การศึกษาการคำนวณแบบควอนตัมด้วยควอนตัมดอตโมเลกุล

STUDY ON QUANTUM COMPUTATION BY QUANTUM DOT MOLECULE

นายณัฐชัย ถนอมธรรม รหัส 52361741

นายนิรวิทธ์ ต้นวงษ์ รหัส 52361918

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2555

ใบรับรองปริญญานิพนธ์

ชื่อหัวข้อโครงงาน	การศึกษาการคำนวณแบบควอนตัมด้วยควอนตัมดอทโมเลกุล		
ผู้ดำเนินโครงงาน	นายณัฐชัย	ถนอมธรรม	รหัส 52361741
	นายนิรวิทธ์	ต้นวงษ์	รหัส 52361918
ที่ปรึกษาโครงงาน	ดร.สุวิทย์	กิระวิทยา	
สาขาวิชา	วิศวกรรมไฟฟ้า		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2555		

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้ปริญญานิพนธ์**ฉบับนี้เป็นส่วนหนึ่ง**ของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า

Suvit Kiravittaya ..... **ที่ปรึกษาโครงงาน**

(ดร.สุวิทย์ กิระวิทยา)

..... **กรรมการ**

(ดร.มุฑิตา สงฆ์จันทร์)

..... **กรรมการ**

(อ.เศรษฐา ตั้งค้าวานิช)

ชื่อหัวข้อโครงงาน	การศึกษาการคำนวณแบบควอนตัมด้วยควอนตัมดอทโมเลกุล		
ผู้ดำเนินโครงงาน	นายณัฐชัย	ถนอมธรรม	รหัส 52361741
	นายนิรวิทธ์	ต้นวงษ์	รหัส 52361918
ที่ปรึกษาโครงงาน	ดร.สุวิทย์	กิระวิทยา	
สาขาวิชา	วิศวกรรมไฟฟ้า		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2555		

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้ เป็นการศึกษาเรียนรู้เกี่ยวกับการคำนวณแบบควอนตัมด้วยควอนตัมดอทโมเลกุล โดยในการคำนวณแบบควอนตัม จะเป็นการคำนวณโดยอาศัย กลศาสตร์ควอนตัม ซึ่งเป็น กฎทางฟิสิกส์สำหรับระบบอะตอมและโมเลกุล และ การคำนวณแบบควอนตัมนี้ถูกแสดงให้เห็นแล้วว่า สามารถใช้ในการแก้ปัญหาบางปัญหาได้รวดเร็วกว่าการคำนวณแบบดั้งเดิม สำหรับในปริญญานิพนธ์นี้ เราจะนำเสนอ การแก้ปัญหาการแยกตัวประกอบของจำนวนเฉพาะ ด้วยระเบียบวิธีของชอร์ โดยการกำหนดค่าตัวเลข ด้วยสถานะของอิเล็กตรอน ในโครงสร้างควอนตัมดอทโมเลกุล ทำให้เราสามารถนำ โครงสร้างควอนตัมดอทโมเลกุลนี้ มาใช้เป็นเครื่องคำนวณแบบควอนตัมได้

Project title	Study on Quantum Computation by Quantum Dot Molecule		
Name	Mr. Nathachai	Thanomtham	ID. 52361741
	Mr. Nirawit	Tonwong	ID. 52361918
Project advisor	Dr. Suwit	Kiravittaya	
Major	Electrical Engineering		
Department	Electrical and Computer Engineering		
Academic year	2012		

Abstract

This project is a study on quantum computation by quantum dot molecule. Quantum computation is a computation based on quantum mechanics, which is a physical law for atomic and molecular systems. It has been shown that this computation can efficiently solve some kind of problem as compared to the classical one. For this project, we present Shor's algorithm for prime number factorization. By relating numbers to the states of electrons in quantum dot molecular structure, one can use quantum dot molecules as quantum computer.

กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงไปได้ ด้วยความกรุณาเป็นอย่างยิ่งจาก ดร. สุวิทย์ กิระวิทยา ซึ่งเป็นอาจารย์ที่ปรึกษาของโครงงาน และ ได้คอยชี้แนะแนวทางตลอดการทำงานในโครงงานนี้ คณะผู้ดำเนินโครงงานจึงขอกราบขอบพระคุณเป็นอย่างสูง และ ขอระลึกถึงความกรุณาของท่านไว้ตลอดไป

ขอขอบคุณ คณาจารย์ทุกท่าน ที่ประสิทธิ์ประสาทวิชาความรู้ ให้กับ คณะผู้ดำเนินโครงงาน นอกจากนี้ ยังต้องขอขอบคุณ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์ ที่ให้ใช้ห้อง เพื่อศึกษาโครงงาน จนทำให้การทำโครงงานสำเร็จลุลวงไปได้

เหนือสิ่งอื่นใด คณะผู้ดำเนินโครงงาน ขอกราบขอบพระคุณบิดามารดา ผู้มอบความรัก เมตตา สติปัญญา รวมทั้งเป็นผู้ให้ทุกสิ่งทุกอย่างตั้งแต่วัยเยาว์ จวบจนปัจจุบัน คอยเป็นกำลังใจ ทำให้ได้รับความสำเร็จอย่างทุกวันนี้ และ ขอบคุณ ทุก ๆ คนในครอบครัว ของคณะผู้ดำเนินโครงงาน ที่ไม่ได้กล่าวไว้ ณ ที่นี้ด้วย

นายณัฐชัย ถนอมธรรม
นายนิรวิทธ์ ต้นวงษ์

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหา

ในปัจจุบัน เครื่องคอมพิวเตอร์ที่เราใช้ในการทำงานทั่วไป มีความเร็วในการประมวลผลค่อนข้างจำกัด โดยความถี่สัญญาณนาฬิกาสูงสุด ที่คอมพิวเตอร์ทั่วไป สามารถทำงานได้ อยู่ที่ประมาณ 3 กิกะเฮิรตซ์ นักวิทยาศาสตร์บางกลุ่ม ได้ค้นคิด และ ศึกษา การคำนวณแบบใหม่ ที่ต่างจากการคำนวณแบบดั้งเดิม เพื่อให้การคำนวณมีประสิทธิภาพมากขึ้น โดยการคำนวณแบบควอนตัม (Quantum computation) เป็นการคำนวณชนิดหนึ่งที่ถูกค้นคิดขึ้น โดยในการคำนวณชนิดนี้เราสามารถใช้ โครงสร้าง ควอนตัมดอทโมเลกุล (Quantum dot molecule) ในการสร้างคอมพิวเตอร์ที่อาศัยการคำนวณแบบควอนตัม

ควอนตัมดอท (Quantum dot) เป็นโครงสร้างที่สามารถกักเก็บอิเล็กตรอนได้ทุกทิศทาง โครงสร้าง ควอนตัมดอท นี้ สามารถสร้างได้จาก สารประกอบกึ่งตัวนำ (Semiconductor compound) เช่น อินเดียมอาเซไนด์ ใน แกลเลียมอาร์เซไนด์ (InAs/GaAs) และ เป็นโครงสร้างที่มีขนาดเล็ก ในระดับนาโนเมตร สำหรับ โครงสร้างของควอนตัมดอทโมเลกุล (Quantum dot molecule) ก็คือ โครงสร้างควอนตัมดอท ที่อยู่ใกล้กันมาก จนเกิดการควบคู่ (coupled) กัน เมื่อมองโครงสร้าง ควอนตัมดอทโมเลกุล นี้ ผ่านเครื่องมือที่สามารถสำรวจโครงสร้างระดับนาโน จะมองเห็นว่าโครงสร้างนี้มีลักษณะเป็นจุด อยู่ใกล้กัน

หลักการทำงานของคอมพิวเตอร์ โดยทั่วไป คือมีการเก็บและประมวลผลตัวเลข ที่เป็นเลขฐานสอง โดย นิยามขนาดของข้อมูล ในหน่วย ไบนารี่ ดิจิต (Binary digit) หรือ บิต (Bit) ซึ่งเป็นพื้นฐานที่ใช้บอกสถานะของข้อมูล ข้อมูลหนึ่งบิต มีสองสถานะ คือ 0 กับ 1 ตามนิยามของเลขฐานสอง ในกรณีของ การคำนวณแบบควอนตัม จะใช้สถานะของอนุภาคเป็นตัวแทนของบิต แต่เนื่องจาก คุณสมบัติของระบบทางควอนตัมที่สามารถสร้าง สถานะทับซ้อน (Superposition state) ได้ ทำให้สถานะของอนุภาคตัวเดียวนี้ สามารถนำมาแทนสถานะระหว่าง 0 และ 1 ได้ โดยอาศัยหลักการของความน่าจะเป็น ซึ่งจะทำให้สามารถทำการประมวลข้อมูลที่อยู่ระหว่าง 0 และ 1 ได้ เราเรียก ข้อมูลที่มีคุณสมบัตินี้ว่า ควอนตัมบิต (Quantum bit) หรือ คิวบิต (Qubit) จาก ทฤษฎีข่าวสาร (Information theory) เราทราบว่า เมื่อ นำหลาย ๆ บิตมาต่อกัน เราก็จะสามารถแทนสถานะหรือข้อมูลได้หลายรูปแบบมากขึ้น อย่างเช่น ถ้ามีข้อมูลขนาด 3 บิต เราจะสามารถเก็บข้อมูลได้ 8 สถานะ เป็นต้น อย่างไรก็ตามในขณะเวลาหนึ่งจะมีเพียงสถานะเดียวปรากฏอยู่ในข้อมูลนั้น แต่ถ้าเปลี่ยนข้อมูลขนาด 3 บิต เป็น 3 คิวบิต จะได้ว่า ในขณะเวลาหนึ่งนั้น จะมีทั้ง 8 สถานะปรากฏอยู่ โดยแต่ละคิวบิต สามารถมีสถานะระหว่าง 0 และ 1 ได้ ดังนั้นข้อมูลขนาด n คิวบิต เราจะสามารถ

เก็บข้อมูลได้ 2^n ตัวในครั้งเดียว และ สามารถประมวลผลข้อมูลที่อยู่ระหว่าง 0 และ 1 ได้ โดยอาศัยหลักการของความน่าจะเป็น ซึ่งทำให้การคำนวณลักษณะนี้ ต่างจาก การคำนวณแบบดั้งเดิมและต่างจากการคำนวณแบบขนาน (Parallel computation) ที่เรารู้จักกัน การคำนวณแบบขนานหมายถึง การช่วยกันประมวลผล ในการประมวลผล ข้อมูลจำนวนมาก/ขนาดใหญ่ ที่จะต้องแบ่งงานกันทำ ระหว่างหลาย ๆ หน่วยประมวลผล ที่อยู่ในคนละสิ่งแวดล้อม (หมายถึงคนละหน่วยประมวลผล และ คนละชุดหน่วยความจำ และ อาจจะใช้คนละระบบปฏิบัติการด้วย) เมื่อเปรียบเทียบ คอมพิวเตอร์แบบควอนตัมที่มีขนาด n คิวบิต กับ คอมพิวเตอร์ทั่วไปที่มี n บิต จะเห็นได้ว่า คอมพิวเตอร์แบบควอนตัมที่มีขนาด n คิวบิต ประมวลผล ข้อมูล 2^n ตัวได้ในครั้งเดียว ในขณะที่ คอมพิวเตอร์ทั่วไปต้องประมวลผล 2^n ครั้ง หรือต้องใช้คอมพิวเตอร์ 2^n ตัวช่วยกันประมวลผล โดยหาก n มีค่ามาก ๆ การคำนวณแบบควอนตัม จะมีประสิทธิภาพ เหนือ การคำนวณแบบดั้งเดิม เพราะ มีการเพิ่มขึ้นของความเร็วในการคำนวณแบบยกกำลัง

1.2 จุดมุ่งหมายของการศึกษา

1. เพื่อศึกษาเรียนรู้และทำความเข้าใจ หลักการของการคำนวณแบบควอนตัม
2. เพื่อศึกษาพื้นฐานของ โครงสร้าง ควอนตัมดอทโมเลกุล โดย ศึกษาเกี่ยวกับ โครงสร้างทางกายภาพ และ โครงสร้างทางอิเล็กทรอนิกส์ เพื่อที่จะสามารถนำไปใช้ ในการอธิบายการคำนวณแบบควอนตัม ด้วยโครงสร้างนี้ได้

1.3 ขอบเขตของโครงงาน

1. ศึกษาและเรียนรู้การคำนวณโดยใช้การคำนวณแบบควอนตัม
2. ศึกษาและเรียนรู้ รูปแบบของควอนตัมดอทโมเลกุล ในการคำนวณแบบควอนตัม

1.4 ขั้นตอนและแผนการดำเนินงาน

รายละเอียด	ปี 2555							ปี 2556		
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1) ศึกษาข้อมูลเบื้องต้นเกี่ยวกับการคำนวณแบบควอนตัม										
2) ศึกษาข้อมูลเบื้องต้นเกี่ยวกับโครงสร้างคอนตัมดอทโมเลกุล										
3) ศึกษาการคำนวณแบบควอนตัมโดยใช้โครงสร้างคอนตัมดอทโมเลกุล										
4) อธิบายการคำนวณแบบควอนตัมโดยใช้โครงสร้างคอนตัมดอทโมเลกุล										
5) จัดทำปริญญานิพนธ์ฉบับสมบูรณ์										

1.5 ประโยชน์ที่คาดว่าจะได้รับจากโครงงาน

1. สามารถเข้าใจและอธิบายพื้นฐาน การคำนวณแบบควอนตัมได้
2. สามารถเข้าใจการคำนวณแบบควอนตัมโดยใช้ โครงสร้างควอนตัมดอทโมเลกุลได้

1.6 งบประมาณ

1. ค่าเข้าเล่มปริญญานิพนธ์	1,200 บาท
2. ค่าถ่ายเอกสาร	800 บาท
รวมเป็นเงินทั้งสิ้น (สองพันบาทถ้วน)	2,000 บาท

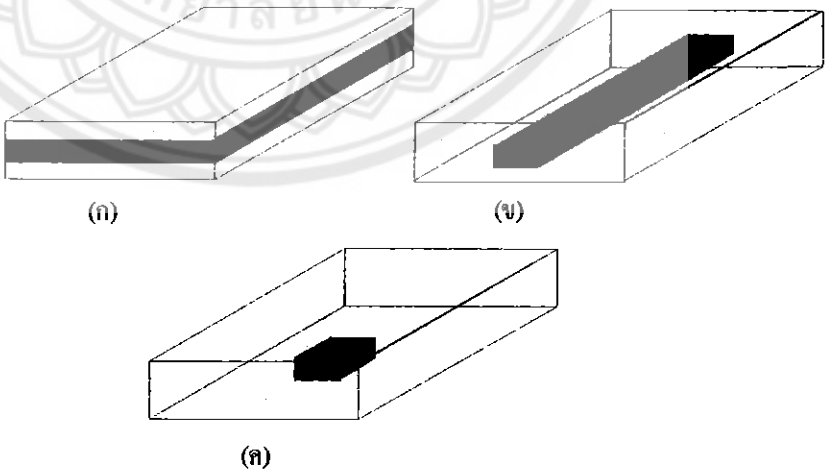
หมายเหตุ: ถัวเฉลี่ยทุกรายการ

บทที่ 2
หลักการและทฤษฎี

นักวิทยาศาสตร์ได้ คิดค้น และ ศึกษา โครงสร้างควอนตัมนาโน (Quantum nanostructures) โดย การศึกษานี้ มีทั้งด้านทฤษฎี และ การทดลอง และ มีการนิยาม โครงสร้างบ่อควอนตัม (Quantum well) เป็นโครงสร้างที่สามารถกักเก็บอิเล็กตรอน ใน 1 มิติ โครงสร้างควอนตัมไวร์ (Quantum wire) เป็นโครงสร้างที่สามารถกักเก็บอิเล็กตรอน ใน 2 มิติ และ โครงสร้างควอนตัมดอท (Quantum dot) เป็นโครงสร้างที่สามารถกักเก็บอิเล็กตรอน ใน 3 มิติ ดังนั้น โครงสร้างควอนตัมดอท มีลักษณะเป็น โครงสร้างที่อิเล็กตรอนไม่สามารถเคลื่อนที่ได้อย่างอิสระในทุกทิศทาง ในปัจจุบัน โครงสร้างควอนตัมนาโนเหล่านี้ มีการใช้งานอยู่ใน สิ่งประดิษฐ์ต่าง ๆ เช่น เลเซอร์สารกึ่งตัวนำ (Semiconductor laser)

