# QUANTUM COMPUTING MODELLING ON FIELD PROGRAMMABLE GATE ARRAY BASED ON STATE VECTOR AND HEISENBERG MODELS

LEE YEE HUI

UNIVERSITI TEKNOLOGI MALAYSIA

# QUANTUM COMPUTING MODELLING ON FIELD PROGRAMMABLE GATE ARRAY BASED ON STATE VECTOR AND HEISENBERG MODELS

LEE YEE HUI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Electrical Engineering)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

MARCH 2017

Dedicated to my beloved parents, supervisors, and friends.

# ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude to my supervisor and teacher, Prof. Dr. Mohamed Khalil-Hani, for his invaluable guidance, constant support and motivation that lead to the fruitful completion of this work. As the advisor of my postgraduate studies (for both Master's and PhD degrees), he has played the vital role in developing my positive personalities, which ensure I am well-prepared to face both career and life challenges in future. I have been extremely lucky to have a supervisor who care so much about my work as well as my personal well-being. My gratitude to him is beyond words.

My sincerest thank to my co-supervisor, Assoc. Prof. Dr. Muhammad Nadzir Marsono, for the patient guidance and advice that he has provided throughout my PhD study. It is highly appreciated that he has always responded to my queries and questions so promptly. Thanks to his excellent cooking skills, we have never found the lack of finger licking delicious food in special events and lab gatherings.

Special thanks to the Australian Government, Department of Education and Training for offering the precious Endeavour Research Fellowship that allowed me to have a 6-month research attachment at The University of Sydney during my PhD study. This has given me wonderful and unforgettable research and life experiences at the beautiful city of Sydney. I must express my gratitude to my host supervisor, Prof. Dr. Philip Leong, for his warm welcome and expert guidance that have made the program successful and beneficial.

I would also like to thank my fellow labmates in both VeCAD Lab and Computer Engineering Lab (The University of Sydney) as well as all those who have contributed directly and indirectly to the completion of this challenging milestone.

Last but not least, I would like to acknowledge with gratitude, the unconditional love and support from my parents and brother throughout this endeavour. They have been the constant source of care, love and concern all these years.

# ABSTRACT

As current trend of miniaturization in computing technology continues, modern computing devices would start to exhibit the behaviour of nanoscopic quantum objects. Quantum computing, which is based on the principles of quantum mechanics, becomes a promising candidate for future generation computing system. However, modelling quantum computing systems on existing classical computing platforms before the realization of viable large-scale quantum computer remains a major challenge. The exploration on the modelling of quantum computing systems on field programmable gate array (FPGA) platform, which offers the potential of massive parallelism and allows computational optimization at register-transfer level, is crucial. Due to the exponential growth of resource utilization with the increase in the number of quantum bits (qubit), existing works on modelling of quantum systems on FPGA platform are restricted to simple case studies using small qubit sizes. This work explores the modelling of quantum computing for emulation on FPGA platform based on two types of data structure: (a) state vector model and (b) Heisenberg model. For the conventional state vector modelling approach, an efficient datapath design that is based on serial-parallel hardware architecture, which allows resource sharing between unitary transformations, is proposed. Heisenberg model has been proven to be efficient in modelling stabilizer circuits, which are critical in error correction operations. In the effort to include the consideration of vital quantum error correction in practical quantum systems, a novel FPGA emulation framework that is based on the Heisenberg model is proposed. Effective algorithms for accurate global phase maintenance are proposed to facilitate the modelling of quantum systems based on the Heisenberg representation. The feasibility of the proposed state vector and Heisenberg emulation models are demonstrated based on a number of case studies with different characteristics, which include quantum Fourier transform, Grover's search algorithm, and stabilizer circuits. Based on the state vector approach, this work has demonstrated the advantage of FPGA emulation over software simulation where hardware emulation of 7-qubit Grover's search is about $3 \times 10^4$ times faster than the software simulation performed on Intel Core i7-4790 processor running at 3.6GHz clock rate. In contrast to the 8-qubit implementation based on the state vector model, the proposed FPGA emulation framework based on the Heisenberg model has successfully modelled 120-qubit stabilizer circuits on the Altera Stratix IV FPGA. In summary, the proposed work in this thesis contributes to the formulation of a proof-of-concept of efficient FPGA emulation framework based on the state vector and Heisenberg models.

# ABSTRAK

Dengan trend pengecilan berterusan dalam teknologi pengkomputeran, peranti komputeran moden mula mempamerkan ciri-ciri objek kuantum nanoskopi. Komputeran kuantum yang berasaskan prinsip-prinsip mekanik kuantum menjadi calon yang berpotensi untuk sistem komputeran generasi masa depan. Walau bagaimanapun, pemodelan sistem komputeran kuantum dengan penggunaan platform komputeran klasikal sedia ada sebelum pengrealisasian komputer kuantum berdaya maju berskala besar masih menjadi cabaran utama. Penerokaan pemodelan sistem komputeran kuantum dengan penggunaan platform tatasusunan get bolehaturcara medan (FPGA) yang menawarkan potensi keselarian besar dan membolehkan pengoptimuman pengkomputeran pada aras pindah-daftar adalah amat penting. Disebabkan penggunaan sumber yang meningkat secara eksponen dengan penambahan saiz bit kuantum (*qubit*), kerja-kerja sedia ada pemodelan sistem kuantum atas platform FPGA adalah terhad kepada kes-kes kajian yang mudah dengan saiz *qubit* yang kecil. Kerja ini meneroka pemodelan komputeran kuantum untuk perlagakan di atas platform FPGA berdasarkan dua jenis struktur data: (a) model vektor-keadaan (b) model Heisenberg. Bagi cara konvensional iaitu model vektor-keadaan, reka bentuk laluan data yang cekap berasaskan seni bina perkakasan siri-selari yang membolehkan perkongsian sumber antara transformasi unitari dicadangkan. Model Heisenberg terbukti berkesan dalam pemodelan litar penstabil yang kritikal dalam operasi pembetulan ralat. Dalam usaha untuk mempertimbangkan pembetulan ralat yang amat penting dalam sistem kuantum yang praktikal, satu rangka kerja perlagakan FPGA yang baru berdasarkan model Heisenberg dikemukakan. Algoritma yang berkesan untuk penyelenggaraan fasa global yang tepat dicadangkan untuk pemodelan sistem kuantum berdasarkan perwakilan Heisenberg. Kebolehlaksanaan model-model perlagakan vektor-keadaan dan Heisenberg yang dicadangkan diperlihatkan berdasarkan beberapa kes kajian dengan ciri-ciri yang berbeza termasuk kuantum jelmaan Fourier, algoritma carian Grover dan litar penstabil. Berdasarkan model vektor-keadaan, kerja ini telah menunjukkan kelebihan perlagakan FPGA berbanding dengan simulasi perisian di mana perlagakan algoritma carian Grover 7-*qubit* adalah kira-kira $3 \times 10^4$ kali lebih cepat daripada simulasi perisian yang dilakukan dengan pemproses Intel Core i7-4790 yang beroperasi pada kadar jam 3.6GHz. Berbeza dengan pelaksanaan 8-*qubit* yang berdasarkan model vektor-keadaan, rangka kerja perlagakan FPGA yang dicadangkan berdasarkan model Heisenberg telah berjaya memodelkan litar penstabil 120-*qubit* menggunakan Altera Stratix IV FPGA. Secara ringkasnya, kerja-kerja yang dicadangkan dalam tesis ini telah menyumbang kepada pembentukan rangka kerja bukti konsep perlagakan FPGA yang cekap berdasarkan model-model vektor-keadaan dan Heisenberg.

