วงจรควอนตัมสำหรับขั้นตอนวิธีการของชอร์

นายวิภู เมธาชวลิต

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

QUANTUM CIRCUITS FOR SHOR'S ALGORITHM

Mr. Wiphoo Methachawalit

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering in Computer Engineering
Department of Computer Engineering
FACULTY OF ENGINEERING
Chulalongkorn University
Academic Year 2020

หัวข้อวิทยานิพนธ์	วงจรควอนตัมสำหรับขั้นตอนวิธีการของชอร์
โดย	นายวิภู เมธาชวลิต
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ศาสตราจารย์ ดร.ประภาส จงสถิตย์วัฒนา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.สุกรี สินธุภิญโญ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ศาสตราจารย์ ดร.ประภาส จงสถิตย์วัฒนา)

..... กรรมการภายนอกมหาวิทยาลัย
(ศาสตราจารย์ ดร.บุญเจริญ ศิริเนาวกุล)

วิภู เมธาชวลิต : วงจรควอนตัมสำหรับขั้นตอนวิธีการของชอร์. (QUANTUM CIRCUITS FOR SHOR'S ALGORITHM) อ.ที่ปรึกษาหลัก : ศ. ดร.ประภาส จงสถิตย์วัฒนา

วิธีขั้นตอนการหาตัวประกอบจำนวนเฉพาะของชอร์เป็นหนึ่งในปัญหาที่น่าสนใจสำหรับคอมพิวเตอร์ควอนตัม โดยงานวิจัยนี้ต้องศึกษาถึงพฤติกรรมของวงจรขั้นตอนวิธีการของชอร์เมื่อนำมาใช้กับคอมพิวเตอร์ควอนตัมในปัจจุบัน โดยเลือกนำการออกแบบวงจรที่นำเสนอไว้โดย สตีเฟ่น เบอรีการ์ด มาทำการทดลองบนคอมพิวเตอร์ควอนตัมของทางบริษัทไอบีเอ็มขนาด 15 คิวบิต

สาขาวิชา	วิศวกรรมคอมพิวเตอร์	ลายมือชื่อนิสิต .....
ปีการศึกษา	2563	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6170270321 : MAJOR COMPUTER ENGINEERING

KEYWORD: Quantum computation, Quantum algorithm, Shor's algorithm, Prime factorization

Wiphoo Methachawalit : QUANTUM CIRCUITS FOR SHOR'S ALGORITHM. Advisor: Prof. PRABHAS CHONGSTITVATANA, Ph.D.

The prime factorization algorithm by Peter Shor is one of the most famous algorithms for quantum computers. The goal of this thesis is to study the behavior of Shor's algorithm and design quantum circuits to run it on existing quantum computers. The proposed quantum circuits are developed from the circuit by Stephane Beauregard. The experiment is done on IBM 15 qubits quantum computer.

Field of Study: Computer Engineering Student's Signature .....

Academic Year: 2020 Advisor's Signature .....

กิตติกรรมประกาศ

งานวิจัยฉบับนี้เสร็จสมบูรณ์ลุล่วงได้ด้วยความอนุเคราะห์จากอาจารย์ที่ปรึกษาวิจัย ศาสตราจารย์ ดร. ประภาส จงสถิตย์วัฒนา อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย สำหรับคำแนะนำ ข้อคิดเห็นต่างๆในการวิจัยนี้มาโดยตลอด รวมทั้งช่วยแก้ไขข้อบกพร่องในงานวิจัยฉบับนี้จนสำเร็จได้ ผู้วิจัยขอกราบขอบคุณ ณ โอกาสนี้

ขอขอบคุณรองศาสตราจารย์ ดร. ชัชวิทย์ อาภรณ์เทวัญ ที่ได้เปิดโอกาสให้เข้าเรียนวิชาพื้นฐาน Quantum Computation และเพื่อนๆในห้องเรียน ที่ช่วยให้คำแนะนำเกี่ยวกับเครื่องมือการใช้งาน IBM Q Experience

ขอขอบคุณเพื่อนๆ และพี่น้อง ใน Lab CU ISL ทั้งกำลังกาย และกำลังใจ สำหรับการทำงานวิจัยฉบับนี้

สุดท้ายนี้ ขอขอบคุณคุณกมลลักษณ์ สุขแสน สำหรับการช่วยตรวจทานและแก้ไขข้อผิดพลาดต่างๆในงานวิจัยฉบับนี้

วิภู เมธาชวลิต

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ปีเตอร์ ชอร์ (Peter Shor) ได้นำเสนอขั้นตอนวิธีการหาตัวประกอบจำนวนเฉพาะ (Shor's Algorithm) [1] ขึ้นเมื่อปี ค.ศ. 1997 ซึ่งพื้นฐานของขั้นตอนวิธีการหาตัวประกอบจำนวนเฉพาะนั้นมาจากความคิดเรื่องของการหาคาบ (ระยะเวลาที่คลื่นผ่านตำแหน่งใดๆ เมื่อคลื่นเคลื่อนที่ครบหนึ่งรอบ) เมื่อมีการใช้คอมพิวเตอร์ควอนตัม ซึ่งชอร์พิสูจน์ด้วยวิธีการทางคณิตศาสตร์ พบว่าขั้นตอนวิธีการที่นำเสนอสามารถหาตัวประกอบจำนวนเฉพาะใช้เวลาลดลง เมื่อเทียบกับขั้นตอนวิธีการบนคอมพิวเตอร์ในปัจจุบัน

หนึ่งปีหลังจากที่ปีเตอร์ ชอร์นำเสนอขั้นตอนวิธีการหาตัวประกอบจำนวนเฉพาะ โทมัส จี แดปเปอร์ (Thomas G. Dapper) ได้นำเสนอวงจรบวกสำหรับคอมพิวเตอร์ควอนตัม [2] ซึ่งวงจรบวกเป็นพื้นฐานของวงจรที่จะนำไปใช้พัฒนาพื้นฐานขั้นตอนวิธีการของชอร์ ต่อมาในปี ค.ศ. 2001 ห้องวิจัยของทางบริษัทไอบีเอ็มที่อัลมาเดน (Almaden) ได้ทดสอบขั้นตอนวิธีการที่ชอร์ได้นำเสนอในปี ค.ศ. 1997 [3] บนคอมพิวเตอร์ควอนตัม ในการทดลองนักวิจัยได้สร้างวงจรเฉพาะสำหรับการหาตัวประกอบจำนวนเฉพาะของสมการ $a^r \bmod N$ โดยวงจรที่สร้างขึ้นสำหรับควอนตัมเมื่อ a มีค่าเท่ากับ 7 และ N มีค่าเท่ากับ 15 ต่อมาในปี ค.ศ. 2003 สตีเฟ่น เบอรีการ์ด (Stephane Beauregard) ได้นำเสนอวิธีการออกแบบวงจรทั่วไปสำหรับขั้นตอนวิธีการของชอร์ วงจรที่ได้นำเสนอนั้นใช้จำนวนคิวบิตนั้นต้องการจำนวน $2n+3$ คิวบิต เมื่อ n คือจำนวนบิตของ N ในสมการ $a^r \bmod N$ [4]

ในปัจจุบันทางบริษัทไอบีเอ็มมีการพัฒนาคอมพิวเตอร์ควอนตัมและเปิดให้นักวิจัยหรือผู้ที่สนใจเข้าทดลองใช้งานในชื่อว่า ไอบีเอ็ม คิว เอ็กซ์พีเรียนซ์ (IBM Q Experience) โดยมีชุดคำสั่งที่พัฒนาด้วยภาษาไพทอนในชื่อ Qiskit ซึ่งมีคอมพิวเตอร์ควอนตัมจำลองและคอมพิวเตอร์ควอนตัมจริงขนาด 5 และ 15 คิวบิต ให้พัฒนาและทดลองวงจรได้ [5] หรือแม้กระทั่งทางบริษัทริเกตติ (Rigetti) ซึ่งก่อตั้งบริษัทขึ้นเมื่อปี พ.ศ. 2556 เพื่อสร้างวงจรคอมพิวเตอร์ควอนตัมเป็นอีกหนึ่งบริษัทที่มีการเปิดให้สามารถใช้งานคอมพิวเตอร์ควอนตัมเพื่อนักวิจัยที่ไปสามารถเข้าไปใช้งานสำหรับการศึกษาวิจัย [6]

1.2 จุดประสงค์ของการวิจัย

งานวิจัยนี้ทำขึ้นโดยมีจุดประสงค์ดังต่อไปนี้

1. ศึกษาขั้นตอนวิธีการของชอร์ [1]
2. ศึกษาวิธีการออกแบบวงจรของสตีเฟ่น เบอรีการ์ด [4] สำหรับขั้นตอนวิธีการของชอร์
3. ทดลองนำการออกแบบวงจรของสตีเฟ่น เบอรีการ์ด [4] สำหรับขั้นตอนวิธีการของชอร์บนคอมพิวเตอร์ควอนตัม
4. ศึกษาถึงพฤติกรรมของคอมพิวเตอร์ควอนตัมเมื่อด้วยการทดลองกับวงจรขั้นตอนวิธีการของชอร์
5. ศึกษาถึงข้อดี ข้อเสีย และข้อจำกัดของวงจรขั้นตอนวิธีการของชอร์บน คอมพิวเตอร์ควอนตัม

โดยงานวิจัยชิ้นนี้ศึกษาและทดลองวงจรหาตัวประกอบจำนวนเฉพาะบนคอมพิวเตอร์ควอนตัม ซึ่งใช้ขั้นตอนวิธีการของชอร์ [1] ที่ได้นำเสนอไว้ ซึ่งสตีเฟ่น เบอรีการ์ด [4] ได้นำเสนอวิธีการออกแบบวงจรทั่วไปสำหรับขั้นตอนวิธีการของชอร์ในปี ค.ศ. 2003 มาประยุกต์ ปรับปรุง และแก้ไขเพื่อใช้สามารถนำไปใช้งานในระบบคอมพิวเตอร์ควอนตัมของบริษัทไอบีเอ็มที่ชื่อว่า IBM Quantum Experience ซึ่งเปิดให้นักวิจัยและผู้สนใจสามารถเข้าไปใช้งาน โดยวงจรที่สตีเฟ่น เบอรีการ์ด นำเสนอไว้นั้นใช้จำนวนคิวบิต *2n+3* คิวบิต สำหรับหาตัวประกอบจำนวนเฉพาะของเลขจำนวนเต็มใดๆขนาด *n* บิตบนคอมพิวเตอร์ปัจจุบัน

เนื่องจากในยุคของชอร์ปี ค.ศ. 1997 ที่ได้นำเสนอขั้นตอนวิธีการของชอร์สำหรับหาตัวประกอบจำนวนเฉพาะของจำนวนเต็มใดๆ [1] มาจนกระทั่งปี ค.ศ. 2003 ที่สตีเฟ่น เบอรีการ์ด นำเสนอการออกแบบวงจรควอนตัมสำหรับขั้นตอนวิธีการของชอร์ [4] ที่นำเสนอไว้นั้น การพัฒนาคอมพิวเตอร์ควอนตัมยังอยู่ในช่วงเริ่มต้น และเป็นการวิจัยที่ไม่ได้มีการเปิดระบบคอมพิวเตอร์ควอนตัมให้นักวิจัยหรือผู้สนใจสามารถเข้าใช้ได้งานอย่างกว้างขวาง แตกต่างจากในปัจจุบันที่ทั้งบริษัทซึ่งสร้างคอมพิวเตอร์ควอนตัมตัวอย่างเช่นไอบีเอ็ม หรือลิเก็ตติ เปิดให้นักพัฒนาที่ต้องการศึกษาหรือเรียนรู้สามารถทดลอง โดยปัจจุบันทาง IBM Quantum Experience เปิดให้ใช้คอมพิวเตอร์ควอนตัมที่มีจำนวน 15 คิวบิตสำหรับนักวิจัยหรือบุคคลที่สนใจทั่วไป และคอมพิวเตอร์ควอนตัมขนาด 20 คิวบิตสำหรับนักวิจัยที่เข้าร่วมโครงการกับทางไอบีเอ็ม ซึ่งเป็นโอกาสที่น่าสนใจในการทดลองนำวงจรที่มีการนำเสนอไว้ในอดีตซึ่งในขณะนั้นไม่มีการเปิดให้ใช้งานคอมพิวเตอร์ควอนตัมอย่างแพร่หลายเทียบกับปัจจุบัน มาทดลองในระบบคอมพิวเตอร์ควอนตัมปัจจุบันเพื่อศึกษาถึงข้อดี ข้อเสีย

และข้อจำกัดเมื่อมีการนำวงจรที่นำเสนอไว้มาดำเนินการปรับปรุงหรือแก้ไขเพื่อให้สามารถทำงานบนระบบคอมพิวเตอร์ควอนตัมปัจจุบัน

1.3 ขอบเขตการวิจัย

งานวิจัยนี้จัดทำขึ้นโดยมีขอบเขตการวิจัยในส่วนของวงจรขั้นตอนวิธีการของชอร์ [1] ที่นำเสนอไว้โดยสตีเฟ่น เบอรีการ์ด [4] บนคอมพิวเตอร์ควอนตัมของบริษัทไอบีเอ็มหรือบริษัทลิเก็ตติ ซึ่งต้องการศึกษาพฤติกรรมของคอมพิวเตอร์ควอนตัมกับวงจรที่มีการนำเสนอไว้ และต้องการศึกษาถึงข้อจำกัด ข้อดีและข้อเสียของวงจรขั้นตอนวิธีการของชอร์ [1] ที่นำเสนอไว้โดยสตีเฟ่น เบอรีการ์ด [4] เมื่อนำมาประยุกต์ใช้งานบนคอมพิวเตอร์ควอนตัม