2.1 ควอนตัมดอท

ควอนตัมดอท เป็นโครงสร้างที่มีความสามารถในการกักเก็บอิเล็กตรอน ได้ในทุกทิศทาง โครงสร้างนี้ สามารถสร้างได้จาก สารประกอบที่มีคุณสมบัติเป็น สารกึ่งตัวนำ เช่น แกลเลียมอาร์เซไนด์ (GaAs) และ อินเดียมอาร์เซไนด์ (InAs) โดยมันเป็นโครงสร้างระดับนาโน เมื่อมองโครงสร้างของควอนตัมดอทนี้ ผ่านเครื่องมือที่สามารถสำรวจโครงสร้างระดับนาโนจะมองเห็นว่าโครงสร้างนี้มีลักษณะเป็นจุด จึงเรียกโครงสร้างนาโนของวัสดุลักษณะเช่นนี้ว่าเป็น "ดอท" [1]



รูปที่ 2.1 ลักษณะ (ก) โครงสร้างบ่อควอนตัม (ข) โครงสร้างควอนตัมไวร์ และ (ค) โครงสร้างควอนตัมดอท

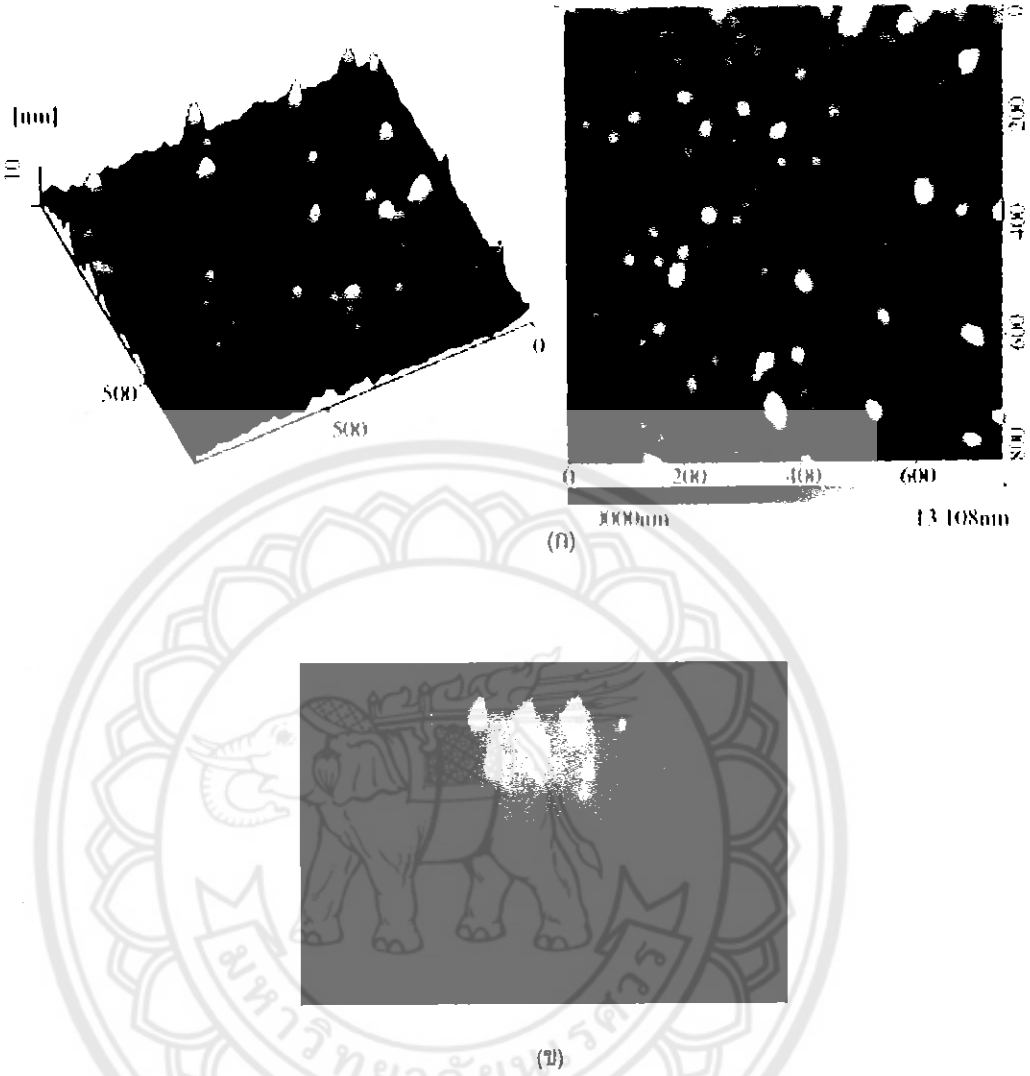
โครงสร้างควอนตัมดอท มีคุณสมบัติ ที่มีความเฉพาะ ทางแสงและทางไฟฟ้า โดยมันถูกนำเสนอว่า เป็นโครงสร้างที่เหมาะนำไปใช้เพิ่มประสิทธิภาพในการทำงานของอุปกรณ์อิเล็กทรอนิกส์ทางแสงต่าง ๆ เช่น ไดโอดเปล่งแสง เลเซอร์ ตัวตรวจจับแสง เซลล์แสงอาทิตย์

ต่อมา ได้มีการพัฒนา วิธีการสร้าง โครงสร้างควอนตัมดอท โดยใช้เทคนิคการปลูกผลึกด้วยลำโมเลกุล (Molecular beam epitaxy, MBE) หรือ เทคนิคการปลูกสารจากไอเคมีของสารประกอบโลหะ-อินทรีย์ (Metal organic chemical vapor deposition, MOCVD) ซึ่งเป็นเทคนิคในการปลูกผลึกบนพื้นผิวสารกึ่งตัวนำ ที่ทำให้ได้ผลึกที่มีความสมบูรณ์สูง ยิ่งไปกว่านั้นยังมีการพัฒนาในรายละเอียดของแต่ละเทคนิค เพื่อใช้เพิ่มประสิทธิภาพของโครงสร้างควอนตัมดอท สำหรับคุณสมบัติด้านต่าง ๆ เช่น การปรับขนาดของชั้นอะตอมและระยะของดอท เป็นต้น จากการศึกษาเบื้องต้น จะสามารถสรุปได้ เป็นความรู้พื้นฐานว่า โครงสร้างควอนตัมนาโนนี้ โดยเฉพาะอย่างยิ่ง โครงสร้างควอนตัมดอท จะสร้างได้โดยใช้เทคนิคการปลูกผลึกด้วยลำโมเลกุล และในระหว่างการสร้างโครงสร้างนี้ เราจะสามารถเห็นผิวของโครงสร้างได้โดย การสังเกตรูปแบบการเลี้ยวเบนของลำอิเล็กตรอนพลังงานสูงที่สะท้อนจากผิว (Reflection high-energy electron diffraction, RHEED) ซึ่งเป็นเทคนิคในการศึกษาลักษณะพื้นผิวของผลึกวิธีหนึ่ง หลังจากการสร้างโครงสร้างควอนตัมดอทนี้ เราสามารถใช้ กล้องจุลทรรศน์แรงอะตอม (Atomic Force Microscopy, AFM) วัดดูลักษณะทางโครงสร้างของควอนตัมดอท และ ใช้การวัดโฟโตลูมิเนสเซนซ์ (Photoluminescence, PL) ในการศึกษา โครงสร้างทางอิเล็กทรอนิกส์ หรือ ระดับพลังงานของอิเล็กตรอน ในโครงสร้าง

2.1.1 การสร้างโครงสร้างควอนตัมดอทด้วยเทคนิคการปลูกผลึกด้วยลำโมเลกุล

เทคนิคการปลูกผลึกด้วยลำโมเลกุล หรือที่เรียกย่อ ๆ ว่า MBE ถูกคิดค้นโดย Arthur และ Cho เป็นเทคนิคที่สามารถสร้างผลึกของสารกึ่งตัวนำ ให้มีการจัดเรียงของอะตอมอย่างเป็นระเบียบ เมื่อไม่นานมานี้ เทคนิคการปลูกผลึกด้วยลำโมเลกุล ถูกนำไปใช้ศึกษาการสร้างโครงสร้างควอนตัมดอท ซึ่งจากการที่ ในระบบเครื่องปลูกผลึกด้วยลำโมเลกุล มีการติดตั้ง การดูรูปแบบการเลี้ยวเบนของลำอิเล็กตรอนพลังงานสูงที่สะท้อนจากผิว ดังนั้นเราจึงสามารถสังเกตได้ว่า ระหว่างทำการปลูกผลึก ผิวหน้า มีลักษณะการจัดเรียงอะตอมแบบใด

ในการปลูกผลึกด้วยลำโมเลกุล หากเราทำการปลูกสารกึ่งตัวนำ ที่มีขนาดค่าคงที่โครงผลึกต่างกัน โครงสร้างควอนตัมดอท ก็สามารถเกิดขึ้นได้เอง โดยกระบวนการจัดเรียงตัวตามธรรมชาติ (Self-organization) โดยสารกึ่งตัวนำ ที่สามารถนำมาใช้ สร้างโครงสร้างควอนตัมดอทแบบจัดเรียงตัวเองได้ ชนิดหนึ่ง คือ อินเดียมอาร์เซไนด์ ในแกลเลียมอาร์เซไนด์ โดย คุณสมบัติทางโครงสร้างของควอนตัมดอทบนผิวหน้านั้น สามารถวัดได้จาก การวัดด้วย กล้องจุลทรรศน์แรงอะตอม [2]



รูปที่ 2.2 (ก) โครงสร้างควอนตัมดอทของสารกึ่งตัวนำอินเดียมอาร์เซไนด์บนพื้นผิวของสารกึ่งตัวนำแกลเลียมอาร์เซไนด์ผ่านกล้องจุลทรรศน์แรงอะตอม (ข) รูปแบบการเลี้ยวเบนของลำอิเล็กตรอนพลังงานสูงที่สะท้อนจากผิวที่วัดขณะทำการสร้างโครงสร้างควอนตัมดอท [3]

2.2 ควอนตัมดอทโมเลกุล

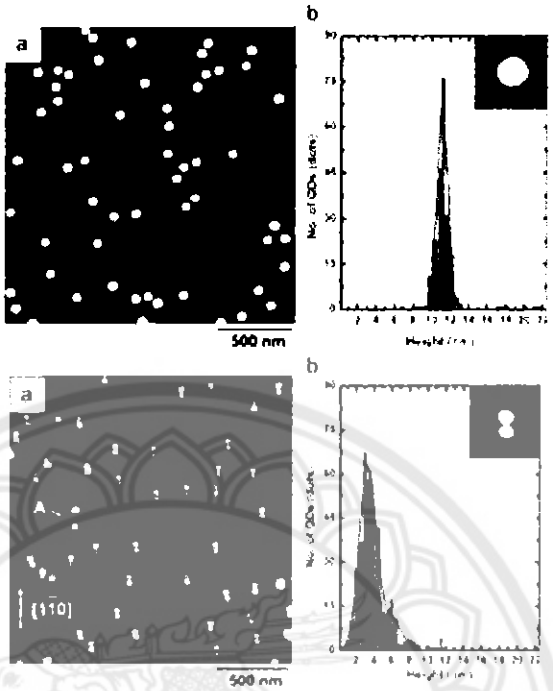
ในการสร้างควอนตัมดอทโมเลกุลนั้น เราจะต้องทำให้ ควอนตัมดอทที่อยู่บนผิวหน้า มีการจัดเรียงตัวในรูปแบบโมเลกุล ซึ่งการจัดเรียงตัวนี้ มีได้หลายรูปแบบ โดยการใช้เทคนิคการปลูกผลึกด้วยเครื่องปลูกชั้นผลึกด้วยลำโมเลกุล เราสามารถสร้างรูปแบบต่าง ๆ ได้ รูปที่ 2.3 แสดงรูปลักษณะการเรียงตัวของควอนตัมดอทโมเลกุลแบบต่าง ๆ ที่มีการสร้างขึ้นได้จริง

รูปที่ 2.3 แสดงกลุ่มของควอนตัมดอทโมเลกุลบนสารกึ่งตัวนำ ที่มี ควอนตัมดอทแบบคู่, ควอนตัมดอทแบบสี่ดอท และควอนตัมดอตแบบหกดอท หรือ แบบวงแหวน [4]

โครงสร้างควอนตัมดอทโมเลกุลที่สร้างขึ้นได้นี้ คือ ควอนตัมดอทโมเลกุลแบบคู่ (Bi-molecule) ควอนตัมดอทแบบ 4 ดอท (Quad-molecule) และ ควอนตัมดอทหกดอท (Hexa-molecule) หรือแบบวงแหวน (Dot ring) จะมีศักยภาพในการใช้งานด้านต่าง ๆ เช่น ในด้านสปินทรอนิกส์ (Spintronics) ที่อาศัยการเก็บข้อมูล ด้วยคุณสมบัติการมีสปินของอิเล็กตรอนในโครงสร้าง โดย การเก็บข้อมูลในลักษณะนี้ ก็มีศักยภาพในการนำมาใช้งานใน ด้านควอนตัมคอมพิวเตอร์ด้วย นอกจากนี้ โครงสร้างควอนตัมดอทแบบสี่ดอท ยังสามารถนำมาใช้ในการคำนวณตามหลักการควอนตัมดอทเซลลูล่าออต โตมาต้า (Quantum-dot cellular automata) ด้วย ดังนั้น จึงกล่าวได้ว่า การพัฒนาเทคนิคการปลูกผลึก โครงสร้าง ควอนตัมดอท โมเลกุล มีความสำคัญอย่างยิ่งต่อการพัฒนา สิ่งประดิษฐ์ทางอิเล็กทรอนิกส์ชนิดใหม่

