{R.4}] \quad \llbracket f\bar{g} \rrbracket = e_1 f e_2 \bar{g} = \overline{e_1 f e_2 g} e_1 f e_2 = \overline{e_1 e_1 f e_2 g} e_1 f e_2 \\ = e_1 \overline{e_1 f e_2 g} e_1 f e_2 = e_1 \bar{f}g e_1 f e_2 = \llbracket \bar{f}g f \rrbracket$$

□

Given this, provided all identity maps are in E , $K_E(\mathbb{X})$ is a restriction category with \mathbb{X} as a full sub-restriction category, via the embedding defined by taking an object A in \mathbb{X} to the object $(A, 1)$ in $K_E(\mathbb{X})$. Furthermore, the property of being an inverse category is preserved by splitting.

Lemma 1.1.11. *When \mathbb{X} is an inverse category, $K_E(X)$ is an inverse category.*

Proof. The inverse of $f : (A, e_1) \rightarrow (B, e_2)$ in $K_E(\mathbb{X})$ is $e_2 f^{(-1)} e_1$ as

$$\llbracket f f^{(-1)} \rrbracket = e_1 f e_2 e_2 f^{(-1)} e_1 = e_1 e_1 f e_2 f^{(-1)} e_1 = e_1 f f^{(-1)} e_1 = e_1 e_1 \bar{f} e_1 = e_1 \bar{f} = \llbracket \bar{f} \rrbracket$$

and

$$\llbracket f^{(-1)} f \rrbracket = e_2 f^{(-1)} e_1 e_1 f e_2 = e_2 f^{(-1)} e_1 f e_2 e_2 = e_2 f^{(-1)} f e_2 \\ = e_2 e_2 \overline{f^{(-1)}} e_2 = e_2 \overline{f^{(-1)}} = \llbracket \overline{f^{(-1)}} \rrbracket$$

□

Proposition 1.1.12. *In a restriction category \mathbb{X} , with meets, let R be the set of restriction idempotents. Then, $K(\mathbb{X}) \cong K_R(\mathbb{X})$ (where $K(\mathbb{X})$ is the split of \mathbb{X} over all idempotents). Furthermore, $K_R(\mathbb{X})$ has meets.*

Proof. The proof below first shows the equivalence of the two categories, then addresses the claim that $K_R(\mathbb{X})$ has meets.

For equivalence, we require two functors,

$$U : K_R(\mathbb{X}) \rightarrow K(\mathbb{X}) \text{ and } V : K(\mathbb{X}) \rightarrow K_R(\mathbb{X}),$$

with:

$$UV \cong I_{K_R(\mathbb{X})} \tag{1.1}$$

$$VU \cong I_{K(\mathbb{X})}. \tag{1.2}$$

U is the standard inclusion functor. V will take the object (A, e) to $(A, e \cap 1)$ and the map $f : (A, e_1) \rightarrow (B, e_2)$ to $(e_1 \cap 1)f$.

V is a functor as:

Well Defined: If $f : (A, e_1) \rightarrow (B, e_2)$, then $(e_1 \cap 1)f$ is a map in \mathbb{X} from A to B and

$$(e_1 \cap 1)(e_1 \cap 1)f(e_2 \cap 1) = (e_1 \cap 1)(fe_2 \cap f) = (e_1 \cap 1)(f \cap f) = (e_1 \cap 1)f,$$

therefore, $V(f) : V((A, e_1)) \rightarrow V((B, e_2))$.

Identities: $V(e) = (e \cap 1)e = e \cap 1$ by lemma 1.1.6.

Composition: $V(f)V(g) = (e_1 \cap 1)f(e_2 \cap 1)g = (e_1 \cap 1)fe_2(e_2 \cap 1)g = (e_1 \cap 1)f(e_2 \cap e_2)g = (e_1 \cap 1)fe_2g = (e_1 \cap 1)fg = V(fg)$.

Recalling from Lemma 1.1.6, $(e \cap 1)$ is a restriction idempotent. Using this fact, the commutativity of restriction idempotents and the general idempotent identities from 1.1.6 on page 6, the composite functor UV is the identity on $K_r(\mathbb{X})$ as when e is a restriction idempotent, $e = e(e \cap 1) = (e \cap 1)e = (e \cap 1)$.

For the other direction, note that for a particular idempotent $e : A \rightarrow A$, this gives the maps $e : (A, e) \rightarrow (A, e \cap 1)$ and $e \cap 1 : (A, e \cap 1) \rightarrow (A, e)$, again by 1.1.6 on page 6. These

maps give the natural isomorphism between I and VU as

$$\begin{array}{ccc}
 (A, e) & \xrightarrow{e} & (A, e \cap 1) \\
 & \searrow e & \downarrow e \cap 1 \\
 & & (A, e)
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 (A, e \cap 1) & \xrightarrow{e \cap 1} & (A, e) \\
 & \searrow e \cap 1 & \downarrow e \\
 & & (A, e \cap 1)
 \end{array}$$

both commute. Therefore, $UV = I$ and $VU \cong I$, giving an equivalence of the categories.

For the rest of this proof, the bolded functions, e.g., \mathbf{f} are in $K_R(\mathbb{X})$. Italic functions, e.g., f are in \mathbb{X} .

To show that $K_R(\mathbb{X})$ has meets, designate the meet in $K_R(\mathbb{X})$ as \cap_K and define $\mathbf{f} \cap_K \mathbf{g}$ as the map given by the \mathbb{X} map $f \cap g$, where $\mathbf{f}, \mathbf{g} : (A, d) \rightarrow (B, e)$ in $K_R(\mathbb{X})$ and $f, g : A \rightarrow B$ in \mathbb{X} . This is a map in $K_R(\mathbb{X})$ as $d(f \cap g)e = (df \cap dg)e = (f \cap g)e = (fe \cap g) = f \cap g$ where the penultimate equality is by [1.1.6 on page 6](#). By definition $\overline{\mathbf{f} \cap_K \mathbf{g}}$ is $\overline{df \cap g}$.

It is necessary to show \cap_K satisfies the four meet properties.

- $\mathbf{f} \cap_K \mathbf{g} \leq \mathbf{f}$: We need to show $\overline{\mathbf{f} \cap_K \mathbf{g}} \mathbf{f} = \mathbf{f} \cap_K \mathbf{g}$. Calculating now in \mathbb{X} :

$$\begin{aligned}
 \overline{df \cap g} f &= \overline{d(f \cap g)} df \\
 &= \overline{df \cap dg} df \\
 &= \overline{f \cap g} f \\
 &= f \cap g
 \end{aligned}$$

which is the definition of $\mathbf{f} \cap_K \mathbf{g}$.

- $\mathbf{f} \cap_K \mathbf{g} \leq \mathbf{g}$: Similarly and once again calculating in \mathbb{X} ,

$$\begin{aligned}
 \overline{df \cap g} g &= \overline{d(f \cap g)} dg \\
 &= \overline{df \cap dg} dg \\
 &= \overline{f \cap g} g \\
 &= f \cap g
 \end{aligned}$$

which is the definition of $\mathbf{f} \cap_K \mathbf{g}$.

- $\mathbf{f} \cap_K \mathbf{f} = \mathbf{f}$: From the definition, this is $f \cap f = f$ which is just \mathbf{f} .
- $\mathbf{h}(\mathbf{f} \cap_K \mathbf{g}) = \mathbf{h}\mathbf{f} \cap_K \mathbf{h}\mathbf{g}$: From the definition, this is given in \mathbb{X} by $h(f \cap g) = hf \cap hg$ which in $K_R(\mathbb{X})$ is $\mathbf{h}\mathbf{f} \cap_K \mathbf{h}\mathbf{g}$.

□

1.1.4 Partial Map Categories

In [11], it is shown that split restriction categories are equivalent to *partial map categories*. The main definitions and results related to partial map categories are given below.

Definition 1.1.13. A collection \mathcal{M} of monics is a *stable system of monics* when it includes all isomorphisms, is closed under composition and is pullback stable.

Stable in this definition means that if $m : A \rightarrow B$ is in \mathcal{M} , then for arbitrary b with codomain B , the pullback

$$\begin{array}{ccc} A' & \xrightarrow{a} & A \\ m' \downarrow & & \downarrow m \\ B' & \xrightarrow{b} & B \end{array}$$

exists and $m' \in \mathcal{M}$. A category that has a stable system of monics is referred to as an \mathcal{M} -category.

Lemma 1.1.14. *If $nm \in \mathcal{M}$, a stable system of monics, and m is monic, then $n \in \mathcal{M}$.*

Proof. The commutative square

$$\begin{array}{ccc} A & \xrightarrow{1} & A \\ n \downarrow & & \downarrow nm \\ A' & \xrightarrow{m} & B \end{array}$$

is a pullback.

□

Given a category \mathbb{C} and a stable system of monics, the *partial map category*, $\text{Par}(\mathbb{C}, \mathcal{M})$ is:

Objects: $A \in \mathbb{C}$

Equivalence Classes of Maps: $(m, f) : A \rightarrow B$ with $m : A' \rightarrow A$ is in \mathcal{M} and $f : A' \rightarrow B$

is a map in \mathbb{C} . i.e.,
$$\begin{array}{ccc} & A' & \\ m \swarrow & & \searrow f \\ A & & B \end{array}.$$

Identity: $1_A, 1_A : A \rightarrow A$

Composition: via a pullback, $(m, f)(m', g) = (m''m, f'g)$ where

$$\begin{array}{ccccc} & & A'' & & \\ & m'' \swarrow & & \searrow f' & \\ & A' & \text{(pb)} & B' & \\ m \swarrow & & & & \searrow g \\ A & & f \searrow & & B & \xleftarrow{m'} & C \end{array}$$

Restriction: $\overline{(m, f)} = (m, m)$

For the maps, $(m, f) \sim (m', f')$ when there is an isomorphism $\gamma : A'' \rightarrow A'$ such that $\gamma m' = m$ and $\gamma f' = f$.

In [12], it is shown that:

Theorem 1.1.15 (Cockett-Lack). *Every restriction category is a full subcategory of a partial map category.*

1.1.5 Restriction products and Cartesian restriction categories

Restriction categories have analogues of products and terminal objects.

Definition 1.1.16. In a restriction category \mathbb{X} a *restriction product* of two objects X, Y is an object $X \times Y$ equipped with *total* projections $\pi_0 : X \times Y \rightarrow X, \pi_1 : X \times Y \rightarrow Y$ where:

$\forall f : Z \rightarrow X, g : Z \rightarrow Y, \exists$ a unique $\langle f, g \rangle : Z \rightarrow X \times Y$ such that

- $\langle f, g \rangle \pi_0 \leq f$,
- $\langle f, g \rangle \pi_1 \leq g$ and

- $\overline{\langle f, g \rangle} = \bar{f} \bar{g} (= \bar{g} \bar{f})$.

Definition 1.1.17. In a restriction category \mathbb{X} a *restriction terminal object* is an object \top such that $\forall X$, there is a unique total map $!_X : X \rightarrow \top$ and the diagram

$$\begin{array}{ccc} X & \xrightarrow{\bar{f}} & X \xrightarrow{!_X} \top \\ \downarrow f & & \nearrow !_Y \\ Y & & \end{array}$$

commutes. That is, $f !_Y = \bar{f} !_X$. Note this implies that a restriction terminal object is unique up to a unique isomorphism.

Definition 1.1.18. A restriction category \mathbb{X} is *Cartesian* if it has all restriction products and a restriction terminal object.

Definition 1.1.19. An object A in a Cartesian restriction category is *discrete* when the diagonal map,

$$\Delta : A \rightarrow A \times A$$

is a partial isomorphism.

A Cartesian restriction category is *discrete* when every object is discrete.

Theorem 1.1.20. A Cartesian restriction category \mathbb{X} is discrete if and only if it has meets.

Proof. If \mathbb{X} has meets, then

$$\Delta(\pi_0 \cap \pi_1) = \Delta\pi_0 \cap \Delta\pi_1 = 1 \cap 1 = 1$$

and as $\langle \pi_0, \pi_1 \rangle$ is identity,

$$\begin{aligned} \overline{\pi_0 \cap \pi_1} &= \overline{\pi_0 \cap \pi_1} \langle \pi_0, \pi_1 \rangle \\ &= \langle \overline{\pi_0 \cap \pi_1} \pi_0, \overline{\pi_0 \cap \pi_1} \pi_1 \rangle \\ &= \langle \pi_0 \cap \pi_1, \pi_0 \cap \pi_1 \rangle \\ &= (\pi_0 \cap \pi_1) \Delta \end{aligned}$$

and therefore, $\pi_0 \cap \pi_1$ is $\Delta^{(-1)}$.

For the other direction, set $f \cap g = \langle f, g \rangle \Delta^{(-1)}$. By the definition of the restriction product:

$$f \cap g = \langle f, g \rangle \Delta^{(-1)} = \langle f, g \rangle \Delta^{(-1)} \Delta \pi_0 = \langle f, g \rangle \overline{\Delta^{(-1)}} \pi_0 \leq \langle f, g \rangle \pi_0 \leq f$$

Similarly, substituting π_1 for π_0 above, this gives $f \cap g \leq g$. For the left distributive law,

$$h(f \cap g) = h \langle f, g \rangle \Delta^{(-1)} = \langle hf, hg \rangle \Delta^{(-1)} = hf \cap hg$$

and finally an intersection of a map with itself is

$$f \cap f = \langle f, f \rangle \Delta^{(-1)} = (f \Delta) \Delta^{(-1)} = f \overline{\Delta} = f$$

as Δ is total. This shows that \cap as defined above is a meet for the Cartesian restriction category \mathbb{X} .

□

We shall refer to a Cartesian restriction category in which every object is discrete as simply a discrete restriction category.

1.1.6 Graphic Categories

In a Cartesian restriction category, a map $A \xrightarrow{f} B$ is called *graphic* when the maps

$$A \xrightarrow{\langle f, 1 \rangle} B \times A \quad \text{and} \quad A \xrightarrow{\langle \bar{f}, 1 \rangle} A \times A$$

have partial inverses. A Cartesian restriction category is *graphic* when all of its maps are graphic.