1.4 ขั้นตอนและวิธีการดำเนินการวิจัย

1. ศึกษาและทำความเข้าใจถึงขั้นตอนวิธีการของชอร์ที่นำเสนอไว้ในปี ค.ศ. 1997 [1] ในการหาตัวประกอบจำนวนเฉพาะด้วยคอมพิวเตอร์ควอนตัม โดยทำความเข้าใจถึงทฤษฎีของคอมพิวเตอร์ควอนตัมที่ชอร์ใช้เป็นส่วนประกอบสำคัญของขั้นตอนวิธีการของการหาตัวประกอบจำนวนเฉพาะ
2. ศึกษาทำงานของคอมพิวเตอร์ควอนตัมให้มีความเข้าใจคุณลักษณะของคิวบิตในคอมพิวเตอร์ควอนตัม ขั้นตอนวิธีการของชอร์นำไปใช้ในการหาตัวประกอบจำนวนเฉพาะ และศึกษาถึงเกตต่างๆของคอมพิวเตอร์ควอนตัม รวมถึงการออกแบบวงจรคอมพิวเตอร์ควอนตัม
3. ทดลองใช้คอมพิวเตอร์ควอนตัมในปัจจุบันที่บริษัทต่างๆ เริ่มมีการเปิดให้นักวิจัยหรือผู้ที่สนใจควอนตัมสามารถทดลองใช้งานคอมพิวเตอร์ควอนตัมที่บริษัทต่างๆ เปิดให้นักวิจัยหรือผู้ที่สนใจสามารถใช้งานและทำการทดลองผ่านทางชุดคำสั่งที่บริษัทเหล่านั้นเปิดให้ใช้งาน ตัวอย่างบริษัทที่มีการเปิดให้ใช้งานคอมพิวเตอร์ควอนตัมคือ บริษัทไอบีเอ็มและบริษัทลิเก็ตติ
4. ทำการทดลองเกตและออกแบบวงจรพื้นฐานของคอมพิวเตอร์ควอนตัมบนระบบคอมพิวเตอร์ควอนตัม โดยเลือกคอมพิวเตอร์ควอนตัมของทางไอบีเอ็มซึ่งใช้งานชุดคำสั่ง Qiskit เป็นการเริ่มต้น
5. ศึกษาการออกแบบวงจรสำหรับขั้นตอนวิธีการของชอร์ที่นำเสนอไว้โดยสตีเฟ่น เบอรีการ์ด [4] ซึ่งวงจรที่นำเสนอไว้นั้นใช้พื้นฐานของวงจรบวก (adder) และวงจรแปลงฟูเรียร์ (Fourier transform) โดยวงจรบวกบนคอมพิวเตอร์ควอนตัมนั้นโทมัส จี แดปเปอร์ ได้มีการนำเสนอไว้ในปี ค.ศ. 1998 [2] และนำวงจรที่มีการนำเสนอไว้นั้นมาทดลองกับคอมพิวเตอร์ควอนตัมของทางบริษัทไอบีเอ็ม

6. วิเคราะห์ สังเคราะห์ ถึงข้อจำกัด ข้อดี และข้อเสียของวงจรสำหรับขั้นตอนวิธีการของชอร์ที่นำเสนอไว้โดยสตีเฟ่น เบอรีการ์ด [4] เมื่อใช้สร้างวงจรบนคอมพิวเตอร์ควอนตัมของบริษัทไอบีเอ็ม รวมทั้งนำเสนอถึงปัญหาที่พบเมื่อมีการนำวงจรที่นำเสนอไว้มาปรับใช้งานกับคอมพิวเตอร์ควอนตัมในปัจจุบัน

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

สิ่งที่คาดหวังจากงานวิจัยนี้คือสามารถบอกถึงข้อจำกัดของทั้งวงจรที่ได้มีการนำเสนอไว้ก่อนช่วงที่จะมีการพัฒนาคอมพิวเตอร์ควอนตัมที่เปิดให้นักวิจัยและผู้สนใจได้ใช้งาน ซึ่งในที่นี่คือกระบวนการขั้นตอนของชอร์ซึ่งได้มีการนำเสนอออกแบบไว้เป็นวงจรโดยสตีเฟ่น เบอรีการ์ด [4] โดยนำมาดำเนินสร้างวงจรที่ได้มีการนำเสนอไว้บนไอบีเอ็ม คิว เอ็กซ์พีเรียนซ์ ซึ่งเป็นคอมพิวเตอร์ควอนตัมที่ทางบริษัทไอบีเอ็มพัฒนาขึ้น

ซึ่งคาดหวังว่างานวิจัยชิ้นนี้สามารถแสดงถึงข้อดี ข้อเสีย รวมถึงข้อจำกัดเมื่อนำวงจรของสตีเฟ่น เบอรีการ์ด [4] ที่นำเสนอไว้สำหรับวิธีการขั้นตอนของชอร์มาดำเนินการบน IBM Quantum Experience ซึ่งอาจจะยังมีข้อจำกัดในเรื่องของสถานะของคิวบิตที่อาจทำให้เกิดข้อผิดพลาดของการทำงานหาตัวประกอบจำนวนเฉพาะจากวงจรที่ได้สร้างขึ้นมา โดยตัวแปรสำคัญของคิวบิตมาจากระยะเวลาของสถานะของคิวบิตเมื่อผ่านเกตต่างๆ และระยะเวลาการเชื่อมโยงของคิวบิต

1.6 ตารางระยะเวลาดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย / สัปดาห์	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1. จัดทำโครงร่างวิทยานิพนธ์																		
2. สอบและปรับแก้ไขโครงร่างวิทยานิพนธ์																		
3. ดำเนินการวิจัยตามแผนการวิจัย																		
3.1 ทำการศึกษาและทดลองออกแบบวงจรสำหรับคอมพิวเตอร์ควอนตัมตามที่เสนอ																		
3.2 วิเคราะห์และสรุปผลการวิจัย																		
4. ดำเนินการตีพิมพ์บทความวิจัยในวารสารวิชาการ																		
5. ดำเนินการทำเล่มวิทยานิพนธ์ฉบับสมบูรณ์																		

ตารางที่ 1 แสดงระยะเวลาดำเนินการวิจัย

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

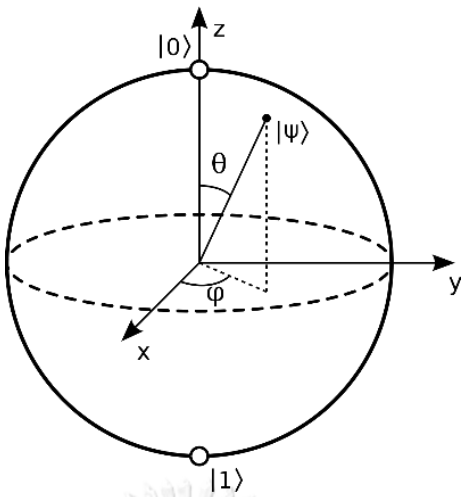
2.1 คอมพิวเตอร์ปัจจุบันและคอมพิวเตอร์ควอนตัม

ความแตกต่างระหว่างคอมพิวเตอร์ปัจจุบันและคอมพิวเตอร์ควอนตัม สิ่งที่เห็นชัดเจนสุดคือบิตในคอมพิวเตอร์ปัจจุบันซึ่งจะมีสถานะการทำงานคือเปิดและปิด (0 หรือ 1) และควอนตัมบิตที่สามารถมีสถานะเป็นความน่าจะเป็นของ 0 และ 1 ซึ่งความน่าจะเป็นนั้นของสถานะ 0 และ 1 จะรวมกันได้ 1.0

บิตในคอมพิวเตอร์ปัจจุบันคือการเปิดและปิดวงจรและกระแสไฟฟ้าไหลผ่าน ถ้ากระแสไฟฟ้าไม่สามารถไหลผ่านได้คือวงจรมีสถานะปิดหรือเรียกว่าศูนย์ และถ้าปล่อยให้กระแสไฟฟ้าสามารถไหลผ่านได้คือวงจรมีสถานะเปิดหรือเรียกว่าหนึ่ง

บิตในคอมพิวเตอร์ควอนตัมหรือเรียกว่าคิวบิตนั้น จะเป็นการวัดสถานะของตำแหน่งของอะตอมบนทรงกลมโบลช (Bloch sphere) ซึ่งสถานะในระบบปัจจุบันสามารถให้คิวบิตเริ่มต้นเป็นค่า $|0\rangle$ หรือ $|1\rangle$ โดย $|0\rangle$ อ่านว่าเค็ทศูนย์สามารถเขียนแสดงด้วยเมทริกซ์ $\begin{bmatrix}1\\0\end{bmatrix}$ โดยตำแหน่งของอะตอมบนทรงกลมโบลชนั้นอยู่ในตำแหน่ง 0 องศาบนแกน z ในภาพที่ 1 และ $|1\rangle$ อ่านว่าเค็ทหนึ่งสามารถเขียนแสดงด้วยเมทริกซ์ $\begin{bmatrix}0\\1\end{bmatrix}$ โดยตำแหน่งของอะตอมบนทรงกลมโบลชนั้นอยู่ในตำแหน่ง 180 องศาตามแกน z ในภาพที่ 1 การวัดผลของคิวบิตนั้นทำในรูปแบบของความน่าจะเป็นที่ผลลัพธ์จะมีค่าเป็น $|0\rangle$ และ $|1\rangle$ โดยคุณสมบัติสำคัญ 2 ประการของคิวบิตคือ ซุปเปอร์โพสิชั่น (Superposition) และเอนแทงเกิลเมนต์ (Entanglement)

1. ซุปเปอร์โพสิชั่น (Superposition) คือความสามารถของคิวบิตที่มีโอกาสจะเป็นทั้ง $|0\rangle$ และ $|1\rangle$
2. เอนแทงเกิลเมนต์ (Entanglement) คือการที่คิวบิตแต่ละคิวบิตมีความสัมพันธ์และส่งผลกระทบต่อกันมีผลทำให้เกิดการเปลี่ยนสถานะได้



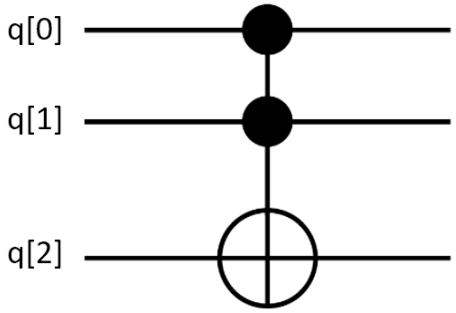
ภาพที่ 1 ทรงกลมโบลช [6]

วงจรในคอมพิวเตอร์ปัจจุบันนั้นประกอบด้วยเกตที่ใช้สำหรับเปลี่ยนสถานะของคิวบิตจาก 0 เป็น 1 หรือ 1 เป็น 0 เนื่องจากสถานะของบิตเป็น 0 หรือ 1 เท่านั้น แต่สำหรับคิวบิตนั้นสามารถอยู่บนตำแหน่งใดๆบนทรงกลมโบลช ตัวอย่างในภาพที่ 1 แสดงสถานะของคิวบิต $|\Psi\rangle$ ซึ่งคิวบิตนั้นไม่ได้มีสถานะเป็น 0 หรือ 1 อย่างใดอย่างหนึ่งเท่านั้น (หากสถานะของคิวบิต $|\Psi\rangle$ มีสถานะเป็น 0 ตำแหน่งของ $|\Psi\rangle$ จะอยู่ในตำแหน่งบวกของแกน z หรือแทนด้วย $|0\rangle$ ในทางตรงกันข้ามหากสถานะของคิวบิต $|\Psi\rangle$ เป็นตำแหน่งของ $|\Psi\rangle$ จะอยู่ในตำแหน่งลบของแกน z หรือแทนด้วย $|1\rangle$) แต่คิวบิต $|\Psi\rangle$ ในภาพที่ 1 นั้นมีสถานะของคิวบิตเป็นทั้ง 0 และ 1 ในเวลาเดียวกัน สามารถเขียนสมการได้ดังนี้ $cos\frac{\theta}{2}|0\rangle + e^{i\Phi}\, sin\frac{\theta}{2}|1\rangle$ ซึ่งปกติสามารถแทนสถานะคิวบิตบนทรงกลมโบลช ในรูปแบบของสถานะจากตัวประกอบของสถานะ $|0\rangle$ และ $|1\rangle$ โดยปัจจุบันการวัดสถานะบน IBM Quantum Experience สามารถวัดสถานะได้ในรูปของความน่าจะเป็นบนแกน $|0\rangle$ และ $|1\rangle$ และสามารถสร้างเกตเพื่อเปลี่ยนสถานะของคิวบิต โดยเกตนั้นจะทำหมุนคิวบิตให้ไปอยู่บนตำแหน่งที่ต้องการของทรงกลมโบลช

วงจรของคอมพิวเตอร์ควอนตัมนั้นต้องเป็นวงจรที่สามารถย้อนกลับได้(Reversible circuit) เหตุผลคือทำให้ความน่าจะเป็นรวมของ $|0\rangle$ และ $|1\rangle$ มีค่าเท่ากับ 1 โดยหนึ่งในเกตที่สามารถย้อนกลับได้คือเกตทอฟโฟลี (Toffoli) เกตที่ได้นำเสนอโดย ทอมมาโซ ทอฟโฟลี (Tommaso Toffoli) ในช่วงเวลาที่ได้ทำงานอยู่ในห้องปฏิบัติการของเอ็มไอที (MIT Laboratory) [7]

เกตทอฟโฟลี ประกอบด้วยอินพุตจำนวน 3 คิวบิต โดยคิวบิตที่ 0 และ 1 คือคิวบิตควบคุม และคิวบิตที่ 2 คือคิวบิตผลลัพธ์ การทำงานของเกตทอฟโฟลี นั้นจะดำเนินการเปลี่ยนสถานะของเอาท์พุตคิวบิตที่ 2 เมื่อคิวบิตที่ 0 และ 1 มีสถานะเป็น 1 จากตารางที่ 2 จะพบว่าเมื่อสถานะของ

อินพุตคิวบิตที่ 0 และ 1 มีค่าเป็น 1 เอาท์พุตคิวบิตที่ 2 จะมีค่าเป็น 1 เมื่ออินพุตเป็น 0 และมีค่าเป็น 0 เมื่ออินพุตเป็น 1 ซึ่งจะเห็นว่าเอาท์พุตมีค่าตรงข้ามกับอินพุตในคิวบิตที่ 2



ภาพที่ 2 สัญลักษณ์ของเกตทอฟโฟลี (Toffoli) หรือเกตซีซีน็อต (CCNOT) บนคอมพิวเตอร์ควอนตัม [8]