# TABLE OF CONTENTS

# LIST OF TABLES

## LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| ALU | - | Arithmetic Logic Unit |
| CNOT | - | Controlled-NOT |
| CU | - | Control Unit |
| CUDA | - | Compute Unified Device Architecture |
| DFT | - | Discrete Fourier Transform |
| DSP | - | Digital Signal Processing |
| EPR | - | Einstein-Podolsky-Rosen |
| FIFO | - | First-In First-Out |
| FPGA | - | Field Programmable Gate Array |
| FRQI | - | Flexible Representation of Quantum Image |
| FSM | - | Finite-State Machine |
| GPU | - | Graphics Processing Unit |
| GUI | - | Graphical User Interface |
| HDL | - | Hardware Description Language |
| IP | - | Intellectual Property |
| PC | - | Personal Computer |
| QFT | - | Quantum Fourier Transform |
| QKD | - | Quantum Key Distribution |
| QMDD | - | Quantum Multiple-Valued Decision Diagram |
| QuIDD | - | Quantum Information Decision Diagram |
| Qubit | - | Quantum Bit |
| RAM | - | Random-Access Memory |
| RTL | - | Register-Transfer Level |
| XQDD | - | X-Decomposition Quantum Decision Diagram |

## LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

Conventional digital computers perform computations based on binary bits of discrete values $0$ and $1$. In past few decades, computer technology has been advancing drastically from thousands to billions of transistors on a single chip. However, as current trend of miniaturization continues, modern computing devices would start to exhibit the behaviour of nanoscopic quantum objects and existing computer science principles may no longer be valid [1]. In this case, quantum computers that are build upon the laws of quantum mechanics will become promising candidates for future generation computing systems. However, to date, the physical realization of practical large-scale quantum computers remains a real challenge, and research is still ongoing. Meanwhile, the theoretical research of quantum computing applications are facilitated using classical computing platforms through simulation and emulation methods [2–5].

## 1.1 An Introduction to Fundamentals of Quantum Computing Models

Quantum computing is based on the properties of quantum mechanics namely *superposition* and *entanglement*. Superposition allows a quantum state to be in more than one basis states simultaneously. An $n$-bit classical computer has a total of $2^n$ possible states, although it allows one basis state at any time whereas a quantum computer with $n$-quantum-bit (qubit) can be in an arbitrary superposition of $2^n$ classical basis states. This superposition property facilitates massive parallelism that enables exponential speed-ups to be achieved in the well-known integer factoring and discrete logarithms algorithms [6], and quadratic speed-ups in solving classically intractable brute-force searching and optimization problems [7, 8].

Entanglement is defined as a strong correlation between two or more qubits. If two qubits are entangled, an action that is performed on one subset of qubit impacts on another. The entanglement property has been exploited for a wide range of applications in quantum information processing – quantum teleportation [9] and quantum key distribution (QKD) [10] are among the most popular ones. In the Einstein-Podolsky-Rosen (EPR) QKD protocol proposed by Ekert [10], a sequence of entangled pairs of qubits are generated and distributed to the sender and receiver. Each of them receives one qubit of each pair. After that, both the sender and receiver measure the entangled qubits regardless of sequence, based on the previously agreed basis. Since the qubit pairs are entangled, when one measures a qubit, it collapses the corresponding qubit of the other to the same random value. Hence, it results in a set of secret key that is shared between the sender and receiver for future secure communication.

Another unique characteristic in quantum computation, which does not apply to the classical approach, is the *no-cloning* theorem. Unlike in classical computing where information can be duplicated as many times as desired, it is impossible to make a copy of an unknown quantum state [11]. The well-known BB84 protocol [12] and B92 protocol [13] in quantum cryptography make use of the no-cloning theorem to detect eavesdropping in the process of quantum secret key transfer.

### 1.1.1 Quantum Bit (Qubit)

In classical computing, the smallest unit of information is the *bit*. A bit can be in either state $0$ or state $1$, and the state of a bit can be represented in matrix form as:

$$state\ 0 \quad = \quad \begin{array}{c@{}c} \begin{matrix}\mathbf{0}\\ \mathbf{1}\end{matrix} & \begin{bmatrix}1\\ 0\end{bmatrix}\end{array} \tag{1.1}$$

$$state\ 1 \quad = \quad \begin{array}{c@{}c} \begin{matrix}\mathbf{0}\\ \mathbf{1}\end{matrix} & \begin{bmatrix}0\\ 1\end{bmatrix}\end{array} \tag{1.2}$$

On the other hand, in quantum computing, the smallest unit of information is the *quantum bit* or *qubit*. To distinguish the classical bit with the quantum qubit, Dirac *ket* notation is used. Using the ket notation, the quantum computational basis states are represented by $|0\rangle$ and $|1\rangle$. The state of a qubit can be represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \begin{array}{c@{}c} \begin{matrix}\mathbf{0}\\ \mathbf{1}\end{matrix} & \begin{bmatrix}\alpha\\ \beta\end{bmatrix}\end{array} \tag{1.3}$$

where both $\alpha$ and $\beta$ are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. A qubit can be in state $|0\rangle$, or in state $|1\rangle$, or in superposition of both basis states. However, on measurement, the superposition is destroyed and the qubit returns to the classical state of bit depending on the probability derived from the complex-valued state vector. $|\alpha|^2$ is the probability where the qubit is in state $|0\rangle$ and $|\beta|^2$ is the probability where the qubit is in state $|1\rangle$ upon measurement.

A qubit can be mapped to an arrow from the origin to a three-dimensional sphere of radius 1 known as Bloch sphere (as illustrated in Figure 1.1). The Bloch sphere provides a way of visualizing a single-qubit state. When a qubit is measured in the standard basis, it collapses to either the north pole, $|0\rangle$ or the south pole, $|1\rangle$. As a quantum transformation that is represented by a unitary matrix is an isometry, geometrically the transformation corresponds to a rotation or an inversion on the Bloch sphere [14].

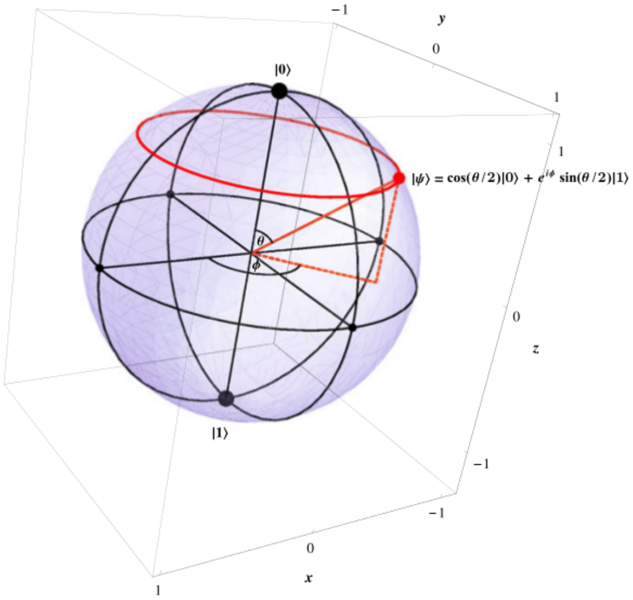

−1
y
0
1
|0⟩
1
$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$
$\theta$
$\phi$
0
z
|1⟩
−1
−1
0
x
1

**Figure 1.1:** Bloch sphere for visualization of a single-qubit state [1].

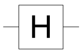
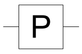
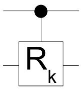
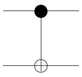
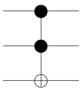
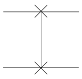
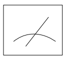
### 1.1.2 Quantum Circuit Model

To describe the transformations in a quantum system, the quantum circuit model, first proposed by Barenco et al. in [15] is widely used. A quantum circuit is the interconnection of quantum gates with quantum wires. A gate transformation is represented by a unitary matrix. For example, a Hadamard gate, $H$ is represented in matrix form as:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{1.4}$$

The Hadamard gate is one of the most useful (single-qubit) quantum transformations. An $N$-by-$N$ matrix $U$ is unitary if $UU^\dagger = U^\dagger U = I_N$ where $U^\dagger$ is the adjoint (conjugate transpose) of $U$. All unitary matrices are invertible and the product of unitary matrices as well as the inverse of unitary matrix are unitary. Since all quantum transformations are reversible, quantum gate operations can always be undone [14]. Table 1.1 shows graphical symbol of the basic quantum gates used in this thesis. Detailed descriptions of the listed quantum gates are given in Subsection 2.1.3.

**Table 1.1:** Graphical symbol of basic quantum gates.

| Gate | Graphical Symbol |
|---|---|
| Hadamard |  |
| Phase-Shift (Phase) |  |
| Controlled Phase-Shift |  |
| Controlled-NOT |  |
| Toffoli |  |
| Swap |  |
| Measurement |  |

### 1.1.3 State Vector Model

A quantum state vector is essentially a complex-valued vector that provides the probability distribution of each possible measurement outcome of a one- or multi-qubit system. An $n$-qubit quantum state vector contains $2^n$ complex numbers, which represent the measurement probability of each basis state. Tensor products and matrix multiplications are the critical operations that are used to update the content of a quantum state vector based on the evolution (or transformations) of the quantum system.