Lemma 1.1.21. *In a Cartesian restriction category:*

- (i) *Graphic maps are closed under composition;*
- (ii) *Graphic maps are closed under the restriction;*

(iii) An object is discrete if and only if its identity map is graphic.

Proof.

- (i) To show closure, it is necessary to show that $\langle fg, 1 \rangle$ has a partial inverse. By Lemma 1.1.8, the uniqueness of the partial inverse gives

$$(\langle f, 1 \rangle; \langle g, 1 \rangle \times 1)^{(-1)} = \langle g, 1 \rangle^{(-1)} \times 1; \langle f, 1 \rangle^{(-1)}.$$

By the definition of the restriction product, $\overline{\langle fg, 1 \rangle} = \overline{fg}$. Additionally, a straightforward calculation shows that $\overline{\langle f, 1 \rangle; \langle g, 1 \rangle \times 1} = \overline{\langle f \langle g, 1 \rangle, 1 \rangle} = \overline{f; \langle g, 1 \rangle} = \overline{\langle f; g, f \rangle} = \overline{fgf} = \overline{fg}$ where the last equality is by [R.2], [R.3] and finally [R.1].

Consider the diagram

$$\begin{array}{ccccc} A & \xrightarrow{\langle f, 1 \rangle} & B \times A & \xrightarrow{\langle g, 1 \rangle \times 1} & C \times B \times A \\ & \searrow \langle fg, 1 \rangle & & & \uparrow 1 \times \langle f, 1 \rangle \\ & & & & C \times A \end{array}$$

From this:

$$\begin{aligned} \langle fg, 1 \rangle (1 \times \langle f, 1 \rangle) (\langle g, 1 \rangle^{(-1)} \times 1) \langle f, 1 \rangle^{(-1)} &= \langle f, 1 \rangle (\langle g, 1 \rangle \times 1) (\langle g, 1 \rangle^{(-1)} \times 1) \langle f, 1 \rangle^{(-1)} \\ &= \langle f, 1 \rangle (\overline{g \times 1}) \langle f, 1 \rangle^{(-1)} \\ &= \overline{\langle f, 1 \rangle (g \times 1)} \langle f, 1 \rangle^{(-1)} \\ &= \overline{\langle f, 1 \rangle (g \times 1) \langle f, 1 \rangle} \\ &= \overline{\langle f, 1 \rangle \langle f, 1 \rangle (g \times 1)} \\ &= \overline{\langle f, 1 \rangle (g \times 1)} \\ &= \overline{\langle fg, 1 \rangle} (= \overline{fg}) \end{aligned}$$

showing that $1 \times \langle f, 1 \rangle (\langle g, 1 \rangle^{(-1)} \times 1) \langle f, 1 \rangle^{(-1)}$ is a right inverse for $\langle fg, 1 \rangle$.

For the other direction, note that in general $hk^{(-1)} = k^{(-1)}h^{(-1)}$ and that we have $\langle fg, 1 \rangle = \langle f, 1 \rangle (\langle g, 1 \rangle \times 1) (1 \times \langle f, 1 \rangle^{(-1)})$, thus $(1 \times \langle f, 1 \rangle) (\langle g, 1 \rangle^{(-1)} \times 1) \langle f, 1 \rangle^{(-1)}$ will also be a left inverse and $\langle fg, 1 \rangle$ is a restriction isomorphism.

- (ii) This follows from the definition of graphic and that $\overline{\langle f, 1 \rangle} = \bar{f} = \overline{\bar{f}}$.
- (iii) Given a discrete object A , the map 1_A is graphic as $\langle 1_A, 1 \rangle = \Delta$ and therefore $\langle 1, 1 \rangle^{(-1)} = \Delta^{(-1)}$. Conversely, if $\langle 1_A, 1 \rangle$ has an inverse, then $\Delta = \langle 1_A, 1 \rangle$ has that same inverse and therefore the object is discrete.

□

Lemma 1.1.22. *A discrete restriction category is precisely a graphic Cartesian restriction category.*

Proof. The requirement is that $\langle f, 1 \rangle$ (and $\langle \bar{f}, 1 \rangle$) each have partial inverses. For $\langle f, 1 \rangle$, the inverse is $\overline{(1 \times f) \Delta^{(-1)}} \pi_1$.

To show this, calculate the two compositions. First,

$$\langle f, 1 \rangle \overline{(1 \times f) \Delta^{(-1)}} \pi_1 = \overline{\langle f, f \rangle \Delta^{(-1)}} \langle f, 1 \rangle \pi_1 = \overline{f \Delta \Delta^{(-1)}} \langle f, 1 \rangle \pi_1 = \bar{f} \langle f, 1 \rangle \pi_1 = \bar{f}.$$

The other direction is:

$$\begin{aligned} \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \langle f, 1 \rangle &= \langle \overline{(1 \times f) \Delta^{(-1)}} \pi_1 f, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \langle \overline{(1 \times f) \Delta^{(-1)}} (1 \times f) \pi_1, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \langle \overline{(1 \times f) \Delta^{(-1)}} \pi_1, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \langle \overline{(1 \times f) \Delta^{(-1)}} \pi_0, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \langle \overline{(1 \times f) \Delta^{(-1)}} (1 \times f) \pi_0, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \langle \overline{(1 \times f) \Delta^{(-1)}} \pi_0, \overline{(1 \times f) \Delta^{(-1)}} \pi_1 \rangle \\ &= \overline{(1 \times f) \Delta^{(-1)}} \langle \pi_0, \pi_1 \rangle \\ &= \overline{(1 \times f) \Delta^{(-1)}} \end{aligned}$$

The one tricky step is to realize

$$\begin{aligned}
\overline{\Delta^{(-1)}}\pi_1 &= \Delta^{(-1)}\Delta\pi_1 \\
&= \Delta^{(-1)} \\
&= \Delta^{(-1)}\Delta\pi_0 \\
&= \overline{\Delta^{(-1)}}\pi_0
\end{aligned}$$

For $\langle \bar{f}, 1 \rangle$, the inverse is $\overline{(1 \times \bar{f})\Delta^{(-1)}}\pi_1$. Similarly to above,

$$\langle \bar{f}, 1 \rangle \overline{1 \times \bar{f}\Delta^{(-1)}}\pi_1 = \overline{\langle \bar{f}, \bar{f} \rangle \Delta^{(-1)}}\langle \bar{f}, 1 \rangle \pi_1 = \overline{\bar{f}\Delta\Delta^{(-1)}}\langle \bar{f}, 1 \rangle \pi_1 = \bar{\bar{f}}\langle \bar{f}, 1 \rangle \pi_1 = \bar{f}.$$

The other direction follows the same pattern as for $\langle f, 1 \rangle$. □

Chapter 2

Reversible computation

Bennet, in [5], showed that it was possible to emulate a standard Turing machine via a reversible Turing machine and vice-versa. This showed the equivalence of standard and reversible Turing machines. We reproduce the essence of this proof below.

2.1 Reversible Turing machines

Turing machines consist of a tape, a read-write head positioned over the tape, a machine state and a set of instructions. The set of instructions may be given as a set of transitions determining the movement of the read-write head, what it writes and the resulting state of the machine.

Definition 2.1.1. Given an alphabet A which does not contain a space, a tape is in *standard format* when:

1. The tape head is positioned directly over a blank space;
2. The spaces to the left (the $+1$ direction) contain only elements of A .
3. All other spaces of the tape are blank.

Definition 2.1.2. A *turing quintuple* is a quintuple $(s, \alpha, \alpha', \delta, s')$ where:

1. $s, s' \in S$, where S is a predefined set of states;
2. $\alpha, \alpha' \in A$ is predefined set of glyphs;
3. $\delta \in \{-1, 0, 1\}$.

Definition 2.1.3. A *standard turing quintuple set* Q consists of a set of turing quintuples such that:

1. If $q_1 = (s_1, \alpha_1, \alpha'_1, \delta_1, s'_1)$ and $q_2 = (s_2, \alpha_2, \alpha'_2, \delta_2, s'_2)$ are in Q , then either $s_1 \neq s_2$ or $\alpha_1 \neq \alpha_2$ or both are not equal.

2. There are two special quintuples contained in Q :

(a) $(s_1, \sqcup, \sqcup, +1, s_2)$ ¹, the *start quintuple*;

(b) $(s_{t-1}, \sqcup, \sqcup, 0, s_t)$, the *end quintuple* where t is the number of states and is the final state of the machine.

Definition 2.1.4. A *standard Turing machine* is given by

- a standard turing quintuple set;
- a tape that starts in standard format;
- and the condition that and if the machine halts, it will halt in state s_t , the final state of the end quintuple and the output will be in standard format.

The turing quintuples may also be regarded as giving the data for a partial function in SETS: $\tau : S \times A \rightarrow A \times \{-1, 0, 1\} \times S$.

Remark 2.1.5. A multi-tape Turing machine with n tapes and read-write heads can be described by modifying definition 2.1.4 such that α is an n -tuple of the set of glyphs for the Turing machine and δ is an n -tuple of movement directions.

Example 2.1.6. Suppose $S = \{start, run, reset, done\}$, $A = \{0, 1, \sqcup\}$ and the Turing machine program is given by the quintuples

$$\begin{aligned}
& (start, \sqcup, \sqcup, +1, run), \\
& (run, 0, 1, +1, run), (run, 1, 0, +1, run), \\
& (run, \sqcup, \sqcup, -1, reset), \\
& (reset, 0, 0, -1, reset), (reset, 1, 1, -1, reset), \\
& (reset, \sqcup, \sqcup, 0, done).
\end{aligned}$$

¹Here, \sqcup is used to signify a blank.

This program will perform a “bit-flip” of all 0s and 1s on the tape until it reads a space, reposition the read head to the standard format and then it will halt.

As we see in example [2.1.6 on the preceding page](#), it is *possible* that a Turing machine program is reversible. If we had chosen the second quintuple to be $(run, 0, 0, +1, run)$ instead, the program would not have been reversible.

The essential property that a Turing machine program needs to be reversible is that the function τ defined from the quintuples is injective. In order to simplify the discovery the function being injective, we reformulate the turing quintuples as quadruples.

Definition 2.1.7. A *turing quadruple* is given by a quadruple

$$(s, [b_1, b_2, \dots, b_n], [b'_1, b'_2, \dots, b'_n], s')$$

such that:

- $s, s' \in S$, some set of states;
- $b_j \in A \cup \{\phi\}$ where A is some alphabet;
- $b'_j \in A + \{-1, 0, 1\}$;
- $b'_j \in \{-1, 0, 1\}$ if and only if $b_j = \phi$.

In this definition, $b_j = \phi$ means that the value of tape j is ignored.

A turing quadruple explicitly splits the read/write action of the Turing machine away from the movement. In a particular step for tape k , the turing machine will either read and write an item or it will not read and then move.

Remark 2.1.8. Any turing quintuple may be split into two turing quadruples by the addition of a new state a'' in A , where the first quadruple will consist of all the read-write operations and leave the Turing machine in state a'' . The second quadruple will start in state a'' and all the b_j will be ϕ , with b'_j being movements on each of the n tapes.

Definition 2.1.9. A set of turing quadruples Q is called *reversible set of turing quadruples* when given $q_1, q_2 \in Q$, with $q_1 = (a, [b_j], [b'_j], a')$ and $q_2 = (c, [d_j], [d'_j], c')$:

- if $a = c$, then there is a k where $b_k, d_k \in A$ and $b_k \neq d_k$;
- if $a' = c'$, then there is a j with $b'_j, d'_j \in A$ and $b'_j \neq d'_j$.

Similarly to turing quintuples, turing quadruples may be taken as the data for a function in SETS:

$$\rho : S \times (A \cup \{\phi\}) \rightarrow (A + \{-1, 0, 1\}) \times S.$$

We can see by inspection that ρ is a reversible partial function when the set of turing quadruples that give ρ is a reversible set of turing quadruples.

Definition 2.1.10. A *reversible Turing machine* is one that is described by a set of reversible turing quadruples.

We will show that a reversible Turing machine with three tapes can emulate a Turing machine.

Theorem 2.1.11 (Bennet[5]). *Given a standard Turing Machine M , it may be emulated by a three tape reversible Turing machine R . In this case, emulated means:*

- M halts on standard input I if and only if R halts on standard input (I, \sqcup, \sqcup) .
- M halts on standard input I producing standard output O , if and only if R halts on input (I, \sqcup, \sqcup) producing standard output (I, \sqcup, O) .

Proof. (Sketch only).

The crux of the proof is to convert the quintuples of M to the quadruples of R as noted in remark 2.1.8 on the previous page. Explicitly for a single tape machine, we have

$$(s, a, a, \delta, s') \mapsto ((s, a, a', s''), (s'', \phi, \delta, s')). \quad (2.1)$$

In Equation (equation (2.1)), s'' is a new state for the machine M , not in the current set of states.

Assign an order to the n quintuples of M , where the start quintuple is the first in the order and the end quintuple comes last. Convert these to quadruples as in Equation (equation (2.1)).

We then proceed to create three groups of quadruples for R . We call these *emulation*, *copy*, and *restore*.

To create the emulation phase quadruples, we examine the pairs of quadruples of M in the sorted order and produce a pair of quadruples for R .

$$\begin{aligned}
\text{Pair 1} \quad & (s_1, \sqcup, \sqcup, s_1'') \mapsto (s_1, [\sqcup, \phi, \sqcup], [\sqcup, +1, \sqcup], e_1) \\
& (s_1'', \phi, \delta, s_2) \mapsto (e_1, [\phi, \sqcup, \phi], [\delta, 1, 0], s_2) \\
& \vdots \\
\text{Pair } j \quad & (s_k, a_j, a_j', s_k'') \mapsto (s_k, [a_j, \phi, \sqcup], [a_j', +1, \sqcup], e_j) \\
& (s_k'', \phi, \delta, s_i) \mapsto (e_j, [\phi, \sqcup, \phi], [\delta_j, j, 0], s_i) \\
& \vdots \\
\text{Pair } n \quad & (s_\ell, \sqcup, \sqcup, s_\ell'') \mapsto (s_\ell, [\sqcup, \phi, \sqcup], [\sqcup, +1, \sqcup], e_n) \\
& (s_\ell'', \phi, 0, s_f) \mapsto (e_n, [\phi, \sqcup, \phi], [0, n, 0], s_f).
\end{aligned}$$

By inspection, one can see that even if the quadruples of M were not a reversible set, the set created for R is a reversible set, due to the writing of the quadruple index on tape 2. Upon completion of the emulation phase, tape 1 will be the same as M would have produced on its single tape, tape 2 will be $[1, 2, \dots, n]$ and tape 3 will be blanks.