อินพุต (Input)			เอาท์พุต (Output)		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

ตารางที่ 2 ตารางความจริงของเกตซีซีน็อต [8]

2.2 ตัวประกอบจำนวนเฉพาะและการเข้ารหัสในปัจจุบัน

การหาตัวประกอบจำนวนเต็มของจำนวนเฉพาะ (integer prime factorization) คือการหาตัวประกอบจำนวนเฉพาะของจำนวนเต็มใดๆ เช่น ตัวประกอบจำนวนเฉพาะของ 15 ประกอบด้วย 3 และ 5 ซึ่งองค์ประกอบจำนวนเฉพาะของจำนวนเต็มใดๆนั้น ได้มีการนำไปใช้เป็นพื้นฐานในการเข้ารหัสของในกระบวนการเข้ารหัสแบบ Public-Key ที่เรียกว่า RSA (Rivest–Shamir–Adleman) [9] ซึ่งเป็นหนึ่งในการเข้ารหัสที่นิยมใช้งานในปัจจุบัน

ปัญหาลอการิทึมแบบไม่ต่อเนื่อง (discrete logarithm problem) ของสมการหารเพื่อหาเศษ $a^r \bmod N$ เป็นตัวอย่างของสมการที่ง่ายในการคิดหาคำตอบทางตรงแต่ยากในการคิดหาคำตอบแบบย้อนกลับซึ่งสมการประเภทนี่เรียกว่า one-way function ซึ่งนำมาใช้ในกระบวนการเข้ารหัสขั้นตอนวิธีการของ RSA นำเสนอไว้ในการเข้ารหัสแบบ Public-Key

ตัวอย่างเมื่อ a มีค่าเท่ากับ 3 และ r มีค่าเท่ากับ 37 และ N มีค่าเท่ากับ 23 สามารถคำนวณหาคำตอบได้ไม่ยาก เพราะคำนวณได้อย่างตรงไปตรงมา คำตอบของ $3^{37} \bmod 23 = 12$ แต่เมื่อต้องการหาคำตอบย้อนกลับเมื่อคำตอบคือ 12 และ a มีค่าเท่ากับ 3 และ N มีค่าเท่ากับ 23 ต้องการทราบว่า r มีค่าเท่าไร ในการคำนวณหาค่าของ r นั้นจะใช้เวลาในการคำนวณเป็นระยะเวลานานเมื่อเทียบกับการคำนวณหาคำตอบของสมการ $a^r \bmod N$ โดยเฉพาะเมื่อ N เป็นจำนวนที่มีค่ามากเวลาในการคำนวณหาค่า r ก็ยิ่งเพิ่มขึ้นเป็นทวีคูณ นี่คือตัวอย่างของ one-way function ที่การหาคำตอบของสมการทำได้อย่างง่ายและใช้เวลาในการคำนวณไม่มาก แต่การหาคำตอบย้อนกลับของสมการนั้นทำได้ยากและใช้เวลาในการคำนวณเป็นระยะเวลานาน

2.3 ขั้นตอนวิธีการของชอร์ [1]

ขั้นตอนวิธีการหาตัวประกอบจำนวนเฉพาะของชอร์ด้วยคอมพิวเตอร์ควอนตัมนั้นประกอบด้วยขั้นตอนวิธีการที่ใช้คอมพิวเตอร์ปัจจุบัน และคอมพิวเตอร์ควอนตัมในการหาตัวประกอบจำนวนเฉพาะสามารถแบ่งออกได้เป็นทั้งหมด 7 ขั้นตอน ดังนี้

1. สุ่มเลือกค่า a ใดๆที่มีค่าน้อยกว่า N
2. คำนวนหาค่าตัวหารร่วมมาก (greatest common divisor) ระหว่าง a และ N
3. ตรวจสอบว่าตัวหารร่วมมากระหว่าง a และ N มีค่าเป็น 1 หรือไม่ หากมีค่าเป็น 1 แสดงว่าคำตอบจำนวนเฉพาะของ N คือ a
4. ให้ใช้วงจรควอนตัมในการคาบของสมการ $a^r \bmod N$
5. ตรวจสอบว่าคาบที่ได้จากข้อที่ 4 เป็นเลขคู่หรือไม่ ถ้าใช่ให้กลับไปทำข้อที่ 1
6. นำค่า r ที่ได้จากข้อที่ 4 มาคำนวน $a^{(r/2)}$ มีค่าเท่ากับ -1 หรือไม่ ถ้าใช่ให้กลับไปทำข้อที่ 1
7. คำนวนหาค่าตัวหารร่วมมากระหว่าง $a^{(r/2)} + 1$ และ N และค่าตัวหารร่วมมากระหว่าง $a^{(r/2)} - 1$ และ N ตัวหารร่วมมากของทั้งสองคือตัวประกอบจำนวนเฉพาะของ N

```
#       loop until found the prime factor of given N

            #       step 1) pick a random number a < N

            #       step 2) compute gcd(a, N)

            #           step 3) if gcd(a, N) != 1 then
            #                   this number is a non-trival factor of N, so
we done
                    #       we are done, we found coprime of N

            #           step 4) otherwise use the quantum period-finding
subroutine
            #                   to find r, the period of the following
function
            #                       f(x) = a**x mod N

            #       step 5) if r is even, go back to step 1)
                    #       goto step 1)

            #       step 6) if a**(r/2) = -1 (mod N), go back to step 1)
                    #       goto step 1)

            #       step 7) gcd( a**(r/2) + 1, N) and gcd( a**(r/2) - 1, N),
            #               both are non-trivial factors of N. we are done

            #       done found non-trivial factor of N
```

ตารางที่ 3 รหัสเทียม (pseudo code) ขั้นตอนวิธีการของชอร์

2.4 คอมพิวเตอร์ควอนตัมของไอบีเอ็ม [10, 11]

คอมพิวเตอร์ควอนตัมของทางไอบีเอ็มใช้เทคโนโลยีตัวนำยิ่งยวดโดยมีพื้นฐานมาจาก Josephson effect ในการเกิดสภาวะไม่เป็นเส้นตรงของการเหนียวนำของแรงดันไฟฟ้า ข้อดีคือสามารถใช้เทคโนโลยีปัจจุบันคือ การสร้างวงจรรวมบนแผ่นราบ สร้างขึ้นโดยการทำงานของเกตอยู่ในระดับนาโนวินาที และยังสามารถเพิ่มระยะเวลาการเชื่อมโยงกันของคิวบิต (qubit coherence) ได้ ซึ่งการพัฒนาคอมพิวเตอร์ควอนตัมนั้นยังต้องการการพัฒนาในส่วนของคุณภาพของคิวบิต ซึ่งสามารถแบ่งออกเป็น 2 ส่วนคือ ระยะเวลาของเกต และระยะเวลาการเชื่อมโยงของคิวบิต

ระยะเวลาของเกตคือระยะเวลาสำหรับการทำงานหนึ่งงาน โดยคอมพิวเตอร์ควอนตัม IBM Q 20 Tokyo นั้นทำงานที่ความถี่ 4.97 GHz ซึ่งคำนวนเป็นระยะเวลาของเกตได้ประมาณ 20 นาโนวินาที

ระยะเวลาการเชื่อมโยงกันของคิวบิตสามารถแบ่งออกได้เป็น 2 ประเภทย่อยดังนี้

1. Relaxation (T1) ระยะเวลาของคิวบิตจากสถานะ excite ที่ $|1\rangle$ ค่อยๆเปลี่ยนเป็นสถานะ Ground คือ $|0\rangle$ (bit-flip error)
2. Dephasing (T2) ระยะเวลาจากสถานะซุปเปอร์โพสิชั่น |+> จนกระทั่งสูญเสียระยะความสัมพันธ์ของ $|0\rangle$ และ $|1\rangle$ (phase-flip error)

โดย IBM Q 20 Tokyo มีค่าเฉลี่ย Relaxation (T1) เฉลี่ยที่ 84.3 โมโครวินาที และ Dephasing (T2) เฉลี่ยที่ 49.6 โมโครวินาที

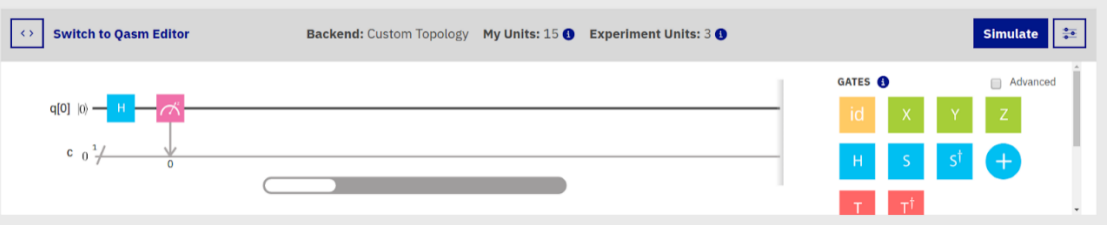
เมื่อทำการคำนวณจำนวนการทำงานต่อระยะเวลาการเชื่อมโยงกัน (coherence) ของ Relaxation ได้ประมาณ 4,215 เกตก่อนที่จะเกิดความผิดพลาดในการกลับคิวบิต (bit-flip error) และสำหรับ Dephasing ได้ประมาณ 2,480 เกตที่จะเกิดความผิดพลาดในการกลับเฟส (phase-flip error) [10]

การพัฒนาวงจรควอนตัมของทาง IBM Quantum Experience นั้นสามารถออกแบบวงจรเพื่อทำงานทดลองวงจรที่ได้ออกแบบนั้นสามารถเป็น 3 ประเภทคือ

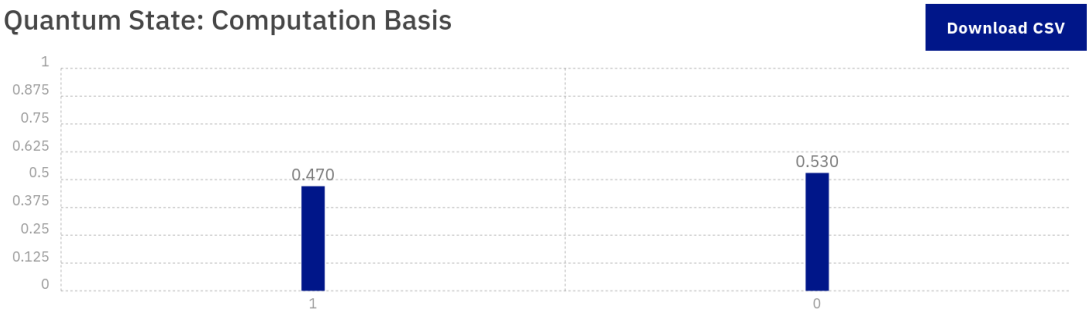
1. จำลองระบบคอมพิวเตอร์ควอนตัมบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน
2. จำลองระบบควอนตัมบนเครื่องของทางไอบีเอ็ม
3. ทดลองบนเครื่องควอนตัมจริงที่ทางไอบีเอ็มสร้างขึ้นและเปิดให้นักวิจัยทดลอง

การออกแบบวงจรสำหรับคอมพิวเตอร์ควอนตัมนั้น ทางไอบีเอ็มได้มีทางเลือกให้กับนักวิจัยและผู้สนใจได้ออกแบบวงจรประกอบด้วย

1. การออกแบบด้วย IBM Q composor [5] ซึ่งมีทางเลือกให้ผู้ใช้งาน 2 แบบ
    - ระบบลากและวางแต่ละเกตลงบนแผงวงจรดังภาพที่ 3
    - ระบบเขียนโปรแกรมด้วยภาษา QASM [11]
2. ทางเลือกคือการใช้ชุดโปรแกรมคำสั่ง Qiskit



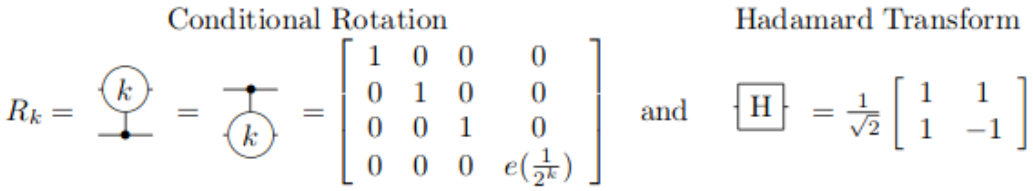
ภาพที่ 3 ตัวอย่างไอบีเอ็ม คิว คอมโพสเซอร์สำหรับการลากและวางเกต โดยวงจรนี้ใช้สำหรับสร้างสถานะซุปเปอร์โพสิชันของคิวบิต [5]



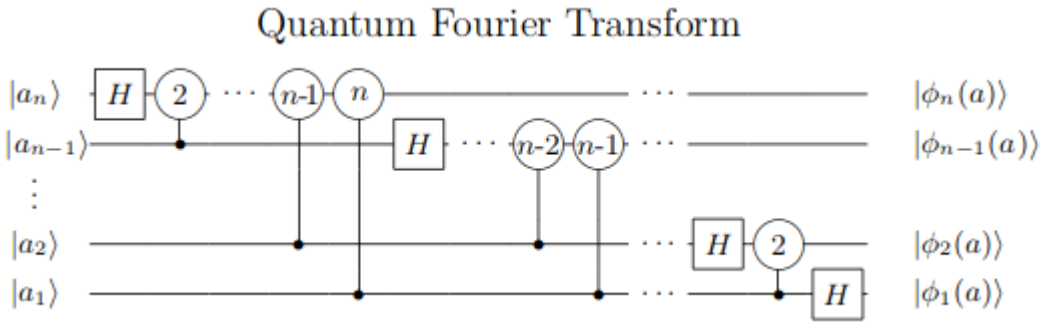
ภาพที่ 4 ผลลัพธ์ของวงจรสร้างสถานะซุปเปอร์โพสิชันของคิวบิตในภาพที่ 3 [5]

2.5 วงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัม (Quantum Fourier transform)

วงจรสำหรับแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัมประกอบด้วยเกตพื้นฐาน 2 ประเภท คือ เกตการหมุนแบบมีเงื่อนไข (conditional rotation gate) และเกตอาดามาร์ (Hadamard gate) (เกตนี้สามารถใช้สำหรับสร้างสถานะซุปเปอร์โพสิชันของคิวบิตได้ดังภาพที่ 3 และ 4) โดยวงจรสามารถสร้างโดยมีรูปแบบของวงจรเป็นไปตามภาพที่ 6 คือเริ่มจากทุกคิวบิตต้องอยู่ในสถานะซุปเปอร์โพสิชันโดยผ่านเกตอาดามาร์ และเกตการหมุนอย่างมีเงื่อนไข เพื่อที่จะสร้างวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัม



ภาพที่ 5 (ซ้าย) สัญลักษณ์และการแสดงในรูปแบบเมทริกซ์ของเกตการหมุนแบบมีเงื่อนไข
(ขวา) สัญลักษณ์และการแสดงในรูปแบบเมทริกซ์ของเกตอาดามาร์ [2, 12]



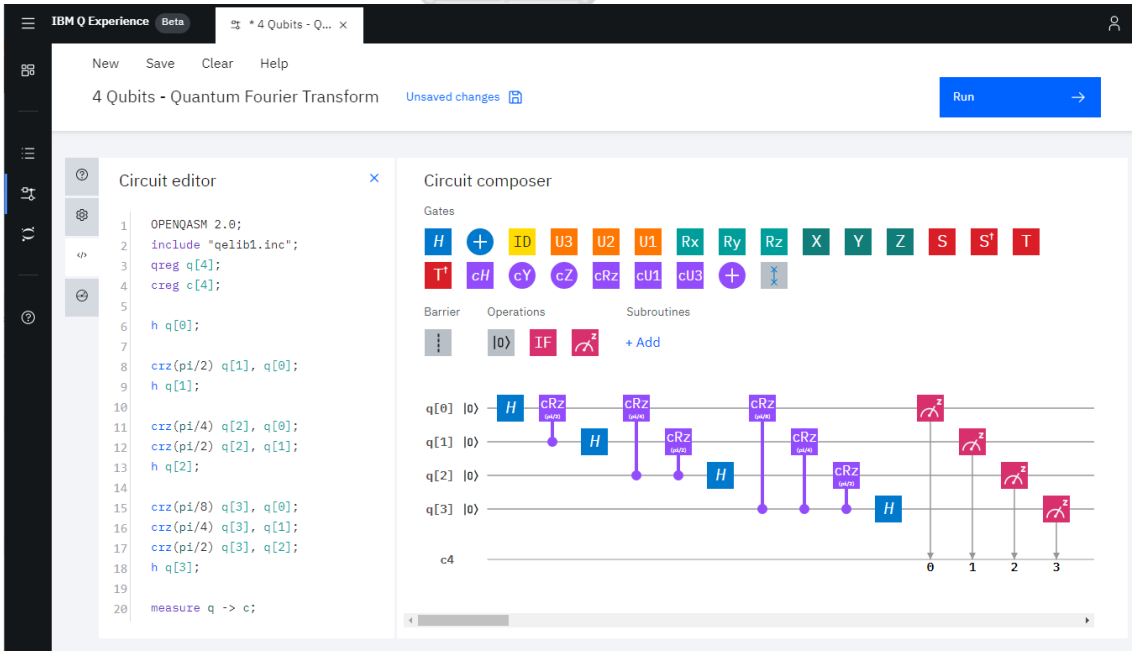
ภาพที่ 6 แสดงตัวอย่างวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัมสำหรับจำนวนคิวบิตใดๆ [2, 12]

$$
\begin{aligned}
|a_n\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n)|1\rangle) && \text{Hadamard transform} \\
&\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n a_{n-1})|1\rangle) && R_2 \text{ rotation conditioned on } a_{n-1} \\
&\quad\vdots && \quad\vdots \\
&\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n a_{n-1}\ldots a_1)|1\rangle) && R_n \text{ rotation conditioned on } a_1 \\
&= |\phi_n(a)\rangle
\end{aligned}
$$

ภาพที่ 7 แสดงสถานะการเปลี่ยนแปลงของคิวบิตใดๆ
เมื่อผ่านวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัมจากวงจรในภาพที่ 6 [2, 12]

ตัวอย่างวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัมสำหรับ 4 คิวบิตนั้นสามารถแสดงได้ในรูปแบบวงจรดังภาพที่ 8 โดยการออกแบบวงจรบนระบบไอบีเอ็ม คิว เอ็กซ์พีเรียนซ์ ที่ใช้ภาษา QASM โดยใช้พื้นฐานการออกแบบวงจรจากภาพที่ 6 โดยมีขั้นตอนดังต่อไปนี้

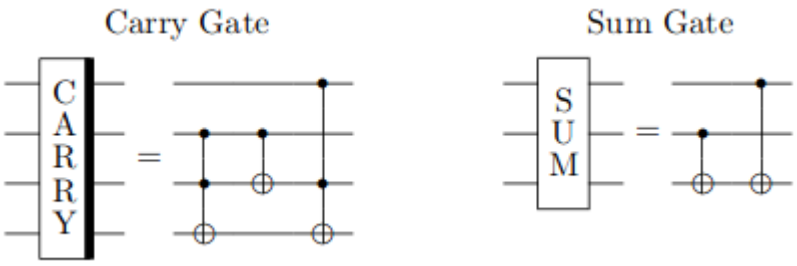
1. สร้างเกตอาดามาร์สำหรับคิวบิตที่ 0
2. สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 1 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 0 ด้วยค่าพาย (Pi) หารด้วย 2 และสร้างเกตอาดามาร์สำหรับคิวบิตที่ 1
3. สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 2 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 0 ด้วยค่าพายหารด้วย 4 สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 2 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 1 ด้วยค่าพายหารด้วย 2 และสร้างเกตอาดามาร์สำหรับคิวบิตที่ 2
4. สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 3 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 0 ด้วยค่าพายหารด้วย 8 สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 3 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 1 ด้วยค่าพายหารด้วย 4 สร้างเกตการหมุนแบบมีเงื่อนไขเมื่อคิวบิตที่ 3 มีค่าเป็น 1 ให้ทำการหมุนคิวบิตที่ 2 ด้วยค่าพายหารด้วย 2 และสร้างเกตอาดามาร์สำหรับคิวบิตที่ 3



ภาพที่ 8 ตัวอย่างวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัมสำหรับ 4 คิวบิต [2, 5, 11, 12]

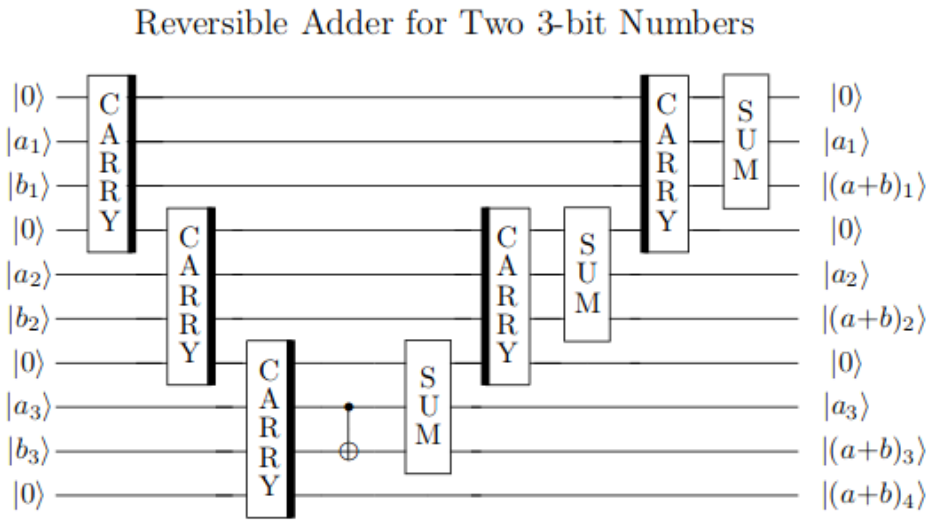
2.6 วงจรบวกบนคอมพิวเตอร์ควอนตัม (Quantum Adder circuit) [2]

วิธีการออกแบบวงจรบวกเลข 2 จำนวนหากใช้ความคิดของคอมพิวเตอร์ปัจจุบันมาออกแบบวงจรบวกเลขสำหรับคอมพิวเตอร์ควอนตัมนั้น วิธีการออกแบบวงจรจะประกอบด้วยใช้เกตแครี่ (carry gate) และเกตรวม (sum gate) ซึ่งส่วนประกอบย่อยของเกตแครี่และเกตรวมนั้น จะถูกสร้างขึ้นจากเกตย่อยๆซึ่งก็คือเกตซีซีน็อต (CCNOT gate) โดยการออกแบบวงจรบวกเลขสำหรับคอมพิวเตอร์ควอนตัมนั้นต้องคำนึงถึงว่าวงจรสามารถทำงานย้อนกลับได้ (reversible circuit) โดยตัวอย่างเกตแครี่และเกตรวมที่สร้างขึ้นนั้นสามารถดูตัวอย่างได้ในภาพที่ 9

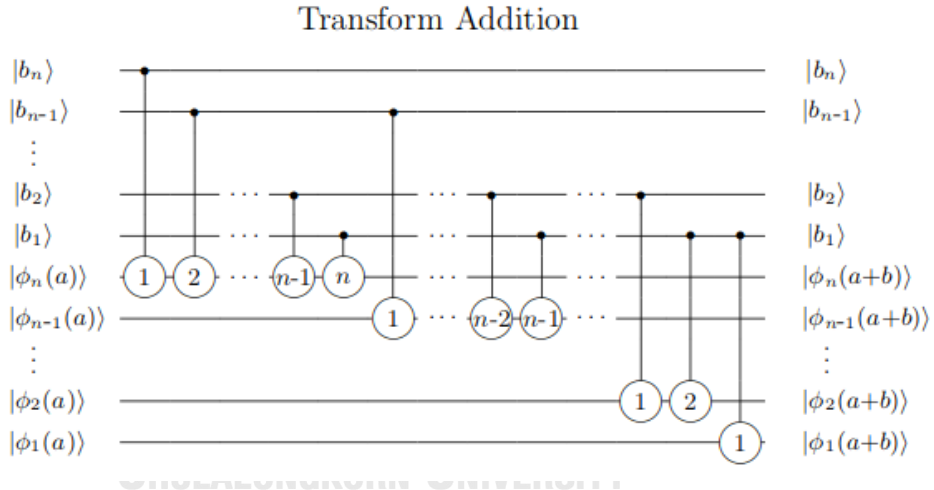


ภาพที่ 9 (ซ้าย) เกตแครี่ที่ประกอบขึ้นจากเกตซีซีน็อต
(ขวา) เกตรวมที่ประกอบขึ้นจากเกตซีซีน็อต [2]

ตัวอย่างของการออกแบบวงจรบวกเลขขนาด 3 บิตที่สามารถย้อนกลับได้ (reversible adder) มีการนำเสนอโดยโทมัส จี แดปเปอร์ ซึ่งประกอบด้วยเกตแครีจำนวนทั้งหมด 5 เกต และเกตรวมทั้งหมดจำนวน 3 เกต และเกตซีซีน็อตที่ไม่รวมอยู่ในเกตแครีและเกตรวมอีก 1 เกต ดังภาพที่ 10 โดยเป็นวงจรที่ใช้ความคิดการออกแบบวงจรมาจากคอมพิวเตอร์คลาสสิก และโทมัส จี แดปเปอร์ยังได้นำเสนอวงจรแปลงการบวก (transform addition) ที่ใช้ความสามารถของคอมพิวเตอร์ควอนตัมซึ่งเกิดจากความคิดในการใช้เกตการหมุนแบบมีเงื่อนไขโดยตัวอย่างวงจรแปลงการบวกที่นำเสนอนั้นออกแบบดังภาพที่ 11 และแสดงการเปลี่ยนสถานะของคิวบิตดังภาพที่ 12



ภาพที่ 10 ตัวอย่างวงจรบวกเลขจำนวน 3 บิตที่สามารถย้อนกลับได้ [2]



ภาพที่ 11 แสดงตัวอย่างวงจรแปลงการบวกบนคอมพิวเตอร์ควอนตัม [2]

$$
\begin{aligned}
|\phi_n(a)\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n a_{n-1}\ldots a_1 + 0.b_n)|1\rangle) && R_1 \text{ rotation from } b_n \\
&\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n a_{n-1}\ldots a_1 + 0.b_n b_{n-1})|1\rangle) && R_2 \text{ rotation from } b_{n-1} \\
&\qquad\vdots && \vdots \\
&\longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + e(0.a_n a_{n-1}\ldots a_1 + 0.b_n b_{n-1}\ldots b_1)|1\rangle) && R_n \text{ rotation from } b_1 \\
&= |\phi_n(a+b)\rangle
\end{aligned}
$$

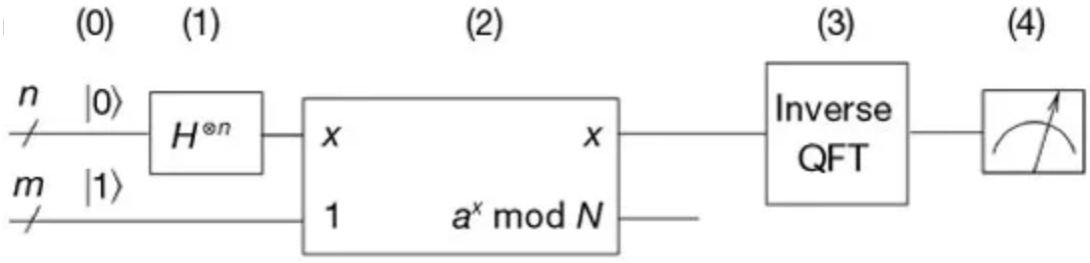
ภาพที่ 12 แสดงสถานการณ์เปลี่ยนแปลงของคิวบิตใดๆ เมื่อผ่านวงจรแปลงการบวกบนคอมพิวเตอร์ควอนตัมจากวงจรในภาพที่ 11 [2]

2.7 วงจรควอนตัมของขั้นตอนกระบวนการของชอร์ (Quantum Shor's circuit) [3, 4]

2.7.1 การทดลองขั้นตอนวิธีการของชอร์บนนิวเคลียร์เมกเนติคเรโซแนนซ์ (nuclear magnetic resonance) [3]