Tensor product (or Kronecker product) is the basic operation that is applied in the formation of a larger quantum system and multi-qubit quantum transformations. A quantum state vector that can be written as the tensor of two vectors is *separable*, whereas a state vector that cannot be expressed as the tensor of two vectors is *entangled* [14]. The tensor operation on two arbitrary 1-qubit transformations is as follows:

$$\begin{bmatrix} a_0 & a_1 \\ a_2 & a_3 \end{bmatrix} \otimes \begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \end{bmatrix} = \begin{bmatrix} a_0b_0 & a_0b_1 & a_1b_0 & a_1b_1 \\ a_0b_2 & a_0b_3 & a_1b_2 & a_1b_3 \\ a_2b_0 & a_2b_1 & a_3b_0 & a_3b_1 \\ a_2b_2 & a_2b_3 & a_3b_2 & a_3b_3 \end{bmatrix} \tag{1.5}$$

The following example illustrates the application of Hadamard gates in mapping a 2-qubit basis state $|00\rangle$ to superposition of basis states with equal probability. Equation (1.6) denotes this transformation in Direc ket notation, whereas (1.7) shows it in the state vector form.

$$|00\rangle \xrightarrow{H\otimes H} \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \tag{1.6}$$

$$\left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\right)\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \tag{1.7}$$

### 1.1.4 Heisenberg Model

Heisenberg model (also known as stabilizer formalism)[1] keeps track of the symmetries of an object instead of representing the object explicitly [16]. Heisenberg model is often used by physicists for describing atomic scale phenomena. Instead of the state vector model, Gottesman in [17] proposed quantum circuit simulation model based on the Heisenberg model, and has demonstrated that it is a more efficient technique for the modelling of certain quantum circuits. In the context of quantum

[1] The terms Heisenberg model and stabilizer formalism are used interchangeably in this thesis.

circuit simulation, the symmetries are operators derived from Pauli matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.8}$$

The Heisenberg model allows compact representations of certain quantum states by keeping track of the Pauli operators that *stabilize* them. A quantum state $|\psi\rangle$ is stabilized by an arbitrary unitary Pauli operator $U$ if $U|\psi\rangle = |\psi\rangle$, i.e., $|\psi\rangle$ is a 1-eigenvector of $U^2$. The key concept behind the stabilizer formalism is to represent an $n$-qubit quantum state by its stabilizer group. Stabilizer group is a group of Pauli literals ($n$-by-$n$ square matrix $A$) that stabilize the desired quantum state vector where the eigenvector $v$ is with eigenvalue $\lambda$ equals to one.

An arbitrary $n$-qubit computational basis state can be represented in the form of stabilizer matrix as shown in (1.9) where the ± sign of each $Z_j$ row ($Z$ literal at position $j$, $I$ literal(s) elsewhere) designates whether the $j^{th}$ qubit of the state is $|0\rangle$ (+) or $|1\rangle$ (-).

$$\begin{matrix} \pm \\ \pm \\ \pm \\ \pm \end{matrix} \begin{bmatrix} Z_1 & I & \dots & I \\ I & Z_2 & I & \vdots \\ \vdots & I & \ddots & I \\ I & \dots & I & Z_n \end{bmatrix} \tag{1.9}$$

On the other hand, an entangled two-qubit quantum state as shown in (1.10) can be specified uniquely by any of the stabilizer matrices given in (1.11).

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} \tag{1.10}$$

$$\mathcal{M}_1 = \begin{matrix} + \\ + \end{matrix} \begin{bmatrix} X & X \\ Z & Z \end{bmatrix}; \mathcal{M}_2 = \begin{matrix} + \\ - \end{matrix} \begin{bmatrix} X & X \\ Y & Y \end{bmatrix}; \mathcal{M}_3 = \begin{matrix} - \\ + \end{matrix} \begin{bmatrix} Y & Y \\ Z & Z \end{bmatrix} \tag{1.11}$$

These stabilizer matrices can be derived from each other through row multiplication without altering the quantum state in which the original stabilizer matrix

[2] Recall that the eigenvalue $\lambda$ and eigenvector $v$ of an $n$-by-$n$ square matrix $A$ are defined as $Av = \lambda v$.

represents. As shown in Table 1.2, multiplication of Pauli operators forms a closed group that are in terms of $I$, $X$, $Y$, $Z$ as well. For simplicity, the Pauli literals $I$, $X$, $Y$, and $Z$ are represented by two-bit 00, 10, 11, and 01, respectively, during the quantum circuit modelling process.

**Table 1.2**: Multiplication table for Pauli matrices. Products of two Pauli operators $U_1$ and $U_2$ are commutative if $U_1 \times U_2 = U_2 \times U_1$. Cells with anticommuting products are denoted in gray.

| | **I** | **X** | **Y** | **Z** |
|---|---|---|---|---|
| **I** | I | X | Y | Z |
| **X** | X | I | *iZ* | *-iY* |
| **Y** | Y | *-iZ* | I | *iX* |
| **Z** | Z | *iY* | *-iX* | I |

As illustrated in (1.12), with reference to Table 1.2, stabilizer matrix $\mathcal{M}_3$ can be easily derived from $\mathcal{M}_1$ by left-multiplying the second row by the first row and replace the first row of $\mathcal{M}_1$ with the multiplication result.

$$\begin{aligned}(Z \otimes Z)(X \otimes X) &= (ZX \otimes ZX) \\ &= (iY \otimes iY) \\ &= -(Y \otimes Y)\end{aligned} \tag{1.12}$$

As Clifford/stabilizer gates transform Pauli literals to other elements in the Pauli group, stabilizer circuits that are composed exclusively of Hadamard, phase and controlled-NOT (CNOT) gates can be simulated efficiently on classical computing platforms via stabilizer formalism. According to Gottesman-Knill theorem [16], stabilizer circuit and single-qubit measurement in the computational basis can be simulated efficiently on a classical computer. Efficient simulation of stabilizer circuits is crucial as practical quantum circuits that are enriched with fault-tolerant modules and error correcting codes are mainly made up of stabilizer sub-circuit and a small number of *non-stabilizer* gates [17].

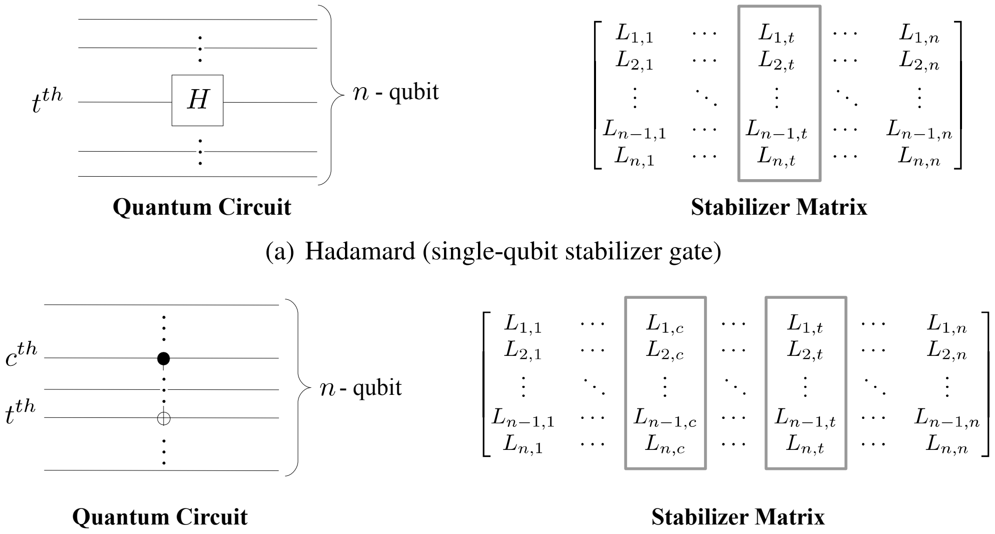
As shown in Table 1.3, transformations of stabilizer gates on Pauli matrices can be performed through *conjugation-by-action*. CNOT gate operation on arbitrary Pauli literals can be derived using the following approach:

$$X \otimes X \equiv (X \otimes I)(I \otimes X) \overset{CNOT}{\longmapsto} (X \otimes X)(I \otimes X) = X \otimes I \tag{1.13}$$

