รหัสอินเตอร์ลีฟมอดิฟายอาร์เรย์สำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

INTERLEAVE MODIFIED ARRAY CODES FOR MAGNETIC RECORDING SYSTEM

วิชาญ สิงห์อุดม
WICHARN SINGHAUDOM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมโทรคมนาคม
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2550

รหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์สำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

INTERLEAVE MODIFIED ARRAY CODES FOR MAGNETIC RECORDING SYSTEM

วิชาญ สิงห์อุดม

WICHARN SINGHAUDOM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2550

INTERLEAVE MODIFIED ARRAY CODES FOR MAGNETIC RECORDING SYSTEM

WICHARN SINGHAUDOM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2007

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ รหัสอินเตอร์ลีฟมอดิฟายอาร์เรย์สำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

Interleave Modified-Array Code for Magnetic Recording System

นักศึกษา นายวิชาญ สิงห์อุดม

รหัสประจำตัว 45061230

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมโทรคมนาคม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.สุทธิชัย นพนาคีพงษ์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ผศ.ดร.พรชัย ทรัพย์นิธิ

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.สุวิพล	สิทธิชีวภาค	
ผศ.ดร.พิเชฐ	ม่วงนวล	
ผศ.ดร.เผ่าภัค	ศิริสุข	
ผศ.ดร.พรชัย	ทรัพย์นิธิ	
ผศ.ดร.สุทธิชัย	นพนาคีพงษ์	

วัน / เดือน/ ปี ที่สอบ 28 พฤษภาคม 2550 เวลา 09.00-11.00 น.

สถานที่สอบ ณ อาคาร 12 ชั้น ชั้น 4 (ห้อง E12-402)

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.จารุวัตร เจริญสุข)

คณบดีบัณฑิตวิทยาลัย

วันที่.....30.....**เดือน**.....พฤษภาคม.....**พ.ศ.**.....2550.....

หัวข้อวิทยานิพนธ์	รหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์สำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก
นักศึกษา	นาย วิชาญ สิงห์อุดม
รหัสนักศึกษา	45061230
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2549
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ.ดร.สุทธิชัย นพนาคีพงษ์
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ผศ.ดร.พรชัย ทรัพย์นิธิ

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้นำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์สำหรับการประยุกต์ใช้งานในระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยจะเน้นรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ โดยผลการจำลองสมรรถนะการทำงานพบว่าค่าอัตราความผิดพลาดบิตข้อมูลของรหัสแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์ต่ำกว่าในกรณีรหัสมอดดิฟายอาร์เรย์ ตั้งแต่อัตรารหัสปานกลางไปจนถึงอัตรารหัสสูงบนช่องสัญญาณรบกวนเกาส์แบบขาว ในขณะที่ยังคงสามารถใช้โครงสร้างการถอดรหัสแบบเดียวกับรหัสแอลดีพีซีแบบทั่วไปได้ อีกทั้งยังคงคุณสมบัติที่ดีของรหัสมอดดิฟายอาร์เรย์ เช่น มี Error floor ที่ต่ำและปราศจากไซเคิลขนาดเท่ากับ 4

Thesis Title	Interleave Modified Array Codes for Magnetic Recording System
Student	Mr. Wicharn Singhaudom
Student ID.	45061230
Degree	Master of Engineering
Program	Telecommunications Engineering
Year	2006
Thesis Advisor	Asst. Prof. Dr. Suthichai Noppanakeepong
Thesis Co-Advisor	Asst. Prof. Dr. Pornchai Supnithi

ABSTRACT

This thesis presents design of Modified Array Codes (MAC) and Interleave Modified Array Codes (IMAC). Both are considered low-density parity-check (LDPC) codes. Simulation results show that the IMAC code provides bit error rate reduction compared to MAC at medium to high code rates in the Additive White Gaussian Noise channel (AWGN). The proposed IMAC codes can still use the same decoding algorithm as the general LDPC codes and offers the advantages of MAC such as low error floor and nonexistent girth of size 4.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงเป็นอย่างดี ก็เนื่องด้วยการสนับสนุนของบุคคลหลายฝ่าย ผู้ทำวิจัย

ขอขอบพระคุณ ผศ.ดร.สุทธิชัย นพนาคีพงษ์ และผศ.ดร.พรชัย ทรัพย์นิธิ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ และอาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วม ที่กรุณาช่วยให้แนวคิด ให้คำปรึกษาในการทำวิจัย ตลอดจนการวิเคราะห์เพื่อแก้ปัญหาต่างๆอันเป็นประโยชน์ต่องานวิจัย และได้กรุณาให้การสนับสนุนโอกาสในการศึกษาวิจัยในระดับต่อไป

ขอขอบพระคุณคณาจารย์ ภาควิชาวิศวกรรมโทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้ผู้ทำวิจัย

ขอขอบคุณ คุณประพัน ลี้กุล และทุกคนในห้องปฏิบัติการวิจัยการสื่อสารดาวเทียม โครงการสำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ (ReCCIT) ที่ให้คำแนะนำต่าง ๆ และกำลังใจเสมอ

ขอขอบคุณบริษัทฟูจิตสึประเทศไทยจำกัด ที่ให้โอกาสในการทำงานเพื่อให้มีรายได้ส่วนหนึ่งสำหรับเป็นทุนในการศึกษาและทำวิจัย

และสุดท้ายนี้ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ และครอบครัว สำหรับการสนับสนุนในทุก ๆ ด้านรวมถึงเป็นกำลังใจให้เสมอมอีกทั้งช่วยผลักดันให้วิทยานิพนธ์ฉบับนี้สำเร็จได้เป็นอย่างดี

วิชาญ สิงห์อุดม

สารบัญ

หน้า

สารบัญ (ต่อ)

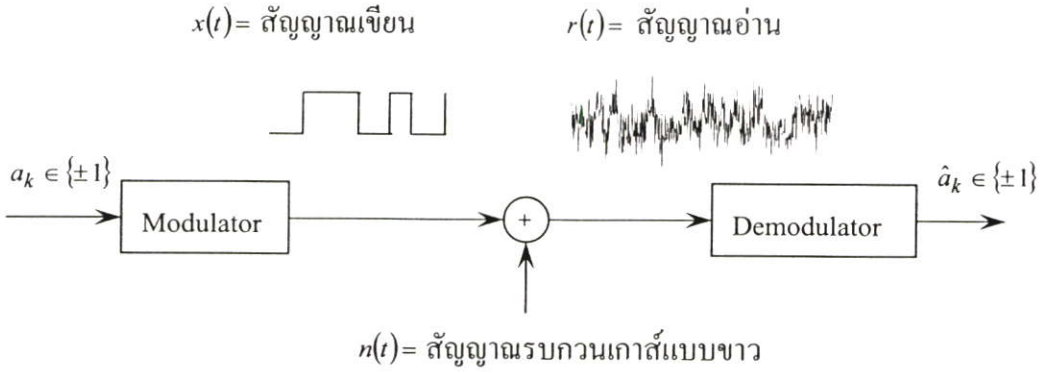
หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา



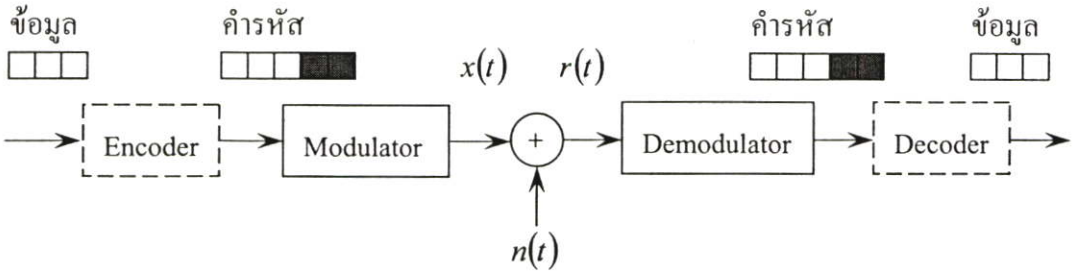
รูปที่ 1.1 แบบจำลองของระบบบันทึกข้อมูลแบบดิจิตอล

พิจารณาแบบจำลองของระบบบันทึกข้อมูลแบบดิจิตอลในรูปที่ 1.1 ที่มีอินพุตเป็น ± 1 และช่องสัญญาณเป็นแบบอุดมคติที่มีเพียงสัญญาณรบกวนเกาส์แบบขาว (Additive White Gaussian Noise: AWGN) ทำการส่งข้อมูลจากอุปกรณ์ภาคส่งผ่านช่องสัญญาณไปยังอุปกรณ์ภาครับนั้น สัญญาณที่อ่านได้มักจะเกิดปัญหาการผิดเพี้ยนของรูปสัญญาณอันเนื่องมาจากผลกระทบของสัญญาณรบกวนจากภายนอกในรูปแบบต่างๆ ปัญหาเหล่านี้เองมักจะส่งผลให้สมรรถนะของสัญญาณที่ภาครับหรือข้อมูลที่ภาครับมีความผิดพลาดเกิดขึ้น ซึ่งสมรรถนะของสัญญาณที่ภาครับจะขึ้นอยู่กับองค์ประกอบหลักที่สำคัญ 2 ประการอันได้แก่

1) คุณสมบัติของตัวกลางหรือช่องสัญญาณที่ใช้ในการส่งผ่าน
2) คุณภาพของสัญญาณที่ใช้ในการส่งผ่านช่องสัญญาณ

เมื่อต้องการเพิ่มสมรรถนะของสัญญาณอ่านให้มีอัตราความผิดพลาดบิต (Bit Error Rate : BER) น้อยลงและอยู่ในระดับที่ยอมรับได้นั้น เมื่อพิจารณาจากองค์ประกอบหลักที่สำคัญ 2 ประการข้างต้นจะพบว่า คุณสมบัติของตัวกลางหรือช่องสัญญาณที่ใช้ในการส่งผ่านนั้นเป็นปัจจัยภายนอกซึ่งเป็นเรื่องยากที่จะทำการแก้ไขคุณสมบัติของตัวกลาง ในขณะที่เมื่อพิจารณาคุณภาพของสัญญาณที่ใช้ในการส่งผ่านช่องสัญญาณนั้น เราสามารถเพิ่มคุณภาพของสัญญาณหรือสมรรถนะของสัญญาณที่ภาครับได้โดย การเพิ่มกำลังส่งของสัญญาณที่ภาคส่งเพื่อให้สัดส่วนของสัญญาณที่ใช้ในการส่งผ่านช่องสัญญาณกับสัญญาณรบกวน (Signal to Noise Ratio : SNR) ให้สูงขึ้น แต่วิธีการนี้อาจจะไม่เหมาะสมนักเนื่องจากการเพิ่มกำลังส่งของสัญญาณจะนำมาซึ่งความ

ต้องการพลังงานของอุปกรณ์ที่ภาคส่งนั้นก็จะมากขึ้น และนั้นก็หมายถึงค่าใช้จ่ายที่จะต้องสูงขึ้น ดังนั้นวิธีการนี้จึงไม่เป็นที่นิยมมากนัก แต่ยังมีเทคนิควิธีการหนึ่งที่เรียกว่าการเข้ารหัสช่องสัญญาณ (channel coding) ที่เรียกว่า ECC (Error Correcting Code) โดยเป็นเทคนิคซึ่งจำเป็นที่จะต้องมีการเพิ่มจำนวนของบิตพิเศษหรือที่เรียกว่าแพริตี้บิตเข้าไปกับชุดข้อมูลเดิมก่อน ที่จะทำการส่งออกข้อมูลชุดใหม่ ที่เรียกว่า คำรหัส (codeword) ผ่านช่องสัญญาณโดยบิตพิเศษที่เพิ่มเข้ามาจะช่วยให้ภาครับสามารถที่จะตรวจจับความผิดพลาดได้ หรือหากเพิ่มจำนวนบิตเข้าไปในจำนวนที่มากพอภาครับก็อาจจะสามารถแก้ไขความผิดพลาด (error correction) ของข้อมูลได้ด้วย



รูปที่ 1.2 แบบจำลองของระบบบันทึกข้อมูลแบบดิจิตอลที่มีการเข้ารหัสช่องสัญญาณ

พิจารณาแบบจำลองของระบบบันทึกข้อมูลแบบดิจิตอลในรูปที่ 1.2 พบว่าส่วนที่เพิ่มเข้ามาคือชุดเข้ารหัส (Encoder) และชุดถอดรหัส (Decoder) อย่างไรก็ดีการเข้ารหัสช่องสัญญาณนั้นมีผลทำให้อัตราบิตข้อมูลที่ต้องส่งจริงมีขนาดสูงขึ้น ถ้าหากช่องสัญญาณมีแบนด์วิดท์ที่จำกัดและต้องการให้การรับส่งของข้อมูลมีความถูกต้องมากขึ้น ก็จะต้องลดค่าอัตราการส่งบิตข้อมูลลง