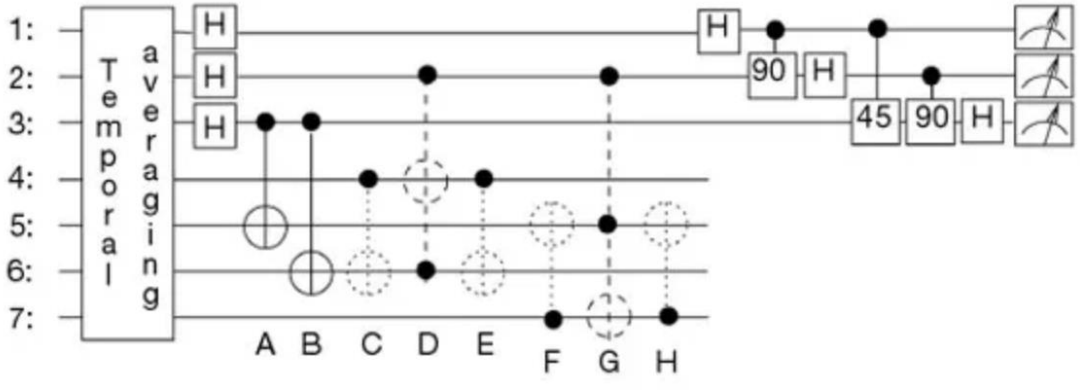
ในปี ค.ศ. 2001 ศูนย์วิจัยของทางบริษัทไอบีเอ็มที่อัลมาเดนได้ทำการทดลองขั้นตอนวิธีการของชอร์โดยการเทคนิคนิวเคลียร์เมกเนติคเรโซแนนซ์ (nuclear magnetic resonance) ในการสร้างคิวบิต [3] โดยงานวิจัยนี้เป็นการทำการทดลองขั้นตอนวิธีการของชอร์สำหรับค่า N ที่มีค่าเท่ากับ 15 โดยวงจรประกอบด้วย 5 ส่วนหลักๆดังภาพที่ 13 คือ

1. กำหนดค่าเริ่มต้นให้กับคิวบิตแต่ละคิวบิต (สัญลักษณ์ (0) ในภาพที่ 13)
2. ให้คิวบิตจำนวนหนึ่งผ่านเกตอาดามาร์ (สัญลักษณ์ (1) ในภาพที่ 13) เพื่อให้คิวบิตอยู่ในสถานะซุปเปอร์โพสิชัน
3. สร้างวงจรสำหรับการคูณด้วย $a^x \ mod \ N$ โดยสุ่มค่าของ x ให้มีค่าระหว่าง a และ N (สัญลักษณ์ (2) ในภาพที่ 13)
4. ให้คิวบิตผ่านวงจรแปลงกลับฟูเรียร์บนคอมพิวเตอร์ควอนตัม (สัญลักษณ์ (3) ในภาพที่ 13)
5. ทำการวัดผลของคิวบิต (สัญลักษณ์ (4) ในภาพที่ 13)



ภาพที่ 13 โครงร่างวงจรสำหรับขั้นตอนวิธีการของชอย์บนนิวเคลียร์เมกเนติคเรโซแนนซ์ [3]

ซึ่งพบว่าวงจรในข้อที่ 2.7.1.3 นั้นเป็นวงจรเฉพาะของ a แต่ละค่าแสดงตัวอย่างได้ในภาพที่ 14 วงจรสำหรับ a มีค่าเท่ากับ 7 และ N มีค่าเท่ากับ 15

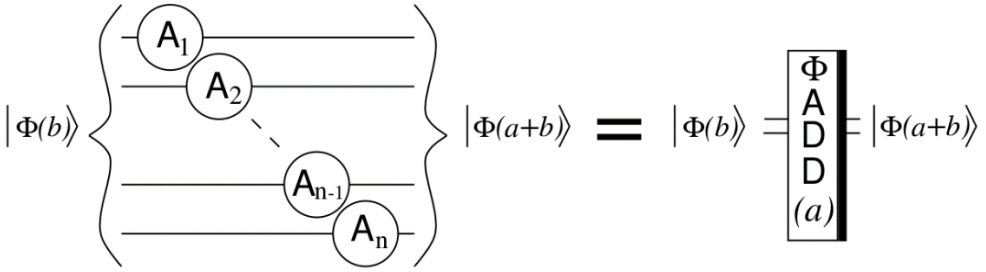


ภาพที่ 14 วงจรในภาพที่ 13 (2) เมื่อ a มีค่าเท่ากับ 7 และ N มีค่าเท่ากับ 15 [3]

2.7.2 วงจรขั้นตอนวิธีการของชอร์นำเสนอโดยสตีเฟ่น เบอรีการ์ด [4]

สำหรับวงจรที่มีการนำเสนอโดยสตีเฟ่น เบอรีการ์ด [4] เพื่อสร้างวงจรทั่วไปสำหรับขั้นตอนวิธีการของชอร์สำหรับหาตัวประกอบจำนวนเฉพาะของสมการ $a^r \bmod N$ โดยมีวงจรพื้นฐาน 2 วงจร ประกอบด้วย วงจรการบวกและวงจรแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัม โดยสามารถแยกย่อยออกเป็นวงจรได้ทั้งหมด 4 วงจรดังต่อไปนี้

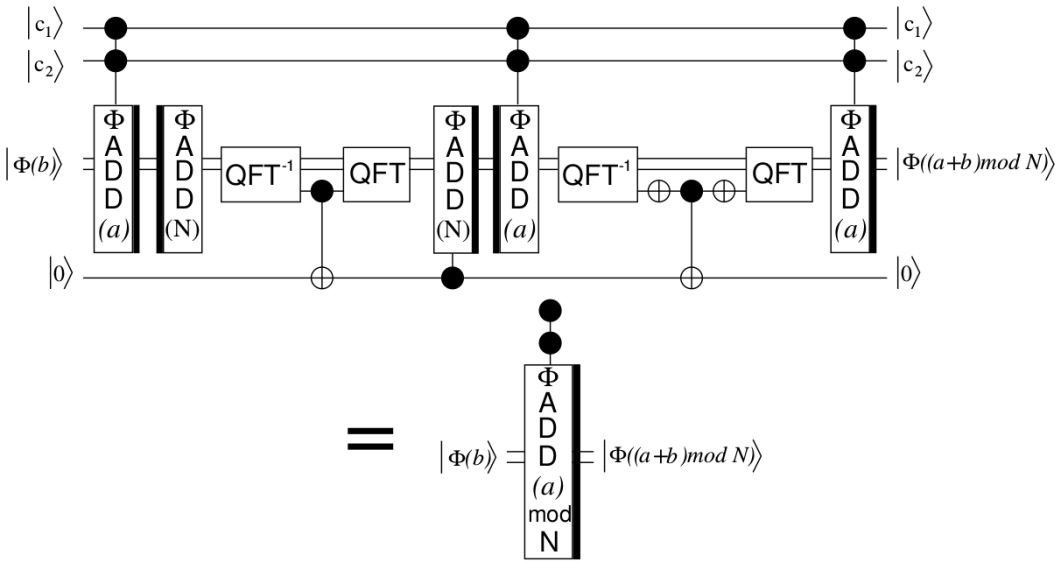
1. วงจรสำหรับบวกเลข 2 จำนวนดังภาพที่ 15 ซึ่งสามารถนำวงจรบวกเลขที่มีการนำเสนอโดยโทมัส จี แดปเปอร์มาสร้างวงจรได้ โดยวงจรนี้จะใช้จำนวนคิวบิตเท่ากับจำนวน $n + 1$ คิวบิต ใช้สำหรับ a หรือ b จำนวน n คิวบิต และ 1 คิวบิตสำหรับตัวทด เมื่อ a และ b บวกเข้าด้วยกันแล้วมีจำนวนมากกว่า n คิวบิต



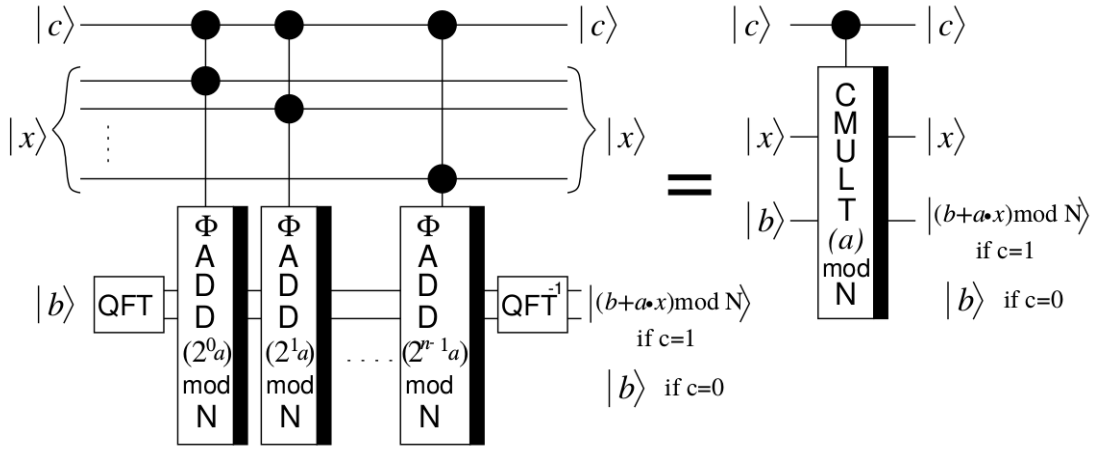
ภาพที่ 15 วงจรบวกเลข 2 จำนวนเป็นวงจรพื้นฐานของวงจรขั้นตอนวิธีการของชอร์ ในภาพคือการบวกระหว่าง a และ b [4]

2. วงจรที่นำวงจรบวกเลข 2 จำนวนในข้อที่ 1 เพื่อใช้เป็นพื้นฐานสำหรับการคำนวนเศษของการหารตามภาพที่ 15 เป็นวงจรสำหรับคำนวนเศษที่เกิดจากการบวก *a* และ *b* เข้าด้วยกันและหารด้วย *N* โดยวงจรที่นำเสนอนั้นมีการนำวงจรแปลงฟูเรียร์และวงจรตรงข้ามการแปลงฟูเรียร์กลับบนคอมพิวเตอร์ควอนตัม โดยเป็นการที่นำ *b* มาบวกด้วย *a* แล้วทำการลบด้วย *N* การลบนั้นเกิดจากการบวกด้วย *N* แล้วทำการใช้วงจรตรงข้ามการแปลงฟูเรียร์บนคอมพิวเตอร์ควอนตัม เพื่อเป็นการคำนวนเศษที่เกิดจากหารด้วย *N* ด้วยมีการใช้คิวบิตจำนวน 1 คิวบิตในการเก็บค่าการลบ (คิวบิต $|0\rangle$ ด้านล่างของภาพที่ 14) จากนั้นทำการบวกด้วย *N* กลับคืน โดยมีการใช้คิวบิตจำนวน 2 คิวบิตในการควบคุมการทำงานของวงจรตามภาพที่ 13 คือ $|C_1\rangle$ และ $|C_2\rangle$ ส่วนวงจรที่เหลืออีกครึ่งหนึ่งเป็นวงจรที่ทำให้วงจรทั้งหมดสามารถทำย้อนกลับได้ โดยจำนวนคิวบิตจะใช้เท่ากับ *n + 3* คิวบิต เมื่อ *n* คือขนาดของจำนวนคิวบิตของ *N*
3. วงจรสำหรับการบวกด้วยจำนวนที่เท่าๆกันแล้วคำนวนหาเศษจากการหารด้วย *N* ภาพที่ 17 เป็นการนำวงจรที่ได้จากข้อที่ 2 มาใช้วงจร โดยแต่ละวงจรที่นำมาประกอบมีค่าเท่ากับสมการ $a^r \bmod N$ เมื่อให้ *r* มีค่าตั้งแต่ 0 ไปถึง *n-1* โดยจำนวนคิวบิตจะใช้เท่ากับ *n + n + 1* คิวบิต เมื่อ *n* คือขนาดของจำนวนคิวบิตของ *N*
4. นำวงจรที่ได้จากข้อที่ 3 มาเชื่อมต่อกันด้วยเกตสลับคิวบิต เพื่อให้วงจรทำงานได้แบบย้อนกลับ โดยจำนวนคิวบิตจะใช้เท่ากับ *2n + 1 + 2* คิวบิต เมื่อ *n* คือขนาดของจำนวนคิวบิตของ *N*

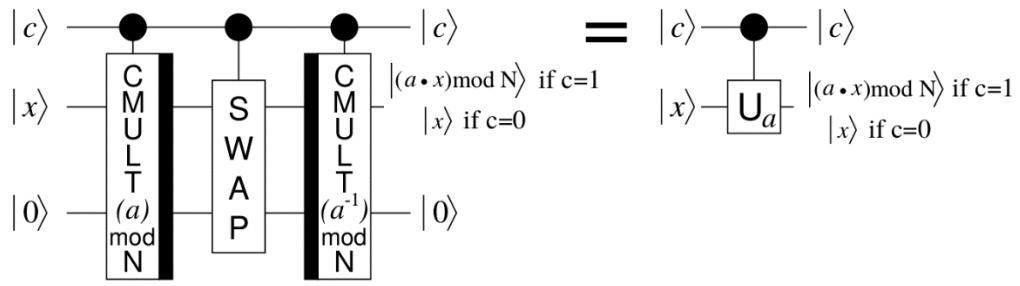
ซึ่งหากคำนวนจำนวนคิวบิตที่ใช้ในการหาตัวประกอบจำนวนเฉพาะเปรียบเทียบกับคอมพิวเตอร์ควอนตัมที่ทางไอบีเอ็มเปิดให้ผู้สนใจใช้งานนั้นมีจำนวนคิวบิตสูงสุดที่ 14 คิวบิต เพราะฉะนั้นถ้าหากใช้การออกแบบวงจรที่นำเสนอไว้โดยสตีเฟ่น เบอรีการ์ด [4] จะสามารถสร้างวงจรสำหรับ *N* จำนวน 5 คิวบิต