For the copy phase, we create the following quadruples:

$$\begin{aligned}
& (s_f, [\sqcup, n, \sqcup], [\sqcup, n, \sqcup], c_1) \\
& (c_1, [\phi, \phi, \phi], [+1, 0, +1], c'_1) \\
& (c'_1, [x, n, \sqcup], [x, n, x], c_1) \quad \text{when } x \neq \sqcup \\
& (c'_1, [\sqcup, n, \sqcup], [\sqcup, n, x], c_2) \\
& (c_2, [\phi, \phi, \phi], [-1, 0, -1], c'_2) \\
& (c'_2, [x, n, x], [x, n, x], c_2) \quad \text{when } x \neq \sqcup \\
& (c'_2, [\sqcup, n, \sqcup], [\sqcup, n, \sqcup], r_\ell).
\end{aligned}$$

In these quadruples, the states $\{c_1, c'_1, c_2, c'_2\}$ should be chosen to be distinct from the states in the emulation phase. As an example, set them as follows:

$$c_1 = (\{c\}, s_1) \quad c'_1 = (\{c'\}, s_1) \quad c_2 = (\{c\}, s_f) \quad c'_1 = (\{c'\}, s_f).$$

At the completion of this phase, tapes 1 and 2 will be unchanged and tape 3 will be a copy of tape 1.

Finally we perform the restore phase where the history will be erased and tape 1 reset to the input. The quadruples that will accomplish this are:

$$\begin{aligned}
\text{Pair } n & \quad (r_n, [\phi, n, \phi], [0, \sqcup, 0], r'_n) \\
& \quad (r'_n, [\sqcup, \phi, \sqcup], [\sqcup, -1, \sqcup], r_{n-1}) \\
& \quad \vdots \\
\text{Pair } j & \quad (r_k, [\phi, j, \phi], [-\delta_j, \sqcup, 0], r'_j) \\
& \quad (r'_j, [a'_j, \phi, \sqcup], [a_j, -1, \sqcup], r_i) \\
& \quad \vdots \\
\text{Pair } 1 & \quad (r_2, [\phi, 1, \phi], [-1, \sqcup, 0], r'_1) \\
& \quad (r'_1, [\sqcup, \phi, \sqcup], [\sqcup, -1, \sqcup], r_1).
\end{aligned}$$

The r states are derived from the s states of the emulation phase.

$$r_j = (\{r\}, s_j) \quad r'_j = (\{r'\}, s_j).$$

In this restore phase, the indexes of the states r match up to the indexes of states s . The quadruples reverse the actions of the emulate phase on tape 1, erase the history on tape 2 and make no change to tape 3.

□

2.2 Reversible automata and linear combinatory algebras

While reversible Turing machines, as described in Section [section 2.1](#), show that reversible computing is as powerful as standard computing, they do not give us a sense of what may be considered to be happening at a higher level.

To accomplish that task we examine the results of the paper “A Structural Approach to Reversible Computation”[\[1\]](#). In this paper, Abramsky gives a description of a reversible automaton together with a linear combinatory algebra. We will begin by revisiting some definitions and constructions necessary for discussing automata. The next subsection will introduce combinatory algebras, after which we will describe the reversible automata of [\[1\]](#) and add a short proof that it can emulate a reversible turing machine.

2.2.1 Automata

We will describe the automata as a term-rewriting system. This requires, of course, giving a few basic definitions. See, e.g., [\[4\]](#).

Definition 2.2.1. An *arity* is a function from a function to the natural numbers. The arity of F is the number of inputs (arguments) required by F .

Definition 2.2.2. A *signature* Σ is a set of *function symbols* F, G, \dots , each of which has an arity.

Remark 2.2.3. We refer to functions with low arity in the following ways:

- *Arity* = 0. These are known as *nullary* functions or constants.
- *Arity* = 1. These are known as *unary* functions.
- *Arity* = 2. These are known as *binary* functions.

Definition 2.2.4. A *term alphabet* is a set A containing a signature Σ and a countably infinite set X , the variables. Furthermore, $\Sigma \cap X = \emptyset$.

Definition 2.2.5. A *term algebra* of the term alphabet $\Sigma \cup X$ is denoted by $T_\Sigma(X)$ and defined as follows:

- $x \in V \implies x \in T_\Sigma$ and
- For any $F \in \Sigma$, with $\text{arity}(F) = n$, and $\{t_1, \dots, t_n\} \subseteq T_\Sigma$, then $F(t_1, \dots, t_n) \in T_\Sigma$. In the case where $\text{arity}(F) = 0$, we write $F \in T_\Sigma$.

Definition 2.2.6. The *ground terms* of a term algebra are those terms that do not contain any variable. The set of these terms is designated as T_Σ .

Remark 2.2.7. Note the ground terms consist of the constants and recursively applying the function symbols of Σ to them.

As we are considering rewrite systems, we will need to consider aspects of substitution and unification.

Definition 2.2.8. A *substitution* is a map $\sigma : T_\Sigma(X) \rightarrow T_\Sigma(X)$ which is natural for all function symbols in Σ . In particular if $\text{arity}(c) = 0$ then $\sigma(c) = c$.

Note that given the above definition a substitution σ is completely determined by its action on variables. If $\sigma : X \rightarrow X$ and is injective, we call σ a renaming. Moreover, if σ restricted to the variables in a term t is an injective map of X on those variables, we call *sigma* a renaming of t .

Substitution allows us to define a partial order on $T_\Sigma(X)$, as follows:

Definition 2.2.9. In $T_\Sigma(X)$, let $\sigma(t) = s$. Then we say s is an *instance* of t , written $s \preceq t$. Moreover, if σ is not just a renaming for t , then we write $s \prec t$. If σ is a renaming of t , we write $s \simeq t$.

Lemma 2.2.10. *Subsumption, as defined in 2.2.9 is a partial order, i.e., it is transitive and reflexive.*

Proof. □

Lemma 2.2.11. *Given terms r, t such that there is at least one s with $s \preceq r$ and $s \preceq t$, then there exists a g such that $g \preceq r$ and $g \preceq t$ and for any s' with $s' \preceq r$ and $s' \preceq t$ we will have $s' \preceq g$.*

Proof.

1. Algorithm to compute supremum of p, q terms.
2. Strict \prec has no infinite ascending chains.
3. Shows main part - there exists.
4. Can now show it is unique up to renaming.

□

The subsumption ordering can be used to derive a similar ordering on substitutions:

Definition 2.2.12. $\sigma \preceq \tau$ if and only if there is a ρ with $\sigma = \tau\rho$, where $\tau\rho$ is the diagrammatic order composition of the two substitutions.

Definition 2.2.13. For terms s, t , if $\sigma(t) = \sigma(s)$, then the substitution σ is called a *unifier* for the terms s, t .

Lemma 2.2.14. *If s, t are terms with a unifier σ , there exists a substitution τ that unifies s, t such that $\tau \preceq \rho$ whenever ρ unifies s, t . τ is called the most general unifier of s and t .*

Proof. Follows from 2.2.11. □

Notation 2.2.15. Following [1], we write $\mathcal{U}(t, u) \downarrow \sigma$ if σ is the most general unifier of terms t, u .

2.2.2 Combinatory Algebra

Definition 2.2.16. A *combinatory algebra* is an algebra with one binary operation, \cdot written in infix notation. The operation is not assumed to be associative. Multi-element expressions such as $a \cdot b \cdot c$ are to be taken as associating to the left, that is,

$$a \cdot b \cdot c = (a \cdot b) \cdot c.$$

The combinatory algebra may possess distinguished elements that are subject to specific rewrite rules.

Definition 2.2.17. *Combinatory logic* is the combinatory algebra with two distinguished elements, K and S , such that the following hold:

$$\begin{aligned} K \cdot x \cdot y &= x \\ S \cdot x \cdot y \cdot z &= x \cdot z \cdot (y \cdot z). \end{aligned}$$

Note that combinatory logic does not require a specific set that must be used for the algebra, simply that it has the two distinguished elements.

Combinatory logic was shown to be equivalent to the λ calculus by

For example, we may define the identity combinator I as $I = S \cdot K \cdot K$. Further combinators may be defined, such as the B combinator, defined by $B \cdot a \cdot b \cdot c = a \cdot (b \cdot c)$. The S and K combinators are complete, in that other combinators such as B may be defined from them. E.g., $B = S \cdot (K \cdot S) \cdot K$. In fact, we may define an alternate combinatory algebra that is equivalent to Combinatory Logic.

Definition 2.2.18. A *BCKW-Combinatory algebra* is a Combinatory Algebra with four distinguish elements, B , C , K , and W subject to the following equations:

$$\begin{aligned} B \cdot a \cdot b \cdot c &= a \cdot (b \cdot c) \\ C \cdot a \cdot b \cdot c &= a \cdot c \cdot b \\ K \cdot a \cdot b &= a \\ W \cdot a \cdot b &= a \cdot b \cdot b \end{aligned}$$

In fact, a BCKW-Combinatory algebra is equivalent to a Combinatory logic.

Lemma 2.2.19. *The distinguished elements of a BCKW-Combinatory algebra may be represented by S and K . Conversely, the S and K of a Combinatory logic may be created from B, C, K and W .*

Proof. For the first statement, we have:

$$\begin{aligned} B &= S \cdot (K \cdot S) \cdot K \\ C &= S \cdot (S \cdot (K \cdot (S \cdot (K \cdot S) \cdot K)) \cdot S) \cdot (K \cdot K) \\ K &= K \\ W &= S \cdot S \cdot (S \cdot K). \end{aligned}$$

Going the other direction, we have:

$$\begin{aligned} I &= W \cdot K \\ K &= K \\ S &= B \cdot (B \cdot (B \cdot W) \cdot C) \cdot (B \cdot B) \text{ and} \\ &= B \cdot (B \cdot W) \cdot (B \cdot B \cdot C). \end{aligned}$$

We show the computations of B and S in detail.

$$\begin{aligned} B \cdot a \cdot b \cdot c &= S \cdot (K \cdot S) \cdot K \cdot a \cdot b \cdot c \\ &= (K \cdot S) \cdot a \cdot (K \cdot a) \cdot b \cdot c \\ &= S \cdot (K \cdot a) \cdot b \cdot c \\ &= K \cdot a \cdot c \cdot (b \cdot c) \\ &= a \cdot (b \cdot c) \end{aligned}$$

$$\begin{aligned} S \cdot a \cdot b \cdot c &= B \cdot (B \cdot W) \cdot (B \cdot B \cdot C) \cdot a \cdot b \cdot c \\ &= (B \cdot W) \cdot ((B \cdot B \cdot C) \cdot a) \cdot b \cdot c \\ &= B \cdot W \cdot ((B \cdot B \cdot C) \cdot a) \cdot b \cdot c \\ &= W \cdot (((B \cdot B \cdot C) \cdot a) \cdot b) \cdot c \\ &= (((B \cdot B \cdot C) \cdot a) \cdot b) \cdot c \cdot c \\ &= B \cdot B \cdot C \cdot a \cdot b \cdot c \cdot c \\ &= B \cdot (C \cdot a) \cdot b \cdot c \cdot c \\ &= (C \cdot a) \cdot (b \cdot c) \cdot c \\ &= C \cdot a \cdot (b \cdot c) \cdot c \\ &= a \cdot c \cdot (b \cdot c) \end{aligned}$$

□

If we use the notation $a^n \cdot b$ to mean $a \cdot a \cdot \dots \cdot a \cdot b$ where a is repeated n times, then we can terms which correspond to the Church numbers of lambda calculus:

$$\bar{n} \equiv (S \cdot B)^n \cdot (K \cdot I)$$

Definition 2.2.20. A partial function $f : \mathbb{N} \rightarrow \mathbb{N}$ is *representable* in combinatory logic if there is a term M_f such that $M_f \cdot \bar{n} = \bar{m}$ whenever $f(n) = m$ and $M_f \cdot \bar{n}$ does not have a normal form if $f(n) \uparrow$.

When we say that combinatory logic with S and K is complete, we mean the following theorem:

Theorem 2.2.21. *The partial functions that are representable in combinatory logic are exactly the partial recursive functions.*

2.2.3 Linear Combinatory Algebra

Definition 2.2.22. A *Linear Combinatory Algebra* $(A, \cdot, !)$ is an algebra A with an applicative binary operation \cdot , an unary operator $! : A \rightarrow A$ and eight distinguished elements: B, C, I, K, D, δ , F and W in A which satisfy the following rules:

1. $B \cdot a \cdot b \cdot c = a \cdot (b \cdot c)$
2. $C \cdot a \cdot b \cdot c = a \cdot c \cdot b$
3. $I \cdot a = a$
4. $K \cdot a \cdot !b = a$
5. $D \cdot !a = a$
6. $\delta \cdot !a = !!a$
7. $F \cdot !a \cdot !b = !(a \cdot b)$
8. $W \cdot a \cdot !b = a \cdot !b \cdot !b$

Note that a Linear Combinatory Algebra always contains a BCKW-Combinatory algebra.

Define $D' = C \cdot (B \cdot B \cdot I) \cdot (B \cdot D \cdot I)$ and the binary operator \bullet on A such that $a \bullet b \equiv a \cdot !b$.