ระบบบันทึกข้อมูลแบบดิจิตอลอีกชนิดหนึ่งก็คือ ระบบบันทึกข้อมูลเชิงแม่เหล็กซึ่งเป็นระบบที่ต้องการความถูกต้อง และความแน่นอนในการเก็บ (เขียน) ข้อมูลสูงมักจะมีการนำข้อมูลดิจิตอลไปทำการเข้ารหัสช่องสัญญาณ ก่อนที่จะเขียนบนแผ่นสื่อเพื่อให้การอ่านข้อมูลมีความผิดพลาดน้อยลงและมีอัตราผิดพลาดของบิตที่ยอมรับได้ งานวิจัยชิ้นนี้จึงได้ทำการศึกษาการเข้ารหัสช่องสัญญาณที่ให้อัตราความผิดพลาดบิตที่เหมาะสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

การเข้ารหัสช่องสัญญาณสามารถแบ่งออกเป็นสองประเภทได้แก่

1) รหัสคอนโวลูชัน (convolution code)

2) รหัสบล็อกเชิงเส้น (linear block code)

รหัสสองชนิดนี้มีความแตกต่างกันที่ขั้นตอนในการเข้ารหัส กล่าวคือ รหัสคอนโวลูชันเป็นรหัสช่องสัญญาณเชิงเส้นชนิดหนึ่งซึ่งจะทำการเข้ารหัสข้อมูลที่ละบิต และเอาต์พุตของตัวเข้ารหัสที่ได้แต่ละครั้งจะขึ้นกับข่าวสารของอินพุตปัจจุบันและข่าวสารที่ผ่านมาด้วย รหัสคอนโวลูชันที่มีชื่อเสียงและเป็นที่รู้จักกันอย่างแพร่หลายคือ รหัสเทอร์โบ (Turbo codes) [1] ซึ่งมี

สมรรถนะการทำงานที่เข้าใกล้ลิมิตของแชนนอน (Shannon) ในขณะที่รหัสบล็อกเชิงเส้นจะทำการเข้ารหัสข้อมูลทีละบล็อก โดยที่เอาต์พุตของตัวเข้ารหัสที่ได้แต่ละครั้งจะไม่ขึ้นกับข่าวสารของอินพุตปัจจุบันและข่าวสารที่ผ่านมาด้วย โดยการเข้ารหัสจะใช้เมตริกส์กำเนิด (generator matrix) หรือบางครั้งสามารถใช้เมตริกส์อีกประเภทหนึ่งที่เรียกว่าเมตริกส์แพริตี้เช็ค (parity check matrix) มีงานวิจัยพบว่ารหัสบล็อกเชิงเส้นเชิงเส้นชนิดหนึ่งที่เรียกว่า รหัสแอลดีพีซี มีสมรรถนะการทำงานที่เข้าใกล้ลิมิตของแชนนอลได้เช่นเดียวกับ รหัสเทอร์โบ [2] วิทยานิพนธ์ฉบับนี้พิจารณาศึกษารหัสช่องสัญญาณแบบแอลดีพีซีที่มีโครงสร้างเมตริกส์แพริตี้เช็คเป็นแบบอาร์เรย์ (รายละเอียดของรหัสแอลดีพีซีแบบอาร์เรย์จะกล่าวโดยละเอียดอีกครั้งในบทที่ 3)

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งหวังเพื่อจะศึกษาเทคนิคการเข้ารหัสช่องสัญญาณ ที่ทำให้อัตราความผิดพลาดบิตที่เหมาะสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก ซึ่งจะเป็นการเพิ่มคุณภาพของสัญญาณหรือสมรรถนะของสัญญาณที่ภาครับ ดังนั้นวิทยานิพนธ์ฉบับนี้จึงนำเสนอหลักการใหม่ โดยหลักการใหม่ที่นำเสนอในวิทยานิพนธ์นี้คือการปรับปรุงเมตริกส์แพริตี้เช็คของรหัสแอลดีพีซีแบบอาร์เรย์ชนิดหนึ่งที่เรียกว่า มอดดิฟายอาร์เรย์ ด้วย Quasi-cyclic matrix ซึ่งเป็นส่วนที่เพิ่มเข้าไปในเมตริกส์แพริตี้เช็คของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ให้กลาย เป็นรหัสแอลดีพีซีแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์ โดยที่ Quasi-cyclic matrix ที่สร้างขึ้นนี้เมื่อทำการยกกำลังเท่ากับขนาดของเมตริกส์จะมีค่าเท่ากับตัวมันเองและเมื่อทำการยกกำลัง Quasi-cyclic matrix เท่ากับขนาดของเมตริกส์ลบหนึ่งจะมีค่าเท่ากับเมตริกส์เอกลักษณ์ ซึ่งสามารถที่จะช่วยให้ระบบมีสมรรถนะที่ดีขึ้น

1.3 สมมติฐานของการศึกษา

รหัสแอลดีพีซีโดยทั่วไปจะใช้เมตริกส์แพริตี้เช็คในการเข้ารหัส โดยสามารถแบ่งรหัสแอลดีพีซีออกเป็นสองประเภทตามโครงสร้างของเมตริกส์แพริตี้เช็คได้แก่

1) เมตริกส์แพริตี้เช็คที่มีโครงสร้างแบบสุ่ม (random parity check matrix)
2) เมตริกส์แพริตี้เช็คแบบมีโครงสร้าง (structured parity check matrix)

ข้อดีของเมตริกส์แพริตี้เช็คที่มีโครงสร้างแบบสุ่ม คือสมรรถนะของอัตราความผิดพลาดบิตที่ภาครับจะดีกว่า รหัสแอลดีพีซีที่ใช้การเข้ารหัสด้วยเมตริกส์แพริตี้เช็คแบบมีโครงสร้าง แต่อย่างไรก็ดีในเรื่องการสร้างเมตริกส์แพริตี้เช็คนั้นจะมีความซับซ้อนสูงกว่ารหัสแอลดีพีซีที่ใช้การเข้ารหัสด้วยเมตริกส์แพริตี้เช็คแบบมีโครงสร้างมาก ด้วยเหตุนี้วิทยานิพนธ์ฉบับนี้ทำการศึกษาการปรับปรุงเมตริกส์แพริตี้เช็คของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ ด้วย Quasi-cyclic matrix

เพื่อให้สมรรถนะของอัตราความผิดพลาดบิตดีขึ้นในขณะที่ ยังคงคุณสมบัติของเมตริกส์แพริตี้เช็คแบบมีโครงสร้างที่สามารถสร้างเมตริกส์แพริตี้เช็คได้ง่าย

1.4 ทฤษฎีหรือแนวคิดที่ใช้ในการวิจัย

รหัสแอลดีพีซีที่คิดค้นขึ้นในครั้งแรกนั้น เมตริกส์แพริตี้เช็คมีโครงสร้างแบบสุ่มหลังจากนั้นจึงมีการนำเสนอรหัสแอลดีพีซีที่เมตริกส์แพริตี้เช็คเป็นแบบมีโครงสร้างที่เรียกว่า รหัสอาร์เรย์ (Array Codes) [3] หลังจากนั้นรหัสมอดดิฟายอาร์เรย์ได้ถูกพัฒนาภายใต้แนวคิดที่ต้องการเพิ่มประสิทธิ ภาพของการเข้ารหัส (สามารถเข้ารหัสได้ง่าย) โดยใช้หลักการของ cyclic shift กับแต่ละแถวของเมตริกส์แพริตี้เช็คของรหัสอาร์เรย์โดยมีชื่อเรียกว่า รหัสมอดดิฟายอาร์เรย์ (Modified Array Codes) [4] วิทยานิพนธ์ฉบับนี้จึงได้ทำการปรับปรุงเมตริกส์แพริตี้เช็คของรหัสมอดดิฟายอาร์เรย์ด้วย Quasi-cyclic matrix ภายใต้แนวคิดที่ทำการ cyclic shift ในระดับบิต และสามารถทำให้สมรรถนะอัตราความผิดพลาดบิตดีขึ้นในช่องสัญญาณรบกวนเกาส์แบบขาว

1.5 ขอบเขตการวิจัย

ขอบเขตของการวิจัยของวิทยานิพนธ์ฉบับนี้ ได้ทำการออกแบบรหัสแอลดีพีซีชนิดอาร์เรย์ที่อัตรารหัสสูงสำหรับการประยุกต์ใช้งานในระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยจะเน้นรหัสแอลดีพีซีแบบมีโครงสร้างที่เมตริกส์แพริตี้เช็คเป็นแบบอาร์เรย์ และจำลองสมรรถนะของรหัสแอลดีพีซีแบบอาร์เรย์ที่ได้ออกแบบไว้โดยใช้คอมพิวเตอร์ในการจำลองระบบด้วยโปรแกรม MATLAB ผลที่ได้แสดงสมรรถนะของอัตราความผิดพลาดบิต ของข้อมูลบนช่องสัญญาณรบกวนเกาส์แบบขาวเปรียบเทียบกับหลักการเดิม

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ สมมติฐานของการศึกษา ทฤษฎีที่ใช้ ขอบเขตของการวิจัย และขั้นตอนการศึกษา

บทที่ 2 การเข้ารหัสช่องสัญญาณแบบรหัสบล็อกเชิงเส้น

บทที่ 3 กล่าวถึงการเข้ารหัสและการถอดรหัสแอลดีพีซี และการออกแบบรหัสแอลดีพีซีชนิดอาร์เรย์ที่อัตรารหัสสูงที่เหมาะสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

บทที่ 4 กล่าวถึงการหาค่าสมรรถนะของระบบ พารามิเตอร์ที่ใช้และผลที่ได้จากการจำลองระบบ เพื่อแสดงให้เห็นว่าวิธีการที่นำเสนอนั้นสามารถที่ช่วยให้ระบบมีสมรรถนะที่ดีขึ้น

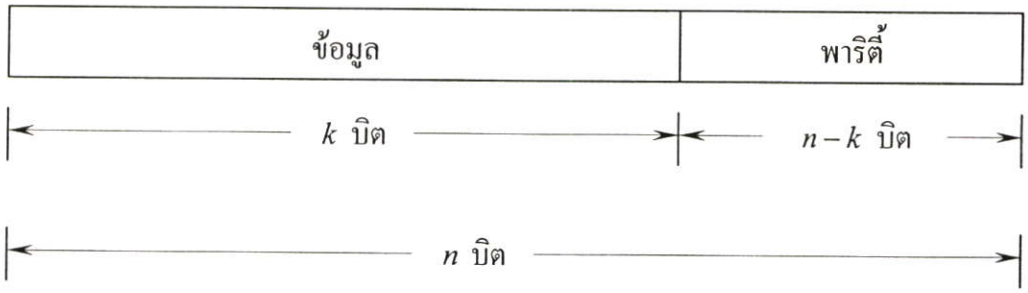
บทที่ 5 เป็นบทสรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2
การเข้ารหัสช่องสัญญาณแบบรหัสบล็อกเชิงเส้น

ในหัวข้อนี้จะกล่าวถึงทฤษฎีพื้นฐานและหลักการทำงานสำหรับการเข้ารหัสช่องสัญญาณ (Channel Coding) ที่เรียกว่ารหัสแก้ไขความผิดพลาด หรือ ECC (Error Correcting Code) แบบรหัสบล็อกเชิงเส้น (Linear Block Codes) ซึ่งเป็นเทคนิคที่สำคัญอย่างหนึ่งที่ใช้ในระบบสื่อสารแบบดิจิตอลซึ่งจะช่วยให้ภาครับสามารถที่จะตรวจจับความผิดพลาด และสามารถแก้ไขบิต หรือสัญลักษณ์ที่ผิดพลาด (error correction) ของข้อมูลได้ด้วย เพื่อให้อัตราบิตผิดพลาดในระบบลดต่ำลง จากนั้นจะแสดงสมรรถนะของระบบที่มีการเข้ารหัสช่องสัญญาณเปรียบเทียบกับระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ ซึ่งเนื้อหาทั้งหมดนี้จะเป็นพื้นฐานในการศึกษาการทำงานของรหัสแอลดีพีซีต่อไป (รายละเอียดของรหัสแอลดีพีซีจะกล่าวโดยละเอียดอีกครั้งในบทที่ 3)

2.1 รหัสบล็อกเชิงเส้น (Linear block codes)