ภาพที่ 16 วงจรบวกระหว่าง b และ a จากนั้นคำนวนเศษที่เกิดจากการหารด้วย N [4]



ภาพที่ 17 วงจรคูณด้วยค่าคงที่และคำนวนเศษที่เกิดจากการหาร [4]



ภาพที่ 18 วงจรแลกเปลี่ยนเพื่อทำให้วงจรเป็นวงจรที่สามารถย้อนกลับได้ [4]

บทที่ 3
การออกแบบการวิจัยและเก็บผลรวบรวมข้อมูล

3.1 วงจรบวกบนคอมพิวเตอร์ควอนตัมของไอบีเอ็ม

3.1.1 คอมพิวเตอร์ควอนตัมของไอบีเอ็ม

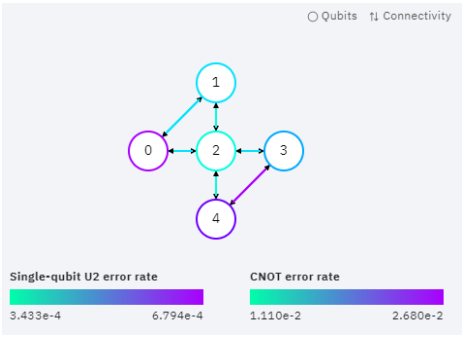
ทางบริษัทไอบีเอ็มมีคอมพิวเตอร์ควอนตัมให้นักวิจัยทดลองใช้งานหลายรุ่นโดยแบ่งออกได้ตามจำนวนคิวบิตและการเชื่อมโยงระหว่างแต่ละคิวบิต เมื่อแบ่งคอมพิวเตอร์ควอนตัมของไอบีเอ็มตามจำนวนคิวบิตสามารถแบ่งออกได้เป็น 1, 5 และ 15 คิวบิต และเครื่องคอมพิวเตอร์ควอนตัมจำลองขนาด 32 คิวบิต ส่วนการแบ่งตามการเชื่อมโยงของแต่ละคิวบิตพบว่าคอมพิวเตอร์ความตัมขนาด 5 คิวบิต มีการเชื่อมโยงของคิวบิต 2 รูปแบบ ประกอบด้วยการเชื่อมโยงแบบใยแมงมุม (พยายามเชื่อมโยงทุกคิวบิตเข้าไว้ด้วยกัน) ตามภาพที่ 19 และการเชื่อมโยงเป็นรูปตัวอักษรที (T) ตามภาพที่ 20 ส่วนภาพที่ 21 แสดงการเชื่อมโยงระหว่างคิวบิตของเครื่องควอนตัมขนาด 15 คิวบิต รูปแสดงการเชื่อมโยงความระหว่างคิวบิตนั้นประกอบด้วยวงกลมแสดงคิวบิต ภายในวงกลมระบุลำดับของคิวบิต และเส้นตรงแสดงความเชื่อมโยงของคิวบิตแต่ละลำดับ

สำหรับการทดลองวงจรบวกบนคอมพิวเตอร์ควอนตัมของไอบีเอ็ม ผู้ทำการวิจัยเลือกการวิจัยสำหรับวงจรบวกขนาด 2 คิวบิต เนื่องจากเหตุผลที่สำคัญ 2 ประการ ประการแรกคือจำนวนคิวบิตที่ต้องการสำหรับวงจรบวกเลขจำนวนเต็มขนาด 2 คิวบิต ซึ่งต้องการเครื่องควอนตัมที่มีจำนวนคิวบิตไม่เกินจำนวน 5 คิวบิต โดยอินพุตสำหรับเลขจำนวนเต็มขนาด 2 คิวบิต 2 จำนวน ต้องการจำนวนคิวบิตทั้งหมด 4 คิวบิต และผลลัพธ์ของการบวกจำนวนต้องการทั้งหมด 3 คิวบิต ประกอบด้วยผลลัพธ์ของค่าผลรวม (sum) การบวกของคิวบิตตำแหน่งที่ 0 ตำแหน่งที่ 1 และคิวบิตสำหรับตัวทด (carry) ประการที่สองคือการทดลองสามารถทดลองบนเครื่องควอนตัมที่แตกต่างกันในด้านสถาปัตยกรรม ได้แก่ การจัดวางตำแหน่งรวมถึงการเชื่อมโยงของแต่ละคิวบิต ซึ่งมีจำนวนทั้งหมด 4 เครื่อง (รวมเครื่องคอมพิวเตอร์ควอนตัมจำลอง)

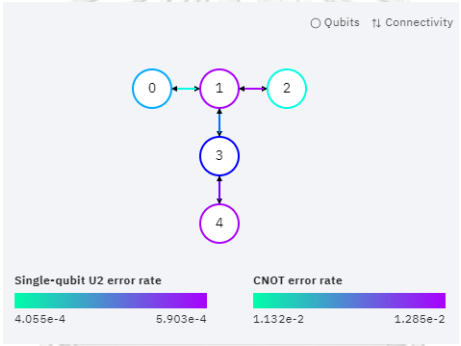
เครื่องคอมพิวเตอร์ควอนตัมของทางบริษัทไอบีเอ็มที่ผู้วิจัยเลือกสำหรับการวิจัยวงจรบวกเลขจำนวนเต็มประกอบด้วย

1. คอมพิวเตอร์ควอนตัมจำลอง ขนาด 32 คิวบิต
2. คอมพิวเตอร์ควอนตัม Essex ขนาด 5 คิวบิต
3. คอมพิวเตอร์ควอนตัม Yorktown ขนาด 5 คิวบิต

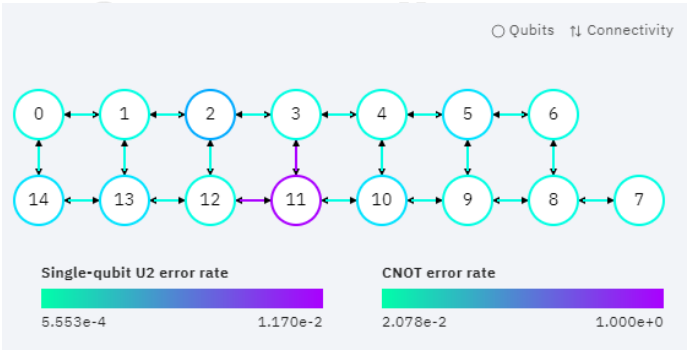
4. คอมพิวเตอร์ควอนตัม Melbourne ขนาด 15 คิวบิต



ภาพที่ 19 แสดงตำแหน่งและการเชื่อมโยงระหว่างคิวบิตบนเครื่องไอบีเอ็มยอร์กทาวน์ (Yorktown)



ภาพที่ 20 แสดงตำแหน่งและการเชื่อมโยงระหว่างคิวบิตบนเครื่องไอบีเอ็มเอสเซ็กซ์ (Essex)



ภาพที่ 21แสดงตำแหน่งและการเชื่อมโยงระหว่างคิวบิตบนเครื่องไอบีเอ็มเมลเบิร์น (Melbourne)

3.2 วงจรบวกเลขจำนวนเต็มบนคอมพิวเตอร์ควอนตัม

3.2.1 วงจรบวกที่นำเสนอไว้โดยโทมัส จี แดปเปอร์

วงจรบวกเลขจำนวนเต็มนำเสนอโดยโทมัส จี แดปเปอร์ มีชื่อว่าวงจรแปลงการบวก (transition addition) ใช้หลักการของควอนตัมฟูเรียร์ทรานส์ฟอร์ม (quantum Fourier transform) เมื่อพิจารณาสมการควอนตัมฟูเรียร์ทรานส์ฟอร์ม สมการที่ 1 โดยสามารถเปลี่ยนรูปสมการเป็นสมการที่ 2 การเปลี่ยนรูปกระทำโดยการเปลี่ยนการบวกจากสัญลักษณ์ ∑ เป็นการบวกแต่ละพจน์แทน

$$|\mathrm{j}\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \tag{1}$$

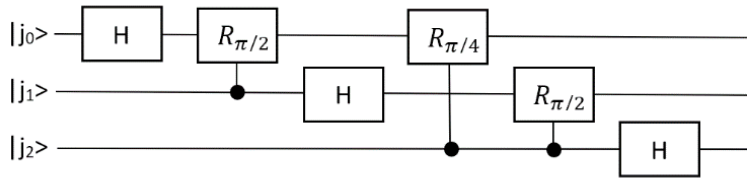
$$|j_1 1, \dots, j_n\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right) \dots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle\right)}{2^{n/2}} \tag{2}$$

สมการที่ 2 หากพิจารณา $\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$ พจน์ของสมการพบว่าเกตสำหรับการควบคุมการหมุน (controlled rotation gate) สัญลักษณ์ R_k เมื่อแสดงเกตในรูปแบบของเมทริกซ์สามารถแสดงได้ตามสมการที่ 3 และเกตอาดามาร์ (Hadamard gate) ใช้สำหรับเปลี่ยนสถานะของคิวบิตให้อยู่ในสถานะ Superposition สามารถแสดงในรูปแบบเมทริกซ์ดังสมการที่ 4

ทั้งสองเกตข้างต้นที่กล่าวมาสามารถนำมาใช้สำหรับการสร้างวงจรควอนตัมฟูเรียร์ทรานส์ฟอร์มได้ดังตัวอย่างวงจรในภาพที่ 22

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \tag{3}$$

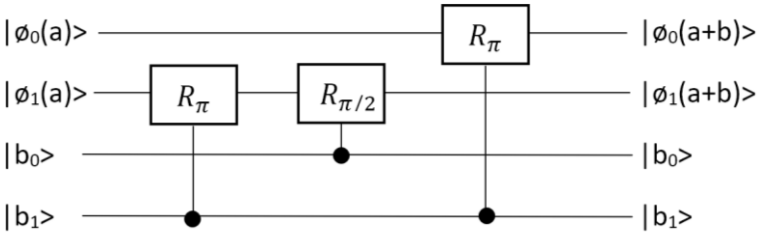
$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{4}$$



ภาพที่ 22 แสดงตัวอย่างวงจรควอนตัมฟูเรียร์ทรานส์ฟอร์มของวงจรขนาด 3 คิวบิต

จากแนวความคิดของสมการควอนตัมฟูเรียร์ทรานส์ฟอร์มในสมการที่ 1 โทมัส จี เด็ปเปอร์ นำเสนอเพื่อประยุกต์ใช้งานสำหรับการสร้างวงจรบวกโดยการใช้เกตความคุมการหมุนกับแต่ละคิวบิต กำหนดให้จำนวนเต็มแทนด้วยตัวแปรในรูปของเลขฐาน 2 แทนจำนวนเต็มใดๆในรูปแบบ $a_{n-1}a_{n-2}...a_1a_0$ เมื่อ $a = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + ... + a_12^1 + a_02^0$ สามารถเขียนเป็นสมการดังสมการที่ 5 และวงจรบวกเลขจำนวนเต็มขนาดสองคิวบิต ในภาพที่ 23 โดยในที่นี่ใช้สัญลักษณ์ a แทนจำนวนเต็มแรก และ b แทนจำนวนเต็มที่สอง ดังนั้นวงจรบวกจำนวนเต็มของ a และ b ประกอบด้วยอินพุตจำนวน 4 คิวบิต ซึ่งคิวบิตของจำนวนเต็ม a แสดงในอินพุตของวงจรตำแหน่งทีคิวบิตที่ 0 และ 1 ส่วนคิวบิตของจำนวนเต็ม b แสดงอินพุตของวงจรในตำแหน่งของคิวบิตที่ 2 และ 3 ในด้านของเอาต์พุตนั้นประกอบด้วยผลลัพธ์ของการบวกจำนวนเต็มของ a และ b ในคิวบิตที่ 0 และ 1 โดยเอาต์พุตคิวบิตที่ 0 แสดงผลลัพธ์จากการบวก a และ b ในคิวบิตที่ 0 และเอาต์พุตคิวบิตที่ 1 แสดงผลลัพธ์จากการบวก a และ b ในคิวบิตที่ 1

$$|\emptyset_{n-1}(a)\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e(0.a_{n-1}...a_0 + 0.b_{n-1}...b_0)|1\rangle) \quad (5)$$

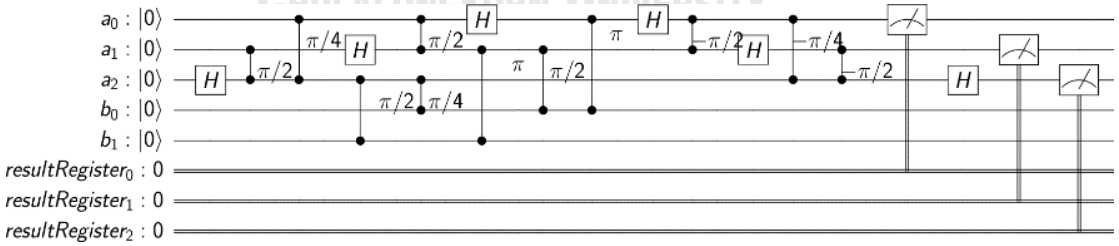


ภาพที่ 23 แสดงวงจรบวกจำนวนเต็มขนาด 2 คิวบิต

3.2.2 วงจรบวกจำนวนเต็มขนาด 2 คิวบิตสำหรับคอมพิวเตอร์ควอนตัมของไอบีเอ็ม

จากวงจรบวกที่นำเสนอโดยโทมัส จี เด็ปเปอร์นั้นการบวกจำนวนเต็ม *n* คิวบิตใดๆ ต้องการ 2 คูณ *n* คิวบิตสำหรับวงจรบวก จากหัวข้อ 3.1.1 คอมพิวเตอร์ควอนตัมของไอบีเอ็มขนาด 5 และ 15 คิวบิต ดังนั้นวงจรบวกที่นำเสนอไว้นั้นหากต้องการนำไปทดลองเพื่อเปรียบเทียบ จะสามารถสร้างวงจรบวกจำนวนเต็มสูงสุดขนาด 2 คิวบิต เพราะวงจรบวกสำหรับจำนวนเต็มขนาด 2 คิวบิตต้องใช้จำนวนคิวบิตจำนวน 4 คิวบิต เมื่อพิจารณาวงจรบวกสำหรับจำนวนเต็มขนาด 2 คิวบิต การบวกของคิวบิตจะสามารถบวกได้แค่ 1 คิวบิต เนื่องจากคิวบิตสำคัญที่สุด (most significant qubit) ใช้สำหรับตัวทด (carry qubit)