สำหรับโครงสร้างควอนตัมดอททั่ว ๆ ไป หากนำไปสร้างให้มีความหนาแน่นสูง มันก็ยังเป็นประโยชน์ต่อการเพิ่มประสิทธิภาพของเลเซอร์สารกึ่งตัวนำสมัยใหม่ และ เซลล์แสงอาทิตย์สมัยใหม่ ที่เรียกว่า ควอนตัมดอทเลเซอร์ และ ควอนตัมดอทโซล่าเซลล์ ตามลำดับ และ สำหรับโครงสร้างควอนตัมดอท ที่มีการเรียงตัวเป็นเส้นตรง หรือ เป็นลวดลายต่าง ๆ ก็ยังมีประโยชน์ต่อการนำไปพัฒนาสิ่งประดิษฐ์ ทางด้าน นาโนอิเล็กทรอนิกส์ (Nanoelectronics) และ นาโนโฟโตนิกส์ (Nanophotonics) อีกด้วย [5]

2.2.1 เปรียบเทียบลักษณะโครงสร้างควอนตัมดอทกับควอนตัมดอทโมเลกุลแบบคู่



รูปที่ 2.4 ภาพจากการวัดด้วยกล้องจุลทรรศน์แรงอะตอม และ ลักษณะความสูงของโครงสร้างควอนตัมดอท (รูปบน) และ โครงสร้างควอนตัมดอทโมเลกุลแบบคู่ (ล่าง) [6]

รูปที่ 2.4 รูปด้านบน เป็นรูปของควอนตัมดอทที่มีลักษณะเป็นจุด ซึ่งมีความสูงประมาณ 10-12 นาโนเมตร ส่วนรูปด้านล่าง เป็นรูปของควอนตัมดอทโมเลกุลแบบคู่ ที่มีลักษณะเป็นจุดโดยมีสองจุดมาอยู่ใกล้กันจนสามารถเกิดการคู่ควบ (Coupling) โดยควอนตัมดอทใน ควอนตัมดอทโมเลกุลแบบคู่ มีความสูงประมาณ 3-4 นาโนเมตร

2.3 พื้นฐานการคำนวณแบบควอนตัม

การคำนวณเชิงควอนตัม (Quantum computing หรือ Quantum computation) เป็นการคำนวณ โดยอาศัยหลักการทางฟิสิกส์ทางด้าน กลศาสตร์ควอนตัม โดยอาศัยคุณสมบัติการทับซ้อน (Superposition) และ ความพัวพัน (Entanglement) ของสถานะของอนุภาคในระดับควอนตัม โดยจากคุณสมบัติทั้ง 2 นี้ จะทำให้ เราสามารถนำการคำนวณนี้ มาใช้แก้ปัญหาบางกรณีได้รวดเร็วยิ่งขึ้น เมื่อเทียบกับ การคำนวณแบบดั้งเดิม

2.3.1 การทับซ้อน (Superposition)

การทับซ้อน เป็นปรากฏการณ์ที่ อนุภาคควอนตัมสามารถปรากฏได้สองที่ในเวลาเดียวกัน โดยการอธิบายหลักการทับซ้อนนี้ จะเหมือนกับ กรณี การทับซ้อนของคลื่น ดังนั้น จึงกล่าวได้ว่า ในระบบควอนตัม อนุภาคจะมีคุณสมบัติเป็นคลื่นด้วย โดยหากเราพิจารณา อนุภาคโฟตอน (แสง) จากการทดลอง ที่ได้มีแสดงให้เห็นแล้วว่า หากนำเอาตัวแยกลำแสง (Beam splitter) มาวางไว้ในลักษณะดังรูปที่ 2.5(ก) เมื่อทำการยิงแสงผ่านกระทบตัวแยกลำแสง ที่มีความสามารถทำให้แยกออกเป็นสองลำ โดยมีความเข้มแสงทั้งสองลำเป็นสัดส่วน 50 ต่อ 50 แล้วนำตัวรับแสงมาตรวจรับแสงที่หักเห (ตัวรับแสง 1) และ ทะลุผ่าน (ตัวรับแสง 2) จะพบว่า ตัวรับแสงทั้งสอง ได้รับแสงที่มีความเข้มเท่ากัน

เมื่อเราพิจารณาแสงซึ่งก็คือ ลำของอนุภาคโฟตอน ที่ยิงเข้าไปในตัวแยกลำแสง เราพบว่าเราจะต้องใช้ความน่าจะเป็น ในการอธิบาย การเลือกหักเห หรือ ทะลุผ่าน ของโฟตอน ตัวหนึ่ง ๆ โดย จากการใช้ ตัวแยกลำแสงแบบ 50 ต่อ 50 จะได้ว่า ความน่าจะเป็นที่โฟตอนตัวหนึ่งจะเลือกทะลุผ่าน เท่ากับ 0.5

(ก) (ข)

รูปที่ 2.5 (ก) การทดลองยิงโฟตอนเดี่ยวกระทบตัวแยกลำแสง (ข) แหล่งกำเนิดแสงสองตัว เปล่งแสงที่มีเฟสต่างกันผ่านตัวแยกลำแสง

ในทำนองกลับกัน เมื่อเราทำการทดลอง โดยปล่อยลำโฟตอนจากตัวเปล่งแสงสองตัว ที่สามารถควบคุมความต่างเฟสของมันได้ (เช่นจาก เลเซอร์ และ อุปกรณ์ทางแสง) เมื่อโฟตอนกระทบตัวแยกลำแสง หากเราพิจารณาว่า โฟตอนแต่ละตัว มีความน่าจะเป็นที่จะเลือกทางเดิน ที่เป็นอิสระต่อกัน เราควรจะได้ผลการทดลองที่ว่า แสง จะผ่านตัวแยกลำแสงออกมาทั้งสองทาง แต่จากการทดลองโดย Hong Ou และ Mandel (1987) พบว่า สถานะของโฟตอนจะสามารถซ้อนทับกันได้ และ จะเกิดการแทรกสอดแบบควอนตัม ซึ่งจะทำให้โฟตอนออกมาทางเดียว (ดูรูปที่ 2.5(ข))

2.3.2 ความพัวพัน (Entanglement)

ความพัวพัน เป็นปรากฏการณ์ทางควอนตัม ที่ไม่มีอยู่ใน ทฤษฎีทางฟิสิกส์ดั้งเดิม นั่นคือ การที่อนุภาคทางควอนตัม สองตัวขึ้นไป ที่มีความเชื่อมโยงกันอยู่ ถึงแม้ว่า จะอยู่ห่างไกลกันแค่ไหนก็ตาม โดยอนุภาคเหล่านี้สามารถส่งข้อมูลถึงกันได้ และ หมายความว่า อะไรที่เกิดกับอนุภาคหนึ่งจะส่งผลต่ออีกอนุภาคหนึ่ง ซึ่งเราเรียก ปรากฏการณ์เหล่านี้ว่า เป็นการพัวพันซึ่งกันและกัน การพัวพันนี้ ได้ถูกใช้ในการพิสูจน์แล้วว่า ข้อมูล สามารถเดินทางได้เร็วกว่าแสง (ซึ่งขัดแย้งกับแนวคิดของไอน์สไตน์ ในสมัยที่คิดค้น ทฤษฎีสัมพัทธภาพ) และ การพัวพันนี้ สามารถอธิบายได้ด้วย กลศาสตร์ควอนตัม ซึ่งทำให้เราสามารถนำมันมาสร้างเป็น การคำนวณเชิงควอนตัม เพราะการคำนวณเชิงควอนตัม คือ การคำนวณ ที่มีลักษณะขนาน คือ สามารถประมวลผลข้อมูลขาเข้าหลาย ๆ ชุดในครั้งเดียว ซึ่งเป็นที่มาของการใช้ คำว่า คิวบิต เป็น บิต ของการคำนวณเชิงควอนตัม

2.4 เปรียบเทียบข้อมูลบิต (Bits) กับ คิวบิต (Qubit)

หลักการทำงานของคอมพิวเตอร์โดยทั่วไปคือมีการประมวลผลเป็น ไบนารี่ ดิจิต หรือ บิต ซึ่งเป็นพื้นฐานที่สุดที่ใช้ บอกสถานะของการทำงานและข้อมูล ข้อมูล 1 บิต มีสองสถานะ คือ "0" กับ "1" ในกรณีของการคำนวณแบบควอนตัม จะใช้สถานะของอนุภาคเป็นตัวแทนของบิต แต่เนื่องจากคุณสมบัติของระบบทางควอนตัม ที่สามารถสร้างการทับซ้อน ทำให้อนุภาคตัวเดียว แทนสถานะระหว่าง 0 และ 1 ซึ่งจะทำให้สามารถทำการเข้ารหัส อนุภาคนั้นที่อยู่ระหว่าง 0 และ 1 ได้ โดยเรียกข้อมูล ที่มีคุณสมบัตินี้ว่า ควอนตัมบิต หรือ คิวบิต ตารางที่ 2.1 แสดงการเปรียบเทียบคุณสมบัติของข้อมูลบิต และ คิวบิต

ตารางที่ 2.1 แสดงการเปรียบเทียบข้อมูลบิต และ คิวบิต [7]

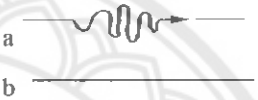
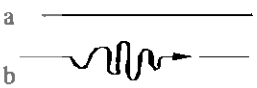
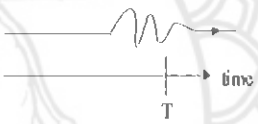
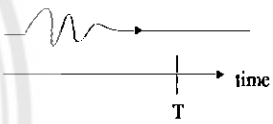
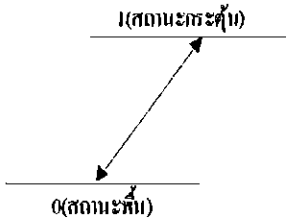
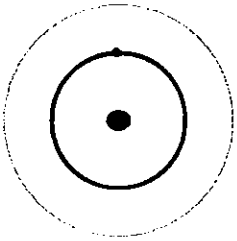
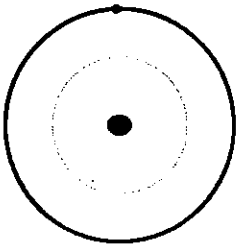
บิต	คิวบิต
มีค่าได้เป็น "0" หรือ "1"	มีค่าเป็นผลรวมเชิงเส้นของ "0" และ "1" (a| 0 >+ b| 1 >)*
สามารถวัดค่าบิตได้โดยแม่นยำ	ไม่สามารถวัดสถานะที่แน่นอนของคิวบิตได้
สามารถวัดค่าบิตได้โดยไม่ทำให้ค่าเดิมเปลี่ยน	การวัดคิวบิตสามารถทำให้ค่าเปลี่ยน
สามารถแยกแยะ "0" และ "1" ออกจากกันได้อย่างชัดเจน	เราไม่สามารถแยกแยะ บางสถานะของกลุ่มคิวบิตใด ๆ (มากกว่าหนึ่งคิวบิตขึ้นไป) อย่างชัดเจนได้
สามารถทำการคัดลอกบิตได้โดยแทบจะไร้ข้อจำกัด	คัดลอกคิวบิตที่ทราบค่าและไม่ทราบค่าได้อย่างค่อนข้างจำกัด
การรู้สถานะของบิตหนึ่ง ไม่มีผลต่อค่าสถานะของอีกบิตหนึ่งที่อยู่ไกลกัน	การรู้สถานะของคิวบิตหนึ่ง จะมีผลต่อค่าสถานะของคิวบิตอื่น ๆ ที่พัวพันกับคิวบิตนั้น ถึงแม้จะอยู่ห่างไกลกันก็ตาม

* ในเอกสารนี้ เราใช้ เครื่องหมาย |.> แทนการบ่งบอกสถานะ ซึ่งอาจมองเป็นฟังก์ชันค่าคงที่หนึ่ง เช่นเดียวกันกับ การมองว่า "0" คือ ระดับแรงดัน 0 โวลต์ และ "1" คือ ระดับแรงดัน 5 โวลต์

ในระบบอิเล็กทรอนิกส์ เราจะนิยาม บิต คือค่าที่ใช้แทนความแตกต่างของแรงดันโวลต์นั้น คือ "0" แทนด้วย ระดับแรงดันศูนย์โวลต์ค่าของ "1" แทนด้วยระดับแรงดัน 5 โวลต์ เพื่อให้ทราบถึงความแตกต่างของข้อมูลเช่น ข้อมูลสามบิตสามารถมีค่าที่เป็นไปได้ 8 ค่าคือ 000, 001, 010, 011, 100, 101, 110 และ 111

สำหรับ คิวบิต คือ ค่าที่ใช้แทนความแตกต่างของข้อมูล เหมือนกับ บิตในคอมพิวเตอร์แบบดั้งเดิม แต่มีความแตกต่างตรงที่คิวบิต จะไม่ใช้ ระดับแรงดัน (หรือกระแส) แต่จะใช้สถานะเชิงควอนตัม ในการแสดง โดย เราจะใช้ สัญลักษณ์ |.> ในการบอกสถานะของคิวบิต ซึ่ง สถานะเชิงควอนตัมนี้ มีได้หลายแบบ ขึ้นกับ ระบบที่นำมาศึกษา โดยสถานะของอิเล็กตรอน ในควอนตัมดอทโมเลกุลแบบคู่ เป็นสถานะหนึ่ง ที่นำมาใช้เป็น คิวบิต ได้

ตารางที่ 2.2 ระบบทางกายภาพของคิวบิต [7]

ระบบกายภาพที่ใช้แทนคิวบิต	คุณสมบัติ	สารสนเทศ (ลอจิก)	
		"0"	"1"
โฟตอน	การจัดเรียงตัวเชิงเส้น(Linear polarization)	แนวตั้ง 	แนวนอน 
	การจัดเรียงตัวเชิงวงกลม (Circular polarization)	ทวนเข็มนาฬิกา (left-circular polarization)	ตามเข็มนาฬิกา (right-circular polarization)
	จำนวนโฟตอน (Photon number)	ไม่มีโฟตอน	มี 1 โฟตอน
	เส้นทางที่แสงเคลื่อนที่ (Photon path)	ผ่านเส้นทาง a 	ผ่านเส้นทาง b 
	ตะกร้าเวลา ก่อน-หลัง (time-bin)	โฟตอนมาถึงก่อน 	โฟตอนถึงทีหลัง 
อิเล็กตรอน	สปิน(spin)	สปินมีทิศ +Z 	สปินมีทิศ –Z 
	ประจุ(charge)	ไม่มีประจุ (ไม่มีอิเล็กตรอน)	มีประจุ (มี 1 อิเล็กตรอน)
นิวตรอน	สปิน(spin)	สปินมีทิศ +Z 	สปินมีทิศ –Z 
อะตอม	ระดับพลังงาน (energy level) 	สถานะพื้น  (ground state)	สถานะกระตุ้น  (excited state)

ตารางที่ 2.2 แสดง ตัวอย่างระบบทางกายภาพ ที่มีผู้นำเสนอให้ใช้ในการคำนวณแบบควอนตัมได้ โดยระบบทางกายภาพที่มีการนำไปใช้ในการคำนวณแบบควอนตัมกันมาก ได้แก่ สถานะของโฟตอน (แสง) และ สถานะของอิเล็กตรอน

2.5 ประโยชน์ของการคำนวณแบบควอนตัมในด้านต่างๆ

การคำนวณแบบควอนตัม สามารถประยุกต์ใช้ประโยชน์ได้ในหลายๆ อย่าง ซึ่งจากการศึกษาพบว่าในปัจจุบัน ได้มีการคิดค้นทดลอง และประยุกต์ใช้ในด้านต่างๆ เช่น