รหัสบล็อกเชิงเส้น $C(n,k,d_{min})$ คือรหัสช่องสัญญาณที่แปลงข้อมูลขนาด k บิตให้เป็นคำรหัสขนาด n บิตโดยมีระยะห่างต่ำสุดระหว่างคำรหัสเท่ากับ d_{min} ให้ข้อมูลขนาดความยาว k บิตแสดงอยู่ในรูปของเวกเตอร์ $\mathbf{m}=[m_1\ m_2\ m_3 \ldots m_k]$ ตัวเข้ารหัสบล็อกเชิงเส้นจะทำการสร้างคำรหัสขนาด n บิตที่แสดงอยู่ในรูปของเวกเตอร์ $\mathbf{C}=[c_1\ c_2\ c_3 \ldots c_n]$ ดังแสดงในรูปที่ 2.1



รูปที่ 2.1 โครงสร้างของรหัสบล็อกเชิงเส้น

โดยบิตจำนวน $n-k$ บิตที่เพิ่มขึ้นมาเรียกว่าบิตพิเศษ หรือบิตพาริตี้ (parity bits) ซึ่งจะช่วยให้ภาครับสามารถที่จะตรวจจับความผิดพลาดได้ หรือหากเพิ่มจำนวนบิตเข้าไปในจำนวนที่มากพอภาครับก็อาจจะสามารถแก้ไขความผิดพลาด (error correction) ของข้อมูลได้ด้วย รหัสบล็อกเชิงเส้นจะทำการเข้า-ถอดรหัสที่ละบล็อก โดยที่ขนาดของบล็อกข้อมูลจะขึ้นอยู่กับระบบสื่อสารที่ใช้อยู่ และอัตราส่วนของจำนวนบิตข้อมูลต่อจำนวนบิตของคำรหัสเรียกว่าอัตรารหัส (code rate) R

หรือ

$$R = \frac{k}{n} \tag{2.1}$$

โดยอัตรารหัสจะมีค่า $0 < R \leq 1$ ในกรณีที่ไม่มีการเข้ารหัสจะได้ $R = 1$ อัตรารหัสบ่งบอกถึงประสิทธิภาพของรหัส ยิ่งค่า R มากขึ้นก็ให้รหัสที่มีประสิทธิภาพที่สูงขึ้น ตารางด้านล่างแสดงตัวอย่างของรหัสบล็อกเชิงเส้นที่มีค่า $k = 3$, $n = 6$ และ $R = 1/2$

ตารางที่ 2.1 รหัสบล็อกที่มี $k = 3$, $n = 6$ และ $R = 1/2$

$\mathbf{m} = [m_1\ m_2\ m_3]$	$\mathbf{C} = [c_1\ c_2\ c_3\ c_4\ c_5\ c_6]$
0 0 0	0 0 0 0 0 0
1 0 0	1 0 0 1 0 0
0 1 0	0 1 1 0 1 0
1 1 0	1 0 1 1 1 0
0 0 1	1 0 1 0 0 1
1 0 1	0 1 1 1 0 1
1 1 0	1 1 0 0 1 1
1 1 1	0 0 0 1 1 1

ให้คำรหัส $\mathbf{C} = [c_1\ c_2\ c_3 \ldots c_n]$ เราสามารถนิยาม น้ำหนักแฮมมิ่ง (Hamming weight) หรือ w_H ของคำรหัส $\mathbf{C}$ จาก

$$w_H(\mathbf{C}) = \text{จำนวนบิตในคำรหัส } \mathbf{C} \text{ ที่มีค่าเท่ากับ } 1$$

ยกตัวอย่างเช่น w_H ([1 0 0 1 0 0]) = 2 เป็นต้น และนิยาม ระยะห่างแฮมมิ่ง (Hamming distance) ระหว่าง $\mathbf{C}_1$ และ $\mathbf{C}_2$ หรือ $d_H(\mathbf{C}_1, \mathbf{C}_2)$ ได้ในรูป

$$\begin{aligned} d_H(\mathbf{C}_1, \mathbf{C}_2) &= \sum_{i=1}^{n} (c_{1,i} \neq c_{2,i}) \\ &= \sum_{i=1}^{n} ((c_{1,i} - c_{2,i}) \neq 0) \\ &= w_H(\mathbf{C}_1 - \mathbf{C}_2) \end{aligned} \tag{2.2}$$

รหัสที่แสดงในตารางที่ 2.1 มีระยะห่างแฮมมิ่ง d_H ([1 1 0 0 1 1], [0 0 0 1 1 1]) = 3 ให้รหัส $\mathbf{C}$ มี มีคำรหัสทั้งหมด 2^k คำรหัส ระยะห่างแฮมมิงระหว่างคำรหัสที่ต่ำสุดเรียกว่า ระยะห่างต่ำสุดของรหัส (minimum distance) หรือ d_{min} กล่าวคือ

$$d_{min} = \min_{i \neq j} \{ d_H(\mathbf{C}_i, \mathbf{C}_j) \} \tag{2.3}$$

โดย $i, j = 1, 2, \ldots 2^k$ รหัสในตารางที่ 2.1 มี $d_{min} = 3$ จำนวนบิตที่รหัสสามารถแก้ความผิดพลาด t หาได้จาก

$$t = \frac{|d_{min} - 1|}{2} \tag{2.4}$$

และจำนวนบิตที่รหัสสามารถตรวจจับบิตผิดพลาด e หาได้จาก

$$e = d_{min} - 1 \tag{2.5}$$

รหัสข้างต้นสามารถแก้บิตผิดพลาด $t = 1$ บิต และตรวจจับบิตผิดพลาด $e = 2$ บิต สังเกตได้ว่า จำนวนอินพุตเท่ากับ 2^k และจำนวนคำรหัสเท่ากับ 2^k เช่นกัน ในการใช้งานจริงขนาดของอินพุต k มีค่าสูง ให้จำนวนคำรหัสจำนวนมาก ทำให้การเข้ารหัสโดยดูจากตารางไม่เหมาะสม เช่น $k = 1024$ ให้จำนวนคำรหัสเท่ากับ 2^{1024} คำ

2.2 เมตริกส์กำเนิด (Generator matrix)

ให้อินพุต $\mathbf{m} = [m_1\ m_2\ m_3 \ldots m_k]$ มีมิติ $1 \times k$ รหัสบล็อกเชิงเส้น (n, k, d_{min}) สร้างโดยการคูณอินพุตกับเมตริกส์กำเนิด $\mathbf{G}$ มีมิติ $k \times n$ ที่อยู่ในรูป

$$\mathbf{G} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1,(n-k)} & 1 & 0 & \cdots & 0 \\ p_{21} & p_{22} & \cdots & p_{2,(n-k)} & 0 & 1 & \cdots & 0 \\ \cdots & & \cdots & & & & \cdots & \\ p_{k,1} & p_{k,2} & \cdots & p_{k,(n-k)} & 0 & 0 & \cdots & 1 \end{bmatrix}_{(k \times n)} \tag{2.6}$$

จากสมการที่ 2.6 สามารถเขียนอยู่ในรูปเมตริกส์พาริตี้ $\mathbf{P}$ และเมตริกส์เอกลักษณ์ $\mathbf{I}$ ได้ดังสมการที่ 2.7

$$\mathbf{G} = [\mathbf{P}\ \mathbf{I}_k]_{(k \times n)} \tag{2.7}$$

และคำรหัส $\mathbf{C} = [c_1\ c_2\ c_3 \ldots c_n]$ มีมิติ $1 \times n$ หาได้จาก

$$\begin{aligned} \mathbf{C} &= \mathbf{mG} \\ &= [p_1\ p_2\ p_3 \cdots p_{n-k}\ m_1\ m_2\ m_3 \ldots m_k]_{(1 \times n)} \end{aligned} \tag{2.8}$$

รหัสที่คำรหัสมีข้อมูล **m** อยู่ในคำรหัส จัดอยู่ในประเภทรหัสเชิงระบบ (Systematic code) ข้อดีคือหลังจากการถอดรหัส สามารถนำข้อมูลเดิมคืนมาได้อย่างง่ายดาย รหัสในตารางที่ 2.1 ข้างต้นมีเมตริกส์กำเนิด ได้แก่

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{(3\,x\,6)} \tag{2.9}$$

จากสมการที่ 2.8 สามารถสร้างสมการคำรหัสได้ดังนี้

$$\mathbf{C} = [m_1 \;\; m_2 \;\; m_3] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= [m_1 + m_3 \;\; m_1 + m_2 \;\; m_2 + m_3 \;\; m_1 \;\; m_2 \;\; m_3]$$

โดยการบวกข้างต้นเป็นการบวกแบบมอดูโล-2 หรือการทำ XOR

2.3 เมตริกส์พาริตี้เช็ค (Parity-check matrix)

ให้เมตริกส์กำเนิด **G** ที่มีมิติ $k\,x\,n$ สามารถหาเมตริกส์พาริตี้เช็ค **H** ที่มีมิติ $(n-k)x\,n$ โดยแถวของเมตริกส์กำเนิด **G** ตั้งฉากกับหลักของเมตริกส์พาริตี้เช็ค **H** เสมอ และให้

$$\mathbf{G}\mathbf{H}^T = \mathbf{0}_{k\,x\,(n-k)} \tag{2.10}$$

โดยแต่ละหลักของเมตริกส์พาริตี้เช็ค **H** ต้องไม่เหมือนกัน ให้เมตริกส์กำเนิด **G** สามารถหาพาริตี้เช็ค **H** ได้จาก

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \;\; \mathbf{P}^T\right] \tag{2.11}$$

ทำการแทนค่าสมการที่ 2.7 และ 2.11 ลงในสมการที่ 2.10

$$\mathbf{G}\mathbf{H}^T = [\mathbf{P} \;\; \mathbf{I}_k] \begin{bmatrix} \mathbf{I}_{n-k} \\ \mathbf{P} \end{bmatrix} = \mathbf{P} + \mathbf{P} = \mathbf{0} \tag{2.12}$$

ระยะห่างต่ำสุดได้ d_{min} ของรหัสสามารถหาได้สองวิธี ได้แก่

1. น้ำหนักต่ำสุดของแถวของเมตริกส์ **G**
2. จำนวนหลักจำนวนน้อยที่สุดที่บวกกันได้ศูนย์ของเมตริกส์ **H**

2.4 การถอดรหัสบล็อกเชิงเส้น

ให้ลำดับสัญญาณที่ได้รับ $\mathbf{r} = \mathbf{C} + \mathbf{e}$ โดยที่ $\mathbf{e} = [e_1\ e_2\ e_3 \ldots e_n]$ คือเวกเตอร์ความผิดพลาดโดย $e_1 = 1$ ทำให้บิต i ของคำรหัสเป็นบิตที่ผิดพลาด

การถอดรหัสด้วยซินโดรม (Syndrome decoding)

การถอดรหัสด้วยซินโดรมจัดเป็นการถอดรหัสแบบฮาร์ดประเภทหนึ่ง โดยทำการตัดสินใจให้สัญญาณที่ได้รับอยู่ในรูปบิต และ ก่อนการถอดรหัส ซินโดรม $\mathbf{S}$ ลำดับสัญญาณที่ได้รับ $\mathbf{r}$ หาได้จาก

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T = (\mathbf{C}+\mathbf{e})\mathbf{H}^T = \mathbf{C}\mathbf{H}^T + \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T \qquad (2.13)$$

ดังนั้นเวกเตอร์หรือลำดับความผิดพลาดที่แตกต่างกันจะให้ซินโดรมที่แตกต่างกัน

ลำดับขั้นในการถอดรหัสด้วยซินโดรม

1. สร้างตารางแพทเทิร์นของบิตผิดพลาดตามความสามารถในการแก้ไขบิตผิดพลาดของรหัสและซินโดรมที่เกี่ยวข้อง
2. คำนวณซินโดรมสำหรับลำดับสัญญาณที่ได้รับ $\mathbf{r}$ โดยคำนวณ $\mathbf{S} = \mathbf{r}\mathbf{H}^T$
3. ค้นหาแพทเทิร์นของบิตผิดพลาดที่มีซินโดรมจากข้อ 2 ให้เป็น $\mathbf{e}$
4. แก้ไขบิตผิดพลาดโดยการบวกสัญญาณที่ได้รับ $\mathbf{r}$ กับ $\mathbf{e}$ ได้คำรหัสที่ทำการทำนาย $\hat{\mathbf{C}} = \mathbf{r} + \mathbf{e}$

ตัวอย่างการการถอดรหัสด้วยวิธีซินโดรม

จากตารางที่ 2.1 รหัสบล็อกเชิงเส้นจะได้รหัส (6, 3, 3) ถ้าให้สัญญาณที่ได้รับ $\mathbf{r}$ = [001110] จากลำดับขั้นในการถอดรหัสด้วยซินโดรม