เมื่อพิจารณาถึงข้อจำกัดข้างต้นของวงจรบวกสำหรับจำนวนเต็มอย่างละเอียดแล้วพบว่าคิวบิตของตัวทดประกอบวงจรบวกสำหรับ *n* คิวบิตใดๆ ต้องการคิวบิตตัวทดขนาด 1 คิวบิต โดยจะต้องใช้ทั้งหมดสำหรับวงจรทั้งหมด 2 คูณ *n* คิวบิตสำหรับอินพุตการบวกจำนวนเต็มสองจำนวน และอีก 1 คิวบิตสำหรับบิตทด เพราะฉะนั้นวงจรบวกจำนวนเต็มใดๆขนาด *n* คิวบิต ต้องการคอมพิวเตอร์ควอนตัมขนาด *2n+1* คิวบิต ดังนั้นวงจรบวกขนาด 2 คิวบิตนั้นต้องใช้คอมพิวเตอร์ควอนตัมขนาด 5 คิวบิต ซึ่งคอมพิวเตอร์ควอนตัมขนาด 5 คิวบิตนี้ทางบริษัทไอบีเอ็มมีเครื่องควอนตัมขนาด 5 คิวบิตขึ้นไปจำนวน 3 เครื่องประกอบด้วยเครื่องคอมพิวเตอร์ควอนตัมยอร์กทาวน์ (Yorktown) เอสเซ็กซ์ (Essex) และเมลเบิร์น (Melbourne) และเมื่อรวมกับเครื่องคอมพิวเตอร์ควอนตัมจำลองขนาด 32 คิวบิต จะสามารถสร้างวงจรบวกเลขจำนวนเต็มใดๆขนาด 2 คิวบิตบนเครื่องคอมพิวเตอร์ควอนตัมได้ถึง 4 เครื่อง แต่เนื่องจากวงจรที่นำเสนอไว้โดยโทมัส จี เด็ปเปอร์ ต้องการ *2n* คิวบิต ไม่สามารถมีคิวบิตตัวทดได้ ทำให้ต้องมีการปรับปรุงและแก้ไขวงจรที่เคยมีการนำเสนอไว้



ภาพที่ 24 แสดงวงจรบวกขนาด 2 คิวบิต ของ a และ b ซึ่ง a มีคิวบิตสำหรับตัวทดขนาด 1 คิวบิต

3.3 การทดลองและผลการทดลอง

ผลการทดลองแสดงดังตารางที่ 1 จากตารางแสดงอัตราความแม่นยำของคำตอบของวงจรบวกบนคอมพิวเตอร์ควอนตัมซึ่งถูกออกแบบสำหรับการบวกระหว่าง 1 คิวบิต และการบวกระหว่าง 2 คิวบิต โดยทำการทดลองบนเครื่องคอมพิวเตอร์ควอนตัมจำนวน 3 เครื่องที่มีสถาปัตยกรรมของระบบที่แตกต่างกัน ได้แก่เครื่อง Essex เครื่อง Yorktown และเครื่อง Melbourne ผู้วิจัยได้ทดลองรันวงจรบวกดังกล่าวจำนวน 8,192 ครั้ง และเลือกผลลัพธ์ที่มีค่าความน่าจะเป็นสูงสุดเป็นคำตอบ

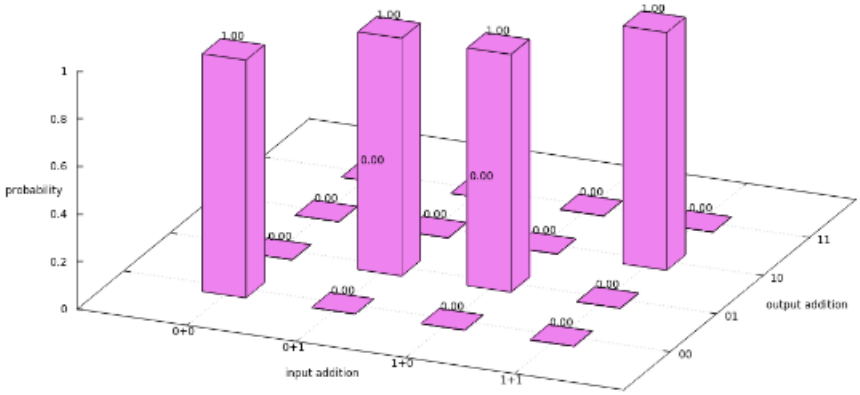
สำหรับการทดลองรันวงจรบวก 1 คิวบิตบนเครื่อง Essex ผลการทดลองมีแนวโน้มที่ดีเนื่องจากให้ผลลัพธ์ที่ถูกต้องเสมอ ดังภาพที่ 26 และให้ผลลัพธ์ที่ถูกต้องมากกว่าเครื่อง Yorktown และเครื่อง Melbourne ซึ่งทั้ง 2 เครื่องให้ผลลัพธ์ที่ถูกต้องเพียง 50% แต่เมื่อพิจารณาผลการทดลองรันวงจรบวก 2 คิวบิตบนเครื่อง Essex กลับได้ผลลัพธ์ที่ถูกต้องเพียง 25% ส่วนเครื่อง Yorktown ให้ผลลัพธ์ที่ถูกต้องรองลงมาคือ 6.25% ในขณะที่เครื่อง Melbourne ไม่ได้ผลลัพธ์ที่ถูกต้องเลย

เมื่อนำค่าความน่าจะเป็นของคำตอบทั้งหมดจากการรันวงจรบวก 1 คิวบิต และ 2 คิวบิตมาแสดงในรูปของกราฟ โดยแกน *XY* แทนระนาบพื้น แกน *X* คือคิวบิตที่เป็นอินพุตเลขฐาน 2 แกน *Y* คือคิวบิตที่เป็นเอาต์พุตเลขฐาน 2 และแกน *Z* คือค่าความน่าจะเป็นของเอาต์พุตหรือคำตอบ ซึ่งอยู่ระหว่าง 0 ถึง 1 สามารถแสดงค่าความน่าจะเป็นของคำตอบทั้งหมดจากการรันวงจรบวก 1 คิวบิตบนเครื่อง simulator เครื่อง Essex เครื่อง Yorktown และเครื่อง Melbourne ในรูปแบบของกราฟได้ดังภาพที่ 25 – 28 ตามลำดับ และภาพที่ 29 – 32 แสดงค่าความน่าจะเป็นของคำตอบทั้งหมดจากการรันวงจรบวก 2 คิวบิตบนเครื่อง simulator เครื่อง Essex เครื่อง Yorktown และเครื่อง Melbourne ตามลำดับ

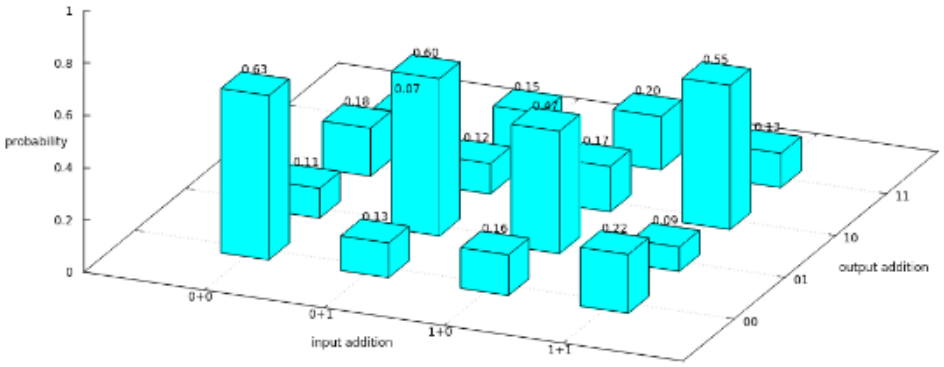
จากกราฟแสดงความน่าจะเป็นของคำตอบจะเห็นได้ว่าสำหรับการรันวงจรบวก 1 คิวบิต และ 2 คิวบิตบนเครื่อง simulator ให้ผลลัพธ์ของคำตอบที่ถูกต้องเสมอ จึงสามารถนำมาใช้เปรียบเทียบกับกราฟแสดงความน่าจะเป็นของคำตอบของวงจรบวกบนเครื่องคอมพิวเตอร์ควอนตัมอื่นๆ เมื่อเปรียบเทียบกราฟแสดงความน่าจะเป็นจากการรันวงจรบวก 1 คิวบิตบนเครื่อง simulator กับเครื่องคอมพิวเตอร์ควอนตัมอื่นๆ จะเห็นได้ว่ากราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Essex (ภาพที่ 26) มีลักษณะใกล้เคียงกับกราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง simulator มากที่สุด เมื่อเทียบกับกราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Yorktown และ Melbourne โดยกราฟแท่งที่สูงที่สุดอยู่ที่ตำแหน่งเดียวกัน ในขณะที่กราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Yorktown (ภาพที่ 27) กราฟแท่งที่สูงที่สุดที่เหมือนกับกราฟแสดงความ

น่าจะเป็นของคำตอบที่รันบนเครื่อง simulator (ภาพที่ 25) คือที่อินพุตเป็น 0+0 และ 1+0 ในขณะที่อินพุต 0+1 และ 1+1 กราฟแท่งที่สูงเป็นอันดับที่ 2 ที่ตรงกับเครื่อง simulator ส่วนกราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Melbourne (ภาพที่ 28) กราฟแท่งที่สูงที่สุดที่เหมือนกับกราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง simulator (ภาพที่ 25) คือที่อินพุตเป็น 0+0 และ 0+1 ในขณะที่อินพุต 1+0 และ 1+1 กราฟแท่งที่สูงเป็นอันดับที่ 2 และอันดับที่ 3 ตามลำดับที่ตรงกับเครื่อง simulator

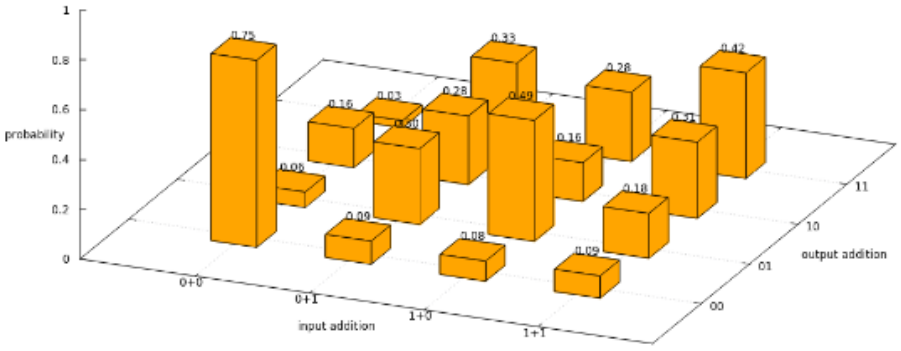
เมื่อเปรียบเทียบกราฟแสดงความน่าจะเป็นของคำตอบของวงจรบวก 2 คิวบิตบนเครื่อง simulator จากภาพที่ 30 – 32 จะเห็นได้ว่าไม่มีกราฟแท่งที่สูงที่สุดอย่างเห็นได้ชัด โดยเฉพาะกราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Melbourne ความน่าจะเป็นของแต่ละคำตอบไม่แตกต่างกันมาก โดยกราฟแท่งที่มีความน่าจะเป็นสูงสุดคือที่เอาต์พุตเป็น 000 และเมื่อพิจารณากราฟแสดงความน่าจะเป็นของคำตอบที่รันบนเครื่อง Essex (ภาพที่ 30) และเครื่อง Yorktown (ภาพที่ 31) ให้กราฟแท่งสูงที่สุดที่ตรงกับเครื่อง simulator เฉพาะที่อินพุตเป็น 00 + 00 และเอาต์พุตเป็น 000



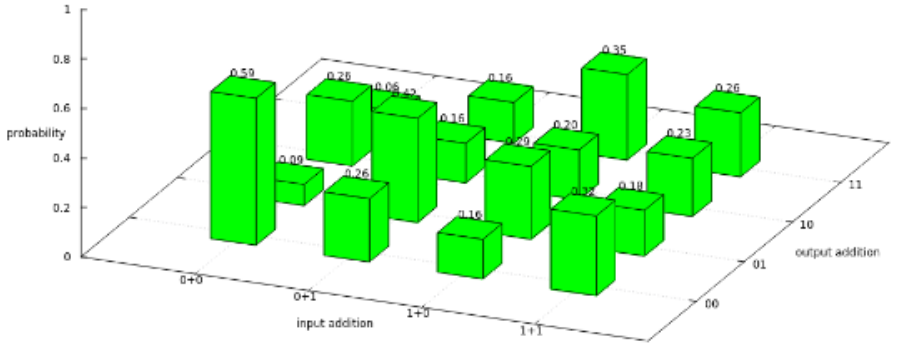
ภาพที่ 25 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 1 คิวบิต บนเครื่อง simulator



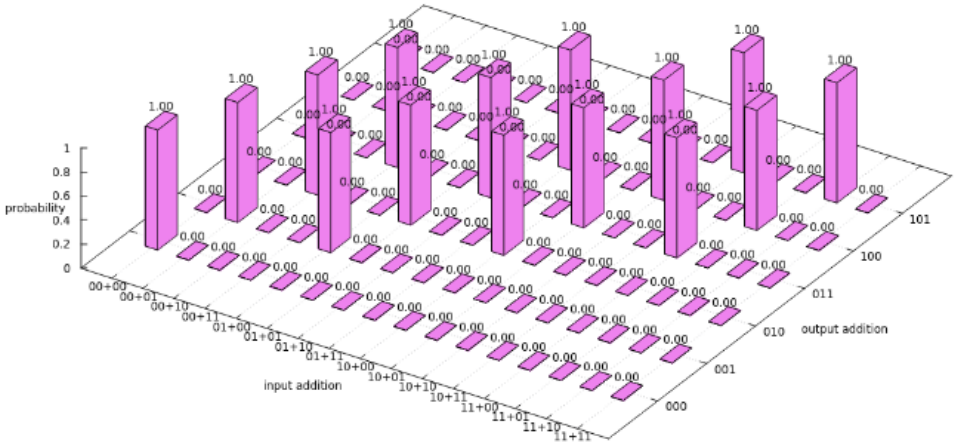
ภาพที่ 26 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 1 คิวบิต บนเครื่อง Essex ขนาด 5 คิวบิต