Then, define the following:

$$\begin{aligned}
B_s &= C \cdot (B \cdot (B \cdot B \cdot B) \cdot (D' \cdot I)) \cdot (C \cdot ((B \cdot B) \cdot F) \cdot \delta) \\
C_s &= D' \cdot C \\
K_s &= D' \cdot K \\
W_s &= D' \cdot W.
\end{aligned}$$

Lemma 2.2.23. *Given and Linear Combinatory Algebra $(A, \cdot, !)$, then (A, \bullet) is a BCKW-Combinatory algebra with B, C, K, W set to B_s, C_s, K_s, W_s from above.*

Proof. We show the calculation for K_s , the others are similar.

$$\begin{aligned}
K_s \bullet a \bullet b &\equiv D' \cdot K \cdot !a \cdot !b \\
&= C \cdot (B \cdot B \cdot I) \cdot (B \cdot D \cdot I) \cdot K \cdot !a \cdot !b \\
&= (B \cdot B \cdot I \cdot K) \cdot (B \cdot D \cdot I) \cdot !a \cdot !b \\
&= B \cdot (I \cdot K) \cdot (B \cdot D \cdot I) \cdot !a \cdot !b \\
&= (I \cdot K) \cdot ((B \cdot D \cdot I) \cdot !a) \cdot !b \\
&= K \cdot ((B \cdot D \cdot I) \cdot !a) \cdot !b \\
&= (B \cdot D \cdot I) \cdot !a \\
&= D \cdot (I \cdot !a) \\
&= D \cdot !a \\
&= a
\end{aligned}$$

□

Chapter 3

Inverse categories

Chapter 4

Quantum computation and circuits

4.1 Linear algebra

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

4.1.1 Basic definitions

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

Definition 4.1.1 (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 4.1.2 (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, $\sum a_j \mathbf{v}_j$ equals $\mathbf{0}$ unless all the a_j are zero.

Definition 4.1.3 (Basis). A *basis* of a vector space V is a linearly independent subset of V that generates V . That is, any vector $u \in V$ is a linear combination of the basis vectors.

4.1.2 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 $A = [a_{ij}] \in F^{m \times n}$, $B = [b_{jk}] \in F^{n \times p}$:

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

Definition 4.1.4 (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 4.1.5 (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 4.1.6 (Trace). The *trace*, $Tr(A)$ of a square matrix $A = [a_{ij}]$ is $\sum a_{ii}$.

Tensor Product

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

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

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 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 , $Tr(S A) \leq Tr(A)$.

4.2 Basic quantum computation

4.2.1 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 α or β zero is said to be in a *classical state*. Any other combination of values is said to be a *superposition*.

[Section 4.3 on page 42](#) will introduce quantum circuits which act on **qubits**. This section will have some forward references to circuits to illustrate points introduced here.

4.2.2 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

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle. \quad (4.1)$$

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

$$p \otimes q = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle \quad (4.2)$$

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

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \quad (4.3)$$

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

4.2.3 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 4.2 on page 43](#) shows how to entangle two **qubits** that start with an initial state of $|00\rangle$. See 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 4.1 on page 44](#).

4.2.4 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

$$q = \alpha |0\rangle + \beta |1\rangle \quad (4.4)$$

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 \(4.1\) on the previous 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:

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle \quad (4.5)$$

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 \(4.3\)](#), 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.

4.2.5 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

$$\nu = \alpha |0\rangle + \beta |1\rangle. \quad (4.6)$$

If ν 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:

$$\nu = |\alpha|^2 \{|0\rangle\} + |\beta|^2 \{|1\rangle\}. \quad (4.7)$$

An external (to the state) observer knows that the state of ν is as expressed in **equation (4.7)**. 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** ν is measured and the results are not examined, ν can be treated as a probabilistic **bit** rather than a **qubit**.

4.2.6 Density matrix notation

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

$$\nu = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{pmatrix}. \quad (4.8)$$

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 (4.7)** would be represented by the density matrix

$$|\alpha|^2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + |\beta|^2 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}. \quad (4.9)$$

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.

4.2.7 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 qq^* , 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^* .

4.3 Quantum circuits

4.3.1 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:

$$\text{---}x\text{---}$$

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 4.1](#). 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 4.3](#).



Figure 4.1: Simple single gate circuit

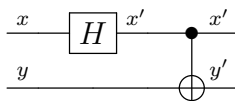


Figure 4.2: Entangling two **qubits**.

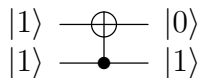


Figure 4.3: Controlled-Not of $|1\rangle$ and $|1\rangle$

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 4.2](#) 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 4.1 on the next page](#).

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







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 4.1: Gates, circuit notation and matrices

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 4.4](#).

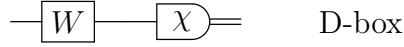


Figure 4.4: Measure notation in quantum circuits

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 4.5](#), the gate U applies to all of the first three **qubits** and the measurement applies to the first two **qubits**.

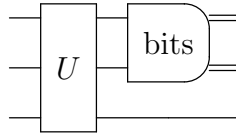


Figure 4.5: Examples of multi-**qubit** gates and measures

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. These forms of control are illustrated by the circuit in [figure 4.6 on the next page](#) with four **qubits** (r_1, r_2, p and q).

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.

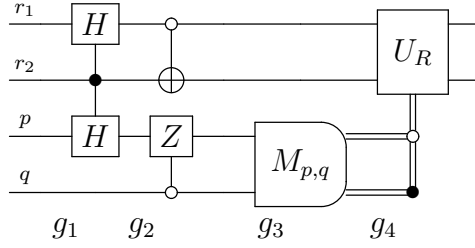


Figure 4.6: Other forms of control for gates

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 4.7](#) 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.

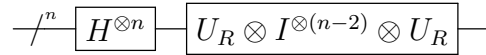


Figure 4.7: n **qubits** on one line

Other common circuit symbols

Two other symbols that are regularly used are the swap and controlled- Z , shown in the circuit in [figure 4.8](#). 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 \(4.10\) on the following page](#).

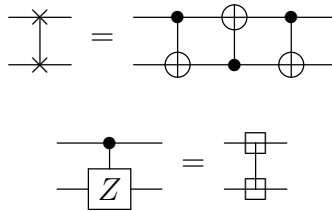


Figure 4.8: Swap and controlled- Z

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (4.10)$$

4.3.2 Syntax of quantum circuits

Quantum circuits were originally introduced by David Deutsch in [7]. 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 4.2 on the next 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.

4.3.3 Examples of quantum circuits

This section will present three quantum algorithms and the associated circuits. Each of these circuits presented may be found in [10].

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.


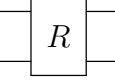
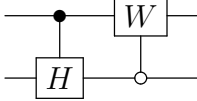

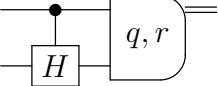
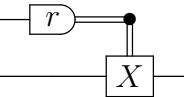
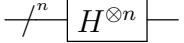
Desired element	Element in a quantum circuit diagram.	Example
qubit	A single horizontal line.	—
Classical bit	A double horizontal line.	=
Single- qubit gates	A box with the gate name (G) inside it, one wire attached on its left and one wire attached on the right.	
Multi- qubit gates	A box with the gate name (R) inside it, n wires on the left side and the same number of wires on the right.	
Controlled qubit 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 D shaped node with optional names or comments inside. One to n single wires are attached on the left (qubits coming in) and 0 to m classical bit wires on the right where $m \leq n$. Classical bits may be dropped as desired.	
Classical control	Control bullets are attached to horizontal classical wires, with vertical classical wires attached to the controlled gate.	
Multiple qubits	Annotate the line with the number of qubits and use tensors on gates.	

Table 4.2: Syntactic elements of quantum circuit diagrams

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 him¹.

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

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 ν 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 4.9](#).

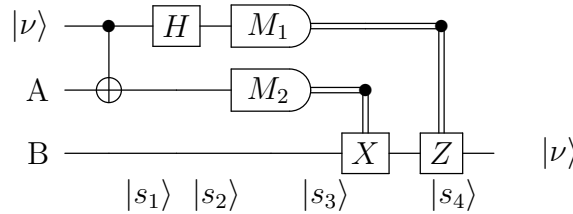


Figure 4.9: Quantum teleportation

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

¹Notice 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**.

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 4.10](#) will solve the problem with just one application. See the appendix, for how this would be done in L-QPL.

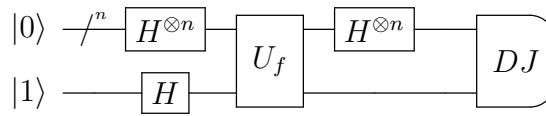


Figure 4.10: Circuit for the Deutsch-Jozsa algorithm

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 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

²The 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.

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 4.11](#) and [figure 4.12](#) 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 3rd to the $n - 3^{\text{rd}}$ lines and interior processing. The L-QPL code for the quantum Fourier transform is in the appendix, In this circuit, the parametrized transform R_n is the rotation transform, given by:

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

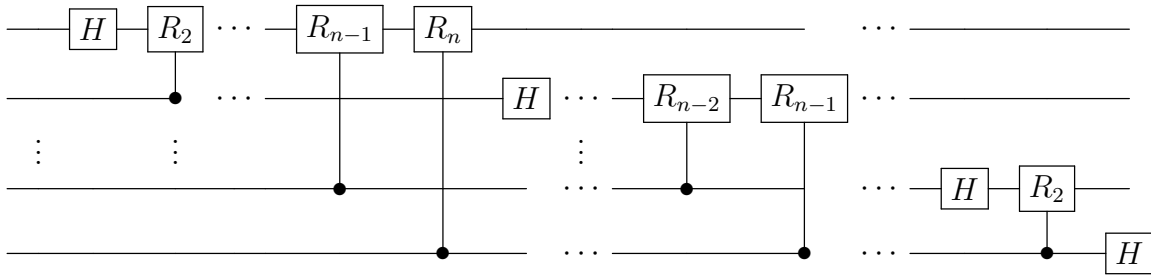


Figure 4.11: Circuit for the quantum Fourier transform

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 4.12 on the following page](#). The L-QPL code for the inverse quantum Fourier transform is in the appendix,

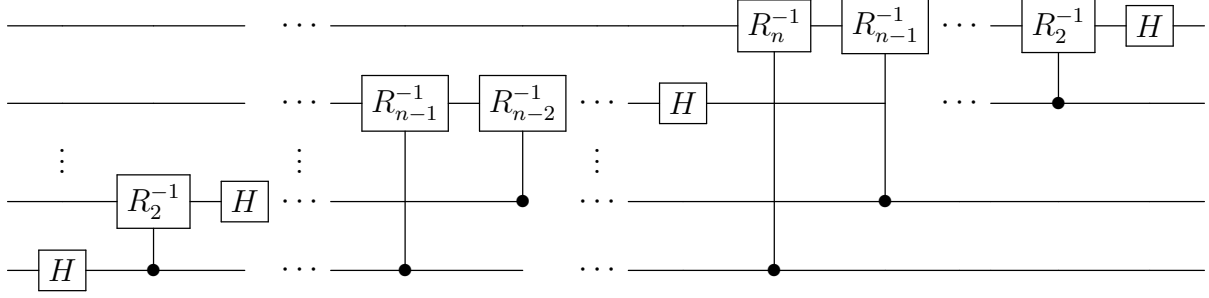


Figure 4.12: Circuit for the inverse quantum Fourier transform

4.4 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.

4.4.1 Renaming

Quantum circuits currently allow renaming to be an implicit part of any gate. The circuit in [figure 4.13](#) gives an operation to explicitly do this and its rewriting in standard circuit notation.

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

Figure 4.13: Renaming of a **qubit** and its equivalent diagram

4.4.2 Wire crossing

Crossing and bending of wires in a circuit diagram is added to allow a simpler presentation of algorithms. The circuit in [figure 4.14 on the following page](#) illustrates the concept of re-organizing and bending of wires.

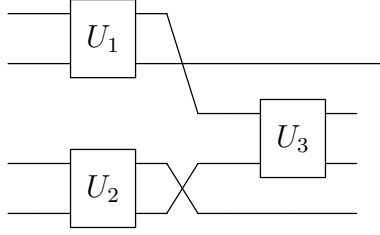


Figure 4.14: Bending

4.4.3 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 4.15** 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.

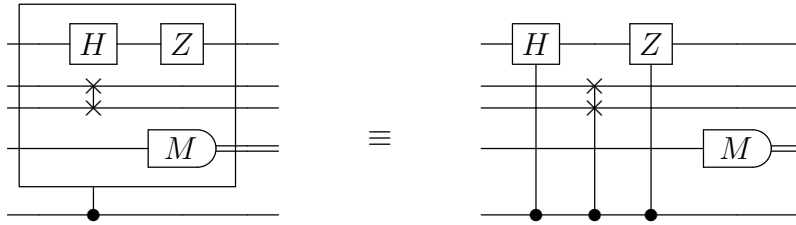


Figure 4.15: Scope of control

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

Naturally, both scoping and bending may be combined as in **figure 4.16**.

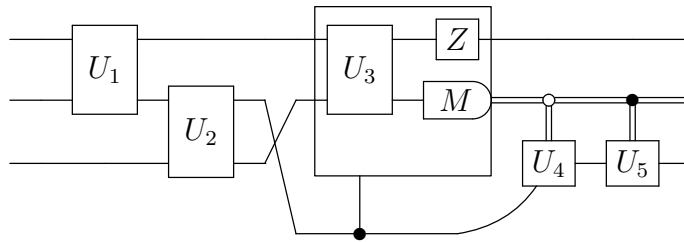


Figure 4.16: Extensions sample

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 4.17](#).

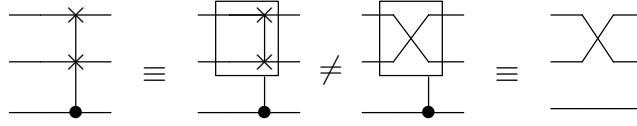


Figure 4.17: Swap in control vs. exchange in control

4.4.4 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 4.18](#). Conversely, a measurement commutes with control of a circuit as in [figure 4.18](#).

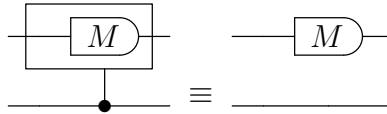


Figure 4.18: Measure is not affected by control

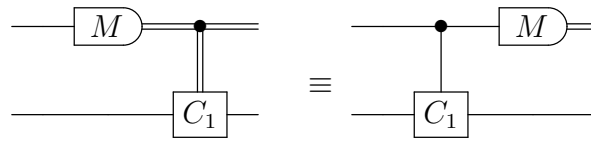


Figure 4.19: Control is not affected by measure

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 4.20 on the next page](#).