1. เนื่องจากรหัสชุดนี้สามารถแก้บิตผิดพลาดได้เพียง 1 บิตสามารถสร้างตารางแพทเทิร์นของบิตผิดพลาดได้โดย

ตารางที่ 2.2 ตารางแพทเทิร์นของบิตผิดพลาด

e	S
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100
010001	111

2. คำนวณซินโดรมสำหรับลำดับสัญญาณที่ได้รับ $\mathbf{r}$ ด้วยสมการ $\mathbf{S} = \mathbf{r}\mathbf{H}^T$

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T = [0\,0\,0\,1\,1\,1\,0]\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix} = [1\,0\,0]$$

3. เมื่อพิจารณาตารางแพทเทิร์นของบิตผิดพลาดในข้อ 1 ได้ $\mathbf{e} = [1\,0\,0\,0\,0\,0]$

4. ความน่าจะเป็นของคำรหัสที่ได้รับคือ $\hat{\mathbf{C}} = \mathbf{r} + \mathbf{e} = [1\,0\,1\,1\,1\,0]$

2.5 อัตราส่วนต่อสัญญาณสัญญาณรบกวน ของสัญลักษณ์รหัส

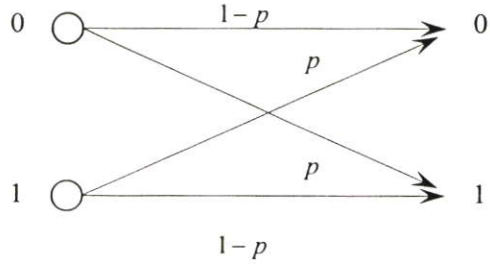
ให้ E_c เป็นพลังงานเฉลี่ยของบิตรหัส E_b เป็นพลังงานเฉลี่ยของบิตข้อมูล อัตราส่วนต่อสัญญาณสัญญาณรบกวน ของรหัสเขียนได้ดังนี้

$$\frac{E_c}{N_o} = R\frac{E_b}{N_o} \tag{2.14}$$

ดังนั้นอัตราส่วนต่อสัญญาณสัญญาณรบกวน สำหรับบิตข้อมูลคือ

$$\frac{E_b}{N_o} = \frac{1}{R}\cdot\frac{E_c}{N_o} \tag{2.15}$$

โดย R คืออัตรารหัส พิจารณาช่องสัญญาณสมมาตรไบนารี (Binary symmetric channel) ที่มีความน่าจะเป็นของบิตผิดพลาด $p = P(0|1) = P(1|0)$ และความน่าจะเป็นของบิตถูกต้อง $P(0|0) = P(1|1) = 1-p$ ดังแสดงในรูปที่ 2.2



รูปที่ 2.2 ช่องสัญญาณสมมาตรไบนารี

ในระบบบีพีเอสเค อัตราบิตผิดพลาดจากช่องสัญญาณ p คือ

$$p = Q\left(\sqrt{\frac{2E_b}{N_o}}\right) \tag{2.16}$$

เมื่อมีการเข้ารหัส อัตราบิตผิดพลาดจากช่องสัญญาณคือ

$$p = Q\left(\sqrt{\frac{2E_c}{N_o}}\right) \tag{2.17}$$

อัตราบิตผิดพลาดเฉลี่ยหลังจากที่มีการถอดรหัสต้องคำนวณในระดับบล็อก กล่าวคือจำนวนบิตผิดพลาดน้อยกว่าหรือเท่ากับ t จะถูกแก้ไขหลังจากการถอดรหัส ความน่าจะเป็นของบิตผิดพลาดเท่ากับ j จาก n บิต $P(n, j)$ คือ

$$P(n,j) = \binom{n}{j} p^j (1-p)^{n-1} \tag{2.18}$$

ดังนั้นอัตราบิตผิดพลาดเฉลี่ยหาได้จากความน่าจะเป็นของจำนวนบิตผิดพลาดมากกว่า t

$$P_B \approx \frac{1}{n} \sum_{j=t+1}^{n} j\binom{n}{j} p^j (1-p)^{n-j} \tag{2.19}$$

2.6 อัตราขยายการเข้ารหัส (Coding gain)

อัตราขยายการเข้ารหัส G หาได้จาก ผลต่างระหว่างอัตราส่วนต่อสัญญาณสัญญาณรบกวนของกรณีที่ไม่มีการเข้ารหัสและกรณีที่มีการเข้ารหัส ณ ระดับความน่าจะเป็นบิตผิดพลาดของระบบที่สนใจอัตราขยายการเข้ารหัส

$$G = \left(\frac{E_b}{N_0}\right)_u (dB) - \left(\frac{E_b}{N_0}\right)_c (dB) \tag{2.20}$$

โดย $\left(\frac{E_b}{N_0}\right)_u$ คืออัตราส่วนต่อสัญญาณสัญญาณรบกวน ในกรณีที่ไม่มีการเข้ารหัส และ $\left(\frac{E_b}{N_0}\right)_c$ คืออัตราส่วนต่อสัญญาณสัญญาณรบกวน ในกรณีที่มีการเข้ารหัส

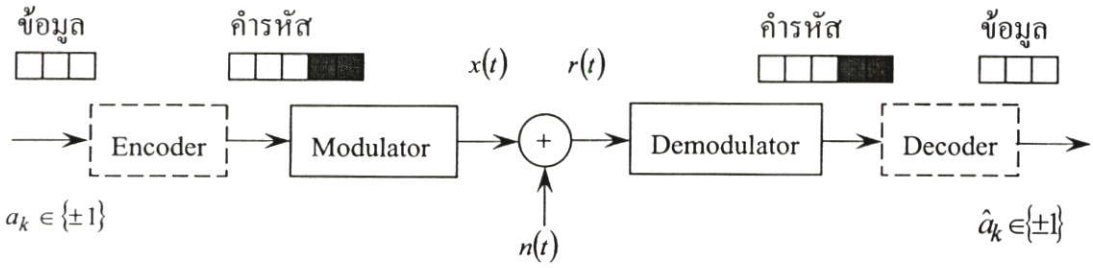
การตรวจเช็คสมรรถนะของระบบที่มีการเข้ารหัสช่องสัญญาณว่าอัตราความผิดพลาดบิตลดลงเท่าไรจากการเข้ารหัสช่องสัญญาณ หรือที่อัตราความผิดพลาดบิตที่ต้องการนั้นอัตราส่วน

ต่อสัญญาณสัญญาณรบกวน ลดลงอย่างไรสามารถตรวจสอบได้จาก Curve ที่เรียกว่า Waterfall ซึ่งอัตราขยายการเข้ารหัสที่ได้มีสอง

ประเภทคือ

1. อัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสในรอบที่ หนึ่ง
2. อัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสที่มีการวนลูป หรือที่เรียกว่า Iteration

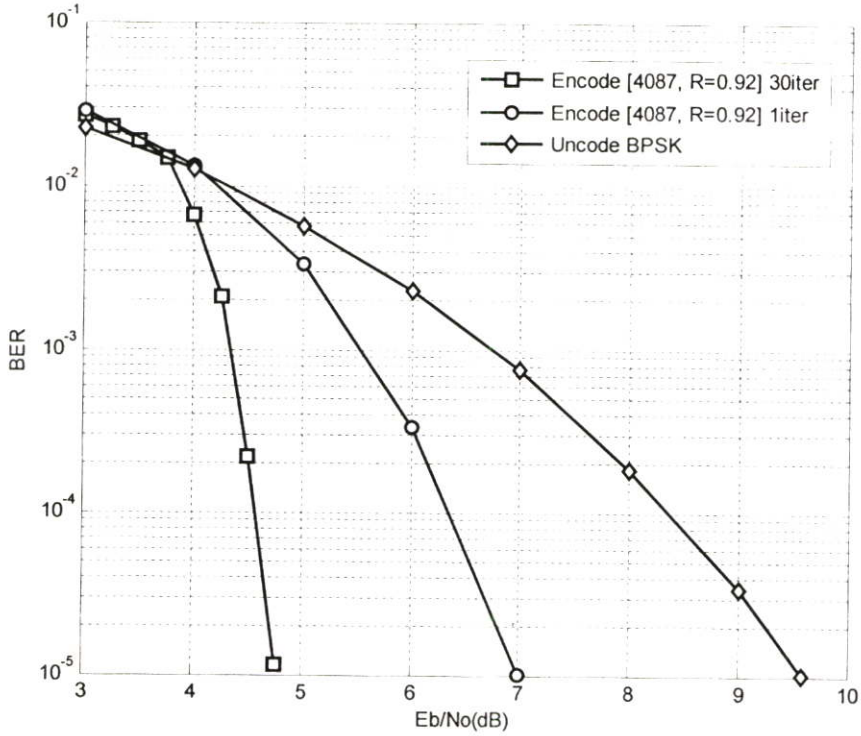
รหัสที่มีการวนลูป หรือ Iteration นั้นถูกสร้างขึ้นครั้งแรกในปี ค.ศ. 1993 (2536) ซึ่งก็คือรหัสเทอร์โบ (Turbo codes) [1] โดยมีสมรรถนะการทำงานที่เข้าใกล้ลิมิตของแชนนอน ทำให้ได้รับความสนใจเป็นอย่างมาก และหลังจากนั้นการถอดรหัสที่มีการวนลูปก็ได้รับความสนใจอย่างแพร่หลายเป็นอย่างมากในการนำไปใช้งานเป็น รหัสแก้ไขความผิดพลาด การทำงานร่วมกับตัวปรับเท่าทางความถี่ หรือที่เรียกว่า Turbo Equalization รวมถึงระบบการกู้คืนสัญญาณเวลา (Timing Recovery) ที่ทำหน้าที่ในการเข้าจังหวะ (synchronize) วงจรชักตัวอย่างกับสัญญาณแอนะลอก ฯลฯ นอกจากนี้เทคนิคการถอดรหัสที่มีการวนลูป ยังได้ถูกนำไปใช้งานสำหรับระบบเครือข่าย ระบบสื่อสารในอวกาศ (deep space network) และระบบโทรศัพท์เคลื่อนที่ตามมาตรฐาน IMT-2000 (W-CDMA) ในปัจจุบันรหัสที่ใช้เทคนิคการถอดรหัสแบบวนลูป กำลังได้รับความสนใจในการนำมาประยุกต์ใช้กับระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยรหัสที่กำลังได้รับความสนใจในการนำมาใช้งานเป็นรหัสแก้ไขความผิดพลาดแทนที่รหัสแก้ไขความผิดพลาดเดิมสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก คือรหัสบล็อกเชิงเส้นเชิงเส้นชนิดหนึ่งที่เรียกว่ารหัสแอลดีพีซี เพื่อเปรียบเทียบสมรรถนะของระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ กับระบบที่มีการเข้ารหัสช่องสัญญาณว่าอัตราขยายการเข้ารหัสสูงขึ้นอย่างไร พิจารณาตัวอย่างระบบระบบสื่อสารแบบดิจิตอลที่มีอินพุตเป็น ±1 และช่องสัญญาณเป็นแบบอุดมคติมีเพียงสัญญาณรบกวนเกาส์แบบขาวที่มีการเข้ารหัสช่องสัญญาณและทำการมอดูเลตแบบ BPSK แสดงดังรูปที่ 2.4



รูปที่ 2.3 แบบจำลองของระบบสื่อสารแบบดิจิตอลที่มีการเข้ารหัสช่องสัญญาณ

รหัสช่องสัญญาณที่ใช้คือรหัสแอลดีพีซี ความยาวคำรหัสที่ใช้ในการจำลองการทำงานคือ 4087 บิต อัตรารหัสที่ใช้คือ 0.92 การถอดรหัสเป็นแบบไม่วนลูป และวนลูป เอสเอ็นอาร์สำหรับบิต

ข้อมูลคือ $\frac{E_b}{N_o} = \frac{1}{R} \cdot \frac{E_c}{N_o}$ เมื่อ E_c เป็นพลังงานเฉลี่ยของบิตรหัส E_b คือ พลังงานเฉลี่ยของบิตข้อมูลอัตราบิตความผิดพลาดบิตถูกคำนวณจนกว่าจะได้บิตผิดพลาดรวมเท่ากับ 1000 ในคำรหัสพิจารณา Waterfall ในรูปที่ 2.4 ซึ่งเป็นการแสดงสมรรถนะอัตราความผิดพลาดบิตข้อมูลของระบบสื่อสารแบบดิจิตอลดังรูปที่ 2.3



รูปที่ 2.4 สมรรถนะอัตราความผิดพลาดบิตของระบบที่มีการเข้ารหัสช่องสัญญาณกับระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ ที่มีการมอดูเลตแบบ BPSK