**Table 1.3**: Conjugation of Pauli literals by stabilizer gates. For CNOT gate, the control and target qubits are denoted by subscript *c* and *t*, respectively.

| Gate | Input | Output |
|---|---|---|
| **Hadamard** | X | Z |
| | Y | -Y |
| | Z | X |
| **Phase** | X | Y |
| | Y | -X |
| | Z | Z |
| **CNOT** | $I_cX_t$ | $I_cX_t$ |
| | $X_cI_t$ | $X_cX_t$ |
| | $X_cX_t$ | $X_cI_t$ |
| | $I_cY_t$ | $Z_cY_t$ |
| | $Y_cI_t$ | $Y_cX_t$ |
| | $Y_cY_t$ | $-X_cZ_t$ |
| | $I_cZ_t$ | $Z_cZ_t$ |
| | $Z_cI_t$ | $Z_cI_t$ |
| | $Z_cZ_t$ | $I_cZ_t$ |

Based on Table 1.3, Pauli literals in a stabilizer matrix $\mathcal{M}$ are updated by column(s) according to the qubit position(s) of which the Clifford gate is applied in a quantum circuit. Figure 1.2 depicts the application of Clifford gate in a quantum circuit and the corresponding column(s) in the stabilizer matrix that requires update.


$t^{th}$
$H$
$n$ - qubit
$L_{1,1}$ $\cdots$ $L_{1,t}$ $\cdots$ $L_{1,n}$
$L_{2,1}$ $\cdots$ $L_{2,t}$ $\cdots$ $L_{2,n}$
$L_{n-1,1}$ $\cdots$ $L_{n-1,t}$ $\cdots$ $L_{n-1,n}$
$L_{n,1}$ $\cdots$ $L_{n,t}$ $\cdots$ $L_{n,n}$
Quantum Circuit
Stabilizer Matrix
$c^{th}$
$t^{th}$
$n$ - qubit
$L_{1,1}$ $\cdots$ $L_{1,c}$ $\cdots$ $L_{1,t}$ $\cdots$ $L_{1,n}$
$L_{2,1}$ $\cdots$ $L_{2,c}$ $\cdots$ $L_{2,t}$ $\cdots$ $L_{2,n}$
$L_{n-1,1}$ $\cdots$ $L_{n-1,c}$ $\cdots$ $L_{n-1,t}$ $\cdots$ $L_{n-1,n}$
$L_{n,1}$ $\cdots$ $L_{n,c}$ $\cdots$ $L_{n,t}$ $\cdots$ $L_{n,n}$
Quantum Circuit
Stabilizer Matrix

(a) Hadamard (single-qubit stabilizer gate)

(b) Controlled-NOT (two-qubit stabilizer gate)

**Figure 1.2:** Column(s) update in stabilizer matrix due to Clifford gate application.

Based on the concepts described above, the Heisenberg representations that correspond to the Hadamard gates operation described in (1.6) is:

$$\begin{matrix} + \\ + \end{matrix}\begin{bmatrix} Z & I \\ I & Z \end{bmatrix} \xmapsto{H \otimes I} \begin{matrix} + \\ + \end{matrix}\begin{bmatrix} X & I \\ I & Z \end{bmatrix} \xmapsto{I \otimes H} \begin{matrix} + \\ + \end{matrix}\begin{bmatrix} X & I \\ I & X \end{bmatrix} \tag{1.14}$$

From (1.7) and (1.14), it can be observed that Heisenberg model provides a more compact representation for a quantum state and allows efficient modelling of Clifford gate operation compared to the state vector model that requires a vector with $2^n$ complex values for storage and involves compute-intensive matrix operations for the transformations. However, Heisenberg model requires more sophisticated bookkeeping algorithms to preserve the *global phase* such that accurate representation of quantum state can be maintained throughout the modelling process. For example, the resulted phase factor from the operation shown in (1.14), which is $\frac{1}{2}$, has to be maintained separately from the stabilizer matrix.

## 1.2 Motivation Towards Proposed Research

Physical realization of a quantum computer is proving to be extremely challenging [14]. Research works into viable large-scale quantum computers are still ongoing, various technologies namely ion-trap [18], nuclear magnetic resonance [19], and superconductor [20] have been attempted. In parallel to efforts to develop physical quantum computers, there is also much effort in the theoretical research of quantum algorithms and applications. Until large-scale practical quantum computers become prevalent, such theoretical research is currently developed using the classical computing platforms, which can be categorized into two types: (a) software simulation, and (b) hardware emulation. The definitions of simulation and emulation vary across different problem domains. In general, simulation reproduces the abstract model of the targeted system to define its operating limit and control system, whereas emulation generates close imitation to the actual behaviour and operation of the system [21].

In classical modelling of quantum computing system, software simulation refers to algorithmic models that are executed on computing platforms with conventional von Neumann architecture, which are inherently sequential in nature. On the other hand, hardware emulation refers to the modelling of quantum systems using field programmable gate array (FPGA) technology. Differing from the conventional hardware emulations, complete imitation of quantum computing systems on FPGA platform is infeasible due to the underlying classical electronics that behave in a totally different manner.

FPGA technology offers the potential of immense parallelism through hardware emulation where significant improvement in speed over the equivalent software simulation can be achieved. Furthermore, FPGA platform allows more control over the parameters and computational optimization at the register-transfer level (RTL) that can hardly be achieved through the software simulation approach. However, since FPGA is still a form of classical digital computing, resource utilization to model a quantum system on such a classical computing platform grows exponentially as the number of qubits increases. The challenge is further compounded by the fact that effective modelling of quantum systems using FPGA technology is non-intuitive, and therefore difficult. In short, the aforementioned strengths and challenges lead to the motivations of our research in this thesis.

## 1.3 Problem Statement

The main challenge in classical modelling of quantum computing systems is related to the exponential increase in resource requirement (includes both computational and memory resources) with the increase in the number of qubits. This issue is inherent in the universal quantum computing modelling independently from the used execution platform (classical computer, graphics processing unit (GPU) or FPGA) [22]. The demand for scalability in the number of qubits is even more critical and challenging for the highly resource-constrained FPGA platform. Although FPGA gives a promising solution for fast execution speed, improving the execution time is of minor interest in the absence of good scalability over larger number of qubits. In this thesis, three main problems on the modelling of quantum systems are identified based on the state vector and Heisenberg models.

The first problem is on FPGA emulation using the conventional state vector approach. To the best of our knowledge, all reported works in literature on FPGA emulation of quantum computing [4, 5, 23, 24] were implemented based on the state vector approach. Using the state vector model, an arbitrary unitary transformation is typically derived from the tensor product of unitary matrix (quantum gate representation) and identity matrices. The arithmetic operations in the resulted unitary transformation matrix are then extracted to facilitate the implementation of FPGA emulation model. However, the conventional tensor product method involves compute-intensive matrix operations and the memory requirement for storing the resulted large-dimension sparse matrix is enormous, which result in severe memory and computational bottlenecks [25, 26].

On the other hand, to ensure efficient FPGA emulation of quantum systems, the choice of suitable hardware architecture is crucial. Due to the strengths of high throughput and low critical path delay, pipeline architecture is chosen by previous works [4, 5, 23] for quantum hardware emulation purposes. However, pipeline implementation requires enormous logic resources as for concurrent (parallel) design, with additional registers to be inserted for pipelining purposes. This has highly restricted the size of quantum system that can be supported by the resource-constrained FPGA emulation platform. Hence, relevant prior works [4, 23, 24] were restricted to small qubit sizes and simple case studies.

The second problem is on the algorithmic aspect of quantum system modelling based on the Heisenberg representation. Similar to classical computing, errors exist in quantum domain but at a larger extent due to decay and environmental noise – a phenomena known as decoherence [27]. To ensure reliable computations on quantum states, error-correcting codes and fault-tolerant procedures are vital in any practical quantum computer. Therefore, error-correcting codes support is required to model real error-prone physical quantum computing on classical platform. However, the inclusion of error correction modules imply that more qubits are required, and hence, the aforementioned scalability problem in classical modelling of quantum computing systems is further compounded.