[Figure 4.21 on the following page](#) shows that scoped control of multiple transforms is the same as controlling those transforms individually. [Figure 4.22 on the next page](#) similarly

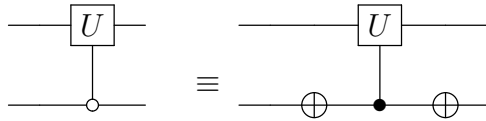


Figure 4.20: Zero control is syntactic sugar

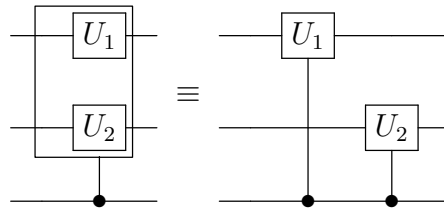


Figure 4.21: Scoped control is parallel control

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

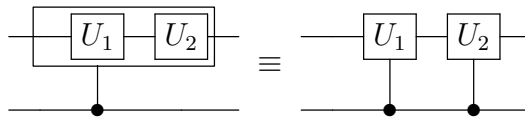


Figure 4.22: Scoped control is serial control

Multiple control commutes with scoping as shown in [figure 4.23](#) to [figure 4.24](#) on the following page.

4.5 An alternate description of quantum circuits

In order to explore transforms of quantum circuits, it is helpful to have an algebraic description which will allow manipulation of the circuits. The goals of the algebraic description are:

- Represent **qubits** and **bits**;
- represent gates;
- allow algorithmic manipulations of the circuit;
- allow proving that correctness of manipulations.

Note that measurement is not included in this representation.

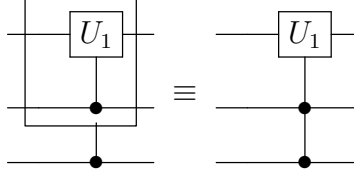


Figure 4.23: Multiple control

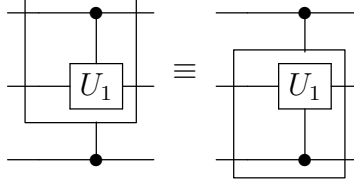


Figure 4.24: Control scopes commute

4.5.1 Base types

The base types **bit** and **qubit** are needed for any circuit. These will be taken as elemental and correspond to the classical notions of “bit” (i.e., 0 or 1) and “qubit” (i.e., $\alpha|0\rangle + \beta|1\rangle$).

Definition 4.5.1. The type **endpoint** is either **bit** or **qubit**.

Definition 4.5.2. The type **Q – Arity** is a partial map from $W \subset \mathbb{N}$ to **Endpoint**.

Definition 4.5.3. A *wire* is an element of $W \subset \mathbb{N}$. A *typed wire* is a wire together with a specified **Q – Arity**.

Definition 4.5.4. 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 4.5.5. 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 [13].

4.5.2 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.

Definition 4.5.6. 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 4.5.7. The type family **QCData** consists of algebraic data types built up from **bit** or **qubit**.

Examples of **QCData** include $(\mathbf{bit}, \mathbf{qubit}, [\mathbf{qubit}])$ and **bit**.

Definition 4.5.8. 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 **qubits** 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.

Chapter 5

Transformations of Quantum Programs

5.1 Subroutines

In the following, we will assume *gate* as above is a given and that $W \subset \mathbb{N}$ is fixed and finite.

We will use typing notation to show membership in W — $w \in W$ is equivalent to $w :: W$.

5.1.1 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 5.1.1. 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 5.1.2. 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

$$\text{dom } C \cap \text{dom } I = \phi \tag{5.1}$$

$$\text{dom } C \cap \text{dom } O = \phi \tag{5.2}$$

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 5.1.3. 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 5.1.4. An *ordering* of a low level subroutine is a pair of bijections, (i, o) such that:

$$i : \text{dom } C \cup \text{dom } I \leftrightarrow \{0, 1, \dots, n - 1\} \quad (5.3)$$

$$o : \text{dom } C \cup \text{dom } O \leftrightarrow \{0, 1, \dots, m - 1\} \quad (5.4)$$

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

5.1.2 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 5.1.5. 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 5.1.6. 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 $(f, g, h, i, ncf, ctrl)$ 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:

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

5.1.3 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 5.1.7. 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 5.1.8. Given the data for a subroutine call as above in 5.1.6 on the previous page, a *structured subroutine call* is a high level structure as in 5.1.7 and a pair of quantum terms (a, b) such that:

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

5.2 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 sub-section 5.1.2 on the previous page.

5.2.1 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 5.2.1. Given a subroutine as in [sub-section 5.1.2 on page 60](#), and a subroutine call $(f, g, h, i, ncf, ctrl_s)$ an *iterated call* of the subroutine $S = ([gates], C, I, O, r, c, n)$ consists of all elements of a subroutine call excepting f plus another tuple of five elements $(f_{in}, f_{out}, c_b, io_b, i_{count})$ where:

- $f_{in} : \text{dom } C \rightarrow W_1 \cap W_2$
- $f_{out} : \text{dom } C \rightarrow W_1 \cap W_2$
- i_{count} is a positive integer,
- c_b is a bijection (permutation) of C to C ,
- io_b is a bijection between I and O .

- $f_{in} + g \in F(C, I, W_1)$
- $f_{out} + h \in F(C, O, W_2)$
- The relation $f_{out} \circ c_b^{i_{count}} \circ f_{in}^{-1}$ is a function.

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

Definition 5.2.2. Given the data for an iterated call, a *structured iterated call* is a high level structure as in [5.1.7 on page 61](#) and a pair of quantum terms (a, b) such that:

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

From the definition, note the C wires may be permuted as desired, but the combination of the f_{in}^{-1} and the permutation must leave the wires in a state where f_{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: $f_{out} \circ c_b^{i_{count}} \circ f_{in}^{-1}$,
- In-out mapping: $h \circ i o_b^{i_{count}} \circ g^{-1}$.

Example 5.2.3 (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 5.2.4 (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 $(g, h, i, ncf, ctrls)$ 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

$$(w_1, w_4) \xrightarrow{f_{in}^{-1}} C = (w_1, w_1, w_4) \xrightarrow{(1,2,3)^5} C = (w_4, w_1, w_1) \xrightarrow{f_{out}} (w'_1(=w_1), w'_4(=w_4)) \quad (5.5)$$

$$(w_2, w_3) \xrightarrow{g^{-1}} I = (w_2, w_3) \xrightarrow{io_b^5 \circ S} O = (w_3, w_2) \xrightarrow{h} (w'_3(=w_3), w'_3(=w_3)) \quad (5.6)$$

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 .

5.2.2 Iteration transformation of a subroutine

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

Definition 5.2.5. The *iteration transform* of a subroutine is a function Σ_i with parameters (n, c_p, io_b) which takes the subroutine $S = (g, C, I, O, r, c, n)$ to $S'(g', C', I', O', r, c, n)$, an itere. The parameters have the following types:

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

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

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

The function Σ_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 $c_p^{n-1+k} = Id$. 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 5.1 on the following page](#)

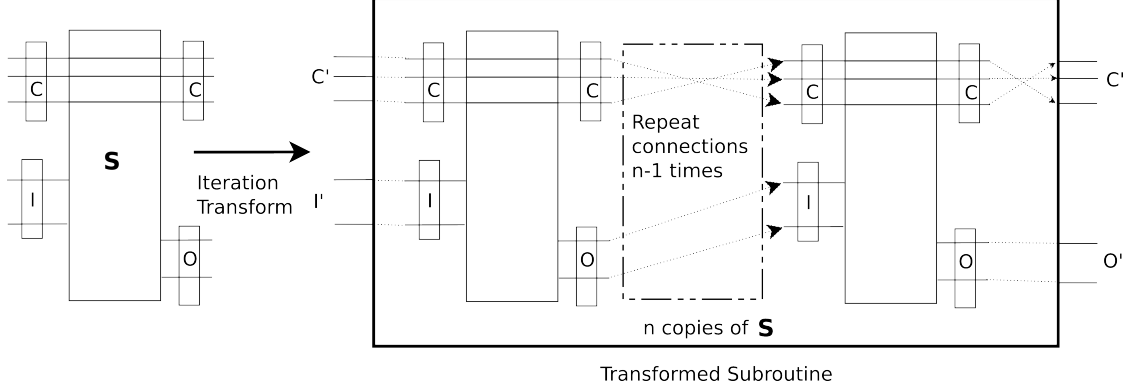


Figure 5.1: Transforming a subroutine to an iterated subroutine

5.2.3 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 5.2.6. Given a subroutine $S = ([gate], C, I, O, c, r, n)$, 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 $(CI_f, CO_f, g, h, ciofb, s_{in}, s_{out})$ 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,

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

Definition 5.2.7. 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:

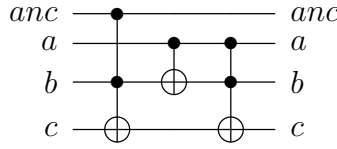
- Does the structured call get rid of the last two items regarding leafsize? Same issue with non-linear safe call.
- For the structured call, it appears to me that there is only one pair of terms a, b with two different (de)structuring morphisms.

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

$$s_{out} + h \circ (s_{out} + cio_f + s_{in})^{len(D)} \circ (g + s_{in})^{-1}.$$

Example 5.2.8 (Fold over Carry). For this example, we use the carry portion of the addition algorithm found in [15].

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:

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

From the mapping s_{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 [5.2.8 on the previous 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 rather than $F(C, K, W)$ we must use $F(\phi, C + K, W)$.

Definition 5.2.9. Given a subroutine $S = ([gate], C, I, O, c, r, n)$, 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 $(I_f, O_f, f_{in}, f_{out}, g, h, c_b, iof_b, s_{in}, s_{out})$ where

- $I_f :: \mathbf{Arity}, \text{dom } I_f \subset \text{dom } I$,
- $O_f :: \mathbf{Arity}, \text{dom } O_f \subset \text{dom } O$,
- $f_{in} : \text{dom } C \rightarrow W_1 \cup W_2$
- $f_{out} : \text{dom } C \rightarrow W_1 \cup W_2$
- $g : \text{dom } I / \text{dom } I_f \rightarrow W_1$
- $h : \text{dom } O / \text{dom } O_f \rightarrow W_2$
- c_b is a bijection (permutation) of C ,

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

Definition 5.2.10. 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:

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

5.2.4 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 5.2.11. The *fold transform* of a subroutine is a function S_f with parameters (n, b_{cio}) which takes the subroutine (g, C, I, O, r, c, n) to the subroutine $(g', C', I', O', r, c, n)$. The parameters have the following types:

$$\begin{aligned} n &:: \mathbf{Int}, n > 0; \\ b_{cio} &:: \mathbf{bijection}(\mathbf{CI} \leftrightarrow \mathbf{CO}) \\ &\text{where } CI \subseteq C \cup I \text{ and } \subseteq C \cup O. \end{aligned}$$

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

$$\{(f, t) | f \in C \cup I, t \in C \cup O, \text{ and } f, t \text{ appear at most once}\}. \quad (5.7)$$

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:

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

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

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

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

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

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

$$\Theta(c) = \begin{cases} c' & \text{if } b_{cio}(c') = c \text{ and } c' \in C, \\ * & \text{if } c \text{ is not the second element of any pair in } b_{cio}, \\ @ & \text{if } b_{cio}(o) = c \text{ and } o \in O. \end{cases}$$

$$\Delta :: C \rightarrow \mathbb{N} \cup \{\infty\}$$

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

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 Γ are required before confirming a value for $\Gamma(c)$. The same argument applies to computing Θ .

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, Γ is of complexity $\mathcal{O}(k \log k)$ and computing Γ for all of C will then be of $\mathcal{O}(k^2 \log k)$. Computing Δ 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_ℓ 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 $x = b_{cio}^{Rank(c)}(c)$. In C' , replace x_n with c_h . After completing this computation, remove any duplicates.

5.2.5 Examples of folding

Example 5.2.12. Consider $S = (-, \{a, b\}, \{c\}, \{d\}, -, -, -)$ and $b_{cio} = \{(a, c), (b, a)\}$ and an iteration count of 3. See [figure 5.2](#).

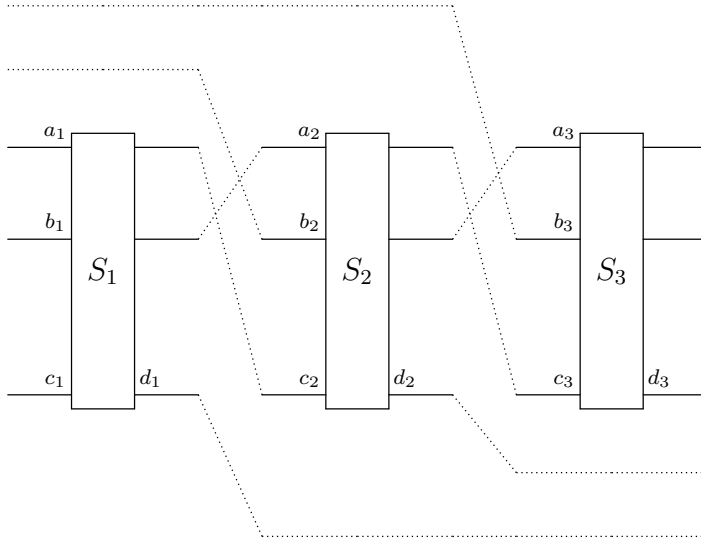


Figure 5.2: Fold with extra in/out

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 5.2.13. Consider $S = (-, \{a, b\}, \{c\}, \{d\}, -, -, -)$ as in 5.2.12 on page 74 and $b_{cio} = \{(a, c), (b, a), (d, b)\}$ and an iteration count of 3. See figure 5.3.