เมื่อพิจารณาอัตราความผิดพลาดบิตข้อมูลที่ 10^{-5} อัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสในรอบที่หนึ่งพบว่าอัตราส่วนต่อสัญญาณสัญญาณรบกวน ลดลงประมาณ 2.6 dB เมื่อเปรียบเทียบกับระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ (Un-code BPSK) และเมื่อพิจารณาอัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสที่มีการวนลูป หรือที่เรียกว่า Iteration อัตราส่วนต่อสัญญาณสัญญาณรบกวน ลดลงประมาณ 5.7 dB เมื่อเปรียบเทียบกับระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ อีกทั้งเมื่อพิจารณาอัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสที่มีการวนลูปจะต่ำกว่าอัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสในรอบที่หนึ่ง ถึงประมาณ 2.2 dB

จากรูปที่ 2.4 แสดงให้เห็นว่า ระบบที่มีการเข้ารหัสช่องสัญญาณมีอัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสในรอบที่หนึ่งสูงกว่าระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ และยังสามารถเพิ่มอัตราขยายการเข้ารหัสให้สูงขึ้นได้อีกโดยอาศัยเทคนิคการถอดรหัสที่มีการวนลูป

จากบทที่ 1 กล่าวถึงปัญหาของระบบสื่อสารที่ถูกผลกระทบของสัญญาณรบกวนจากภายนอกในรูปแบบต่างๆ ซึ่งจะส่งผลให้สมรรถนะของสัญญาณที่ภาครับหรือข้อมูลที่ภาครับมีความผิดพลาดเกิดขึ้น เมื่อต้องการเพิ่มสมรรถนะที่ดีของสัญญาณที่ภาครับให้อัตราความผิดพลาดบิตน้อยลงและอยู่ในระดับที่ยอมรับได้ เทคนิควิธีการหนึ่งที่เรียกว่าการเข้ารหัสช่องสัญญาณ โดยการเพิ่มบิตพาริตี้เข้ามาจะช่วยให้ภาครับสามารถที่จะตรวจจับความผิดพลาดรวมถึงสามารถแก้ไขความผิดพลาดของข้อมูลได้ด้วย จากนั้นในบทที่ 2 ได้กล่าวถึงทฤษฎีพื้นฐาน และหลักการทำงานสำหรับการเข้ารหัสช่องสัญญาณแบบรหัสบล็อกเชิงเส้น (Linear Block Codes) รวมถึงแสดงสมรรถนะของระบบที่มีการเข้ารหัสช่องสัญญาณว่า ที่อัตราความผิดพลาดบิตที่ต้องการนั้นอัตราส่วนต่อสัญญาณสัญญาณรบกวน ลดลงเมื่อเทียบกับระบบที่ไม่มีการเข้ารหัสช่องสัญญาณ รวมถึงอัตราขยายการเข้ารหัสที่ได้จากการถอดรหัสแบบวนลูปยังให้สมรรถนะที่ดีขึ้นเมื่อเทียบกับการเข้ารหัสช่องสัญญาณที่ไม่มีการวนลูป ในบทที่ 3 จะกล่าวถึงการเข้ารหัสและการถอดรหัสแอลดีพีซี ซึ่งเป็นรหัสบล็อกเชิงเส้นชนิดหนึ่งที่มีการถอดรหัสแบบวนลูป

บทที่ 3
การเข้ารหัสและถอดรหัสแอลดีพีซี

บทที่ 3 จะกล่าวถึงประวัติความเป็นมาของรหัสแอลดีพีซี หลักการทำงานสำหรับการเข้าเข้ารหัสและการถอดรหัสแอลดีพีซีที่ใช้การสุ่มข้อมูล "0" และ "1" หนึ่ง ขึ้นมาเพื่อใช้ในการสร้างเมตริกส์พาริตี้เช็คทำให้เมตริกส์พาริตี้เช็คที่ได้มีโครงสร้างแบบสุ่ม (random parity check matrix) มาใช้ในการสร้างคำรหัส จากนั้นจะกล่าวถึงรหัสแอลดีพีซีที่ใช้การเข้ารหัสด้วยเมตริกส์พาริตี้เช็คแบบมีโครงสร้าง (structure parity check matrix) ที่โครงสร้างเมตริกส์พาริตี้เช็คเป็นแบบอาร์เรย์ หรือที่เรียกว่ารหัสแอลดีพีซีแบบอาร์เรย์ ซึ่งถูกพัฒนาขึ้นมาเพื่อแก้ปัญหาความซับซ้อนในการสร้างเมตริกส์พาริตี้ของรหัสแอลดีพีซีที่มีโครงสร้างของเมตริกส์พาริตี้เป็นแบบสุ่ม เพื่อเพิ่มสมรรถนะของอัตราความผิดพลาดบิตของข้อมูลที่ภาครับให้สูงขึ้น จะนำเสนอรหัสแอลดีพีซีแบบอาร์เรย์ที่มีการสลับบิตของข้อมูลในเมตริกส์พาริตี้เช็ค ซึ่งเป็นหลักการใหม่ที่นำเสนอในวิทยานิพนธ์นี้เพื่อเป็นพื้นฐานในการออกแบบรหัสแอลดีพีซีชนิดอาร์เรย์ที่มีอัตรารหัสสูง ซึ่งเหมาะสำหรับระบบบันทึกข้อมูลข้อมูลเชิงแม่เหล็ก

3.1 รหัสแอลดีพีซี

รหัสแอลดีพีซี หรือชื่อในภาษาอังกฤษว่า Low Density Parity Check (LDPC) Codes คือรหัสที่มีจำนวนของเลขหนึ่งน้อยเมื่อเทียบกับขนาดของเมตริกส์พาริตี้เช็คทั้งนี้ก็เพื่อให้มีระยะห่างต่ำสุดของรหัส หรือ d_{min} (minimum distance) สูง ได้ถูกสร้างขึ้นครั้งแรกในปี ค.ศ.1960 (2503) ในวิทยานิพนธ์ระดับปริญญาเอกของ R.Gallager ที่ Massachusetts Institute of Technology (MIT) [5] ประเทศสหรัฐอเมริกา โดยจัดเป็นรหัสช่องสัญญาณแบบบล็อกเชิงเส้นชนิดหนึ่งที่การเข้ารหัสจะดำเนินการผ่านเมตริกส์พาริตี้เช็ค $\mathbf{H}$ ที่มีโครงสร้างแบบสุ่ม แต่รหัสแอลดีพีซียังไม่เป็นที่สนใจมากนักในขณะนั้น ในปี ค.ศ.1981(2524) R.M.Tanner [6] ได้นำเสนอการใช้กราฟแสดงความสัมพันธ์ที่เกิดจากการเข้ารหัสที่ชื่อว่า Tanner Graph หรือ Bipartite Graph ซึ่งทำให้สามารถนำภาพที่ได้มาช่วยในการออกแบบการถอดรหัสได้ง่ายขึ้น จนกระทั่งในปี ค.ศ.1990(2533) D.J.C. Mackay [2] ได้แสดงผลงานวิจัยที่พบว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานที่เข้าใกล้ลิมิตของแชนนอลได้เช่นเดียวกับรหัสเทอร์โบ ทำให้หลังจากนั้นรหัสแอลดีพีซีจึงได้รับความสนใจอย่างแพร่หลาย

รหัสแอลดีพีซีสามารถแบ่งออกเป็นสองประเภทหลักคือ รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งในเมตริกส์พาริตี้เช็คเป็นแบบคงที่ (Regular LDPC codes) ซึ่งเป็นรหัสที่มีรูปแบบเดียวกับรหัสของ R.Gallager และรหัสแอลดีพีซีอีกชนิดหนึ่งที่มีการกระจายตัวของเลขหนึ่งเป็น

แบบไม่คงที่ (Irregular Regular LDPC codes) ซึ่งเป็นรหัสที่พัฒนามาจาก Regular LDPC codes การเข้ารหัสจะเริ่มต้นจากการสร้างเมตริกส์พาริตี้เช็ค **H** ในหัวข้อถัดไปจึงจะอธิบายถึงโครงสร้างของเมตริกส์ **H** จากนั้นจะกล่าวถึงขั้นตอนและวิธีการถอดรหัสแอลดีพีซี

3.1.1 รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งเป็นแบบคงที่ (Regular LDPC codes)

รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งเป็นแบบคงที่ (Regular LDPC codes) นั้นมีที่มา จากการที่จำนวนเลขหนึ่งในแต่ละแถว หรือแต่ละหลักของเมตริกส์พาริตี้เป็นค่าคงที่

นิยาม : Regular LDPC codes

รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งเป็นแบบคงที่ $C(n, W_r, W_c)$ นิยามโดยเมตริกส์พาริตี้เช็คขนาด $m \times n$ เมื่อ

1) $\mathbf{H}_{m\times n}$ ที่สร้างขึ้นเกิดจากการการสุ่มข้อมูลศูนย์ หนึ่ง
2) W_c คือ จำนวนเลขหนึ่งในหลักของเมตริกส์พาริตี้เช็ค โดยที่ $W_c << m$
3) W_r คือ จำนวนเลขหนึ่งในแถวของเมตริกส์พาริตี้เช็ค และ $W_r = W_c(n/k)$, $W_r << n$
4) **H** ที่สร้างขึ้นจะต้องปราศจากไซเคิลขนาดเท่ากับ 4
5) อัตรารหัส $R = 1-(W_c / W_r)$

ค่าความหนาแน่นของเลขหนึ่ง $\rho = (W_r / n) = (W_c / m)$ ทำให้ $m = (W_c / W_r) \cdot n$ และ $\lim_{n\to\infty} \rho = 0$ รหัสนี้มีความยาวข้อมูลอินพุตเท่ากับ $n-m$ บิต ความยาวคำรหัสเท่ากับ n และจำนวนพาริตี้เช็คเท่ากับ m บิต

พิจารณา Regular LDPC ขนาด (10, 5) ซึ่งมีค่า W_c = 2 และ $W_r = W_c(n/k)$ = 2 x (10/5) = 4 เมตริกส์ **H** ที่ได้คือ

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{(m=5, n=10)} \tag{3.1}$$

ตัวอย่างเมตริกส์พาริตี้เช็คที่ได้ในสมการที่ 3.1 นั้นสอดคล้องกับเงื่อนไขทั้ง 4 ข้อ กล่าวคือ $W_c = 2$ W_r = 4 รวมถึงปราศจากไซเคิลขนาดเท่ากับ 4 และเพื่อความเข้าใจคุณสมบัติของไซเคิลขนาดเท่ากับ 4 พิจารณานิยามของไซเคิลของรหัสแอลดีพีซี

นิยามของไซเคิลขนาดเท่ากับ 4

เมตริกส์พาริตี้เช็คใด ๆ จะมีไซเคิลขนาดเท่ากับ 4 เมื่อตำแหน่งของเลข 1 ใน **H** เกิดลูปปิดตามสมการที่ 3.2

$$(A_{i,j}),(A_{i,b}),(A_{a,b}),(A_{a,j}) \tag{3.2}$$

เมื่อ A เป็นเมื่อตำแหน่งของเลข 1 ใน **H** และค่าคงที่ i, j, a, b เป็นค่าของแถว และหลักของ **H** โดยที่ $i, a \le m$ และ $j, b \le n$ หรืออาจกล่าวได้ว่าไซเคิลขนาดเท่ากับ 4 ใน เมตริกส์พาริตี้เช็ค คือ ลูปปิดของเลขหนึ่งที่มีการใช้แถว และหลักร่วมกันเท่ากับ 2 แถว และ 2 หลัก

พิจารณา Regular LDPC ขนาด (10, 5) ซึ่งมีค่า W_c = 2 และ $W_r = W_c(n/k)$ = 4 และมีไซเคิลขนาดเท่ากับ 4

$$\mathbf{H} = \begin{bmatrix} \tilde{1} & 1 & 1 & \tilde{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \hat{1} & \hat{1} & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & \hat{1} & \hat{1} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \tilde{1} & 0 & 0 & \tilde{1} & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{(m=5,n=10)} \tag{3.3}$$

จาก 3.5 จะพบว่าเกิดไซเคิลขนาดเท่ากับ 4 จำนวนถึง 2 ไซเคิล กล่าวคือ

ไซเคิลที่ 1: ตำแหน่งของ $\tilde{1}$ กับลูปปิด $(A_{1,1}),(A_{1,4}),(A_{5,4}),(A_{5,1})$

ไซเคิลที่ 2: ตำแหน่งของ $\hat{1}$ กับลูปปิด $(A_{2,5}),(A_{2,6}),(A_{3,6}),(A_{3,5})$

เหตุผลของไซเคิลขนาดเท่ากับ 4 ที่เป็นเรื่องต้องห้ามสำหรับรหัสแอลดีพีซีก็คือ อัลกอริทึมสำหรับการถอดรหัสนั้นจะอาศัยหลักการของความน่าจะเป็นในการส่งผ่านข้อมูล โดยที่ความน่าจะเป็นของแต่ละเหตุการณ์นั้นเป็นอิสระต่อกัน ซึ่งผลของการมีไซเคิลนี้จะทำให้ความน่าจะเป็นในการส่งผ่านข้อมูลนี้ไม่เป็นอิสระต่อกัน และจะส่งผลต่อสมรรถนะของการถอดรหัสเป็นอย่างมากผลกระทบของการมีไซเคิลขนาดเท่ากับ 4 นี้จะกล่าวโดยละเอียดอีกครั้งในเรื่องของการถอดรหัส

3.1.2 รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งเป็นแบบไม่คงที่ (Irregular LDPC Codes)

รหัสแอลดีพีซีที่มีการกระจายตัวของเลขหนึ่งเป็นแบบไม่คงที่ (Irregular LDPC codes) นั้นมีที่มาจากการที่จำนวนเลขหนึ่งในแต่ละแถว หรือแต่ละหลักของเมตริกส์พาริตี้เช็คมีจำนวนไม่คงที่ในทุกแถวหรือทุกหลักของเมตริกส์พาริตี้เช็ค Irregular LDPC ถูกพัฒนาขึ้นมาในปี ค.ศ.