In the effort to tackle the scalability and error correction issues, García [3, 28] has proposed a more efficient representation of quantum states that is based on the Heisenberg model for quantum circuit simulation. García's proposal, which is called *stabilizer frames* data structure, offers a more compact storage than the conventional state vector approach for certain quantum states. It also allows for efficient simulation of error-correcting and fault-tolerant circuits that are mainly consist of stabilizer gates.

Nevertheless, with the approach using Heisenberg model, sophisticated and compute-intensive bookkeeping algorithms are required to ensure accurate global phases are maintained throughout the simulation process [3]. However, the details on the critical operations in the global phase maintenance algorithm for stabilizer gate application are not revealed in [3]. The efficiencies of these operations are critical since they significantly impact on the overall simulation and FPGA emulation performance in terms of speed and resource utilization. Practical and universal quantum circuits contain both stabilizer and non-stabilizer gates [27, 29]. However, the global phase maintenance algorithm presented in [3] is restricted to the application of stabilizer gates and the phase factor that is due to non-stabilizer gates operation is not taken into consideration.

The third problem is on FPGA emulation based on the Heisenberg model. Although error-correcting codes and fault-tolerant modules are crucial in practical quantum circuits, emulating quantum computing systems with error correcting features on FPGA platform poses highly challenging scalability issue if the conventional state vector model is applied [22]. To include quantum error correction features and to achieve more resource-efficient implementation, an FPGA emulation framework based on the Heisenberg model is required. Nevertheless, direct mapping of the algorithms presented by García in [3] on the FPGA platform is impractical and inefficient due to their inherent sequential computations that were designed for quantum circuit simulations on classical computers. Thus, a new FPGA emulation modelling approach based on the Heisenberg model is required.

## 1.4 Objectives

The goal of this research is to propose an efficient quantum computing model on classical digital computing architecture based on FPGA. Hence, the main objectives of this work are as follows:

1. To propose efficient algorithm and hardware architecture that facilitate the development of quantum computing models based on the conventional state vector approach targeted for resource-efficient FPGA emulation.
2. To propose effective algorithms that ensure accurate global phase maintenance for the modelling of quantum systems based on the Heisenberg model.
3. To develop a novel quantum circuit modelling technique and scalable hardware architecture based on the Heisenberg model for FPGA emulation.

## 1.5 Scope of Work

The scope of the work presented in this thesis is as follows:

- Quantum circuit model is used to represent the evolution or transformations of a quantum system.
- The proposed simulation and FPGA emulation modelling techniques are developed based on the state vector and Heisenberg models.
- In this work, software simulation models are developed to serve as golden reference models for the proposed FPGA emulation works. The implemented simulation models are verified against the corresponding mathematical models based on the selected case studies. The simulation models are developed using C programming language without the use of any external library. They are compiled using the GCC compiler under Ubuntu Linux operating system and executed on personal computer (PC) with Intel Core i7 processor.
- SystemVerilog hardware description language (HDL) is used to design the proposed FPGA hardware models. Hardware implementations are compiled for Altera Stratix IV FPGA using Quartus II synthesis tool. Design verification is performed using Modelsim-Altera software through SystemVerilog testbenches. Board-level verification is out of the scope of this work.
- Quantum Fourier transform and Grover's search are the core of many useful quantum algorithms that provide substantial speed-ups over the classical approaches [30]. On the other hand, Gottesman-Knill theorem states that an important subclass of quantum circuits, known as stabilizer circuits, can be simulated efficiently on classical computing platforms [16]. Hence, the case studies that are used to verify and analyse the performance of the proposed models are (a) quantum Fourier transform (QFT), (b) Grover's search algorithm, and (c) stabilizer circuits.

## 1.6 Contributions

The proposed work in this thesis contributes to the formulation of a proof-of-concept of efficient FPGA emulation framework based on the state vector and Heisenberg representations. The proposed emulation models can be extended to model practical large qubit sizes quantum computing systems by deploying state-of-the-art FPGA devices and also clusters of FPGAs. In summary, the main contributions of this thesis are as follows:

1. Based on the state vector model, this thesis proposes an efficient extraction method to obtain useful arithmetic operations from the unitary transformations of arbitrary single-qubit gates and two-qubit controlled gates. The proposed method generates the exact computation outcomes as the conventional tensor product approach without the need for storing the large-dimension unitary transformation matrix and requires only linear computation operations. In addition, a serial-parallel FPGA emulation architecture is developed based on the state vector representation where linear reduction in resource utilization is achieved compared to pipeline implementations as found in previous works [4, 5, 23]. The proposed serial-parallel architecture allows 7-qubit QFT implementation whereas the pipeline implementation can only scale up to 5-qubit. Based on the state vector model, this work has also demonstrated the advantage of FPGA emulation over software simulation where hardware emulation of 7-qubit Grover's search is about $3 \times 10^4$ times faster than the software simulation performed on Intel Core i7-4790 processor running at 3.6GHz clock rate.
2. Unlike the previous work presented by García in [3], which did not consider the phase factor due to the non-stabilizer gates application in Heisenberg model, in this thesis, global phase maintenance algorithms for both stabilizer and non-stabilizer gates operations are proposed. Furthermore, the details of the vital operations that facilitate the global phase maintenance process are presented. These details are critical as maintaining global phase involves compute-intensive operations that contribute most to the total execution time.
3. This work developed a novel FPGA emulation framework that is based on the Heisenberg model. The related algorithms for modelling of quantum circuit are redesigned to suit for efficient FPGA implementations. For this, a custom hardware emulation architecture is proposed. With the proposed novel FPGA emulator that is based on the Heisenberg representation, the emulations of 120-qubit stabilizer circuit and 9-qubit QFT circuit are successfully implemented.

## 1.7 Thesis Organization

The rest of the thesis is structured as follows.

Chapter 2 provides the theoretical background and an overview of the quantum computing research. Brief introductions to various quantum computing branches namely quantum hardware, quantum information theory, quantum information processing and communication, and quantum algorithms are given and relevant prior works on quantum design automation are reviewed in detail.

Chapter 3 covers the methodology for the work presented in this thesis. It includes the general approach taken in this research, as well as the tools and platforms used for verification and implementation purposes. In addition, descriptions of the case studies used to demonstrate the feasibility of the proposed work are presented here.

Chapter 4 describes the proposed method that facilitates efficient extraction of useful arithmetic elements from the unitary transformation operations. In addition, the modelling of the QFT and Grover's search algorithm based on the state vector model is presented. Furthermore, the advantages and disadvantages of different hardware architectural choices are studied and that lead to the formulation of the proposed serial-parallel architecture. Results and analysis on the efficiency of the proposed emulation architecture against other hardware architectures as well as benchmarking against related quantum computing simulation are given.

Chapter 5 presents the modelling technique and algorithms that are based on the Heisenberg model. Here, the proposed algorithms for maintaining global phases for both stabilizer and non-stabilizer gates operations are described in detail. Verifications of the proposed algorithms are performed against the golden reference simulation models that are developed using the state vector approach.

Chapter 6 details out the architectural designs and implementations of the proposed FPGA emulation hardware based on the Heisenberg model. Experimental results and discussion on the efficiency of the proposed emulation models as well as benchmarking against the equivalent simulation models are presented. Detailed analysis on the advantages and disadvantages of the state vector and Heisenberg models for the modelling of quantum systems is provided in this chapter.

Chapter 7 concludes the work done in this research, summarizes the contributions, and suggests directions for future research.

by optimizing the hardware architecture of the Heisenberg emulation models.

Stabilizer/Clifford gates by themselves do not form a universal set for quantum computations [143]. It is shown that at least one type of non-stabilizer gate that does not preserve the computational basis (such as T gate [143] or Toffoli gate [142]) is required to form a complete universal quantum gates set. In order to facilitate the modelling of universal quantum computations, it is crucial to include a quantum circuit decomposition module [102, 144] in an FPGA emulation framework. The quantum circuit decomposition unit converts arbitrary quantum gates in a quantum circuit to the universal gate set (such as stabilizer gates and Toffoli gate) that can be modelled efficiently on the developed FPGA emulation platform.