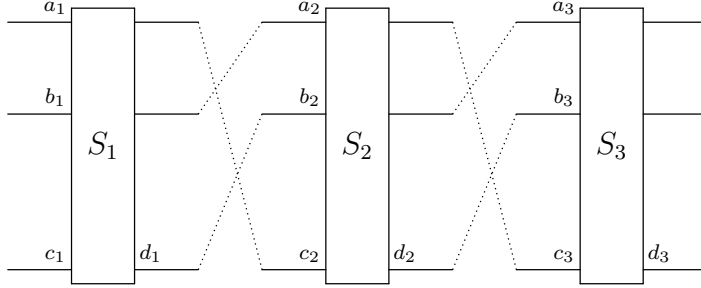


Figure 5.3: Fold with three iterations

From the data, we have:

$$\begin{aligned}
 \Omega(a) &= @ \text{ and} & \Gamma(a) &= 0, \\
 \Omega(b) &= a \text{ and} & \Gamma(b) &= 1, \\
 \Theta(b) &= @ \text{ and} & \Delta(b) &= 0, \\
 \Theta(a) &= b \text{ and} & \Delta(a) &= 1.
 \end{aligned}$$

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 5.2.14. Consider $C = (-, \{r, a\}, \{b, c\}, \{d, e\}, -, -, -)$, $b_{cio} = \{(e, r)\}$ and an iteration count of 4. See [figure 5.4](#).

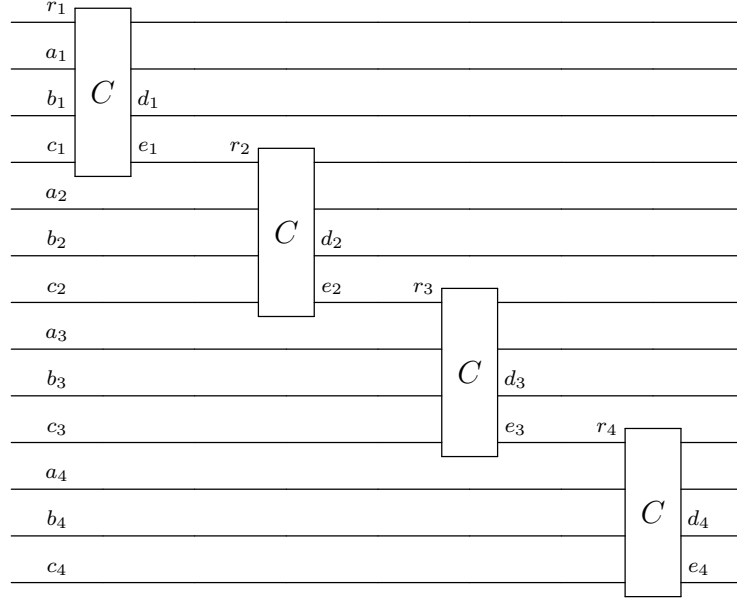


Figure 5.4: Fold of Carry

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 is in b_{cio} , therefore we 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:

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

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

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

5.3 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 [5.2.11 on page 71](#) 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.

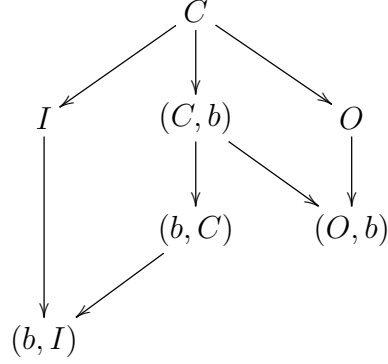
The algorithm steps are:

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, ϕ)
 - (b) For all $c \in C_j$, if $(-, c) \notin \mathcal{C}$, add the pair (ϕ, c)
 - (c) For all $o \in O_j$, if $(o, -) \notin \mathcal{C}$, add the pair (o, ϕ)
 - (d) For all $i \in I_j$, if $(-, i) \notin \mathcal{C}$, add the pair (ϕ, 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”.

5.3.1 Examples of folding with Alternate Algorithm

Example 5.3.1. We repeat 5.2.12 on page 74, that is, $S = (-, \{a, b\}, \{c\}, \{d\}, -, -, -)$ and $b_{cio} = \{(a, c), (b, a), (d, b)\}$ and an iteration count of 3. See figure 5.3 on page 76.

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:

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

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.

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

Chapter 6

Synthesis of quantum operations

6.1 Introduction to synthesis

An important problem in quantum information theory is the decomposition of arbitrary unitary operators into gates from some fixed universal set [10]. Depending on the operator to be decomposed, this may either be done exactly or to within some given accuracy ϵ ; the former problem is known as *exact synthesis* and the latter as *approximate synthesis* [8].

6.2 Exact synthesis of multi-qubit operators

Here, we focus on the problem of exact synthesis for n -qubit operators, using the Clifford+ T universal gate set. Recall that the Clifford group on n qubits is generated by the Hadamard gate H , the phase gate S , the controlled-not gate, and the scalar $\omega = e^{i\pi/4}$ (one may allow arbitrary unit scalars, but it is not convenient for our purposes to do so). It is well-known that one obtains a universal gate set by adding the non-Clifford operator T [10].

$$\begin{aligned} \omega = e^{i\pi/4}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \\ CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \end{aligned} \tag{6.1}$$

In addition to the Clifford+ T group on n qubits, as defined above, we also consider the slightly larger group of Clifford+ T operators “with ancillas”. We say that an n -qubit operator U is a Clifford+ T operator *with ancillas* if there exists $m \geq 0$ and a Clifford+ T

operator U' on $n + m$ qubits, such that $U'(|\phi\rangle \otimes |0\rangle) = (U|\phi\rangle) \otimes |0\rangle$ for all n -qubit states $|\phi\rangle$.

Kliuchnikov, Maslov, and Mosca [8] showed that a single-qubit operator U is in the Clifford+ T group if and only if all of its matrix entries belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. They also showed that the Clifford+ T groups “with ancillas” and “without ancillas” coincide for $n = 1$, but not for $n \geq 2$. Moreover, Kliuchnikov et al. conjectured that for all n , an n -qubit operator U is in the Clifford+ T group with ancillas if and only if its matrix entries belong to $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. They also conjectured that a single ancilla qubit is always sufficient in the representation of a Clifford+ T operator with ancillas. This section of the thesis will prove these conjectures. In particular, this yields an algorithm for exact Clifford+ T synthesis of n -qubit operators. We also obtain a characterization of the Clifford+ T group on n qubits without ancillas.

It is important to note that, unlike in the single-qubit case, the circuit synthesized here are not in any sense canonical, and very far from optimal. Thus, the question of *efficient* synthesis is not addressed here.

6.2.1 Algebraic background

We first introduce some notation and terminology, following [8] where possible. Recall that \mathbb{N} is the set of natural numbers including 0, and \mathbb{Z} is the ring of integers. We write $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ for the ring of integers modulo 2. Let \mathbb{D} be the ring of *dyadic fractions*, defined as $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$.

Let $\omega = e^{i\pi/4} = (1 + i)/\sqrt{2}$. Note that ω is an 8th root of unity satisfying $\omega^2 = i$ and $\omega^4 = -1$. We will consider three different rings related to ω :

Definition 6.2.1. Consider the following rings. Note that the first two are subrings of the complex numbers, and the third one is not:

- $\mathbb{D}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{D}\}$.

- $\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{Z}\}.$
- $\mathbb{Z}_2[\omega] = \{p\omega^3 + q\omega^2 + r\omega + s \mid p, q, r, s \in \mathbb{Z}_2\}.$

Note that the ring $\mathbb{Z}_2[\omega]$ only has 16 elements. The laws of addition and multiplication are uniquely determined by the ring axioms and the property $\omega^4 = 1 \pmod{2}$. We call the elements of $\mathbb{Z}_2[\omega]$ *residues* (more precisely, residue classes of $\mathbb{Z}[\omega]$ modulo 2).

Remark 6.2.2. The ring $\mathbb{D}[\omega]$ is the same as the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ mentioned in the statement of Theorem 6.2.22. However, as already pointed out in [8], the formulation in terms of ω is far more convenient algebraically.

Remark 6.2.3. The ring $\mathbb{Z}[\omega]$ is also called the *ring of algebraic integers* of $\mathbb{D}[\omega]$. It has an intrinsic definition, i.e., one that is independent of the particular presentation of $\mathbb{D}[\omega]$. Namely, a complex number is called an *algebraic integer* if it is the root of some polynomial with integer coefficients and leading coefficient 1. It follows that ω , i , and $\sqrt{2}$ are algebraic integers, whereas, for example, $1/\sqrt{2}$ is not. The ring $\mathbb{Z}[\omega]$ then consists of precisely those elements of $\mathbb{D}[\omega]$ that are algebraic integers.

Conjugate and norm

Remark 6.2.4 (Complex conjugate and norm). Since $\mathbb{D}[\omega]$ and $\mathbb{Z}[\omega]$ are subrings of the complex numbers, they inherit the usual notion of complex conjugation. We note that $\omega^\dagger = -\omega^3$. This yields the following formula:

$$(a\omega^3 + b\omega^2 + c\omega + d)^\dagger = -c\omega^3 - b\omega^2 - a\omega + d. \quad (6.2)$$

Similarly, the sets $\mathbb{D}[\omega]$ and $\mathbb{Z}[\omega]$ inherit the usual norm from the complex numbers. It is given by the following explicit formula, for $t = a\omega^3 + b\omega^2 + c\omega + d$:

$$\|t\|^2 = t^\dagger t = (a^2 + b^2 + c^2 + d^2) + (cd + bc + ab - da)\sqrt{2}. \quad (6.3)$$

Definition 6.2.5 (Weight). For $t \in \mathbb{D}[\omega]$ or $t \in \mathbb{Z}[\omega]$, the *weight* of t is denoted $\|t\|_{\text{weight}}$, and is given by:

$$\|t\|_{\text{weight}}^2 = a^2 + b^2 + c^2 + d^2. \quad (6.4)$$

Note that the square of the norm is valued in $\mathbb{D}[\sqrt{2}]$, whereas the square of the weight is valued in \mathbb{D} . We also extend the definition of norm and weight to vectors in the obvious way: For $u = (u_j)_j$, we define

$$\|u\|^2 = \sum_j \|u_j\|^2 \quad \text{and} \quad \|u\|_{\text{weight}}^2 = \sum_j \|u_j\|_{\text{weight}}^2.$$

Lemma 6.2.6. Consider a vector $u \in \mathbb{D}[\omega]^n$. If $\|u\|^2$ is an integer, then $\|u\|_{\text{weight}}^2 = \|u\|^2$.

Proof. Any $t \in \mathbb{D}[\sqrt{2}]$ can be uniquely written as $t = a + b\sqrt{2}$, where $a, b \in \mathbb{D}$. We can call a the *dyadic part* of t . Now the claim is obvious, because $\|u\|_{\text{weight}}^2$ is exactly the dyadic part of $\|u\|^2$. \square

Denominator exponents

Definition 6.2.7. Let $t \in \mathbb{D}[\omega]$. A natural number $k \in \mathbb{N}$ is called a *denominator exponent* for t if $\sqrt{2}^k t \in \mathbb{Z}[\omega]$. It is obvious that such k always exists. The least such k is called the *least denominator exponent* of t .

More generally, we say that k is a denominator exponent for a vector or matrix if it is a denominator exponent for all of its entries. The least denominator exponent for a vector or matrix is therefore the least k that is a denominator exponent for all of its entries.

Remark 6.2.8. Our notion of least denominator exponent is almost the same as the “smallest denominator exponent” of [8], except that we do not permit $k < 0$.

Residues

Remark 6.2.9. The ring $\mathbb{Z}_2[\omega]$ is not a subring of the complex numbers; rather, it is a quotient of the ring $\mathbb{Z}[\omega]$. Indeed, consider the *parity function* $\overline{(\cdot)} : \mathbb{Z} \rightarrow \mathbb{Z}_2$, which is the

$\rho(t)$	$\rho(\sqrt{2}t)$	$\rho(t^\dagger t)$	$\rho(t)$	$\rho(\sqrt{2}t)$	$\rho(t^\dagger t)$
0000	0000	0000	1000	0101	0001
0001	1010	0001	1001	1111	1010
0010	0101	0001	1010	0000	0000
0011	1111	1010	1011	1010	0001
0100	1010	0001	1100	1111	1010
0101	0000	0000	1101	0101	0001
0110	1111	1010	1110	1010	0001
0111	0101	0001	1111	0000	0000

Table 6.1: Some operations on residues

unique ring homomorphism. It satisfies $\bar{a} = 0$ if a is even and $\bar{a} = 1$ if a is odd. The parity map induces a surjective ring homomorphism $\rho : \mathbb{Z}[\omega] \rightarrow \mathbb{Z}_2[\omega]$, defined by

$$\rho(a\omega^3 + b\omega^2 + c\omega + d) = \bar{a}\omega^3 + \bar{b}\omega^2 + \bar{c}\omega + \bar{d}.$$

We call ρ the *residue map*, and we call $\rho(t)$ the *residue* of t .

Convention 6.2.10. Since residues will be important for the constructions of this paper, we introduce a shortcut notation, writing each residue $p\omega^3 + q\omega^2 + r\omega + s$ as a string of binary digits $pqrs$.

What makes residues useful for our purposes is that many important operations on $\mathbb{Z}[\omega]$ are well-defined on residues. Here, we say that an operation $f : \mathbb{Z}[\omega] \rightarrow \mathbb{Z}[\omega]$ is *well-defined on residues* if for all t, s , $\rho(t) = \rho(s)$ implies $\rho(f(t)) = \rho(f(s))$.

For example, two operations that are obviously well-defined on residues are complex conjugation, which takes the form $(pqrs)^\dagger = rqps$ by (equation (6.2)), and multiplication by ω , which is just a cyclic shift $\omega(pqrs) = qrsp$. Table table 6.1 shows two other important operations on residues, namely multiplication by $\sqrt{2}$ and the squared norm.

Definition 6.2.11 (k -Residue). Let $t \in \mathbb{D}[\omega]$ and let k be a (not necessarily least) denominator exponent for t . The k -residue of t , in symbols $\rho_k(t)$, is defined to be

$$\rho_k(t) = \rho(\sqrt{2}^k t).$$

Definition 6.2.12 (Reducibility). We say that a residue $x \in \mathbb{Z}_2[\omega]$ is *reducible* if it is of the form $\sqrt{2}y$, for some $y \in \mathbb{Z}_2[\omega]$. Moreover, we say that $x \in \mathbb{Z}_2[\omega]$ is *twice reducible* if it is of the form $2y$, for some $y \in \mathbb{Z}_2[\omega]$.