- การเข้ารหัสความหนาแน่นสูงเชิงควอนตัม (Quantum superdense coding)

เป็นการประยุกต์ใช้สถานะพัวพัน ในรูปแบบสถานะของเบลล์ (Bell States) ในการแทนข้อมูลดิจิตอลสองบิต และสามารถใช้ในสื่อสารข้อมูลสองบิต ด้วยการส่งสถานะควอนตัมเพียงคิวบิตเดียว ซึ่งในสถานะเบลล์นั้น จะเป็นแสดงสถานะพัวพัน ระหว่างอนุภาคคิวบิต ในกรณีนี้จะพิจารณาสองอนุภาค (สองคิวบิต) ซึ่งมีการแสดงความพัวพัน 4 รูปแบบ ได้แก่

$$(|00\rangle + |11\rangle)/\sqrt{2} \quad , \quad (|10\rangle + |01\rangle)/\sqrt{2}$$
$$(|00\rangle - |11\rangle)/\sqrt{2} \text{ และ } (|10\rangle - |01\rangle)/\sqrt{2}$$

- การควบคุมความผิดพลาดเชิงควอนตัม

สิ่งที่เป็นอุปสรรคต่อความสำเร็จ ในการสื่อสารหรือประมวลผลข้อมูลเชิงควอนตัมแต่ละครั้ง คือ การมีอันตรกิริยากับสิ่งแวดล้อม ซึ่งทำให้เกิดความผิดพลาดของข้อมูลควอนตัม โดยคุณสมบัติทางควอนตัมคือ การทับซ้อนเชิงตำแหน่ง และ ความพัวพันทางควอนตัมบางส่วนหรือทั้งหมดได้สูญเสียไป ในปี ค.ศ. 1993 เดวิด ดอยช์ (Devid Deutsch) เสนอวิธีการทำให้ข้อมูลสามารถคืนสภาพ ได้โดยการใช้สถานะของควอนตัม ที่มีลักษณะเหมือนกันซ้อนๆ กันหลายคิวบิต เพื่อแทนข้อมูลเดียวกันในลักษณะสมมาตร โดยเมื่อความผิดพลาดเกิดขึ้น จะทำให้ความสมมาตรดังกล่าวสูญเสียไป และ สามารถตรวจพบได้ โดยการตรวจสอบสถานะควอนตัม ส่วนที่ไม่เกิดข้อผิดพลาด

- การแยกตัวประกอบด้วยอัลกอลิทึมเชิงควอนตัม

เป็นการแยกตัวกอบด้วย ขั้นตอนอัลกอลิทึม วิธีแบบชอร์ (Shor's algorithm) โดย อาศัยหลักการเชิงควอนตัม เพื่อให้เกิดความรวดเร็ว ในการหาตัวประกอบยิ่งขึ้น โดยในการศึกษาการ

คำนวณ แบบควอนตัมด้วย ควอนตัมดอท โมเลกุล นี้ เราจะทำ การศึกษาใน เรื่องของ การแยกตัวประกอบด้วย ขั้นตอนอัลกอริทึมวิธีแบบชอร์ (Shor's algorithm)

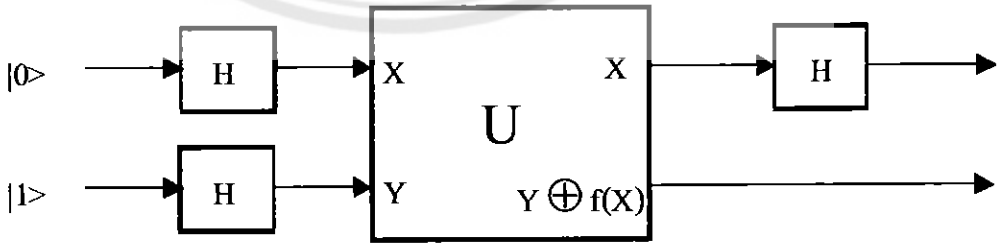
2.6 พื้นฐานวิธีเชิงควอนตัม (Quantum algorithms)

เดวิด ดอยช์ (David Deutsch) และริชาร์ด จอสซา (Richard Jozsa) ร่วมกันเสนอกระบวนวิธีแก้ปัญหาเชิงควอนตัมเป็นวิธีแรก ซึ่งอาศัยคุณสมบัติ การทับซ้อนเชิงตำแหน่ง มาช่วยในการแก้ปัญหา และการวิเคราะห์คุณลักษณะของฟังก์ชันที่เป็นฟังก์ชันคงที่ (Constant function) หรือฟังก์ชันสมดุล (Balanced function) โดยเราจะเรียก กระบวนการวิธีดังกล่าวนี้ว่า ' วิธีของ ดอยช์ – จอสซา (Deutsch – Jozsa algorithm) ซึ่งจากคุณสมบัติการทับซ้อนเชิงตำแหน่งของสถานะทางควอนตัม ทำให้สามารถได้คำตอบเร็วขึ้นเป็นเอกซ์โพเนนเชียล

ต่อมา แดน ไซมอน (Dan Simon) ได้เสนอวิธีการทางควอนตัม ในการหาคาบของฟังก์ชัน และจากสิ่งที่ แดน ไซมอนได้เสนอไปนั้น ทำให้ปีเตอร์ ชอร์ (Peter Shor) ได้ค้นพบวิธีเชิงควอนตัมสำหรับ ในการแยกตัวประกอบ และ การหาลอการิทึม ที่ไม่ต่อเนื่องในทางเวลา เป็นแบบโพลิโนเมียล (Polynomial) แทนที่จะเป็นเอกซ์โพเนนเชียล (Exponential) ดังเช่น วิธีที่ใช้ในคอมพิวเตอร์เชิงดิจิตอลแบบดั้งเดิม

2.6.1 วิธีของ ดอยช์ – จอสซา (Deutsch – Jozsa algorithm)

วิธีของ ดอยช์ – จอสซา เป็นวิธีการคำนวณเชิงควอนตัมวิธีแรก ที่มีประสิทธิภาพสูงกว่าการคำนวณแบบดั้งเดิม โดยระเบียบวิธีนี้ ถูกนำเสนอเพื่อทำการสาธิตให้เห็นว่า การแก้ปัญหาด้วยการคำนวณเชิงควอนตัม สามารถทำได้จริง และ มีประสิทธิภาพในการคำนวณสูงกว่า วิธีการที่ใช้ในคอมพิวเตอร์ปัจจุบัน



รูปที่ 2.6 ขั้นตอนการทำงานแบบวิธีของ ดอยช์ – จอสซา บนสองคิวบิต [7]

2.6.2 วิธีของชอร์ (Shor's algorithm)

ขั้นตอนวิธีนี้เป็นขั้นตอนวิธีควอนตัม (ขั้นตอนวิธีที่ทำงานบนควอนตัมคอมพิวเตอร์) ที่ใช้ในการแยกตัวประกอบของจำนวนเต็ม ซึ่งโดยทั่วไปแล้วจะใช้ในการแก้ปัญหา เมื่อทำการกำหนดจำนวนเต็ม N แล้ว ให้หาตัวประกอบเฉพาะของ N

ในควอนตัมคอมพิวเตอร์นั้น การแยกตัวประกอบด้วย ขั้นตอนวิธีของชอร์ จะใช้เวลาในการทำงานไม่เกินฟังก์ชันพหุนาม (Polynomial) ของขนาดข้อมูลโดยจะใช้เวลาเป็น $O((\log N)^3)$ ซึ่งแสดงให้เห็นว่า เป็นการแก้ปัญหา การแยกตัวประกอบของจำนวนเต็ม ที่มีประสิทธิภาพในควอนตัมคอมพิวเตอร์ วิธีนี้จัดเป็นวิธีที่เร็วกว่าหลายๆ วิธีที่มีประสิทธิภาพที่รู้จักกันทั่วๆ ไป ที่มักจะใช้เวลาเป็นฟังก์ชันเลขชี้กำลัง (Exponential) ขนาดของข้อมูล ในการแยกตัวประกอบโดยใช้ขั้นตอนวิธีของชอร์นั้นประกอบด้วย 2 ส่วนคือ

1. ส่วนลดรูปปัญหา โดยส่วนนี้ จะใช้ลดรูปปัญหาจากปัญหา การแยกตัวประกอบเป็นปัญหาในการหาลำดับ ซึ่งส่วนนี้จะสามารถทำได้ในคอมพิวเตอร์ทั่วไป
2. ส่วนแบบวิธีการควอนตัมที่ใช้ในการแก้ปัญหาในการหาลำดับ

2.7 การแยกตัวประกอบด้วยอัลกอริทึม (Algorithms for quantum computation)

อัลกอริทึมที่จะนำมาใช้ในการแยกตัวประกอบของจำนวนเฉพาะด้วยการคำนวณแบบควอนตัม คือ ขั้นตอนอัลกอริทึมของชอร์ (Shor's algorithm) ซึ่งเป็นการแยกตัวประกอบที่เป็นจำนวนเฉพาะของจำนวนเต็มด้วยเวลาที่แปรผันตรงกับค่า N^3 เมื่อ N คือจำนวนบิตของตัวเลขในการคำนวณ ซึ่งหากใช้วิธีการคำนวณด้วยคอมพิวเตอร์แบบดั้งเดิม จะต้องใช้เวลาการคำนวณที่แปรผันตรงกับ 2^N โดยสิ่งที่อยู่เบื้องหลังการทำงานของวิธีการแยกตัวประกอบของชอร์ คือ คุณสมบัติทับซ้อน ซึ่งมีอยู่ในระบบควอนตัม

2.7.1 การแยกตัวประกอบด้วยวิธีของชอร์

วิธีแยกตัวประกอบตามอัลกอริทึมของชอร์ [7] สามารถทำได้ โดยการหาคาบของลำดับตัวเลข ซึ่งอาศัยการหาคาบของฟังก์ชัน ร่วมกับ การหาตัวหารร่วมมาก (ห.ร.ม.) ของจำนวนเต็ม โดยเราสามารถสรุปอัลกอริทึมของชอร์ ได้เป็นขั้นตอนต่อไปนี้

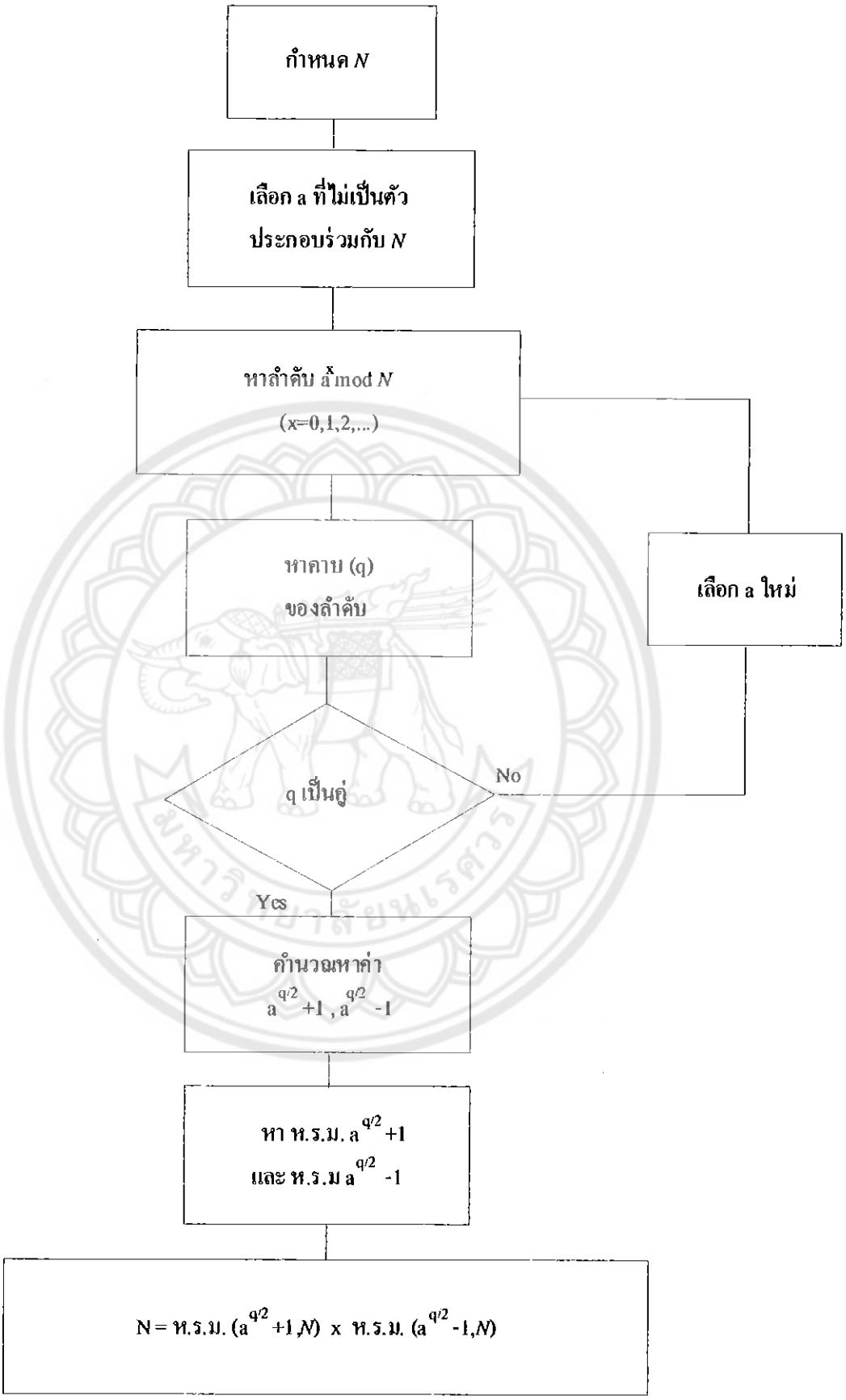
1) กำหนดให้ จำนวนเต็มที่ต้องการแยกตัวกอบคือ N
2) เลือกจำนวนเต็ม a ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ N กล่าวคือไม่มีตัวประกอบร่วมกับ N (ยกเว้นค่า 1 เท่านั้น เพราะ 1 เป็นตัวประกอบร่วมกับจำนวนเต็มทุกตัว)

3) หาลำดับ $a^x \bmod N$ เมื่อ $x = 0, 1, 2, 3, \ldots$ และ mod N หมายถึงหารด้วย N แล้วคงไว้แต่เศษ

4) หาคาบของลำดับ $\{ a^x \bmod N \}$ ให้คาบแทนด้วย q กล่าวคือ $a^{(x+q)} \bmod N = a^x \bmod N$ หาก q เป็นเลขคู่ ให้ไปต่อขั้นตอน 5 แต่ถ้า q เป็นเลขคี่ให้ไปเริ่มขั้นตอน 2 โดยเปลี่ยนค่า a ใหม่

5) คำนวณหา $a^{q/2}+1$ และ $a^{q/2}-1$ โดยถ้าหาก $a^{q/2}+1$ หารด้วย N ลงตัวให้กลับไปเริ่มขั้นตอนที่ 2 โดยเปลี่ยนค่า a ใหม่