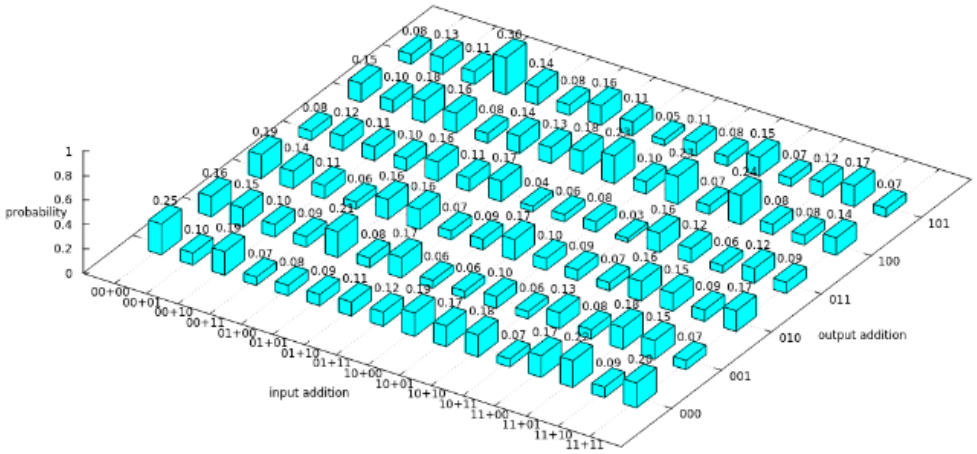
ภาพที่ 27 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 1 คิวบิต บนเครื่อง Yorktown ขนาด 5 คิวบิต



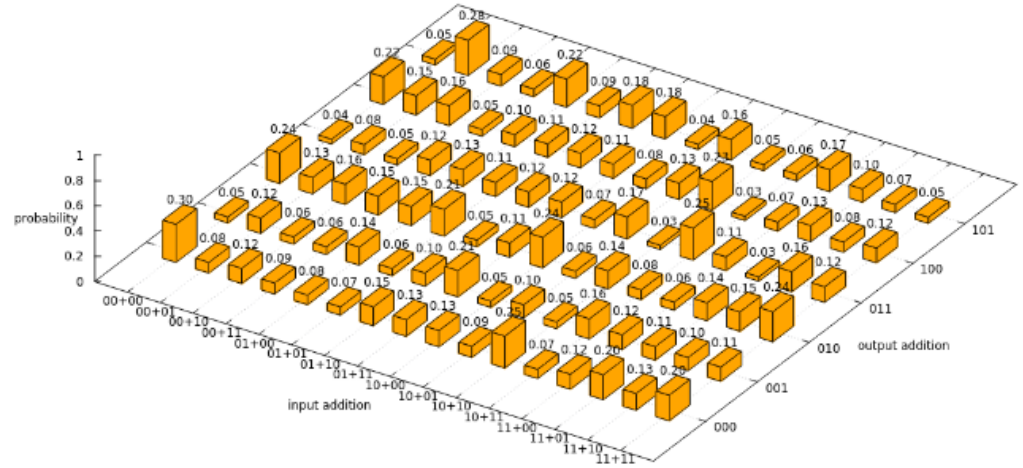
ภาพที่ 28 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 1 คิวบิต บนเครื่อง Melbourne ขนาด 15 คิวบิต



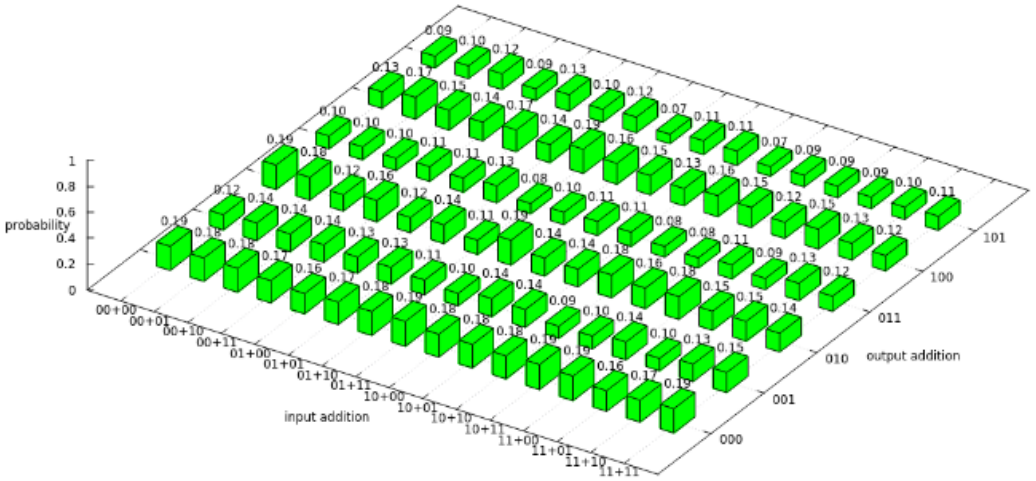
ภาพที่ 29 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 2 คิวบิต บนเครื่อง simulator



ภาพที่ 30 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 2 คิวบิต บนเครื่อง Essex ขนาด 5 คิวบิต



ภาพที่ 31 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 2 คิวบิต บนเครื่อง Yorktown ขนาด 5 คิวบิต



ภาพที่ 32 กราฟแสดงค่าความน่าจะเป็นของทุกคำตอบของวงจรบวก 2 คิวบิต บนเครื่อง Melbourne ขนาด 15 คิวบิต

บทที่ 4
สรุปผลการวิจัย

4.1 สรุปผลการวิจัย

งานวิจัยนี้นำเสนอวงจรบวกสำหรับ 1 คิวบิต และ 2 คิวบิต บนเครื่องคอมพิวเตอร์ควอนตัมของไอบีเอ็มที่แตกต่างกันจำนวน 3 เครื่อง วงจรบวกที่สร้างอ้างอิงจากงานวิจัยของโทมัส จี แดปเปอร์ [2] การต่อวงจรลงบนอุปกรณ์จริงสามารถทำได้โดยไม่ต้องมีความรู้เดิมเกี่ยวกับการเชื่อมต่อของคิวบิตบนเครื่องคอมพิวเตอร์ควอนตัมของไอบีเอ็ม ซึ่งเป็นสถานการณ์จริงที่เราใช้อุปกรณ์ IBM โดยที่เราไม่ทราบล่วงหน้าว่าเครื่องมือสร้างวงจรมีการทำงานอย่างไร

จากผลการทดลองสามารถสรุปได้ว่าวงจรบวก 1 คิวบิตบนเครื่อง Essex ให้ความแม่นยำของคำตอบที่ดีที่สุด เมื่อเปรียบเทียบกับวงจรบวก 1 คิวบิตบนเครื่อง Yorktown และวงจรบวก 1 คิวบิตบนเครื่อง Melbourne โดยให้ผลลัพธ์ของคำตอบของทุกๆอินพุตได้ถูกต้อง ในขณะที่ผลลัพธ์ของคำตอบของวงจรบวก 1 คิวบิตบนเครื่อง Yorktown และ Melbourne ให้ผลลัพธ์ของคำตอบที่ถูกต้องเพียง 50% อย่างไรก็ตามเมื่อพิจารณาผลการทดลองสำหรับวงจรบวก 2 คิวบิตบนเครื่อง Essex กลับพบว่าผลลัพธ์ของคำตอบที่ถูกต้องลดลงไปอย่างมาก โดยอัตราความแม่นยำของคำตอบเพียง 25% สอดคล้องกับผลลัพธ์ของคำตอบของวงจรบวก 2 คิวบิตบนเครื่อง Yorktown และ Melbourne ที่ก็ลดลงอย่างมากเช่นกัน โดยเครื่อง Yorktown มีอัตราความแม่นยำของคำตอบเพียง 6.25% ส่วนอัตราความแม่นยำของคำตอบของเครื่อง Melbourne คือ 0% ซึ่งความน่าจะเป็นของคำตอบทุกคำตอบค่อนข้างใกล้เคียงกัน และอาจกล่าวได้ว่าความน่าจะเป็นของทุกๆคำตอบไม่แตกต่างกันอย่างมีนัยสำคัญ

เครื่องคอมพิวเตอร์ควอนตัมของไอบีเอ็มทั้ง 3 เครื่อง เมื่อเพิ่มจำนวนคิวบิตในวงจรบวก ความแตกต่างของความน่าจะเป็นระหว่างคำตอบที่ถูกต้องและคำตอบอื่นๆ มีแนวโน้มลดลงอย่างมาก ยกตัวอย่างเช่น เครื่อง Melbourne แม้ว่าอัตราความแม่นยำของคำตอบของวงจรบวก 2 คิวบิตเป็น 0% แต่เมื่อพิจารณาความแตกต่างของความน่าจะเป็นระหว่างคำตอบที่ถูกต้องและคำตอบที่มีความน่าจะเป็นสูงสุด แตกต่างกันเพียง 4% ซึ่งแสดงให้เห็นว่าเมื่อเพิ่มจำนวนคิวบิต ความมั่นใจในคำตอบของเครื่องคอมพิวเตอร์ควอนตัมมีความมั่นใจลดลง ดังจะเห็นได้จากความน่าจะเป็นของแต่ละคำตอบค่อนข้างใกล้เคียงกัน ดังนั้นการใช้ความน่าจะเป็นของคำตอบที่สูงสุดเพียงอย่างเดียวในการแทนคำตอบของวงจรบวกบนเครื่องคอมพิวเตอร์ควอนตัมอาจไม่ใช่วิธีที่ดีที่สุด ณ ปัจจุบันนี้

จากงานวิจัยนี้ อาจกล่าวได้ว่าเราอาจไม่สามารถสร้างวงจรบวกบนเครื่องคอมพิวเตอร์ควอนตัมที่ใหญ่ขึ้นได้ถ้าเราไม่มีความรู้เกี่ยวกับสถาปัตยกรรมของเครื่องคอมพิวเตอร์ควอนตัม ผู้วิจัยหวังว่างานวิจัยนี้จะมีประโยชน์ไม่มากก็น้อยสำหรับนักวิจัยท่านอื่นๆที่จะนำงานวิจัยนี้ไปปรับปรุงคุณภาพของผลลัพธ์ของคำตอบในการรันวงจรบวก หรือวงจรใดๆ บนเครื่องคอมพิวเตอร์ควอนตัม

4.2 มุมมองต่องานวิจัยในอนาคต

คอมพิวเตอร์ควอนตัมนั้นยังอยู่ในช่วงของการพัฒนาให้ห้องวิจัยของบริษัทต่างๆ ซึ่งยังมีความไม่แน่นอนว่าสุดท้ายคอมพิวเตอร์ควอนตัมที่บุคคลหรือบริษัทต่างๆสามารถเข้าถึงได้จะใช้เทคโนโลยีใดซึ่งอาจจะไม่จำเป็นต้องเป็นในรูปแบบที่ต้องมีการออกแบบวงจรจำเพาะก็เป็นได้ ฉะนั้นแล้วความรู้และความเข้าใจในพื้นฐานของควอนตัม และวิธีขั้นตอนที่มีการนำเสนอไว้เช่นวิธีขั้นตอนการหาตัวประกอบจำนวนเฉพาะของชอร์จึงเป็นสิ่งสำคัญเพราะหากมีความเข้าใจที่ดีพอจึงจะสามารถประยุกต์ตามเทคโนโลยีที่มีการเปลี่ยนไปได้

บรรณานุกรม

1. Shor, P.W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM J. Comput., 1997. **26**(5): p. 1484-1509.
2. Draper, T.G. *Addition on a Quantum Computer*. 2000 June 1, 2019]; Available from: https://arxiv.org/abs/quant-ph/0008033.
3. Vandersypen, L.M.K., et al., *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.* Nature, 2001. **414**(6866): p. 883-887.
4. Beauregard, S., *Circuit for Shor's algorithm using 2n+3 qubits.* Quantum Info. Comput., 2003. **3**(2): p. 175-185.
5. IBM. *IBM Q Experience*. May 1, 2019]; Available from: https://quantumexperience.ng.bluemix.net.
6. Rigetti. *Rigetti QPU Specifications*. May 1, 2019]; Available from: https://www.rigetti.com/qpu.
7. Toffoli, T., *Reversible Computing.* Laboratory for Computer Science, Massachusetts Institute of Technology, 1980(MIT/LCS/TM-151).
8. Wikipedia. *Toffoli Gate*. May 1, 2019]; Available from: https://en.wikipedia.org/wiki/Toffoli_gate.
9. Wikipedia. *RSA (cryptosystem)*. May 1, 2019]; Available from: https://en.wikipedia.org/wiki/RSA_(cryptosystem).
10. Sheldon, J.G.a.S. *Cramming More Power Into a Quantum Device*. March 4, 2019]; Available from: https://www.ibm.com/blogs/research/2019/03/power-quantum-device/.
11. Andrew W. Cross, L.S.B., John A. Smolin, Jay M. Gambetta. *Open Quantum Assembly Language*. 2017 January 10, 2017]; Available from: https://arxiv.org/abs/1707.03429.
12. Nielsen, M.A. and I.L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 2011: Cambridge University Press. 708.

ประวัติผู้เขียน

ชื่อ-สกุล นายวิภู เมธาชวลิต

วุฒิการศึกษา ปี พ.ศ. 2560 จบการศึกษา นิติศาสตรบัณฑิต
มหาวิทยาลัยสุโขทัยธรรมาธิราช นนทบุรี ประเทศไทย

ปี พ.ศ. 2553 จบการศึกษา วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี กรุงเทพมหานคร ประเทศไทย

ปี พ.ศ. 2549 จบการศึกษา ระดับมัธยมศึกษา สายการเรียนวิทย์-คณิต
โรงเรียนระยองวิทยาคม ระยอง ประเทศไทย

ที่อยู่ปัจจุบัน จังหวัดกรุงเทพมหานคร ประเทศไทย