In a recent work by Smelyanskiy et al. [22], a parallel distributed-memory quantum simulator, which can simulate up to 49 qubits on the TACC Stampede supercomputer, was presented. To achieve comparable scalability on FPGA platform, the use of clusters of state-of-the-art FPGAs has to be explored such that sufficient computational and memory resources are available for hardware emulations of such a scale. Along with the use of FPGAs clusters, the research into efficient communications, interconnections, and logic circuit synthesis are vital. By improving the scalability of an FPGA emulation framework, the modelling of real-world large-scale quantum computing applications with error-correcting codes and fault-tolerant procedures is feasible.

# REFERENCES

1. Williams, C. P. and Clearwater, S. H. *Explorations in quantum computing*. Springer. 1998.

2. Viamontes, G. F., Markov, I. L. and Hayes, J. P. Improving QuIDD-based Simulation. *Quantum Circuit Simulation*, 2009: 133–152.

3. García-Ramírez, H. J. *Hybrid Techniques for Simulating Quantum Circuits using the Heisenberg Representation*. Ph.D. Thesis. The University of Michigan. 2014.

4. Khalid, A. U., Zilic, Z. and Radecka, K. FPGA emulation of quantum circuits. *IEEE International Conference on Computer Design: VLSI in Computers and Processors. ICCD 2004*. IEEE. 2004. 310–315.

5. Rivera-Miranda, J. F., Caicedo-Beltrán, A., Valencia-Payán, J. D., Espinosa-Duran, J. M. and Velasco-Medina, J. Hardware emulation of Quantum Fourier Transform. *IEEE Second Latin American Symposium on Circuits and Systems (LASCAS), 2011*. IEEE. 2011. 1–4.

6. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *35th Annual Symposium on Foundations of Computer Science, 1994 Proceedings*. IEEE. 1994. 124–134.

7. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 1997. 79(2): 325.

8. Malossini, A., Blanzieri, E. and Calarco, T. Quantum genetic optimization. *IEEE Transactions on Evolutionary Computation*, 2008. 12(2): 231–241.

9. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W. K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 1993. 70(13): 1895.

10. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Physical review letters*, 1991. 67(6): 661–663.

11. Wootters, W. K. and Zurek, W. H. A single quantum cannot be cloned. *Nature*, 1982. 299(5886): 802–803.

12. Bennett, C. H., Brassard, G. *et al.* Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. New York. 1984, vol. 175. 8.

13. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 1992. 68(21): 3121.

14. Yanofsky, N. S. and Mannucci, M. A. *Quantum computing for computer scientists*. vol. 20. Cambridge University Press Cambridge. 2008.

15. Barenco, A., Deutsch, D., Ekert, A. and Jozsa, R. Conditional quantum dynamics and logic gates. *Physical Review Letters*, 1995. 74(20): 4083.

16. Gottesman, D. The Heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998.

17. Gottesman, D. *Stabilizer codes and quantum error correction*. Ph.D. Thesis. California Institute of Technology. 1997.

18. Monroe, C., Meekhof, D., King, B., Itano, W. and Wineland, D. Demonstration of a fundamental quantum logic gate. *Physical Review Letters*, 1995. 75(25): 4714.

19. Gershenfeld, N. A. and Chuang, I. L. Bulk spin-resonance quantum computation. *science*, 1997. 275(5298): 350–356.

20. Mooij, J., Orlando, T., Levitov, L., Tian, L., Van der Wal, C. H. and Lloyd, S. Josephson persistent-current qubit. *Science*, 1999. 285(5430): 1036–1039.

21. McGregor, I. The relationship between simulation and emulation. *Proceedings of the Winter Simulation Conference*. IEEE. 2002, vol. 2. 1683–1688.

22. Smelyanskiy, M., Sawaya, N. P. and Aspuru-Guzik, A. qHiPSTER: The Quantum High Performance Software Testing Environment. *arXiv preprint arXiv:1601.07195*, 2016.

23. Aminian, M., Saeedi, M., Zamani, M. S. and Sedighi, M. FPGA-based circuit model emulation of quantum algorithms. *IEEE Computer Society Annual Symposium on VLSI. ISVLSI'08*. IEEE. 2008. 399–404.

24. Conceição, C. and Reis, R. Automatic Generation of Co-Processor for Simulation of Quantum Algorithms on FPGA.

25. Khalil-Hani, M., Lee, Y. H. and Marsono, M. N. An Accurate FPGA-Based Hardware Emulation on Quantum Fourier Transform. *Australasian Symposium on Parallel and Distributed Computing (AusPDC)*, 2015. 1: a1b3.

26. Tabakin, F. QDENSITY/QCWAVE: A Mathematica quantum computer simulation update. *Computer Physics Communications*, 2016. 201: 171–172.

27. Nielsen, M. A. and Chuang, I. L. *Quantum computation and quantum information*. Cambridge university press. 2010.

28. García, H. J. and Markov, I. L. Simulation of Quantum Circuits via Stabilizer Frames. *IEEE Transactions on Computers*, 2015. 64(8): 2323–2336.

29. Aaronson, S. and Gottesman, D. Improved simulation of stabilizer circuits. *Physical Review A*, 2004. 70(5): 052328.

30. Shor, P. W. Why haven't more quantum algorithms been found? *Journal of the ACM (JACM)*, 2003. 50(1): 87–90.

31. Feynman, R. P. Simulating physics with computers. *International journal of theoretical physics*, 1982. 21(6): 467–488.

32. Schrödinger, E. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*. Cambridge Univ Press. 1935, vol. 31. 555–563.

33. Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H. and Zeilinger, A. Experimental quantum teleportation. *Nature*, 1997. 390(6660): 575–579.

34. Perkowski, M. A. Multiple-valued quantum circuits and research challenges for logic design and computational intelligence communities. *IEEE Connections*, 2005. 3(4): 6–12.

35. Narayanan, A. and Menneer, T. Quantum artificial neural network architectures and components. *Information Sciences*, 2000. 128(3): 231–255.

36. Cory, D. G., Fahmy, A. F. and Havel, T. F. Ensemble quantum computing by NMR spectroscopy. *Proceedings of the National Academy of Sciences*, 1997. 94(5): 1634–1639.

37. Kane, B. E. A silicon-based nuclear spin quantum computer. *Nature*, 1998. 393(6681): 133–137.

38. Brennen, G. K., Caves, C. M., Jessen, P. S. and Deutsch, I. H. Quantum logic gates in optical lattices. *Physical Review Letters*, 1999. 82(5): 1060.

39. Imamog, A., Awschalom, D. D., Burkard, G., DiVincenzo, D. P., Loss, D., Sherwin, M., Small, A. *et al.* Quantum information processing using quantum dot spins and cavity QED. *Physical Review Letters*, 1999. 83(20): 4204.

40. Leuenberger, M. N. and Loss, D. Quantum computing in molecular magnets. *Nature*, 2001. 410(6830): 789–793.

41. Knill, E., Laflamme, R. and Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature*, 2001. 409(6816): 46–52.

42. Harneit, W. Fullerene-based electron-spin quantum computer. *Physical Review A*, 2002. 65(3): 032322.

43. Ohlsson, N., Krishna Mohan, R. and Kröll, S. Quantum computer hardware based on rare-earth-ion-doped inorganic crystals. *Optics Communications*, 2002. 201(1): 71–77.

44. Nizovtsev, A., Kilin, S. Y., Jelezko, F., Gaebal, T., Popa, I., Gruber, A. and Wrachtrup, J. A quantum computer based on NV centers in diamond: optically detected nutations of single electron and nuclear spins. *Optics and spectroscopy*, 2005. 99(2): 233–244.

45. Jones, J. A., Mosca, M. and Hansen, R. H. Implementation of a quantum search algorithm on a quantum computer. *Nature*, 1998. 393(6683): 344–346.

46. Brickman, K.-A., Haljan, P., Lee, P., Acton, M., Deslauriers, L. and Monroe, C. Implementation of Grover's quantum search algorithm in a scalable system. *Physical Review A*, 2005. 72(5): 050306.