2001(2544) โดย T.Richardson [7] และด้วยเหตุที่การกระจายตัวของเลขหนึ่งเป็นแบบไม่คงที่ค่าความหนาแน่นของเลขหนึ่ง ρ ที่นิยามไว้กับ Regular LDPC นั้นจึงเปลี่ยนไปดังนี้

นิยาม : Irregular LDPC codes คือรหัสแอลดีพีซีที่

1) ค่าความหนาแน่นของเลขหนึ่งของแต่ละแถวนิยามโดย $[\rho_2,\ \rho_3,\ldots,\ \rho_n]$

2) ค่าความหนาแน่นของเลขหนึ่งของแต่ละหลักนิยามโดย $[\lambda_2,\ \lambda_3,\ldots,\ \lambda_n]$

3) อัตรารหัส $R = 1-\left[\left(\sum_{j=2}^{n}\rho_j/j\right)/\left(\sum_{j=2}^{n}\lambda_j/j\right)\right]$

ด้วยวิธีการของ T.Richardson นั้นสมรรถนะการทำงานของ Irregular LDPC ดีกว่า Regular LDPC ของ D.J.C. Mackey แต่ก็มีหลายงานวิจัย [8-9] พบว่า Irregular LDPC ในแบบของ T.Richardson นั้นจะทำงานได้ดีสำหรับอัตรารหัส $R \le 3/4$ และที่ความยาวคำรหัส $n \ge 5000$

3.1.3 การเข้ารหัสแอลดีพีซี

หลังจากสร้างเมตริกส์พาริตี้เช็ค $\mathbf{H}$ แล้วจากนั้นอาศัยความสัมพันธ์ในการสมการที่ 3.4 ในการสร้างคำรหัส

$$\mathbf{C}_{(1\times n)}\mathbf{H}^{T}_{(n\times m)} = \mathbf{0}_{(1\times m)} \qquad (3.4)$$

เมื่อ $\mathbf{C} = [c_1\ c_1\ c_2\ c_2\ \ldots\ c_n]_{(1\times n)}$ เป็นเมตริกส์คำรหัสขนาด $(1\times n)$

$\mathbf{0}_{(1\times m)}$ เป็นเมตริกส์ศูนย์ขนาด $(1\times m)$

ในกรณีรหัสเชิงระบบ เมตริกส์ค่ารหัส $\mathbf{C}$ เขียนได้ในรูป

$$\mathbf{C} = [p_1\ p_1\ p_2\ \ldots\ p_{n-k}\ m_1\ m_2\ m_3\ \ldots\ m_k\ ]_{(1\times n)}$$

หรือ

$$\mathbf{C} = \left[\mathbf{p}_{(1\times n-k)}\,|\,\mathbf{m}_{(1\times k)}\right]_{(1\times n)} \qquad (3.5)$$

โดย

$\mathbf{p}_{(1\times n-k)}$ คือ เมตริกส์พาริตี้ขนาด $(1\times n-k)$ และ $\mathbf{m}_{(1\times k)}$ คือเมตริกส์ข้อมูลขนาด $(1\times k)$

เขียนเมตริกส์พาริตี้เช็ค $\mathbf{H}$ ในรูป

$$\mathbf{H} = [\mathbf{H}_1\,|\,\mathbf{H}_2]$$

$$\mathbf{H}^{T} = \begin{bmatrix}\mathbf{H}_1^{T}\\ \mathbf{H}_2^{T}\end{bmatrix} \qquad (3.6)$$

จากนั้นแทนค่าสมการ 3.5 และสมการ 3.6 ลงในสมการที่ 3.4

$$\mathbf{CH}^T = [\mathbf{p} \mid \mathbf{m}]\begin{bmatrix}\mathbf{H}_1^T \\ \mathbf{H}_2^T\end{bmatrix} = \mathbf{0}$$

$$\mathbf{CH}^T = \mathbf{mH}_1^{\mathbf{T}} + \mathbf{pH}_2^{\mathbf{T}} = \mathbf{0} \tag{3.7}$$

$$\mathbf{p} = \mathbf{mH}_1^{\mathbf{T}} + \left(\mathbf{H}_2^{\mathbf{T}}\right)^{-1} \tag{3.8}$$

เมตริกส์พาริตี้เช็ค $\mathbf{H}_2$ มีขนาดเท่ากับ $(m \times m)$

การเข้ารหัส คือการคำนวณค่าเมตริกส์ **p** จากสมการที่ 3.8 จากนั้นทำการแทนค่า **p** ลงในสมการที่ 3.5 ก็จะได้คำรหัสสำหรับรหัสแอลดีพีซี ส่วนสมการที่ 3.4 ใช้ในการตรวจความถูกต้องของคำรหัส

3.1.4 การถอดรหัสแอลดีพีซี

การเข้ารหัสมีผลทำให้ข้อมูลแต่ละบิตมีความสัมพันธ์กัน ผ่านทางโครงสร้างของเมตริกส์พาริตี้เช็ค **H** ซึ่งการถอดรหัสก็จะอาศัยความสัมพันธ์เหล่านี้มาช่วยในการถอดรหัส อัลกอริทึมสำหรับการถอดรหัสแอลดีพีซีนั้นมีชื่อเรียกที่หลากหลายทั้ง sum-product algorithm (SPA), belief propagation algorithm (BPA) และ message passing algorithm (MPA) ซึ่งเป็นรูปแบบการถอดรหัสที่เรียกว่า soft iterative decoding โดยขั้นตอนการถอดรหัสจะประกอบด้วยขั้นตอนหลักสองขั้นตอน คือ สร้างสมการจากโครงสร้างของเมตริกส์พาริตี้เช็ค **H** แล้วจึงเขียนแผนภาพ Tanner Graph จากนั้นจึงทำการคำนวณหาค่าของข้อมูลแต่ละบิตตามโครงสร้างของอัลกอริทึมที่ใช้ในการถอดรหัส

1) สร้างสมการจากโครงสร้างของเมตริกส์พาริตี้เช็ค **H** และเขียนแผนภาพ Tanner Graph พิจารณา Regular LDPC ขนาด (10, 5) ซึ่งมีค่า $W_c = 2$ และ $W_r = 4$ ตามสมการที่ 3.1 เมตริกส์พาริตี้เช็ค **H** ที่ได้คือ

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{(m=5, n=10)}$$

จากโครงสร้างของเมตริกส์พาริตี้เช็ค **H** จะได้ความสัมพันธ์เป็นสมการที่แสดงความสัมพันธ์ของแต่ละบิต โดยที่แต่ละแถวของเมตริกส์ **H** จะเรียกว่า โหนดเช็ค (Check Node) และแต่ละหลักจะเรียกว่า โหนดสัญลักษณ์ (Bit Node) สมการแสดงได้โดย

โหนดเช็ค ที่ 1: $c_1 + c_2 + c_3 + c_4 = 0$ (3.9)

โหนดเช็ค ที่ 2: $c_1 + c_5 + c_6 + c_7 = 0$ (3.10)

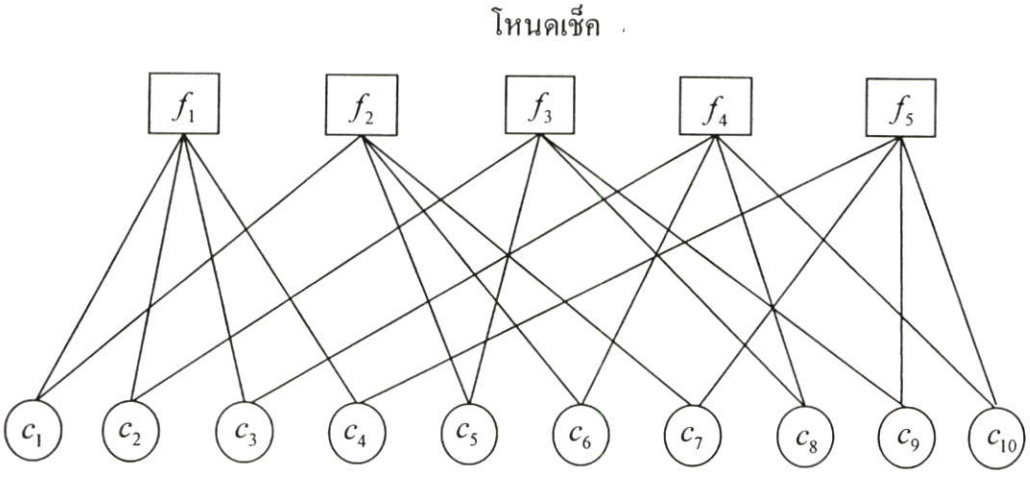
โหนดเช็ค ที่ 3: $c_2 + c_5 + c_8 + c_9 = 0$ (3.11)

โหนดเช็ค ที่ 4: $c_3 + c_6 + c_8 + c_{10} = 0$ (3.12)

โหนดเช็ค ที่ 5: $c_4 + c_7 + c_9 + c_{10} = 0$ (3.13)

โดย c_i แทนตำแหน่งของเลขหนึ่งของแต่ละโหนดสัญลักษณ์ในโหนดเช็คที่กำลังพิจารณา

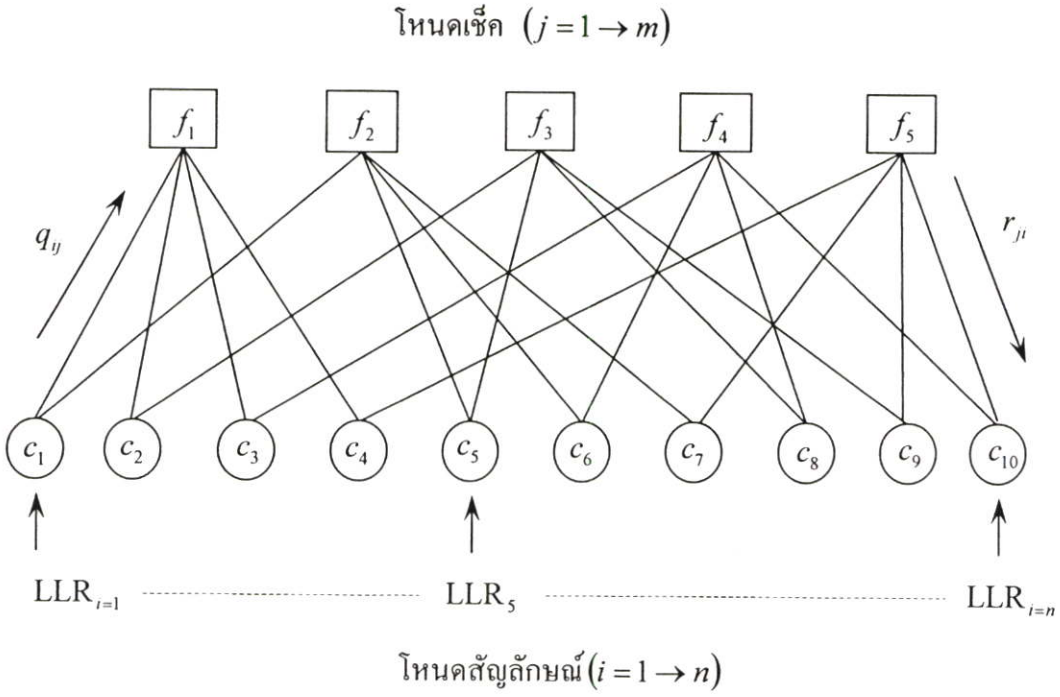
จากสมการข้างต้นเราสามารถสร้างกราฟ Tanner เพื่อช่วยในการถอดรหัส โดยเริ่มจากวาดรูปสี่เหลี่ยมตามจำนวนของโหนดเช็ค จากนั้นวาดรูปวงกลมตามจำนวนของโหนดสัญลักษณ์ ในขั้นตอนสุดท้ายเป็นการลากเส้นตรงเชื่อมความสัมพันธ์ระหว่างโหนดเช็ค และ โหนดสัญลักษณ์ ตามความสัมพันธ์ในสมการที่ 3.9 – 3.13