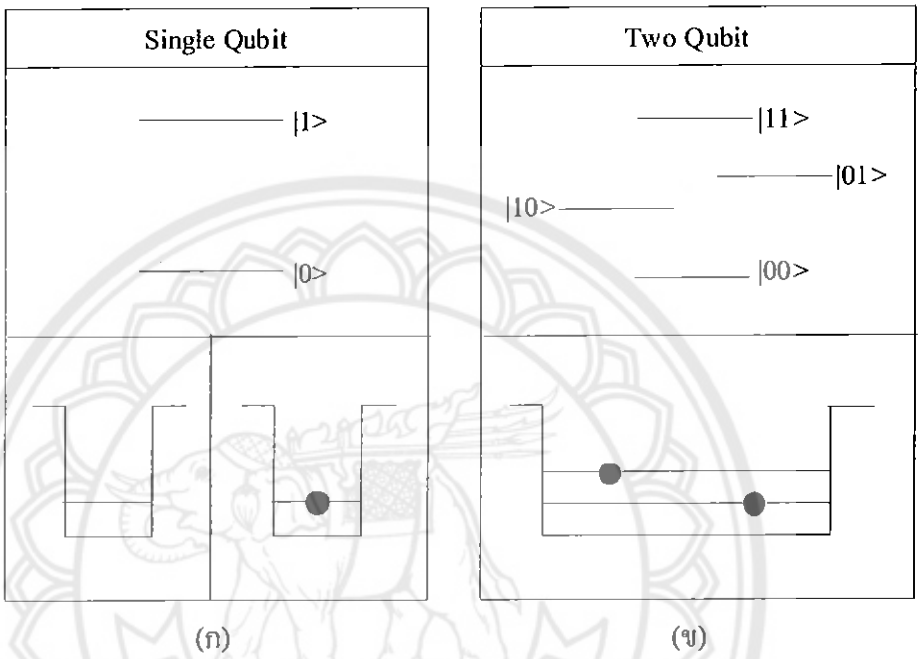
6) หา ห.ร.ม. ของ $a^{q/2}+1$ และ N และ ห.ร.ม. ของ $a^{q/2}-1$ และ N จะได้ว่า ค่า ห.ร.ม. ทั้งสองนี้ เป็นตัวประกอบเฉพาะ (prime factor) ของ N หรือ เขียนได้เป็น $N =$ ห.ร.ม. $(a^{q/2}+1, N) \times$ ห.ร.ม. $(a^{q/2}-1, N)$



รูปที่ 2.7 แผนภาพแสดงการแยกตัวประกอบของจำนวนเฉพาะ

บทที่ 3
การคำนวณแบบควอนตัมด้วยควอนตัมดอทโมเลกุลแบบคู่

3.1 สถานะของคิวบิตในโครงสร้างควอนตัมดอท และ ควอนตัมดอทโมเลกุลแบบคู่



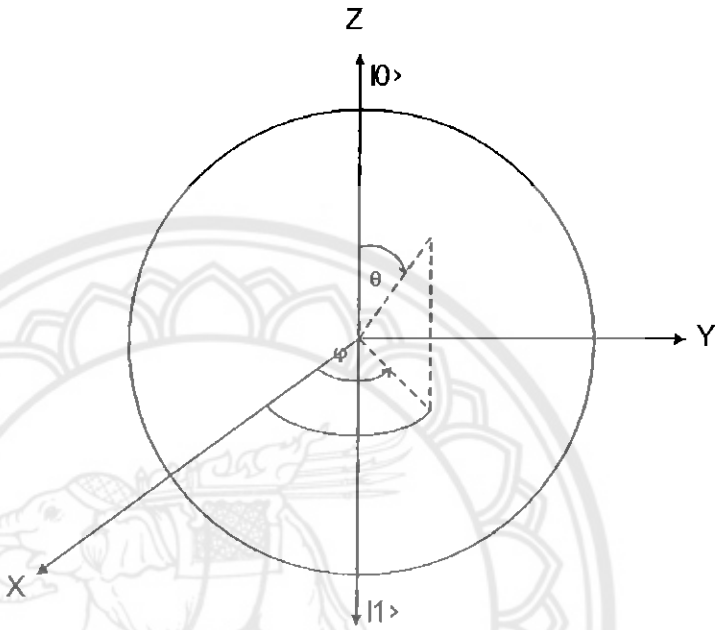
รูปที่ 3.1(ก) เป็นการแสดงสถานะของคิวบิตในโครงสร้างควอนตัมดอท และ (ข) ควอนตัมดอทโมเลกุลแบบคู่ [8]

จากรูปที่ 3.1 รูปด้านซ้าย เป็นการแสดงสถานะของคิวบิตในควอนตัมดอทแบบเดี่ยว โดยจะอยู่ในรูปแบบของชั้นระดับพลังงานในโครงสร้างนาโนของสารกึ่งตัวนำ ถ้าอิเล็กตรอนอยู่ในสถานะพื้น เราจะนิยามคิวบิตเป็น |0> และ ถ้าอิเล็กตรอนอยู่บนสถานะที่ถูกกระตุ้นไปอยู่ที่ระดับพลังงานสูงขึ้น เราจะนิยามเป็น |1> สำหรับการกระตุ้นอิเล็กตรอนนั้น ทำได้โดยการใช้แสง โดยหากแสงที่ใช้ มีพลังงานที่เหมาะสม จะทำให้เราสามารถกำหนดสถานะเริ่มต้น ที่อยู่ระหว่าง |0> และ |1> ได้อย่างอิสระ

รูปด้านขวา ในรูปที่ 3.1 เป็นการเป็นการแสดงสถานะของอิเล็กตรอนในควอนตัมดอทแบบคู่ จะเห็นว่าสถานะของอิเล็กตรอนมีได้ 4 สถานะ ดังนั้น จึงมี 2 คิวบิต ซึ่งแทนด้วย ตัวเลขสองตัว โดย แต่ละคิวบิต มีค่าหลัก ๆ คือ |0> และ |1> ดังนั้นเราจึงสามารถเขียนสถานะของระบบที่มีสองคิวบิตได้เป็น $|ij\rangle$ โดยที่ i และ $j = 0$ หรือ 1 อิเล็กตรอนแต่ละตัวจะมีพลังงานในระดับพลังงาน

ต่าง ๆ เมื่อได้รับพลังงานจากภายนอก เช่น จากการกระตุ้นด้วยแสง จะทำให้สถานะของอิเล็กตรอน (คิวบิต) เกิดการเปลี่ยนสถานะไป ซึ่งก็คือ การประมวลค่าที่เก็บอยู่ใน คิวบิต

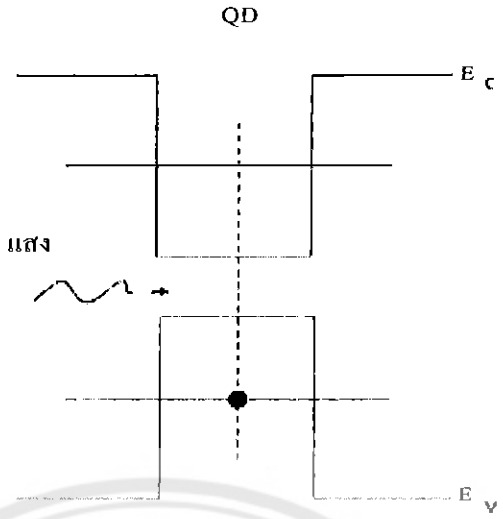
3.1.1 ลักษณะของคิวบิตในโครงสร้างควอนตัมดอท



รูปที่ 3.2 การแทนค่าคิวบิตด้วยเวกเตอร์ที่ชี้ไปบนผิวทรงกลมบล๊อซ [9]

รูปที่ 3.2 เป็นการนำเสนอค่าที่เก็บอยู่ในคิวบิต (หรือสถานะของอิเล็กตรอนในควอนตัมดอทแบบเดี่ยว) ซึ่งจะอธิบายในรูปแบบของเวกเตอร์ ที่ชี้ไปบนผิวทรงกลมบล๊อซ (Bloch sphere) โดยสถานะของอิเล็กตรอนนั้น สามารถเป็นผลรวมเชิงเส้น (linear combination) ของทั้งสองสถานะหลัก คือทั้ง |0> และ |1> โดยเป็นไปตามหลักการของการทับซ้อน โดยทั่วไปเราสามารถเขียน ค่าของคิวบิตเดี่ยว ใด ๆ ได้ คือ

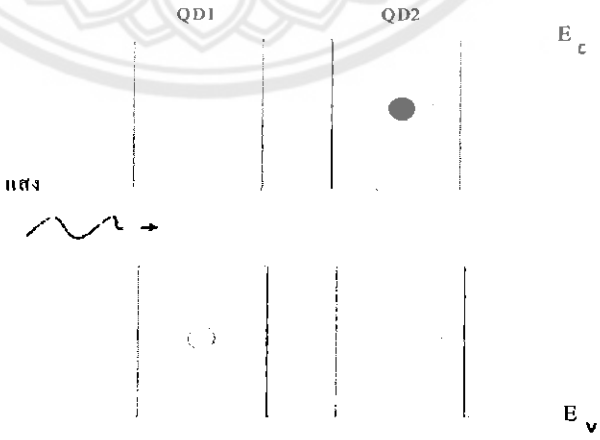
$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \qquad (3.1)$$



รูปที่ 3.3 แสดงระดับพลังงานในโครงสร้างของควอนตัมดอท

รูปที่ 3.3 แสดงลักษณะ แถบพลังงานของโครงสร้างควอนตัมดอทแบบเดี่ยว เมื่อเราทำการกระตุ้นอิเล็กตรอนที่อยู่ในระดับพลังงานในโครงสร้างของควอนตัมดอท ด้วยแสง (โฟตอน) จะทำให้อิเล็กตรอนนั้นเกิดการเปลี่ยนระดับพลังงานและเปลี่ยนสถานะ และ ทำให้ค่าของคิวบิตเปลี่ยนแปลงไปด้วย เราสามารถทำการแทนค่าสถานะ เป็น |1> ด้วยค่ามุม θ เท่ากับ π และ φ เท่ากับ 0 ในสมการ (3.1)

3.1.2 ลักษณะของคิวบิตในโครงสร้างควอนตัมดอทโมเลกุลแบบคู่

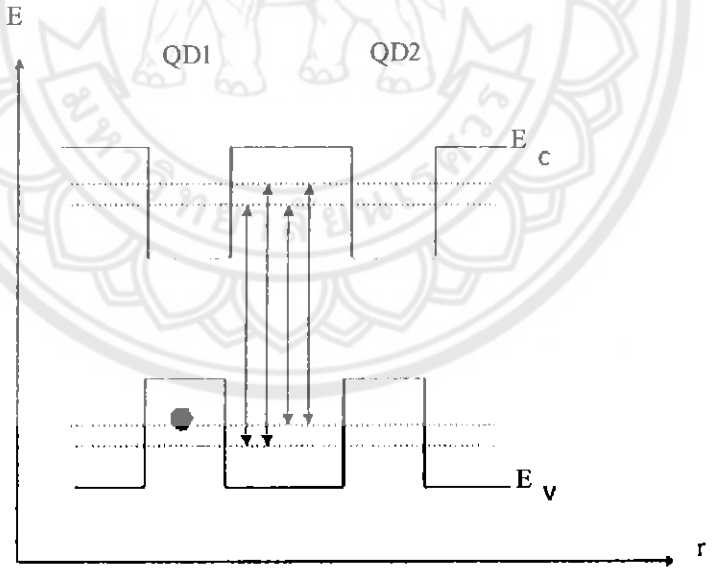


รูปที่ 3.4 แสดงระดับพลังงานในโครงสร้างของควอนตัมดอทโมเลกุลแบบคู่ โดยวงกลมสีขาวคือ โฮล และวงกลมสีดำคืออิเล็กตรอน

รูปที่ 3.4 เป็นการแสดงคู่อิเล็กตรอนโฮล (electron-hole pair) หรือ เอ็กซิตอน (exciton) ที่เกิดขึ้นในโครงสร้างควอนตัมดอทโมเลกุลแบบคู่ โดยการนำเสนอ คู่ อิเล็กตรอนโฮล นี้ จะแสดงในแผนภาพแถบพลังงาน หากเราทำการกระตุ้น อิเล็กตรอนในโครงสร้าง ด้วยแสง (โฟตอน) ที่มีพลังงานที่เหมาะสม จะทำให้มันเปลี่ยนระดับพลังงานไป และ จะทำให้ค่าของคิวบิตที่นิยามตามสถานะของพาหะนี้ เปลี่ยนแปลงไปด้วย โดยหาก ระดับพลังงานในทั้งควอนตัมดอททั้งสอง มีค่าเท่ากัน ก็จะเกิดการพัวพันของสถานะของอิเล็กตรอนขึ้น กล่าวอีกแบบหนึ่งคือ เราจะไม่ทราบอย่างแน่ชัดว่า อิเล็กตรอนที่เปลี่ยนระดับพลังงานแล้ว จะไปอยู่ที่ดอทด้านซ้าย หรือ ขวา ในรูปที่ 3.4 ดังนั้น จากคุณสมบัติการทับซ้อนได้ของอนุภาคควอนตัม ทำให้เขียนค่าของสถานะที่ไม่ทราบนี้ได้เป็น

$$|\psi\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \tag{3.2}$$

เมื่อนิยามให้ |0> คือ สถานะที่อิเล็กตรอนอยู่ที่ดอทซ้าย และ |1> คือ สถานะที่อิเล็กตรอนอยู่ที่ดอทขวา



รูปที่ 3.5 แสดงระดับพลังงานในโครงสร้างของควอนตัมดอทโมเลกุลแบบคู่ เมื่อพิจารณาระดับพลังงานที่อยู่สูงขึ้นไป ในโครงสร้างควอนตัมดอทแต่ละตัว

รูปที่ 3.5 เป็นการแสดงถึงสถานะที่เป็นไปได้ในโครงสร้างของควอนตัมดอทโมเลกุลแบบคู่เมื่อพิจารณาระดับพลังงานที่อยู่สูงขึ้นไป ในโครงสร้างควอนตัมดอทแต่ละตัว เมื่อมีการกระตุ้น

ด้วยแสง (โฟตอน) จะทำให้อิเล็กตรอนในโครงสร้าง สามารถเปลี่ยนแปลงระดับพลังงานไปได้ขึ้นกับพลังงานของโฟตอนที่ใช้กระตุ้น โดยหาก โครงสร้างควอนตัมดอทโมเลกุลนี้ แต่ละดอทมีสองระดับพลังงาน ก็จะทำให้เราสามารถ กำหนดค่า คิวบิต จำนวนสองคิวบิต จาก โครงสร้างควอนตัมดอทโมเลกุลแบบคู่นี้ ซึ่งจะมีค่าหลัก ๆ คือ 00, 01, 10, 11 ซึ่ง เลขตัวแรก อาจหมายถึง การไม่มี (0) หรือ มี (1) อิเล็กตรอน ในแถบนำไฟฟ้า ของดอทซ้าย และ เลขตัวที่สอง หมายถึง การไม่มี (0) หรือ มี (1) อิเล็กตรอน ในแถบนำไฟฟ้าของดอทขวา