47. DiCarlo, L., Chow, J., Gambetta, J., Bishop, L. S., Johnson, B., Schuster, D., Majer, J., Blais, A., Frunzio, L., Girvin, S. *et al.* Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature*, 2009. 460(7252): 240–244.

48. Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C. and O'Brien, J. L. Quantum computers. *Nature*, 2010. 464(7285): 45–53.

49. Amin, M. H., Dickson, N. G. and Smith, P. Adiabatic quantum optimization with qudits. *Quantum information processing*, 2013. 12(4): 1819–1829.

50. King, A. D., Hoskinson, E., Lanting, T., Andriyash, E. and Amin, M. H. Degeneracy, degree, and heavy tails in quantum annealing. *arXiv preprint arXiv:1512.07325*, 2015.

51. Rønnow, T. F., Wang, Z., Job, J., Boixo, S., Isakov, S. V., Wecker, D., Martinis, J. M., Lidar, D. A. and Troyer, M. Defining and detecting quantum speedup. *arXiv preprint arXiv:1401.2910*, 2014.

52. Shannon, C. E. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2001. 5(1): 3–55.

53. Ohya, M. *Quantum entropy and its use*. Springer. 2004.

54. Bernstein, E. and Vazirani, U. Quantum complexity theory. *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*. ACM. 1993. 11–20.

55. Jozsa, R. and Schumacher, B. A new proof of the quantum noiseless coding theorem. *Journal of Modern Optics*, 1994. 41(12): 2343–2349.

56. Schumacher, B. Quantum coding. *Physical Review A*, 1995. 51(4): 2738.

57. Legeza, Ö. and Sólyom, J. Quantum data compression, quantum information generation, and the density-matrix renormalization-group method. *Physical Review B*, 2004. 70(20): 205118.

58. Cleve, R. and DiVincenzo, D. P. Schumacher's quantum data compression as a quantum computation. *Physical Review A*, 1996. 54(4): 2636.

59. Bostroem, K. and Felbinger, T. Lossless quantum data compression and variable-length coding. *Physical Review A*, 2002. 65(3): 032313.

60. Ahlswede, R. and Cai, N. On lossless quantum data compression with a classical helper. *IEEE Transactions on Information Theory*, 2004. 50(6): 1208–1219.

61. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 1995. 52(4): R2493.

62. Steane, A. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 1996. 452(1954): 2551–2577.

63. Knill, E., Laflamme, R., Ashikhmin, A., Barnum, H., Viola, L. and Zurek, W. H. Introduction to quantum error correction. *arXiv preprint quant-ph/0207170*, 2002.

64. Zoller, P., Beth, T., Binosi, D., Blatt, R., Briegel, H., Bruss, D., Calarco, T., Cirac, J., Deutsch, D., Eisert, J. *et al.* Quantum information processing and communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 2005. 36(2): 203–228.

65. Molina-Terriza, G., Vaziri, A., Ursin, R. and Zeilinger, A. Experimental quantum coin tossing. *Physical review letters*, 2005. 94(4): 040501.

66. Ambainis, A. A new protocol and lower bounds for quantum coin flipping. *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. ACM. 2001. 134–142.

67. Brassard, G. and Crépeau, C. Quantum bit commitment and coin tossing protocols. In: *Advances in Cryptology-CRYPT0'90*. Springer. 49–61. 1991.

68. Brassard, G., Crépeau, C., Jozsa, R. and Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. *34th Annual Symposium on Foundations of Computer Science, 1993. Proceedings.* IEEE. 1993. 362–371.

69. Brassard, G. and Crépeau, C. A bibliography of quantum cryptography. *Sigact News*, 1993. 24(3): 16–20.

70. Brassard, G. and Crépeau, C. 25 years of quantum cryptography. *ACM Sigact News*, 1996. 27(3): 13–24.

71. Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., Sanguinetti, B., Thew, R. and Zbinden, H. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 2015. 9(3): 163–168.

72. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. and Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 2013. 7(5): 378–381.

73. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J. Experimental quantum cryptography. *Journal of cryptology*, 1992. 5(1): 3–28.

74. Ma, X.-S., Herbst, T., Scheidl, T., Wang, D., Kropatschek, S., Naylor, W., Wittmann, B., Mech, A., Kofler, J., Anisimova, E. *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 2012. 489(7415): 269–273.

75. Yin, J., Ren, J.-G., Lu, H., Cao, Y., Yong, H.-L., Wu, Y.-P., Liu, C., Liao, S.-K., Zhou, F., Jiang, Y. *et al.* Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 2012. 488(7410): 185–188.

76. Grossberg, S. Birth of a learning law. *Neural Networks*, 1998. 11(1): 1–7.

77. Sgarbas, K. N. The road to quantum artificial intelligence. *arXiv preprint arXiv:0705.3360*, 2007.

78. Wittek, P. *Quantum machine learning: what quantum computing means to data mining*. Academic Press. 2014.

79. Dunjko, V., Taylor, J. M. and Briegel, H. J. Quantum-enhanced machine learning. *Physical Review Letters*, 2016. 117(13): 130501.

80. Bieberich, E. Non-local quantum evolution of entangled ensemble states in neural nets and its significance for brain function and a theory of consciousness. *arXiv preprint quant-ph/9906011*, 1999.

81. Perus, M. Mind: neural computing plus quantum consciousness. *Mind Versus Computer, Edited by M. Gams, M. Paprzychi and X. Wu, by IOS press*, 1997: 156–170.

82. Purushothaman, G. and Karayiannis, N. B. Quantum neural networks (QNNs): inherently fuzzy feedforward neural networks. *IEEE Transactions on Neural Networks*, 1997. 8(3): 679–693.

83. SaiToh, A., Rahimi, R. and Nakahara, M. A quantum genetic algorithm with quantum crossover and mutation operations. *Quantum information processing*, 2014. 13(3): 737–755.

84. Ventura, D. and Martinez, T. Quantum associative memory. *Information Sciences*, 2000. 124(1): 273–296.

85. Njafa, J.-P. T., Engo, S. N. and Woafo, P. Quantum associative memory with improved distributed queries. *International Journal of Theoretical Physics*, 2013. 52(6): 1787–1801.

86. Benjamin, S. C. and Hayden, P. M. Multiplayer quantum games. *Physical Review A*, 2001. 64(3): 030301.

87. Guo, H., Zhang, J. and Koehler, G. J. A survey of quantum games. *Decision Support Systems*, 2008. 46(1): 318–332.

88. Tucci, R. R. An Introduction to Quantum Bayesian Networks for Mixed States. *arXiv preprint arXiv:1204.1550*, 2012.

89. Tucci, R. R. Quantum Bayesian Nets. *International Journal of Modern Physics B*, 1995. 9(03): 295–337.

90. Venegas-Andraca, S. E. Quantum walks: a comprehensive review. *Quantum Information Processing*, 2012. 11(5): 1015–1106.

91. Summy, G. and Wimberger, S. Quantum random walk of a Bose-Einstein condensate in momentum space. *Physical Review A*, 2016. 93(2): 023638.

92. Rivest, R. L., Shamir, A. and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978. 21(2): 120–126.

93. Grover, L. K. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM. 1996. 212–219.

94. Schützhold, R. and Schaller, G. Adiabatic quantum algorithms as quantum phase transitions: First versus second order. *Physical Review A*, 2006. 74(6): 060304.

95. Baritompa, W. P., Bulger, D. W. and Wood, G. R. Grover's quantum algorithm applied to global optimization. *SIAM Journal on Optimization*, 2005. 15(4): 1170–1184.

96. Simon, D. R. On the power of quantum computation. *SIAM Journal on Computing*, 1997. 26(5): 1474–1483.

97. Hallgren, S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM (JACM)*, 2007. 54(1): 4.

98. Mosca, M. and Ekert, A. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In: *Quantum Computing and Quantum Communications*. Springer. 174–188. 1999.

99. Bacon, D., Childs, A. M. and van Dam, W. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. *46th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2005*. IEEE. 2005. 469–478.

100. Grover, L. K. and Sengupta, A. M. From coupled pendulums to quantum search. *Mathematics of quantum computation*, 2002: 119–134.

101. Lukac, M. and Perkowski, M. Evolutionary approach to quantum symbolic logic synthesis. *IEEE Congress on Evolutionary Computation, CEC 2008.(IEEE World Congress on Computational Intelligence)*. IEEE. 2008. 3374–3380.