Lemma 6.2.13. *For a residue x , the following are equivalent:*

- (a) x is reducible;
- (b) $x \in \{0000, 0101, 1010, 1111\}$;
- (c) $\sqrt{2}x = 0000$;
- (d) $x^\dagger x = 0000$.

Moreover, x is twice reducible iff $x = 0000$.

Proof. By inspection of Table [table 6.1](#). □

Lemma 6.2.14. *Let $t \in \mathbb{Z}[\omega]$. Then $t/2 \in \mathbb{Z}[\omega]$ if and only if $\rho(t)$ is twice reducible, and $t/\sqrt{2} \in \mathbb{Z}[\omega]$ if and only if $\rho(t)$ is reducible.*

Proof. The first claim is trivial, as $\rho(t) = 0000$ if and only if all components of t are even. For the second claim, the left-to-right implication is also trivial: assume $t' = t/\sqrt{2} \in \mathbb{Z}[\omega]$. Then $\rho(t) = \rho(\sqrt{2}t')$, which is reducible by definition. Conversely, let $t \in \mathbb{Z}[\omega]$ and assume that $\rho(t)$ is reducible. Then $\rho(t) \in \{0000, 0101, 1010, 1111\}$, and it can be seen from Table [table 6.1](#) that $\rho(\sqrt{2}t) = 0000$. Therefore, $\sqrt{2}t$ is twice reducible by the first claim; hence t is reducible. □

Corollary 6.2.15. *Let $t \in \mathbb{D}[\omega]$ and let $k > 0$ be a denominator exponent for t . Then k is the least denominator exponent for t if and only if $\rho_k(t)$ is irreducible.*

Proof. Since k is a denominator exponent for t , we have $\sqrt{2}^k t \in \mathbb{Z}[\omega]$. Moreover, k is least if and only if $\sqrt{2}^{k-1} t \notin \mathbb{Z}[\omega]$. By Lemma [6.2.14](#), this is the case if and only if $\rho(\sqrt{2}^k t) = \rho_k(t)$ is irreducible. □

Definition 6.2.16. The notions of residue, k -residue, reducibility, and twice-reducibility all extend in an obvious componentwise way to vectors and matrices. Thus, the residue $\rho(u)$ of a vector or matrix u is obtained by taking the residue of each of its entries, and similar for k -residues. Also, we say that a vector or matrix is reducible if each of its entries is reducible, and similarly for twice-reducibility.

Example 6.2.17. Consider the matrix

$$U = \frac{1}{\sqrt{2}^3} \begin{pmatrix} -\omega^3 + \omega - 1 & \omega^2 + \omega + 1 & \omega^2 & -\omega \\ \omega^2 + \omega & -\omega^3 + \omega^2 & -\omega^2 - 1 & \omega^3 + \omega \\ \omega^3 + \omega^2 & -\omega^3 - 1 & 2\omega^2 & 0 \\ -1 & \omega & 1 & -\omega^3 + 2\omega \end{pmatrix}.$$

It has least denominator exponent 3. Its 3-, 4-, and 5-residues are:

$$\begin{aligned} \rho_3(U) &= \begin{pmatrix} 1011 & 0111 & 0100 & 0010 \\ 0110 & 1100 & 0101 & 1010 \\ 1100 & 1001 & 0000 & 0000 \\ 0001 & 0010 & 0001 & 1000 \end{pmatrix}, \\ \rho_4(U) &= \begin{pmatrix} 1010 & 0101 & 1010 & 0101 \\ 1111 & 1111 & 0000 & 0000 \\ 1111 & 1111 & 0000 & 0000 \\ 1010 & 0101 & 1010 & 0101 \end{pmatrix}, \quad \rho_5(U) = 0. \end{aligned}$$

6.2.2 Decomposition into two-level matrices

Recall that a *two-level matrix* is an $n \times n$ -matrix that acts non-trivially on at most two vector components [10]. If

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a 2×2 -matrix and $j \neq \ell$, we write $U_{[j,\ell]}$ for the two-level $n \times n$ -matrix defined by

$$U_{[j,\ell]} = \begin{matrix} & \dots & j & \dots & \ell & \dots \\ \vdots & \left(\begin{array}{c|c|c|c|c} I & & & & \\ \hline & a & & b & \\ \hline & & I & & \\ \hline & c & & d & \\ \hline & & & & I \end{array} \right) & \\ j & & & & & \\ \vdots & & & & & \\ \ell & & & & & \\ \vdots & & & & & \end{matrix},$$

and we say that $U_{[j,\ell]}$ is a two-level matrix *of type U*. Similarly, if a is a scalar, we write $a_{[j]}$ for the one-level matrix

$$a_{[j]} = \begin{matrix} & \dots & j & \dots \\ \vdots & \left(\begin{array}{c|c|c} I & & \\ \hline & a & \\ \hline & & I \end{array} \right) & \\ j & & & \\ \vdots & & & \end{matrix},$$

and we say that $a_{[j]}$ is a one-level matrix *of type a*.

Lemma 6.2.18 (Row operation). *Let $u = (u_1, u_2)^T \in \mathbb{D}[\omega]^2$ be a vector with denominator exponent $k > 0$ and k -residue $\rho_k(u) = (x_1, x_2)$, such that $x_1^\dagger x_1 = x_2^\dagger x_2$. Then there exists a sequence of matrices U_1, \dots, U_h , each of which is H or T , such that $v = U_1 \cdots U_h u$ has denominator exponent $k - 1$, or equivalently, $\rho_k(v)$ is defined and reducible.*

Proof. It can be seen from Table [table 6.1](#) that $x_1^\dagger x_1$ is either 0000, 1010, or 0001.

- Case 1: $x_1^\dagger x_1 = x_2^\dagger x_2 = 0000$. In this case, $\rho_k(u)$ is already reducible, and there is nothing to show.
- Case 2: $x_1^\dagger x_1 = x_2^\dagger x_2 = 1010$. In this case, we know from Table [table 6.1](#) that $x_1, x_2 \in \{0011, 0110, 1100, 1001\}$. In particular, x_1 is a cyclic permutation of

x_2 , say, $x_1 = \omega^m x_2$. Let $v = HT^m u$. Then

$$\begin{aligned}\rho_k(\sqrt{2}v) &= \rho_k\left(\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \omega^m \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}\right) \\ &= \rho_k\begin{pmatrix} u_1 + \omega^m u_2 \\ u_1 - \omega^m u_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + \omega^m x_2 \\ x_1 - \omega^m x_2 \end{pmatrix} = \begin{pmatrix} 0000 \\ 0000 \end{pmatrix}.\end{aligned}$$

This shows that $\rho_k(\sqrt{2}v)$ is twice reducible; therefore, $\rho_k(v)$ is defined and reducible as claimed.

- Case 3: $x_1^\dagger x_1 = x_2^\dagger x_2 = 0001$. In this case, we know from Table [table 6.1](#) that $x_1, x_2 \in \{0001, 0010, 0100, 1000\} \cup \{0111, 1110, 1101, 1011\}$. If both x_1, x_2 are in the first set, or both are in the second set, then x_1 and x_2 are cyclic permutations of each other, and we proceed as in case 2. The only remaining cases are that x_1 is a cyclic permutation of 0001 and x_2 is a cyclic permutation of 0111, or vice versa. But then there exists some m such that $x_1 + \omega^m x_2 = 1111$. Letting $u' = HT^m u$, we have

$$\begin{aligned}\rho_k(\sqrt{2}u') &= \rho_k\left(\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \omega^m \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}\right) \\ &= \rho_k\begin{pmatrix} u_1 + \omega^m u_2 \\ u_1 - \omega^m u_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + \omega^m x_2 \\ x_1 - \omega^m x_2 \end{pmatrix} = \begin{pmatrix} 1111 \\ 1111 \end{pmatrix}.\end{aligned}$$

Since this is reducible, u' has denominator exponent k . Let $\rho_k(u') = (y_1, y_2)$. Because $\sqrt{2}y_1 = \sqrt{2}y_2 = 1111$, we see from Table [table 6.1](#) that $y_1, y_2 \in \{0011, 0110, 1100, 1001\}$ and $y_1^\dagger y_1 = y_2^\dagger y_2 = 1010$. Therefore, u' satisfies the condition of case 2 above. Proceeding as in case 2, we find m' such that $v = HT^{m'} u' = HT^{m'} HT^m u$ has denominator exponent $k - 1$. This finishes the proof. \square

Lemma 6.2.19 (Column lemma). *Consider a unit vector $u \in \mathbb{D}[\omega]^n$, i.e., an n -dimensional column vector of norm 1 with entries from the ring $\mathbb{D}[\omega]$. Then there exist a sequence U_1, \dots, U_h of one- and two-level unitary matrices of types X , H , T , and ω such that $U_1 \cdots U_h u = e_1$, the first standard basis vector.*

Proof. The proof is by induction on k , the least denominator exponent of u . Let $u = (u_1, \dots, u_n)^T$.

- Base case. Suppose $k = 0$. Then $u \in \mathbb{Z}[\omega]^n$. Since by assumption $\|u\|^2 = 1$, it follows by Lemma 6.2.6 that $\|u\|_{\text{weight}}^2 = 1$. Since u_1, \dots, u_n are elements of $\mathbb{Z}[\omega]$, their weights are non-negative integers. It follows that there is precisely one j with $\|u_j\|_{\text{weight}} = 1$, and $\|u_\ell\|_{\text{weight}} = 0$ for all $\ell \neq j$. Let $u' = X_{[1,j]}u$ if $j \neq 1$, and $u' = u$ otherwise. Now u'_1 is of the form ω^{-m} , for some $m \in \{0, \dots, 7\}$, and $u'_\ell = 0$ for all $\ell \neq 1$. We have $\omega_{[1]}^m u' = e_1$, as desired.
- Induction step. Suppose $k > 0$. Let $v = \sqrt{2}^k u \in \mathbb{Z}[\omega]^n$, and let $x = \rho_k(u) = \rho(v)$. From $\|u\|^2 = 1$, it follows that $\|v\|^2 = v_1^\dagger v_1 + \dots + v_n^\dagger v_n = 2^k$. Taking residues of the last equation, we have

$$x_1^\dagger x_1 + \dots + x_n^\dagger x_n = 0000. \quad (6.5)$$

It can be seen from Table table 6.1 that each summand $x_j^\dagger x_j$ is either 0000, 0001, or 1010. Since their sum is 0000, it follows that there is an even number of j such that $x_j^\dagger x_j = 0001$, and an even number of j such that $x_j^\dagger x_j = 1010$. We do an inner induction on the number of irreducible components of x . If x is reducible, then u has denominator exponent $k - 1$ by Corollary 6.2.15, and we can apply the outer induction hypothesis. Now suppose there is some j such that x_j is irreducible; then $x_j^\dagger x_j \neq 0000$ by Lemma 6.2.13. Because of the evenness property noted above, there must exist some $\ell \neq j$ such that $x_j^\dagger x_j = x_\ell^\dagger x_\ell$. Applying Lemma 6.2.18 to $u' = (u_j, u_\ell)^T$, we find a sequence \vec{U} of

row operations of types H and T , making $\rho_k(\vec{U}u')$ reducible. We can lift this to a two-level operation $\vec{U}_{[j,\ell]}$ acting on u ; thus $\rho_k(\vec{U}_{[j,\ell]}u)$ has fewer irreducible components than $x = \rho_k(u)$, and the inner induction hypothesis applies. \square

Lemma 6.2.20 (Matrix decomposition). *Let U be a unitary $n \times n$ -matrix with entries in $\mathbb{D}[\omega]$. Then there exists a sequence U_1, \dots, U_h of one- and two-level unitary matrices of types X, H, T , and ω such that $U = U_1 \cdots U_h$.*

Proof. Equivalently, it suffices to show that there exist one- and two-level unitary matrices V_1, \dots, V_h of types X, H, T , and ω such that $V_h \cdots V_1 U = I$. This is an easy consequence of the column lemma, exactly as in e.g. [10, Sec. 4.5.1]. Specifically, first use the column lemma to find suitable one- and two-level row operations V_1, \dots, V_{h_1} such that the leftmost column of $V_{h_1} \cdots V_1 U$ is e_1 . Because $V_{h_1} \cdots V_1 U$ is unitary, it is of the form

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & U' \end{array} \right).$$

Now recursively find row operations to reduce U' to the identity matrix. \square

Example 6.2.21. We will decompose the matrix U from Example 6.2.17. We start with the first column u of U :

$$u = \frac{1}{\sqrt{2}^3} \begin{pmatrix} -\omega^3 + \omega - 1 \\ \omega^2 + \omega \\ \omega^3 + \omega^2 \\ -1 \end{pmatrix},$$

$$\rho_3(u) = \begin{pmatrix} 1011 \\ 0110 \\ 1100 \\ 0001 \end{pmatrix}, \quad \rho_3(u_j^\dagger u_j) = \begin{pmatrix} 0001 \\ 1010 \\ 1010 \\ 0001 \end{pmatrix}.$$

Rows 2 and 3 satisfy case 2 of Lemma 6.2.18. As they are not aligned, first apply $T_{[2,3]}^3$ and then $H_{[2,3]}$. Rows 1 and 4 satisfy case 3. Applying $H_{[1,4]}T_{[1,4]}^2$, the residues become

$\rho_3(u'_1) = 0011$ and $\rho_3(u'_4) = 1001$, which requires applying $H_{[1,4]}T_{[1,4]}$. We now have

$$H_{[1,4]}T_{[1,4]}H_{[1,4]}T_{[1,4]}^2H_{[2,3]}T_{[2,3]}^3u = v = \frac{1}{\sqrt{2}^2} \begin{pmatrix} 0 \\ 0 \\ \omega^2 + \omega \\ -\omega + 1 \end{pmatrix},$$

$$\rho_2(v) = \begin{pmatrix} 0000 \\ 0000 \\ 0110 \\ 0011 \end{pmatrix}, \quad \rho_2(v_j^\dagger v_j) = \begin{pmatrix} 0000 \\ 0000 \\ 1010 \\ 1010 \end{pmatrix}.$$