รูปที่ 3.1 Tanner Graph

2) การคำนวณหาค่าของข้อมูลแต่ละบิตตามโครงสร้างของอัลกอริทึมที่ใช้ในการถอดรหัส

จาก Tanner Graph จะสามารถถอดรหัสได้ด้วยหลายวิธีแต่วิทยานิพนธ์นี้ใช้วิธีการที่เรียกว่า Log-Domain SPA Decoder



รูปที่ 3.2 แสดงการส่งผ่านข้อมูลระหว่าง โหนดสัญลักษณ์ และ โหนดเช็ค

โดยหลักการทำงานจะเป็นการแลกเปลี่ยนข่าวสารแบบซอฟต์ระหว่างโหนดสัญลักษณ์ i และโหนดเช็ค j พิจารณารูปที่ 3.2 อินพุตของการถอดรหัสจะอยู่ในรูปของอัตราส่วนความน่าเป็นจริงแบบล็อก (Log Likelihood Ratios : LLRs) ของตัวแปรสุ่ม c_i ตามสมการที่ 3.15 โดยในแต่ละบิต โหนดสัญลักษณ์ i จะส่งค่าความน่าจะเป็นของข่าวสารแบบซอฟต์ไปที่ โหนดเช็ค j ผ่านตามเส้นความสัมพันธ์ที่เชื่อมถึงกันและจากนั้นที่ โหนดเช็ค j ก็จะทำการคำนวณค่าความน่าจะเป็นของข่าวสารที่ส่งมาจากโหนดสัญลักษณ์ i แล้วจึงส่งผลที่ได้ของข่าวสารแบบซอฟต์ไปให้ โหนดสัญลักษณ์ i อีกครั้ง เพื่อนำข้อมูลที่ได้ไปใช้ในการตัดสินใจว่าควรจะเป็น 0 หรือ 1

นิยามให้

q_{ij} คือความน่าจะเป็นของข่าวสารบิตที่ i ที่ส่งจาก โหนดสัญลักษณ์ i ไปที่ โหนดเช็ค j ว่าเป็น 0 หรือ 1

r_{ji} คือความน่าจะเป็นของข่าวสารบิตที่ i ที่ส่งจาก โหนดเช็ค j ไปที่ โหนดสัญลักษณ์ i ว่าเป็น 0 หรือ 1

ขั้นตอนและวิธีการสำหรับ Log Domain SPA algorithm จะประกอบด้วย 5 ขั้นตอนหลัก คือ

<u>ขั้นตอนที่ 1</u>: คำนวณค่าเริ่มต้นของ $L(q_{ij})$ ที่ส่งจากโหนดสัญลักษณ์ i ไปยัง โหนดเช็ค j ของในแต่ละบิต i ตั้งแต่บิตที่ 1 จนถึงบิตที่ n ผ่านสมการที่ 3.14

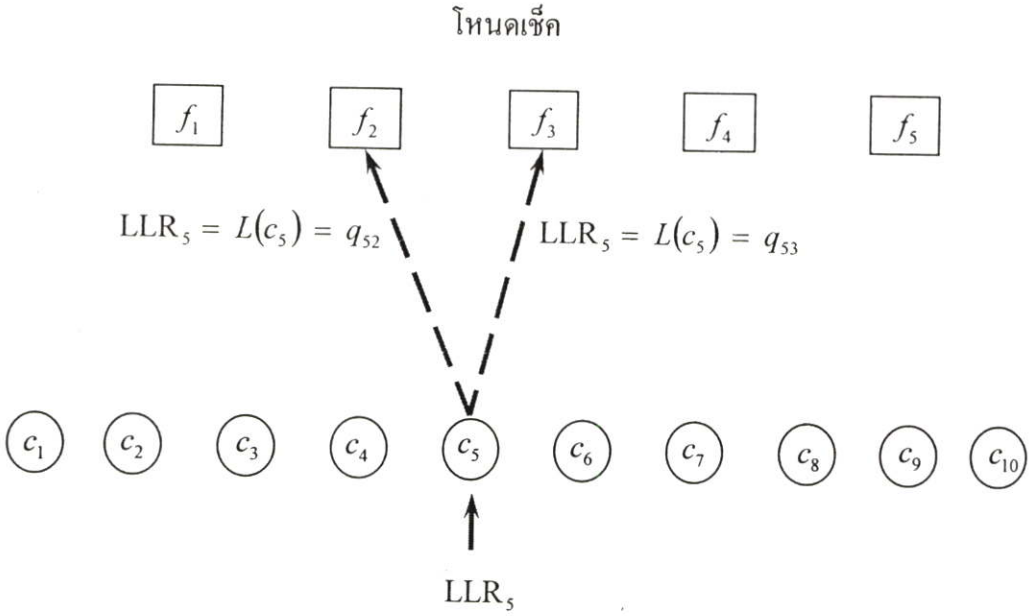
$$L(q_{ij}) = L(c_i) = 2y_i/\sigma^2 \qquad (3.14)$$

$$L(c_i) = \text{LLR}_i = \log\left[P(c_i = 0 \mid y_i)/P(c_i = 1 \mid y_i)\right] \qquad (3.15)$$

เมื่อ $L(c_i)$ คือ อัตราส่วนความน่าเป็นจริงแบบล็อก

y_i คือ สัญญาณที่ได้รับผ่านช่องสัญญาณ

σ^2 คือ ค่าเบี่ยงเบนของสัญญาณรบกวนเกาส์แบบขาว



รูปที่ 3.3 แสดงค่า $L(q_{ij})$ ที่ส่งจาก โหนดสัญลักษณ์ i ไปยัง โหนดเช็ค j

<u>ขั้นตอนที่ 2</u>: คำนวณค่า $L(r_{ji})$ ที่ส่งจาก โหนดเช็ค j ไปที่ โหนดสัญลักษณ์ i ตามเส้นความสัมพันธ์ที่เชื่อมถึงกันผ่านสมการที่ 3.16 ของในแต่ละบิต i ตั้งแต่บิตที่ 1 ถึงบิตที่ n

$$L(r_{ji}) = \prod_{i' \in V_j \setminus i} \alpha_{i'j} \cdot \phi\left(\sum_{i' \in V_j \setminus i} \phi(\beta_{i'j})\right) \qquad (3.16)$$

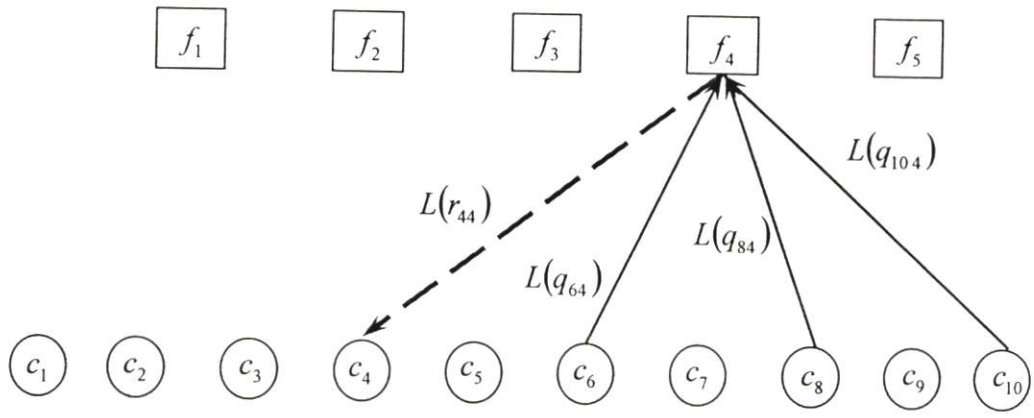
เมื่อ

$$\alpha_{ij} = \text{sgn}\{L(q_{ij})\} \text{ และ } \beta_{ij} = \left| L(q_{ij}) \right|$$

นิยามให้

$$\phi(x) = \log\{(e^x + 1)/(e^x - 1)\} \qquad (3.17)$$

$V_{j\setminus i}$ โดยแทนการพิจารณาข่าวสารจากทุกโหนดสัญลักษณ์ ที่เชื่อมต่อกับโหนดเช็ค j ยกเว้นโหนดสัญลักษณ์ ที่กำลังพิจารณา รูปที่ 3.4 แสดงแผนภาพการคำนวณค่า $L(r_{44})$

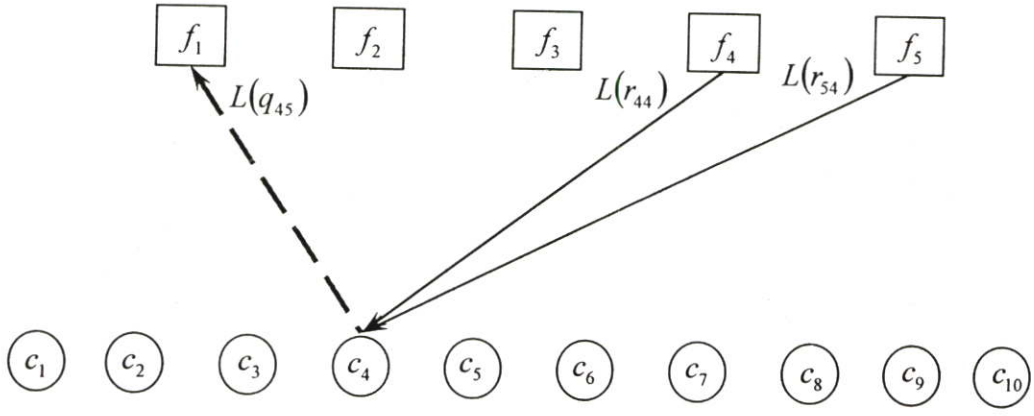


รูปที่ 3.4 แสดงค่า $L(r_{ji})$ ที่ส่งจาก โหนดเช็ค j ไปยัง โหนดสัญลักษณ์ i

<u>ขั้นตอนที่ 3</u>: จะเป็นการปรับปรุงข่าวสารของ $L(q_{ij})$ เพื่อที่จะใช้เป็นอินพุตของการถอดรหัสแบบวนซ้ำที่ส่งจาก โหนดสัญลักษณ์ i ไปยัง โหนดเช็ค j ของในแต่ละบิต i ตั้งแต่บิตที่ 1 จนถึงบิตที่ n ผ่านทางสมการที่ 3.18

$$L(q_{ij}) = L(c_i) + \sum_{j' \in C_i \setminus j} L(r_{j'i}) \qquad (3.18)$$

$C_{i\setminus j}$ แทนการพิจารณาผลรวมของข่าวสาร $L(r_{ji})$ จากทุกโหนดเช็ค j ที่เชื่อมต่อกับโหนดสัญลักษณ์ ยกเว้นข่าวสารที่ใช้เส้นทางเดียวกับ $L(q_{ij})$ รูปที่ 3.5 แสดงแผนภาพการปรับปรุงข่าวสารของ $L(q_{ij})$