3.2 การคำนวณโดยใช้ลอจิกเกตแบบควอนตัม

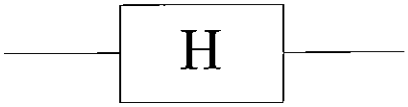
การคำนวณโดยใช้ลอจิกเกตแบบควอนตัม เป็น การคำนวณที่มี คุณสมบัติย้อนกลับได้ (Reversible computing) และ สามารถประมวลผลสถานะของอนุภาคเชิงควอนตัมที่มีคุณสมบัติทับซ้อน (Superposition) ของค่าที่คำนวณได้ ซึ่ง ลอจิกเกตแบบควอนตัม ที่มีผู้ศึกษา และ นิยาม เพื่อใช้เป็นเกตพื้นฐานในการคำนวณแบบควอนตัมมีหลายแบบ เช่น เกตฮาดามาร์ด (Hadamard gate), เกตเพาลิ (Pauli gate), เกตเลื่อนเฟส (Phase shift gate), เกตควบคุม (Controlled gate), เกตทอฟฟอลิ (Toffoli gate), เกตเฟรดคิน (Fredkin gate) เป็นต้น โดย การสร้าง ลอจิกเกตแบบควอนตัม ต่าง ๆ (Universal quantum gate) สามารถทำได้โดย ใช้ เกตเพียงสองชนิด คือ เกตฮาดามาร์ด ซึ่ง ทำงานกับคิวบิตเดี่ยว และ เกตกลับค่าแบบถูกควบคุม (Controlled-NOT gate) ซึ่ง ทำงานกับ สองคิวบิต ดังนั้น ในหัวข้อนี้ เราจะกล่าวถึงเกตสองชนิดนี้ เป็นหลัก

3.2.1 การดำเนินการบนคิวบิตเดี่ยว

เกตฮาดามาร์ด

การแปลงฮาดามาร์ด (Hadamard transformation) เป็นการเปลี่ยนรูปแบบที่ง่ายที่สุด ในการคำนวณแบบควอนตัม โดยจะเรียกลอจิกนี้ว่า เกตฮาดามาร์ด ซึ่งแทนด้วยสัญลักษณ์ H ดังแสดงในรูปที่ 3.6 โดย การอธิบายด้วยภาพ ทำได้โดย การพิจารณา ค่าของคิวบิตเดี่ยว ดังแสดงในรูปที่ 3.2 การแปลงฮาดามาร์ด ด้วย เกตฮาดามาร์ด เป็นการหมุน ของ เวกเตอร์คิวบิต ซึ่งอาจหมายถึง การเปลี่ยนจากสถานะพื้นฐานของอิเล็กตรอนในควอนตัมดอท เช่น $|0\rangle$ เป็นสถานะที่มีการทับซ้อน คือ $(|0\rangle+|1\rangle)/\sqrt{2}$ หรือ เปลี่ยนจาก $|1\rangle$ เป็น โดย $(|0\rangle-|1\rangle)/\sqrt{2}$ รูปแบบทั่วไป ของการแปลงฮาดามาร์ด แสดงได้ดังสมการ

$$H(\alpha|0\rangle+\beta|1\rangle)=\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|0\rangle-|1\rangle}{\sqrt{2}} \qquad (3.3)$$



รูปที่ 3.6 แสดงสัญลักษณ์ของเกตฮาดามาร์ด [10]

3.2.2 การดำเนินการบนหลายคิวบิต

เกตกลับค่าแบบถูกควบคุม (Controlled-NOT gate หรือ C-NOT gate)

เกตกลับค่าแบบถูกควบคุมนี้ จะคล้ายกับเกตเอ็กซ์คลูซีฟออร์ (XOR gate) ในการคำนวณด้วยคอมพิวเตอร์แบบดั้งเดิม โดยเกตลอจิกประเภทนี้จะมีบิตหนึ่งเป็นบิตที่ควบคุมผลลัพธ์ของบิตอื่น บิตที่ใช้ควบคุมเรียกว่าบิตควบคุม (Control bit) ในขณะบิตที่ถูกควบคุมเรียกว่าบิตเป้าหมาย (Target bit) โดยตารางค่าความจริงของเกตชนิดนี้ สำหรับ ในกรณีข้อมูลขาเข้า มีค่าหลัก แสดงดังตารางที่ 3.1

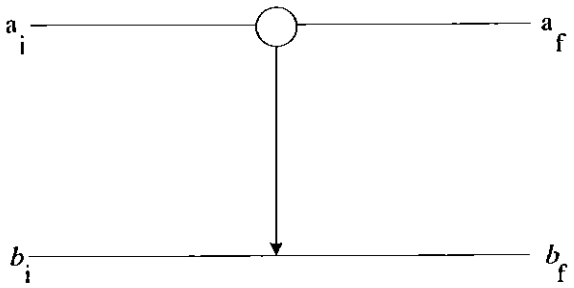
ตารางที่ 3.1 ตารางค่าความจริงของเกตกลับค่าแบบถูกควบคุม

a_i (Input Control qubit)	b_i (Input Target qubit)	a_f (Output Control qubit)	b_f (Output Target qubit)
|0>	|0>	|0>	|0>
|0>	|1>	|0>	|1>
|1>	|0>	|1>	|1>
|1>	|1>	|1>	|0>

โดยอาจเขียนเป็น

$$a_f = a_i, b_f = \begin{cases} b_i & if \quad a_i = 0 \\ \overline{b_i} & if \quad a_i = 1 \end{cases} \tag{3.4}$$

จากสมการข้างบน เราบอกได้ว่า เกตชนิดนี้ เป็นเกตที่มีคุณสมบัติย้อนกลับได้ นั่นคือ ถ้าเราสามารถรู้ค่าของ a_f และ b_f แล้ว เราจะทำให้สามารถหาค่าของ a_i และ b_i ซึ่งเป็นข้อมูลขาเข้าได้ สำหรับสัญลักษณ์ของเกตชนิดนี้ แสดงดังรูปที่ 3.7



รูปที่ 3.7 แสดงสัญลักษณ์ของเกตกลับค่าแบบถูกควบคุม [10]

ในกรณีที่บิตเป้าหมายขาเข้า ของเกตชนิดนี้ เป็นค่าที่มีการทับซ้อนกัน คือ $|b_i\rangle = \alpha|0\rangle + \beta|1\rangle$ หากบิตควบคุม มีค่าเป็น $|a_i\rangle = |1\rangle$ เราก็อาจจะเขียน ข้อมูลขาเข้าในรูปแบบ**เวกเตอร์ โดยให้** แต่ละบิต แทนด้วย เวกเตอร์แถว ขนาด สองแถว และ จะได้ว่า $|a_i b_i\rangle$ คือ

$$|a_i b_i\rangle = \begin{bmatrix} 0 \\ 1 \\ \alpha \\ \beta \end{bmatrix} \tag{3.5}$$

และจะได้ว่า ข้อมูลขาออกจากเกตชนิดนี้ คือ

$$|a_f b_f\rangle = \begin{bmatrix} 0 \\ 1 \\ \beta \\ \alpha \end{bmatrix} \tag{3.6}$$

สำหรับกรณีที่บิตควบคุม มีค่าเป็น $|0\rangle$ บิตเป้าหมายจะไม่ถูกเปลี่ยนแปลง

เกตยูนิเวอร์ซอล หรือ ยูเกต (Universal gate หรือ U-gate)

เกตยูนิเวอร์ซอลนี้ เป็นเกตที่มีลักษณะการทำงานเป็นแบบ 2 คิวบิต โดยที่คิวบิตแรกทำหน้าที่เป็นบิตควบคุม (เหมือนเกตกลับค่าแบบถูกควบคุม) โดยมีรูปทั่วไปของการเปลี่ยนสถานะเมื่อส่งคิวบิตผ่านเกตชนิดนี้ ดังนี้ [10]

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |1\rangle U|0\rangle = |1\rangle(x_{00}|0\rangle + x_{10}|1\rangle) \\ |11\rangle &\rightarrow |1\rangle U|1\rangle = |1\rangle(x_{01}|0\rangle + x_{11}|1\rangle) \end{aligned} \tag{3.7}$$

โดยเรากำหนดสัญลักษณ์ $|ab\rangle = |a\rangle|b\rangle$ และ U คือ การแปลงเวกเตอร์ จาก $|0\rangle$ ไปยัง $x_{00}|0\rangle + x_{10}|1\rangle$ และ จาก $|1\rangle$ ไปยัง $x_{01}|0\rangle + x_{11}|1\rangle$ โดยที่ x_{00}, x_{10}, x_{01} และ x_{11} เป็นค่าคงที่ใด ๆ

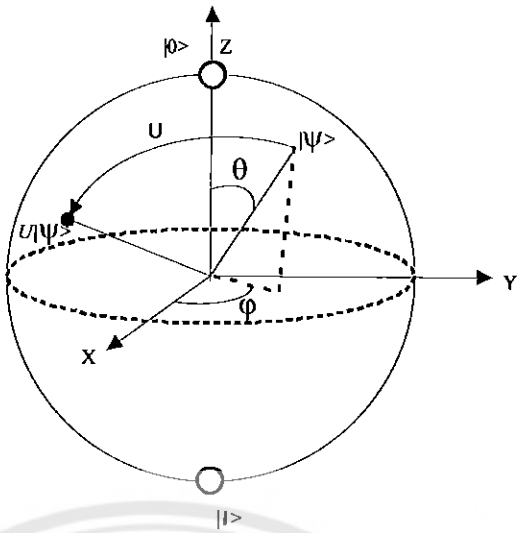
โดยทั่วไป หากเขียน U ด้วยรูปแบบเมตริกซ์ที่กระทำบนเวกเตอร์สถานะ จะสามารถเขียนได้เป็น

$$U = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix} \tag{3.8}$$

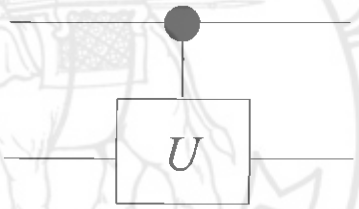
ดังนั้น เราสามารถเขียนแสดง เกตยูนิเวอร์ซอล นี้ ในรูปแบบเมตริกซ์ คือ

$$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{bmatrix} \tag{3.9}$$

โดย เราอาจจะอธิบาย การเปลี่ยนแปลงสถานะของบิตเป้าหมาย ได้โดยการใช้ทรงกลมบล็อซ ดังแสดงในรูปที่ 3.8 โดยที่มุมที่เกี่ยวข้อง (θ และ ψ) จะสัมพันธ์กับค่า x_{00}, x_{10}, x_{01} และ x_{11}



รูปที่ 3.8 การแปลงคิวบิต โดยใช้เกตยูนิเวอร์ซอล โดยพิจารณาจากการ**หมุนของเวกเตอร์**สถานะเป้าหมายบนผิวทรงกลมบล็อช [7]



รูปที่ 3.9 รูปสัญลักษณ์ของ เกตยูนิเวอร์ซอล [7]

บทที่ 4

ผลการคำนวณแบบควอนตัม

4.1 การคำนวณแบบควอนตัมเพื่อใช้ในการแยกตัวประกอบของจำนวนเฉพาะ อธิบายโดยวิธีอัลกอริทึมของชอร์ (Shor's Algorithm)

จากวิธีการคำนวณเชิงควอนตัมที่ได้กล่าวไว้ในบทที่ 2 ได้นำมาใช้ในการคำนวณการแยกตัวประกอบของจำนวนเฉพาะ โดยใช้วิธีแยกตัวประกอบตามอัลกอริทึมของชอร์ (Shor's Algorithm) โดยการหาคาบของลำดับตัวเลข ซึ่งอาศัยการหาคาบของฟังก์ชันร่วมกับการหาตัวหารร่วมมาก (ห.ร.ม.) ของจำนวนเต็ม โดยทางคณะผู้จัดทำได้สรุปอัลกอริทึมของชอร์ และใช้โปรแกรมโปรแกรมแมทแลป (Matlab) ในการสร้างโค้ดและทดสอบ ซึ่งเป็นโปรแกรมที่มีวิธีใช้งานที่ง่ายและสะดวกในการทดลอง

Matlab Code:

พื้นฐานของคำสั่ง (Basic Command) ที่ใช้ในการสร้างโค้ดตามอัลกอริทึมของชอร์ในแมทแลปมีดังต่อไปนี้

- unidrnd (N-1) คือการสุ่มค่าเพื่อนำมาใช้งาน
- mod (x1,x2) คือการหาค่าเศษของการหาร x1 ด้วย x2
- gcd (x1,x2) คือการหา ห.ร.ม. ของ x1 และ x2
- length (N) คือขอบเขตของจำนวนตัวเลขทั้งหมด
- fft (x1,N) คือการแปลงฟูเรียร์แบบเร็ว (fft) เพื่อใช้ในการหาคาบ
- abs (x1) คือการทำเลขทุกตัวให้มีค่าเป็นบวกทั้งหมด
- round (N) คือการหาค่าจำนวนเต็มที่ใกล้ N มากที่สุด
- if . . . end คือคำสั่งที่ใช้ทำการทดสอบเงื่อนไขความสัมพันธ์ว่าเป็นจริงหรือเป็นเท็จแล้วจึงกระทำคำสั่งที่อยู่ภายใต้เงื่อนไขนั้น
- while . . . end คือคำสั่งที่ใช้ทำการทดสอบเงื่อนไขทุก ๆ รอบของการวนซ้ำ ถ้าผลการทดสอบให้ค่าเป็นจริง โปรแกรมจะกระทำคำสั่งทั้งหมดภายใน while ลูปหนึ่งรอบ แล้วกลับมาตรวจสอบอีกครั้งและจะทำแบบนี้ต่อไปเรื่อย ๆ จนกว่าผลการทดสอบจะเป็นเท็จ จึงจะกระทำคำสั่งหลังจากคำสั่ง end
- for . . . end คือคำสั่งที่ใช้กระทำคำสั่งทั้งหมด (ซึ่งอาจจะมีมากกว่า 1 คำสั่ง) ในจำนวนรอบที่คงที่

4.2 ตัวอย่างการแยกตัวประกอบจำนวนเฉพาะด้วยวิธีอัลกอริทึมของชอร์

ตัวอย่างที่ 1 แยกตัวประกอบของ 21 เมื่อเราทำการสุ่มให้ค่า $a = 8$ สามารถแยกตัวประกอบโดยกระบวนการดังที่กล่าวมาเริ่มจาก

- กำหนดให้ $N = 21$
- เลือก $a = 8$ ซึ่ง ห.ร.ม. ของ 8 และ 21 เท่ากับ 1 แสดงว่า 8 และ 21 เป็นจำนวนเฉพาะสัมพัทธ์กัน
- ลำดับ $a^x \bmod N$ { $8^0 \bmod 21 = 1$, $8^1 \bmod 21 = 8$, $8^2 \bmod 21 = 1$, $8^3 \bmod 21 = 8$,...}
- หาคาบ ลำดับในขั้นตอนที่แล้วมีลักษณะซ้ำ{1,8,1,8,...} ดังนั้น คาบ คือ 2 ($q = 2$)
- $a^{q/2} + 1 = 8^1 + 1 = 9$ และ $a^{q/2} - 1 = 8^1 - 1 = 7$
- หาตัวหารร่วมมาก ห.ร.ม. (9,21) = 3 และ ห.ร.ม. (7,21) = 7

  คำตอบ ได้ตัวประกอบของ 21 คือ 3 และ 7 นั่นคือ $21 = 3 \times 7$

เมื่อทำการหาค่าในโปรแกรมแมทแลป จะได้ดังนี้

Which number do you want for factorization = 21

The factoring number is...

21

The random number(a) is...