Rows 3 and 4 satisfy case 2, while rows 1 and 2 are already reduced. We reduce rows 3 and 4 by applying $H_{[3,4]}T_{[3,4]}$. Continuing, the first column is completely reduced to e_1 by further applying $\omega_{[1]}^7 X_{[1,4]} H_{[3,4]} T_{[3,4]}^3$. The complete decomposition of u is therefore given by

$$W_1 = \omega_{[1]}^7 X_{[1,4]} H_{[3,4]} T_{[3,4]}^3 H_{[3,4]} T_{[3,4]} \\ H_{[1,4]} T_{[1,4]} H_{[1,4]} T_{[1,4]}^2 H_{[2,3]} T_{[2,3]}^3.$$

Applying this to the original matrix U , we have $W_1 U =$

$$\frac{1}{\sqrt{2}^3} \begin{pmatrix} \sqrt{2}^3 & 0 & 0 & 0 \\ 0 & \omega^3 - \omega^2 + \omega + 1 & -\omega^2 - \omega - 1 & \omega^2 \\ 0 & 0 & \omega^3 + \omega^2 - \omega + 1 & \omega^3 + \omega^2 - \omega - 1 \\ 0 & \omega^3 + \omega^2 + \omega + 1 & \omega^2 & \omega^3 - \omega^2 + 1 \end{pmatrix}.$$

Continuing with the rest of the columns, we find $W_2 = \omega_{[2]}^6 H_{[2,4]} T_{[2,4]}^3 H_{[2,4]} T_{[2,4]}$, $W_3 = \omega_{[3]}^4 H_{[3,4]} T_{[3,4]}^3 H_{[3,4]}$, and $W_4 = \omega_{[4]}^5$. We then have $U = W_1^\dagger W_2^\dagger W_3^\dagger W_4^\dagger$, or explicitly:

$$U = T_{[2,3]}^5 H_{[2,3]} T_{[1,4]}^6 H_{[1,4]} T_{[1,4]}^7 H_{[1,4]} \\ T_{[3,4]}^7 H_{[3,4]} T_{[3,4]}^5 H_{[3,4]} X_{[1,4]} \omega_{[1]} \\ T_{[2,4]}^7 H_{[2,4]} T_{[2,4]}^5 H_{[2,4]} \omega_{[2]}^2 H_{[3,4]} T_{[3,4]}^5 H_{[3,4]} \omega_{[3]}^4 \omega_{[4]}^3.$$

6.2.3 Main result

Consider the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$, consisting of complex numbers of the form

$$\frac{1}{2^n} (a + bi + c\sqrt{2} + di\sqrt{2}),$$

where $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. Our goal is to prove the following theorem, which was conjectured by Kliuchnikov et al. [8]:

Theorem 6.2.22. *Let U be a unitary $2^n \times 2^n$ matrix. Then the following are equivalent:*

- (a) *U can be exactly represented by a quantum circuit over the Clifford+ T gate set, possibly using some finite number of ancillas that are initialized and finalized in state $|0\rangle$.*
- (b) *The entries of U belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$.*

Moreover, in (a), a single ancilla is always sufficient.

Proof. First note that, since all the elementary Clifford+ T gates, as shown in (equation (6.1)), take their matrix entries in $\mathbb{D}[\omega] = \mathbb{Z}[\frac{1}{\sqrt{2}}, i]$, the implication (a) \implies (b) is trivial. For the converse, let U be a unitary $2^n \times 2^n$ matrix with entries from $\mathbb{D}[\omega]$. By Lemma 6.2.20, U can be decomposed into one- and two-level matrices of types X , H , T , and ω . It is well-known that each such matrix can be further decomposed into controlled-not gates and multiply-controlled X , H , T , and ω -gates, for example using Gray codes [10, Sec. 4.5.2]. But all of these gates have well-known exact representations in Clifford+ T with ancillas, see e.g. [2, Fig. 4(a) and Fig. 9] (and noting that a controlled- ω gate is the same as a T -gate). This finishes the proof of (b) \implies (a).

The final claim that needs to be proved is that a circuit for U can always be found using at most one ancilla. It is already known that for $n > 1$, an ancilla is sometimes necessary [8]. To show that a single ancilla is sufficient, in light of the above decomposition, it is enough to show that the following can be implemented with one ancilla:

- (a) a multiply-controlled X -gate;
- (b) a multiply-controlled H -gate;
- (c) a multiply-controlled T -gate.

We first recall from [2, Fig. 4(a)] that a singly-controlled Hadamard gate can be decomposed into Clifford+ T gates with no ancillas:

$$\begin{array}{c} \bullet \\ | \\ \text{---} [H] \text{---} \end{array} = \begin{array}{c} \bullet \\ | \\ \text{---} [S] [H] [T] \oplus [T^\dagger] [H] [S^\dagger] \text{---} \end{array}$$

We also recall that an n -fold controlled iX -gate can be represented using $O(n)$ Clifford+ T gates with no ancillas. Namely, for $n = 1$, we have

$$\text{Controlled-}iX = \text{Controlled-}S \circ \text{CNOT},$$

and for $n \geq 2$, we can use

with further decompositions of the multiply-controlled not-gates as in [3, Lem. 7.2] and [10, Fig. 4.9]. We then obtain the following representations for (a)–(c), using only one ancilla:

Figure 1 illustrates three quantum circuit identities for multi-controlled gates. Each part (a), (b), and (c) shows an equivalence between a multi-controlled gate and a sequence of multi-controlled gates with decreasing numbers of controls, ending with a single-controlled gate.

- (a) **X gate identity:** A multi-controlled X gate (with n controls) is equivalent to a sequence of multi-controlled X gates with $n-1$, $n-2$, ..., 2, and 1 controls, followed by a single-controlled X gate.
- (b) **H gate identity:** A multi-controlled H gate (with n controls) is equivalent to a sequence of multi-controlled H gates with $n-1$, $n-2$, ..., 2, and 1 controls, followed by a single-controlled H gate.
- (c) **T gate identity:** A multi-controlled T gate (with n controls) is equivalent to a sequence of multi-controlled T gates with $n-1$, $n-2$, ..., 2, and 1 controls, followed by a single-controlled T gate.

☐

Remark 6.2.23. The fact that one ancilla is always sufficient in Theorem 6.2.22 is primarily of theoretical interest. In practice, one may assume that on most quantum computing architectures, ancillas are relatively cheap. Moreover, the use of additional ancillas can significantly reduce the size and depth of the generated circuits (see e.g. [14]).

6.2.4 The no-ancilla case

Lemma 6.2.24. *Under the hypotheses of Theorem 6.2.22, assume that $\det U = 1$. Then U can be exactly represented by a Clifford+ T circuit with no ancillas.*

Proof. This requires only minor modifications to the proof of Theorem 6.2.22. First observe that whenever an operator of the form HT^m was used in the proof of Lemma 6.2.18, we can instead use $T^{-m}(iH)T^m$ without altering the rest of the argument. In the base case of Lemma 6.2.19, the operator $X_{[1,j]}$ can be replaced by $iX_{[1,j]}$. Also, in the base case of Lemma 6.2.19, whenever $n \geq 2$, the operator $\omega_{[1]}$ can be replaced by $W_{[1,2]}$, where

$$W = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}.$$

Therefore, the decomposition of Lemma 6.2.20 can be performed so as to yield only two-level matrices of types

$$iX, \quad T^{-m}(iH)T^m, \quad \text{and } W, \tag{6.6}$$

plus at most one one-level matrix of type ω^m . But since all two-level matrices of types (equation (6.6)), as well as U itself, have determinant 1, it follows that $\omega^m = 1$. We finish the proof by observing that the multiply-controlled operators of types (equation (6.6)) possess ancilla-free Clifford+ T representations, with the latter two given by

$$\begin{array}{c} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} = \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \\ \boxed{T^{-m}(iH)T^m} \quad \boxed{T^m} \boxed{S} \boxed{H} \boxed{T} \boxed{iX} \boxed{T^\dagger} \boxed{H} \boxed{S^\dagger} \boxed{T^{-m}} \end{array}$$

$$\begin{array}{c} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} = \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \\ \boxed{W} \quad \boxed{iX} \boxed{T} \boxed{iX} \boxed{T^\dagger} \end{array}$$

□

As a corollary, we obtain a characterization of the n -qubit Clifford+ T group (with no ancillas) for all n :

Corollary 6.2.25. *Let U be a unitary $2^n \times 2^n$ matrix. Then the following are equivalent:*

(a) U can be exactly represented by a quantum circuit over the Clifford+ T gate set on n qubits with no ancillas.

(b) The entries of U belong to the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$, and:

- $\det U = 1$, if $n \geq 4$;
- $\det U \in \{-1, 1\}$, if $n = 3$;
- $\det U \in \{i, -1, -i, 1\}$, if $n = 2$;
- $\det U \in \{\omega, i, \omega^3, -1, \omega^5, -i, \omega^7, 1\}$, if $n \leq 1$.

Proof. For (a) \implies (b), it suffices to note that each of the generators of the Clifford+ T group, regarded as an operation on n qubits, satisfies the conditions in (b). For (b) \implies (a), let us define for convenience $d_0 = d_1 = \omega$, $d_2 = i$, $d_3 = -1$, and $d_n = 1$ for $n \geq 4$. First note that for all n , the Clifford+ T group on n qubits (without ancillas) contains an element D_n whose determinant is d_n , namely $D_n = I$ for $n \geq 4$, $D_3 = T \otimes I \otimes I$, $D_2 = T \otimes I$, $D_1 = T$, and $D_0 = \omega$. Now consider some U satisfying (b). By assumption, $\det U = d_n^m$ for some m . Let $U' = U D_n^{-m}$, then $\det U' = 1$. By Lemma 6.2.24, U' , and therefore U , is in the Clifford+ T group with no ancillas. \square

Remark 6.2.26. Note that the last condition in Corollary 6.2.25, namely that $\det U$ is a power of ω for $n \leq 1$, is of course redundant, as this already follows from $\det U \in \mathbb{Z}[\frac{1}{\sqrt{2}}, i]$ and $|\det U| = 1$. We stated the condition for consistency with the case $n \geq 2$.

Remark 6.2.27. The situation of Theorem 6.2.22 and Corollary 6.2.25 is analogous to the case of classical reversible circuits. It is well-known that the not-gate, controlled-not gate, and Toffoli gate generate all classical reversible functions on $n \leq 3$ bits. For $n \geq 4$ bits, they generate exactly those reversible boolean functions that define an *even permutation* of their inputs (or equivalently, those that have determinant 1 when viewed in matrix form) [9]; the addition of a single ancilla suffices to recover all boolean functions.

6.2.5 Complexity

The proof of Theorem 6.2.22 immediately yields an algorithm, albeit not a very efficient one, for synthesizing a Clifford+ T circuit with ancillas from a given operator U . We estimate the size of the generated circuits.

We first estimate the number of (one- and two-level) operations generated by the matrix decomposition of Lemma 6.2.20. The row operation from Lemma 6.2.18 requires only a constant number of operations. Reducing a single n -dimensional column from denominator exponent k to $k - 1$, as in the induction step of Lemma 6.2.19, requires $O(n)$ operations; therefore, the number of operations required to reduce the column completely is $O(nk)$.

Now consider applying Lemma 6.2.20 to an $n \times n$ -matrix with least denominator exponent k . Reducing the first column requires $O(nk)$ operations, but unfortunately, it may *increase* the least denominator exponent of the rest of the matrix, in the worst case, to $3k$. Namely, each row operation of Lemma 6.2.18 potentially increases the denominator exponent by 2, and any given row may be subject to up to k row operations, resulting in a worst-case increase of its denominator exponent from k to $3k$ during the reduction of the first column. It follows that reducing the second column requires up to $O(3(n - 1)k)$ operations, reducing the third column requires up to $O(9(n - 2)k)$ operations, and so on. Using the identity $\sum_{j=0}^{n-1} 3^j(n - j) = (3^{n+1} - 2n - 3)/4$, this results in a total of $O(3^n k)$ one- and two-level operations for Lemma 6.2.20.

In the context of Theorem 6.2.22, we are dealing with n qubits, i.e., a $2^n \times 2^n$ -operator, which therefore decomposes into $O(3^{2^n} k)$ two-level operations. Using one ancilla, each two-level operation can be decomposed into $O(n)$ Clifford+ T gates, resulting in a total gate count of $O(3^{2^n} nk)$ elementary Clifford+ T gates.

Chapter 7

Conclusions and future work

Bibliography

- [1] S. Abramsky. A structural approach to reversible computation. *Theoretical Computer Science*, 347(3):441–464, 2005.
- [2] Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. Version 2, arXiv:1206.0758v2, August 2012.
- [3] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, 1995. Available from arXiv:quant-ph/9503016v1.
- [4] Erik Barendsen, Inge Bethke, Jan Heering, Richard Kennaway, Paul Klint, Vincent van Oostrom, Femke van Raamsdonk, Fer-Jan de Vries, and Hans Zantema. Cambridge University Press, The Edinburgh Building, Cambridge, CB2 2RU, UK, 2003.
- [5] Charles H. Bennet. Logical reversibility of computation. *IBM Journal of Research and Development*, 6:525–532, 1973.
- [6] J.R.B. Cockett, Xiuzhan Guo, and Pieter Hofstra. Range categories ii: Towards regularity. Submitted for Publication, June 2012.
- [7] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London Ser. A*, A425:73–90, 1989.
- [8] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. arXiv:1206.5236v2, June 2012.
- [9] Julien Musset. Générateurs et relations pour les circuits booléens réversibles. Technical Report 97-32, Institut de Mathématiques de Luminy, 1997. Available from <http://iml.univ-mrs.fr/editions/>.
- [10] 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.
- [11] Robin Cockett and Stephen Lack. Restriction categories I: categories of partial maps. *Theoretical Computer Science*, 270:223–259, 2002.
- [12] Robin Cockett and Stephen Lack. Restriction categories II: Partial map classification. *Theoretical Computer Science*, 294:61–102, 2003.
- [13] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

- [14] Peter Selinger. Quantum circuits of T -depth one. *Physical Review A*, 2013. To appear. Available from arXiv:1210.0974.
- [15] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Physical Review A*, 54:147, 1995.