102. Shende, V. V., Prasad, A. K., Markov, I. L. and Hayes, J. P. Synthesis of reversible logic circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2003. 22(6): 710–722.

103. Ozhigov, Y. Fast quantum verification for the formulas of predicate calculus. *arXiv preprint quant-ph/9809015*, 1998.

104. Buhrman, H. and Špalek, R. Quantum verification of matrix products. *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*. ACM. 2006. 880–889.

105. Mohammadzadeh, N., Sedighi, M. and Saheb Zamani, M. Quantum physical synthesis: improving physical design by netlist modifications. *Microelectronics Journal*, 2010. 41(4): 219–230.

106. Ceder, G., Morgan, D., Fischer, C., Tibbetts, K. and Curtarolo, S. Data-mining-driven quantum mechanics for the prediction of structure. *MRS bulletin*, 2006. 31(12): 981–985.

107. Fischer, C. C., Tibbetts, K. J., Morgan, D. and Ceder, G. Predicting crystal structure by merging data mining with quantum mechanics. *Nature materials*, 2006. 5(8): 641–646.

108. Khalid, A. U. *FPGA emulation of quantum circuits*. Master's Thesis. McGill University. 2005.

109. Gutiérrez, E., Romero, S., Trenas, M. and Zapata, E. Simulation of quantum gates on a novel GPU architecture. *International Conference on Systems Theory and Scientific Computation*. 2007.

110. Gutiérrez, E., Romero, S., Trenas, M. A. and Zapata, E. L. Quantum computer simulation using the CUDA programming model. *Computer Physics Communications*, 2010. 181(2): 283–300.

111. Fritzsche, S. The Feynman tools for quantum information processing: Design and implementation. *Computer Physics Communications*, 2014. 185(6): 1697–1718.

112. Solcà, R., Kozhevnikov, A., Haidar, A., Tomov, S., Dongarra, J. and Schulthess, T. C. Efficient implementation of quantum materials simulations on distributed CPU-GPU systems. *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. ACM. 2015. 10.

113. Piccinini, E., Benedetti, C., Siloi, I., Paris, M. G. and Bordone, P. GPU-accelerated algorithms for many-particle continuous-time quantum walks. *arXiv preprint arXiv:1612.00746*, 2016.

114. McDaniel, T., D'Azevedo, E., Li, Y. W., Kent, P., Wong, M. and Wong, K. Delayed Update Algorithms for Quantum Monte Carlo Simulation on GPU. *Proceedings of the XSEDE16 Conference on Diversity, Big Data, and Science at Scale*. ACM. 2016. 13.

115. Che, S., Li, J., Sheaffer, J. W., Skadron, K. and Lach, J. Accelerating compute-intensive applications with GPUs and FPGAs. *Symposium on Application Specific Processors, SASP 2008*. IEEE. 2008. 101–107.

116. Negovetic, G., Perkowski, M., Lukac, M. and Buller, A. Evolving quantum circuits and an FPGA-based Quantum Computing Emulator. *Proc. Fifth Intern. Workshop on Boolean Problems*. 2002. 15–22.

117. Saito, K., Suzuki, Y., Fujishima, M. and Hoh, K. High-Speed Emulation of the Quantum Computing Based on Logic Operations. *Solid State Devices and Materials*, 2002: 376–377.

118. Goto, Y. and Fujishima, M. Efficient quantum computing emulation system with unitary macro-operations. *Japanese journal of applied physics*, 2007. 46(4S): 2278.

119. Mohamed, T., Badawy, W. and Jullien, G. On using FPGAs to accelerate the emulation of quantum computing. *Canadian Conference on Electrical and Computer Engineering, 2009. CCECE'09*. IEEE. 2009. 175–179.

120. Conceicao, C. and Reis, R. Efficient emulation of quantum circuits on classical hardware. *IEEE 6th Latin American Symposium on Circuits & Systems (LASCAS), 2015*. IEEE. 2015. 1–4.

121. Arvizu-Mondragón, A., López-Leyva, J. A., Ureña, J. L., Mendieta-Jiménez, F. J., Sánchez, L. and de Dios, J. FPGA-based emulation of a synchronous phase-coded quantum cryptography system. *Computación y Sistemas*, 2015. 19(1): 185–195.

122. Venegas-Andraca, S. and Ball, J. Processing images in entangled quantum systems. *Quantum Information Processing*, 2010. 9(1): 1–11.

123. Latorre, J. I. Image compression and entanglement. *arXiv preprint quant-ph/0510031*, 2005.

124. Le, P. Q., Dong, F. and Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Information Processing*, 2011. 10(1): 63–84.

125. Le, P. Q., Iliyasu, A. M., Dong, F. and Hirota, K. Efficient Color Transformations on Quantum Images. *JACIII*, 2011. 15(6): 698–706.

126. Lomont, C. Quantum convolution and quantum correlation algorithms are physically impossible. *arXiv preprint quant-ph/0309070*, 2003.

127. Klappenecker, A. and Rotteler, M. Discrete cosine transforms on quantum computers. *Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis, ISPA 2001*. IEEE. 2001. 464–468.

128. Tseng, C.-C. and Hwang, T.-M. Quantum circuit design of 8× 8 discrete cosine transform using its fast computation flow graph. *IEEE International Symposium on Circuits and Systems, ISCAS 2005*. IEEE. 2005. 828–831.

129. Fijany, A. and Williams, C. P. *Quantum wavelet transforms: Fast algorithms and complete circuits*. Springer. 1999.

130. Shiou-An, W., Chin-Yung, L., Sy-Yen, K. *et al.* An XQDD-based verification method for quantum circuits. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 2008. 91(2): 584–594.

131. Miller, D. M. and Thornton, M. A. QMDD: A decision diagram structure for reversible and quantum circuits. *36th International Symposium on Multiple-Valued Logic*. IEEE. 2006. 30–30.

132. Zhang, W.-W., Gao, F., Liu, B., Wen, Q.-Y. and Chen, H. A watermark strategy for quantum images based on quantum fourier transform. *Quantum Information Processing*, 2013. 12(2): 793–803.

133. Curtis, D. and Meyer, D. A. Towards quantum template matching. *Optical Science and Technology, SPIE's 48th Annual Meeting*. International Society for Optics and Photonics. 2004. 134–141.

134. Durr, C. and Hoyer, P. A quantum algorithm for finding the minimum. *arXiv preprint quant-ph/9607014*, 1996.

135. Montanaro, A. Quantum pattern matching fast on average. *arXiv preprint arXiv:1408.1816*, 2014.

136. Du, S., Yan, Y. and Ma, Y. Quantum-Accelerated Fractal Image Compression: An Interdisciplinary Approach. *IEEE Signal Processing Letters*, 2015. 22(4): 499–503.

137. Knill, E., Leibfried, D., Reichle, R., Britton, J., Blakestad, R., Jost, J., Langer, C., Ozeri, R., Seidelin, S. and Wineland, D. Randomized benchmarking of quantum gates. *Physical Review A*, 2008. 77(1): 012307.

138. Frigo, M. and Johnson, S. G. The Design and Implementation of FFTW3. *Proceedings of the IEEE*, 2005. 93(2): 216–231. Special issue on "Program Generation, Optimization, and Platform Adaptation".

139. Wecker, D. and Svore, K. M. LIQUi$|\rangle$: A software design architecture and domain-specific language for quantum computing. *arXiv preprint arXiv:1402.4467*, 2014.

140. Weimer, H., Müller, M., Lesanovsky, I., Zoller, P. and Büchler, H. P. A Rydberg quantum simulator. *Nature Physics*, 2010. 6(5): 382–388.

141. Kilts, S. *Advanced FPGA design: architecture, implementation, and optimization*. John Wiley & Sons. 2007.

142. Aharonov, D. A simple proof that Toffoli and Hadamard are quantum universal. *arXiv preprint quant-ph/0301040*, 2003.

143. Shi, Y. Both Toffoli and controlled-NOT need little help to do universal

quantum computation. *arXiv preprint quant-ph/0205115*, 2002.

144. Saeedi, M. and Markov, I. L. Synthesis and optimization of reversible circuits - a survey. *ACM Computing Surveys (CSUR)*, 2013. 45(2): 21.