8

The gcd is... (can use if gcd = 1)

1

q =

2

a1 =

9

a2 =

7

b1 =

3

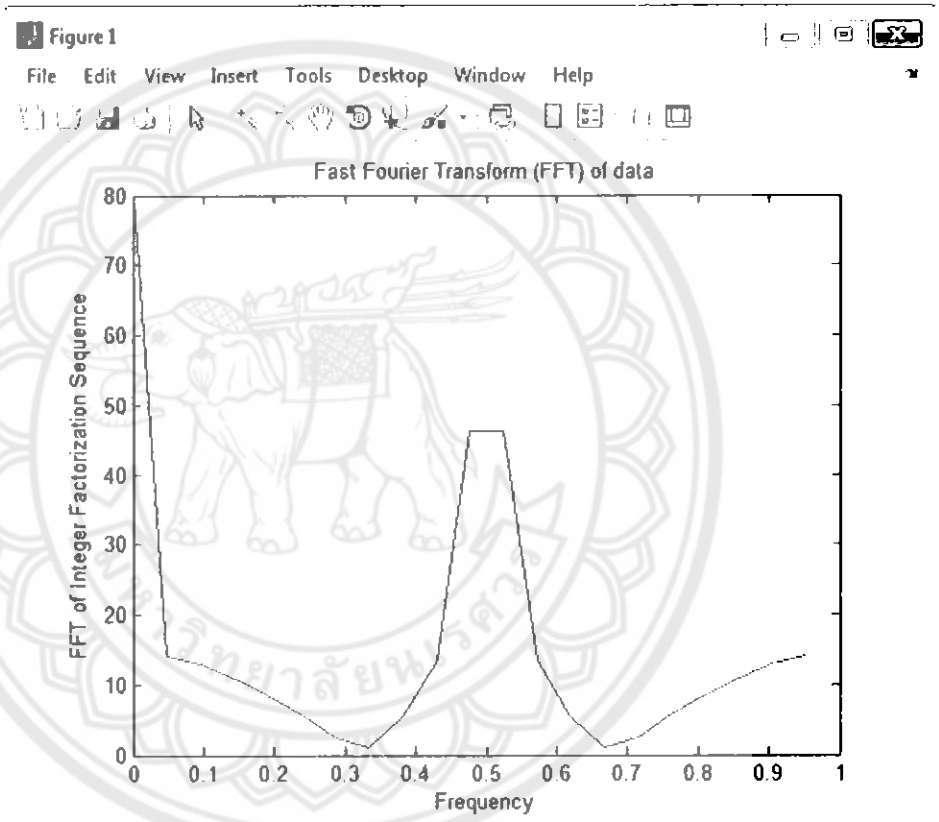
b2 =

7

The factor are...

3

7



รูปที่ 4.1 กราฟการแปลงฟูเรียร์แบบเร็วของการแยกประกอบ 21 โดยที่มีค่า a เท่ากับ 8

จากรูปที่ 4.1 เป็นกราฟการแปลงฟูเรียร์แบบเร็ว (FFT) ที่แสดงในรูปแบบของจำนวนเต็มที่ต้องการใช้แยกตัวประกอบ (N=21) เมื่อเราทำการสุ่มค่า a ได้เท่ากับ 8 ทำให้กราฟการแปลงฟูเรียร์แบบเร็วของจำนวนเต็มเทียบกับค่าของความถี่นี้ มีค่าแอมปริจูดสูงสุดลำดับที่สองอยู่ที่ 0.5 และจะสามารถนำไปคำนวณเพื่อหาคาบ (q) คือ q = (1/freq(2)) = 1/0.5 = 2 จึงจะสามารถนำค่าคาบนี้ ไปแยกตัวประกอบของค่า 21 ได้

<u>ตัวอย่าง 2</u> แยกตัวประกอบของ 33 เมื่อเราทำการสุ่มให้ค่า $a = 10$ สามารถแยกตัวประกอบโดยกระบวนการดังที่กล่าวมาเริ่มจาก

- กำหนดให้ $N = 33$
- เลือก $a = 10$ ซึ่ง ห.ร.ม. ของ 10 และ 33 เท่ากับ 1 แสดงว่า 10 และ 33 เป็นจำนวนเฉพาะสัมพัทธ์กัน
- ลำดับ $a^x \bmod N$ { $10^0 \bmod 33 = 1$, $10^1 \bmod 33 = 10$, $10^2 \bmod 33 = 1$, $10^3 \bmod 33 = 10$,... }
- หาคาบลำดับในขั้นตอนที่แล้ว มีลักษณะซ้ำ {1,10,1,10,...} ดังนั้น คาบ คือ 2 ($q = 2$)
- $a^{q/2} + 1 = 10^1 + 1 = 11$ และ $a^{q/2} - 1 = 10^1 - 1 = 9$
- หาตัวหารร่วมมาก ห.ร.ม. (11,33) = 11 และ ห.ร.ม. (9,33) = 3

  <u>คำตอบ</u> ได้ตัวประกอบของ 33 คือ 11 และ 3 นั่นคือ $33 = 11 \times 3$

เมื่อทำการหาค่าในโปรแกรมแมทแลป จะได้ดังนี้

Which number do you want for factorization = 33

The factoring number is...

33

The random number(a) is...

10

The gcd is... (can use if gcd = 1)

1

Ok!... The number can be factorized.

q =

2

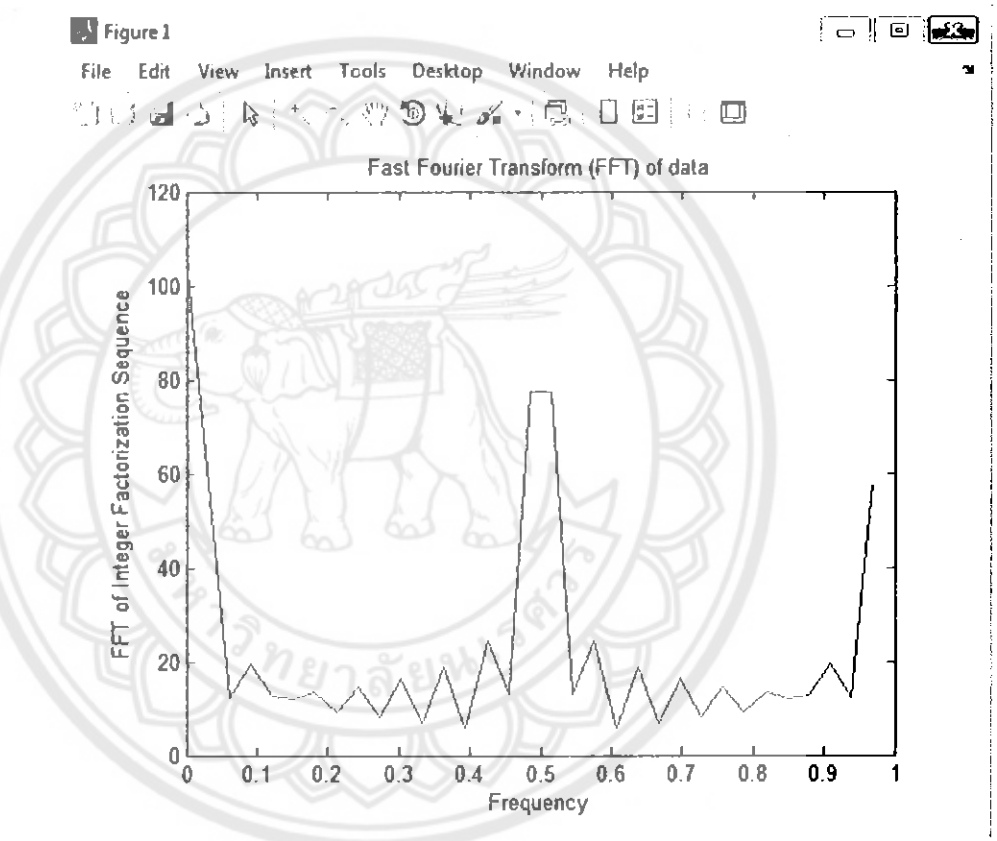
a1 =

11

a2 =

9

```
b1 =

    11

b2 =

     3

The factor are ...

    11

     3
```



รูปที่ 4.2 กราฟการแปลงฟูเรียร์แบบเร็วของการแยกประกอบ 33 โดยที่มีค่า a เท่ากับ 10

จากรูปที่ 4.2 เป็นกราฟการแปลงฟูเรียร์แบบเร็ว (FFT) ที่แสดงในรูปแบบของจำนวนเต็มที่ต้องการใช้แยกตัวประกอบ (N=33) เมื่อเราทำการสุ่มค่า a ได้เท่ากับ 10 ทำให้กราฟการแปลงฟูเรียร์แบบเร็วของจำนวนเต็มเทียบกับค่าของความถี่นี้ มีค่าแอมปริจูดสูงสุดลำดับที่สองอยู่ที่ 0.5 และจะสามารถนำไปคำนวณเพื่อหาคาบ (q) คือ $q = (1/freq(2)) = 1/0.5 = 2$ จึงจะสามารถนำค่าคาบนี้ ไปแยกตัวประกอบของค่า 33 ได้

ตัวอย่าง 3 จงแยกตัวประกอบของ 2519

3.1) เมื่อเราทำการสุ่มให้ค่า $a = 230$ สามารถแยกตัวประกอบโดยกระบวนการดังที่กล่าวมาเริ่มจาก

- กำหนดให้ $N = 2519$
- เลือก $a = 230$ ซึ่ง ห.ร.ม. ของ 230 และ 2519 เท่ากับ 1 แสดงว่า 230 และ 2519 เป็นจำนวนเฉพาะสัมพัทธ์กัน
- ลำดับ $a^x \bmod N$ { $230^0 \bmod 2519 = 1$, $230^1 \bmod 2519 = 230$, $230^2 \bmod 2519 = 1$, $230^3 \bmod 2519 = 230$,... }
- หาคาบ ลำดับในขั้นตอนที่แล้ว มีลักษณะซ้ำ {1,230,1,230,...} ดังนั้น คาบ คือ 2 ($q = 2$)
- $a^{q/2} + 1 = 230^1 + 1 = 231$ และ $a^{q/2} - 1 = 230^1 - 1 = 229$
- หาตัวหารร่วมมาก ห.ร.ม. (231,2519) = 11 และ ห.ร.ม. (229,2519) = 229

  คำตอบ ได้ตัวประกอบของ 2519 คือ 11 และ 229 นั่นคือ $2519 = 11 \times 229$

3.2) เมื่อเราทำการสุ่มให้ค่า $a = 2289$ สามารถแยกตัวประกอบโดยกระบวนการดังกล่าวมาเริ่มจาก

- กำหนดให้ $N = 2519$
- เลือก $a = 2289$ ซึ่ง ห.ร.ม. ของ 2289 และ 2519 เท่ากับ 1 แสดงว่า 2289 และ 2519 เป็นจำนวนเฉพาะสัมพัทธ์กัน
- ลำดับ $a^x \bmod N$ {$2289^0 \bmod 2519 = 1$, $2289^1 \bmod 2519 = 2289$, $2289^2 \bmod 2519 = 1$, $2289^3 \bmod 2519 = 2289$,...}
- หาคาบลำดับในขั้นตอนที่แล้วมีลักษณะซ้ำ {1,2289,1,2289,...}ดังนั้น คาบ คือ 2 ($q = 2$)
- $a^{q/2} + 1 = 2289^1 + 1 = 2290$ และ $a^{q/2} - 1 = 2289^1 - 1 = 2288$
- หาตัวหารร่วมมาก ห.ร.ม. (2289,2519) = 229 และ ห.ร.ม. (2288,2519) = 11

  คำตอบ ได้ตัวประกอบของ 2519 คือ 229 และ 11 นั่นคือ $2519 = 229 \times 11$

จากตัวอย่างทั้งหมดสามารถอธิบายได้คือ เมื่อทำการหาค่าของการแยกตัวประกอบตามโค้ดในโปรแกรมแมทแลป เป็นไปตามขั้นตอนดังต่อไปนี้

1) เราจะกำหนดค่าที่เราต้องการจะแยกตัวประกอบ (N)

2) ทำการสุ่มตัวเลข (a) ที่จะนำไปใช้ในการคำนวณ

3) หาค่า ห.ร.ม ของ (a,N) เมื่อค่าที่ได้ มีค่าเท่ากับ 1 ถือว่าผ่านสามารถนำไปใช้หาตัวประกอบได้

4) หาคาบที่ได้นั่นคือ q

5) a1 คือค่าของ $a^{q/2}+1$

6) a2 คือค่าของ $a^{q/2}-1$

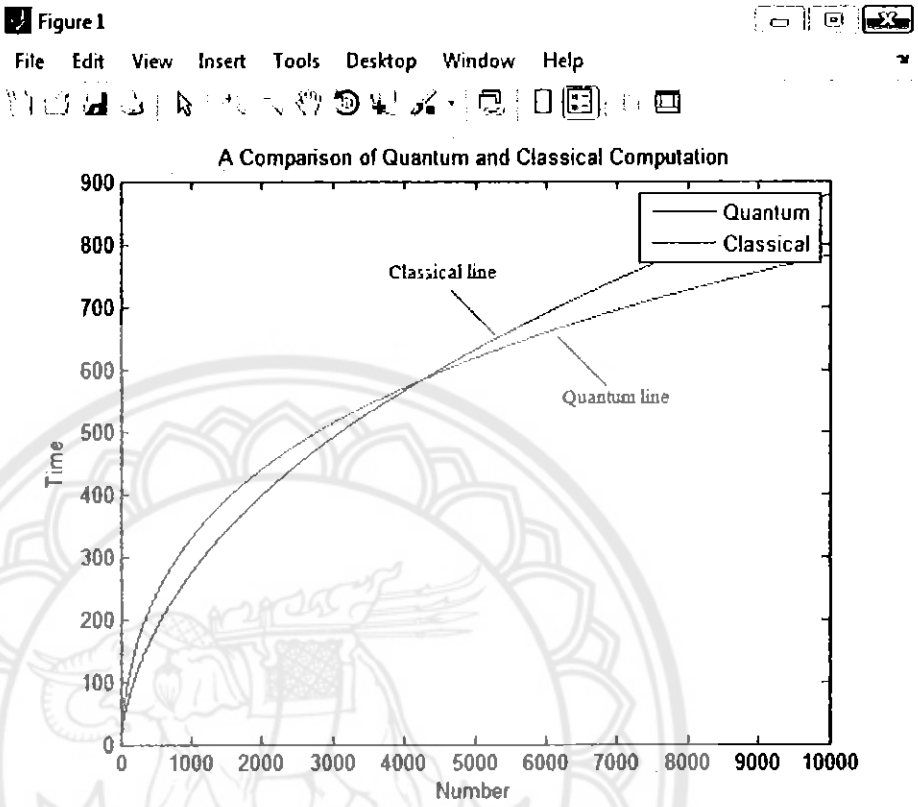
7) b1 คือค่า ห.ร.ม. ของ (a1,N)

8) b2 คือค่า ห.ร.ม. ของ (a2,N)

9) ตัวประกอบที่แยกได้ของ N คือ b1 และ b2

หมายเหตุ จะพบว่าในตัวอย่างที่ 3 เราต้องการคำนวณการแยกตัวประกอบของ 2519 ซึ่งเป็นจำนวนที่มีค่าค่อนข้างมาก เนื่องจากในโปรแกรมแมทแลปนั้นมีข้อจำกัดในการคำนวณตัวเลขที่มีค่ามากๆ จึงทำให้การสุ่มค่า a บางค่าเกิดปัญหา นั่นคือการคำนวณค่าที่ a^x ที่ลำดับสูงๆ ทำไม่ได้ จะเกิดการ error เกิดขึ้น นอกจากนั้น ยังไม่สามารถทำการพล็อตกราฟ FFT ได้ เนื่องจากติดปัญหาที่โปรแกรมแมทแลปไม่สามารถพล็อตกราฟค่ามากๆได้ และจากการดูค่าของลำดับพบว่าลำดับของจำนวน 2519 จะใช้ได้แค่ 6 ค่าแรกเท่านั้น เราจึงจำกัดการหา q ด้วยลำดับเพียงแค่ 6 ตัวแรก เนื่องจากเราจำกัดคาบ (q) ดังนั้น คณะผู้จัดทำจึงได้แก้ปัญหาด้วยการคำนวณด้วยมือ โดยวิธีการคำนวณย้อนกลับจึงทราบว่ามีค่า a สองค่าเท่านั้นที่ใช้ได้ คือ a เท่ากับ 230 และ 2289 ที่จะสามารถแยกตัวประกอบภายใต้เงื่อนไขที่เรากำหนดได้

4.3 เปรียบเทียบการคำนวณแบบควอนตัมกับการคำนวณแบบดั้งเดิม



รูปที่ 4.3 เปรียบเทียบการคำนวณแบบควอนตัม (เส้นสีน้ำเงิน)
กับการคำนวณแบบดั้งเดิม (เส้นสีแดง)

จากรูปที่ 4.3 เป็นกราฟที่แสดงการเปรียบเทียบการคำนวณแบบควอนตัม กับการคำนวณแบบดั้งเดิม ในการแยกตัวประกอบของจำนวนเต็มด้วยวิธีของชอร์ โดยที่การคำนวณแบบควอนตัมนั้น จะใช้เวลาในการทำงานเป็นแบบโพลิโนเมียลคือ O ((log N) ^{3}) (ใช้ได้ในเฉพาะกรณีที่เกี่ยวข้องกับการคำนวณแบบควอนตัม ในการแยกตัวประกอบจำนวนเฉพาะด้วยวิธีของชอร์) ส่วนการคำนวณแบบดั้งเดิม จะใช้เวลาในการทำงานเป็นแบบเอ็กโพเนนเชียล O ($e^{1.9 (\log N)1/3 (\log \log N)2/3}$) (ใช้ได้ในกรณีที่เกี่ยวข้องกับการคำนวณแบบดั้งเดิม ในการแยกตัวประกอบจำนวนเฉพาะที่มีจำนวนตัวเลขมากกว่า 100 หลัก) จึงทำให้การคำนวณแบบควอนตัม มีประสิทธิภาพมากกว่าการคำนวณแบบดั้งเดิม เมื่อมีจำนวนตัวเลขที่มากขึ้น โดยจะอาศัยหลักการของการแปลงฟูเรียร์แบบเร็ว (FFT) มาใช้ในการหาคาบของจำนวนนั้นๆ เพื่อทำการแยกตัวประกอบจำนวนเฉพาะต่อไป [11]

บทที่ 5
สรุปผลและข้อเสนอแนะ

5.1 สรุปผลจากการศึกษา

ในโครงงานนี้ เราได้ศึกษาเรื่อง การคำนวณแบบควอนตัม และควอนตัมดอทโมเลกุล เพื่อนำไปใช้ในการแยกตัวประกอบโดยใช้อัลกอริทึมของชอร์ ซึ่งพบว่ามีความรวดเร็วและสะดวกกว่าการคำนวณด้วยมือ

5.1.1 ควอนตัมดอทโมเลกุล

จากการที่ได้ศึกษาพบว่า ควอนตัมดอทโมเลกุล เป็นโครงสร้างของสารกึ่งตัวนำที่มีความสามารถในการกักเก็บอิเล็กตรอน โดยโครงสร้างที่เราใช้ในการศึกษาคือ ควอนตัมดอทโมเลกุลแบบคู่ ซึ่งจะมีคุณสมบัติการทับซ้อน และ การพัวพัน จึงทำให้เราสามารถแก้ปัญหาการแยกตัวประกอบด้วยจำนวนเฉพาะได้รวดเร็วขึ้น

5.1.2 การคำนวณแบบควอนตัม

การคำนวณแบบควอนตัมเป็นการคำนวณโดยอาศัยกฎทางฟิสิกส์ด้านกลศาสตร์ควอนตัม ซึ่งประกอบด้วย การทับซ้อนและการพัวพัน อาศัยการแทนค่าของคิวบิตเนื่องจากค่าที่ได้ในคิวบิตสามารถเป็นได้ทั้ง "0" และ "1" จากทฤษฎี จึงพบว่าทำให้เราสามารถคำนวณแบบขนาน และ ทำให้เราสามารถแก้ปัญหาในบางกรณีได้อย่างรวดเร็ว และยังพบว่าในการคำนวณแบบควอนตัมนั้น ยังสามารถนำไปใช้ประโยชน์ได้อีกหลายอย่างนอกจากการนำมาคำนวณด้วยควอนตัมดอท

5.1.3 พื้นฐานการแยกตัวประกอบด้วยอัลกอริทึม

จากการศึกษาพบว่า การแยกตัวประกอบด้วยอัลกอริทึมของชอร์ (Shor's algorithm) เพราะว่ามีคุณสมบัติทับซ้อนเชิงตำแหน่ง ช่วยให้คำนวณลำดับ $a^x \bmod N$ โดยผ่านรีจิสเตอร์เพียงครั้งเดียว ซึ่งเมื่อประมวลเวลาที่ใช้ทั้งหมดแล้ว จะอยู่ที่อันดับ n^3 เมื่อ n เป็นความยาวของตัวเลขที่ต้องการแยกตัวประกอบ

จากผลการทดลองในตัวอย่างของบทที่ 4 เราพบว่าการแยกตัวประกอบด้วยวิธีของชอร์นั้นมีความรวดเร็วขึ้นมากกว่าการคำนวณด้วยมือ แต่เนื่องจากโปรแกรมที่ใช้เป็นโปรแกรมแมทแลป มีข้อจำกัด และอาจมีความผิดพลาดเกิดขึ้น โดยพบว่าเมื่อทำในโปรแกรมแมทแลปแล้วค่า N ที่มีค่าน้อยๆ จะสามารถทำการสุ่มหาค่า a ได้ง่าย และสามารถหาคาบมาใช้ในการคำนวณได้ แต่เมื่อค่า N

มีค่ามากๆดังตัวอย่าง จะพบว่าในการสุ่มหาค่า a ที่นำมาใช้ในการแยกตัวประกอบนั้น เป็นไปได้ยาก และในการหาคาบของค่านั้นๆก็จะเป็นไปได้ยากด้วยเช่นกัน แต่เราจะเห็นได้ว่าเมื่อค่า N มีค่ามากขึ้น จะทำให้ความเร็วในการคำนวณน้อยลง

5.2 ปัญหาและแนวทางแก้ไข

จากการศึกษาพบปัญหาในด้านของการสืบค้นเนื้อหา และ การเรียนรู้ทำความเข้าใจ เนื่องจากเรื่องที่ศึกษานี้ เป็นเรื่องที่มีเนื้อหาอยู่ในระดับขั้นสูง ในที่นี้เราจึงสามารถศึกษา/อธิบายได้เพียงในระดับเบื้องต้นเท่านั้น นอกจากนี้ การศึกษาที่นำเสนอนี้ การเชื่อมต่อระหว่าง โครงสร้างควอนตัมดอทโมเลกุล และ การนำไปใช้ในการคำนวณแบบควอนตัม ยังไม่ชัดเจนเท่าที่ควร แนวทางการแก้ไข คือ ถ้ามีการนำไปศึกษาเพิ่มเติม จะพบว่าในการควบคุมสถานะคิวบิต (อิเล็กตรอนในควอนตัมดอทโมเลกุล) สามารถทำได้โดยการควบคุมด้วยแสง เพื่อให้การคำนวณด้วยอัลกอริทึมเชิงควอนตัม เช่น การแยกตัวประกอบจำนวนเฉพาะ มีความชัดเจนมากยิ่งขึ้น

เอกสารอ้างอิง

[1] S. Kiravittaya, M.Sawadsaringkarn and S.Panyakeow, "Quantum dots structure for optoelectronic devices"

[2] S. Kiravittaya, M.Sawadsaringkarn and S.Panyakeow, "InAs/GaAs self-organized quantum dots on (4 1 1)A GaAs by molecular beam epitaxy ", Journal of Crystal Growth,Volumes 227–228, 2001, Pages 1010–1015.

[3] T. Suzuki, Y. Temko, M.C. Xu, K. Jacobi, "The atomic structure of InAs quantum dots on GaAs (1 1 2)A", Surface Science, Volume 595, December 2005, Pages 194–202.

[4] S. Kiravittaya, R. Songmuang, A. Rastelli, H. Heidemeyer and O. G. Schmidt, "Multi - scale ordering in self-assembled InAs/GaAs (001) quantum dots", Nanoscale Research Letter, Volume 1, 2006, Pages 1-10.

[5] ศ. ดร. สมศักดิ์ ปัญญาแก้ว, รศ. ดร. มนตรี สวัสดิ์ศฤงฆาร, รศ. ดร. บรรยง โตประเสริฐพงศ์ , รศ. ดร. ชุมพล อันตรเสน, รศ. ดร. สมชัย รัตนธรรมพันธ์, รศ. ดร. ทรงพล กาญจนชูชัย , ดร. ชนินทร์ วิศวินธานนท์, นาย ศุภโชค ไทยน้อย และ นาย พรชัย ช่างม่วง, "รายงานการวิจัยเรื่อง การวิจัยพื้นฐานสารกึ่งตัวนำที่มีโครงสร้างนาโนแบบจัดเรียงตัวเอง โดยวิธีปลูกชั้นผลึกด้วยลำโมเลกุล", คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550-2553

[6] S. Suraprapapich, Y.M. Shen, V.A. Odnoblyudov, Y. Fainman, S. Panyakeow and C.W. Tu, "Self-assembled lateral Bi-quantum-dot molecule formation by gas-source molecular beam epitaxy ", Journal of Crystal Growth, Volumes 301-302, 2007, Pages 735-739.

[7] นาย พบพร ด่านวิรุทัย และ นาย เกียรติศักดิ์ ศรีพิมานวัฒน์ และ คณะ, "พัฒนาการสารสนเทศเชิงควอนตัม", ชุดหนังสือสารสนเทศเชิงควอนตัม 1, 2555

[8] Y. Wu, X. Li, D. Steel, D. Gammon, L.J. Sham, "Coherent optical control of semiconductor quantum dots for quantum information processing", Physica E : Low - dimensional Systems and Nanostructures, Volume 25, Pages 242–248.

[9] A. Steane, "Quantum Computing", Reports on Progress in Physics, Volume 61, 1998, Pages 117-173.

[10] http://en.wikipedia.org/wiki /Quantum_gate

[11] http://en.wikipedia.org/wiki/Shor's_algorithm

ภาคผนวก ก

รายละเอียดเกี่ยวกับ Matlab Code ที่ใช้ในการแยกตัวประกอบด้วยวิธีของชอร์

```
disp ('Welcome to "Shor" Factoring Algorithm!!!...') ;
disp ('_____') ;
disp ('Please remind that, There are four restrictions for Shor algorithm.') ;
disp ('1)The number to be factored (N) must be >= 15') ;
disp ('2)The number to be factored (N) must be "Odd" number') ;
disp ('3)The number must not be prime') ;
disp ('4)The number must not be prime power') ;
disp ('5)The value period (p) must not be "Odd" number') ;
disp ('_____') ;
%%Part1: Input and Random value
N = input ('Which number do you want for factorization = ') ;
disp ('The factoring number is...')
disp (N)
a = randi (N-1);
% a=input('The random number(a) = ');
disp ('The random number(a) is...')
disp (a)
%%Part2: Check the conditions
while mod (N,2)==0
disp ('The number is "Even"... Please try again!')
N = input ('Which number do you want for factorization = ') ;
end
j = 1:100 ;
while N==power (a,j)
disp ('The number is "Prime power"... Please try again!')
N = input ('Which number do you want for factorization = ') ;
end
m = gcd(a,N) ;
disp ('The gcd is... (can use if gcd = 1)')
disp (m)
if m==1 ;
disp ('Ok!... The number can be factorized.') ;
```

```
for p = 1:N ;
mo (p) = mod (a.^p,N) ;
end
% N=length(y);%get the whole number
t = 0:1:N ;
Fs = 1 ;%sampling rate
Ts = 1/Fs ;%sampling time interval
%%%Get fft Part%%%
k = 0:N-1 ;  %create a vector from 0 to N-1
T = N/Fs ;%get the frequency interval
f= k/T ;%create the frequency range
X1 = fft (mo,N) ;  %fft to data
X = abs(X1) ;
[sortedValues1,sortIndex] = sort (X(:),'descend') ;
maxindex = sortIndex (2:end) ;
index = maxindex (1) ;
freq = f(index) ;  %find the period with maximum point
q = round(1/freq)
a1 = round (a.^(q/2))+1
a2 = round (a.^(q/2))-1
b1 = gcd (a1,N)
b2 = gcd (a2,N)
disp ('The factor are...') ;
disp (b1) ; disp (b2) ;
return
end
while m>0 ;
disp ('Random number(a) can not use...Try again!') ;
a = randi (N-1) ;
disp ('New random number(a) ...') ;
disp (a) ;
m = gcd (a,N) ;
```

```
disp ('The gcd is... (can use if gcd = 1)')
disp (m)

for p = 1:N ;
mo (p) = mod (a.^p,N) ;
end
% N=length(y);%get the whole number
t  = 0:1:N-1 ;
Fs = 1 ;%sampling rate
Ts = 1/Fs ;%sampling time interval
%%%Get fft Part%%%
k = 1:N ;  %create a vector from 0 to N-1
T = N/Fs ;%get the frequency interval
F = k/T ;%create the frequency range
X1 = fft (mo,N) ;  %fft to data
X = abs (X1) ;
[sortedValues1,sortIndex] = sort (X(:),'descend') ;
maxindex = sortIndex (2:end) ;
index = maxindex (1) ;
freq = f(index) ;  %find the period with maximum point
q = round(1/freq)
a1 = round (a.^(q/2))+1
a2 = round (a.^(q/2))-1
b1 = gcd (a1,N)
b2 = gcd (a2,N)
disp ('The factor are...') ;
disp (b1) ; disp (b2) ;
return
end
```

ภาคผนวก ข

รายละเอียดเกี่ยวกับ Matlab Code ที่ใช้ในการพล็อตกราฟเปรียบเทียบความเร็วของการคำนวณแบบควอนตัมกับการคำนวณแบบดั้งเดิม

```
N = 10:10000;
x = power(log(N),3);
y = exp(1.9*power(log(N),(1/3)).*power(log(log(N)),(2/3)));
plot(N,x);
holdon;
plot(N,y,'r');
xlabel('Number');
ylabel('Time');
title('A Comparison of Quantum and Classical Computation');
legend('Quantum','Classical')
```