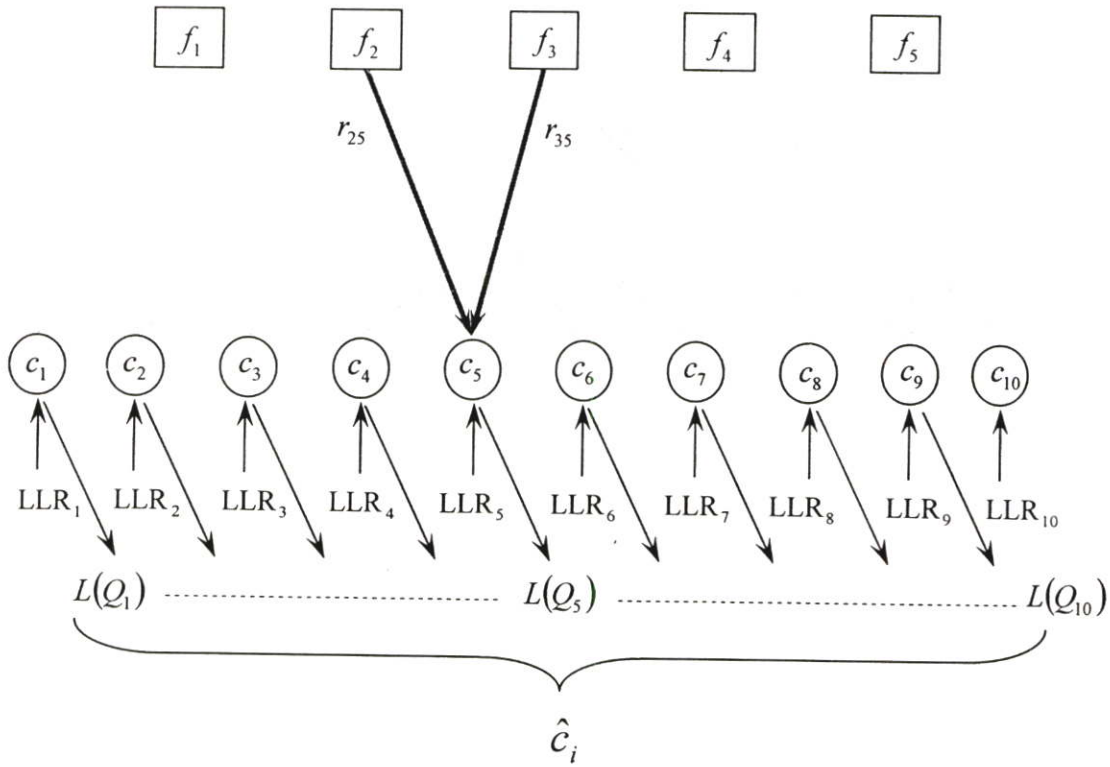


รูปที่ 3.5 ข่าวสารของ $L(q_{ij})$ เพื่อที่จะใช้เป็นอินพุตของการถอดรหัสแบบวนซ้ำ

ขั้นตอนที่ 4: เป็นการคำนวณหาค่าซอฟต์เอาต์พุตของการถอดรหัสของแต่ละบิต i ตั้งแต่บิตที่ 1 ถึงบิตที่ n ผ่านสมการที่ 3.19

$$L(Q_i) = L(c_i) + \sum_{j \in C_i} L(r_{ji}) \tag{3.19}$$

รูปที่ 3.6 แสดงแผนภาพการหาค่าซอฟต์เอาต์พุตของการถอดรหัส



รูปที่ 3.6 แสดงแผนภาพการหาค่าซอฟต์เอาต์พุตของการถอดรหัส

ขั้นตอนที่ 5: เป็นการนำค่าซอฟต์เอาต์พุตที่ได้จากขั้นตอนที่ 4 ของแต่ละบิตมาทำการตัดสินใจแบบฮาร์ดผ่านสมการที่ 3. 20

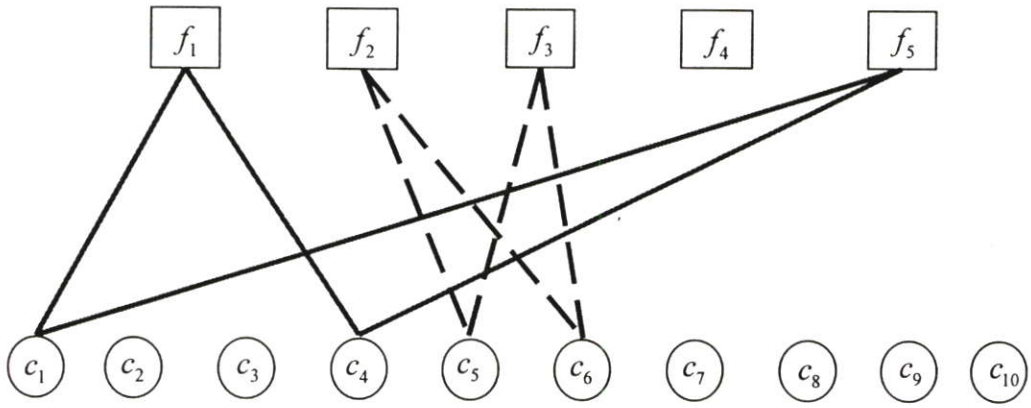
$$\hat{c}_i = 1 \text{ ถ้า มิฉะนั้น } \hat{c}_i = 0 \tag{3.20}$$

จากขั้นตอนที่ 1 – 5 ก็จะเป็นการเสร็จสิ้นขั้นตอนในการถอดรหัสหนึ่งลูป ซึ่งจะพบว่าถ้าระบบที่ใช้การถอดรหัสแบบไม่มีการวนซ้ำขั้นตอนที่ 3 ก็สามารถยกเลิก และข้ามมายังขั้นตอนที่ 4 ได้เลย

หรือในกรณีที่ใช้การวนซ้ำก็จะทำตามขั้นตอนที่ 1 – 5 ตามจำนวนรอบการวนซ้ำที่ได้กำหนดไว้ หรือใช้สมการ $\hat{c} \cdot \mathbf{H}^T = \mathbf{0}$ ช่วยเป็นเงื่อนไขเสร็จสิ้นขั้นตอนในการถอดรหัส

จากหัวข้อที่ 3.1.1 ที่กล่าวถึงเงื่อนไขของการสร้างเมตริกส์พาริตี้เช็ค **H** ว่าจะต้องปราศจากไซเคิลขนาดเท่ากับ 4 และได้อธิบายถึงนิยามของไซเคิลนั้นเมื่อพิจารณาจากอัลกอริทึมการถอดรหัสจะพบว่าเป็นการอาศัยการแลกเปลี่ยนข่าวสารแบบซอฟต์ ระหว่างโหนดสัญลักษณ์ i และโหนดเช็ค j กับหลักการของความน่าจะเป็นว่าเหตุการณ์แต่ละเหตุการณ์นั้นเป็นอิสระต่อกัน ซึ่งในกรณีของเมตริกส์พาริตี้เช็ค **H** ที่มีไซเคิลขนาดเท่ากับ 4 นั้นจะมีผลทำให้เกิดลูปปิด และเหตุการณ์การแลกเปลี่ยนข่าวสารแบบซอฟต์จะไม่เป็นอิสระต่อกัน

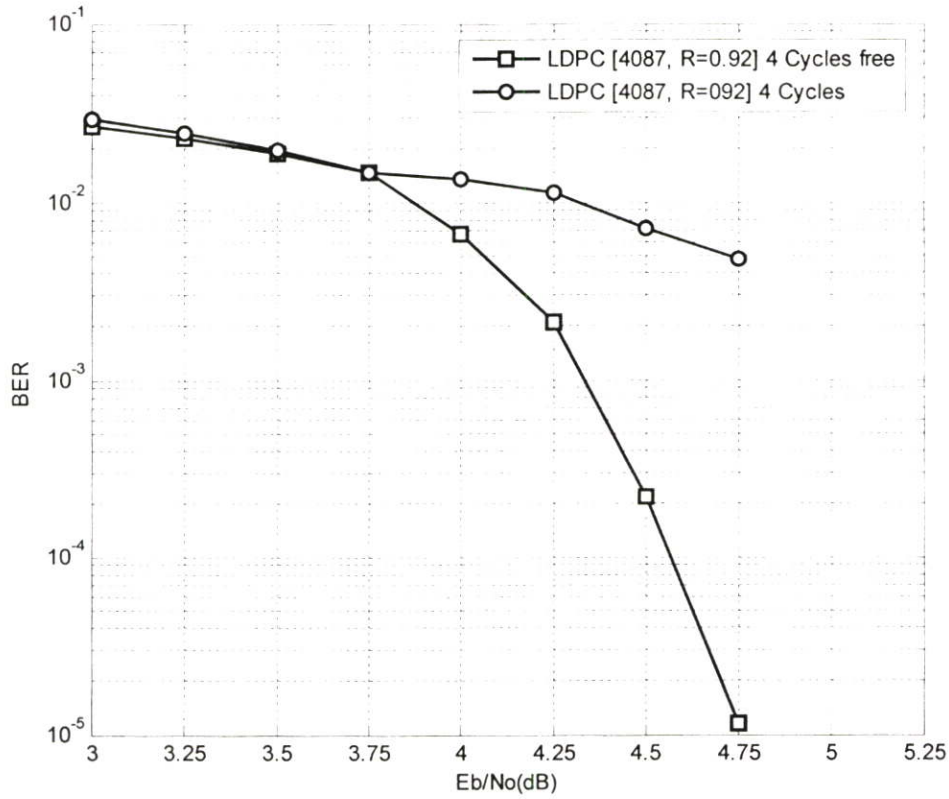
พิจารณาเมตริกส์พาริตี้เช็ค **H** ในสมการที่ 3.3 แล้วสร้าง Tanner Graph จะพบว่ามีไซเคิลขนาดเท่ากับ 4 จำนวนสองไซเคิล โดยไซเคิลแรกจะพบที่โหนดสัญลักษณ์ c_1, c_4 กับโหนดเช็ค f_1, f_5 ส่วนไซเคิลที่สองจะพบที่ โหนดสัญลักษณ์ c_5, c_6 กับ โหนดเช็ค f_2, f_3



รูปที่ 3.7 แสดงแผนภาพของเมตริกส์พาริตี้เช็ค **H** ที่มีไซเคิลขนาดเท่ากับ 4

รูปที่ 3.8 เป็นการจำลองสมรรถนะการทำงานของระบบบันทึกข้อมูลแบบดิจิตอลที่มีอินพุต ±1 และช่องสัญญาณเป็นแบบอุดมคติที่มีเพียงสัญญาณรบกวนเกาส์แบบขาว และใช้วิธีการเข้ารหัสช่องสัญญาณ แบบแอลดีพีซีที่มีเมตริกส์พาริตี้เช็ค **H** มีไซเคิลขนาดเท่ากับ 4 เปรียบกับมีเมตริกส์พาริตี้เช็คที่ไม่มีไซเคิลขนาดเท่ากับ 4 กับความยาวคำรหัสขนาด 4087 ด้วยอัตรารหัส 0.92 เท่ากัน โดยทำการมอดูเลตแบบ Binary Phase shift keying (BPSK)

โดย E_b เป็นพลังงานเฉลี่ยของบิตข้อมูลและ $\frac{N_0}{2}$ คือค่าความหนาแน่น สเปกตรัมกำลังงานซึ่งมีหน่วยเป็น W/Hz จากผลการจำลองสมรรถนะการทำงานอัตราความผิดพลาดบิตจะพบว่ารหัสแอลดีพีซีที่มีไซเคิลขนาดเท่ากับ 4 จะส่งผลต่อสมรรถนะอัตราความผิดพลาดบิตโดยให้อัตราบิตผิดพลาดที่สูงกว่าที่อัตราส่วนต่อสัญญาณสัญญาณรบกวน เท่ากัน



รูปที่ 3.8 แสดงสมรรถนะการทำงานของรหัสแอลดีพีซีที่มีไซเคิลขนาดเท่ากับ 4

กล่าวโดยสรุปสำหรับหัวข้อ 3.1 เป็นการกล่าวถึงประวัติความเป็นมาของรหัสแอลดีพีซี หลักการทำงานสำหรับการเข้ารหัสและการถอดรหัสแอลดีพีซี ซึ่งพบว่าข้อด้อยของรหัสแอลดีพีซีที่ได้กล่าวมาก่อนหน้านี้มีดังนี้

Regular LDPC การสร้างเมตริกส์พาริตี้เช็ค **H** ได้จากการสุ่มข้อมูลศูนย์ หนึ่ง ในแถวและหลัก โดยจะต้องมีการควบคุมจำนวนของเลขศูนย์ หนึ่ง ในแถวและหลักนั้น นอกเหนือจากนี้ตำแหน่งของเลขหนึ่งที่ได้จะต้องไม่ทำให้เกิดไซเคิลขนาดเท่ากับ 4 ความซับซ้อนจะเพิ่มขึ้นตามขนาดของเมตริกส์ **H**

Irregular LDPC มีสมรรถนะการทำงานที่ดีกว่ารหัส Regular LDPC แต่มีข้อจำกัดว่ารหัสจะมีสมรรถนะที่ดีเมื่ออัตรารหัส $R \leq 3/4$ และมีความยาวคำรหัส $n \geq 5000$

ในหัวข้อต่อไปจะกล่าวถึงรหัสแอลดีพีซีที่ใช้การเข้ารหัสด้วยเมตริกส์พาริตี้เช็คที่มีโครงสร้างเป็นแบบอาร์เรย์ หรือที่เรียกว่ารหัสแอลดีพีซีแบบอาร์เรย์ ซึ่งถูกพัฒนาขึ้นมาเพื่อแก้ปัญหาความซับซ้อนในการสร้างเมตริกส์พาริตี้ของรหัสแอลดีพีซีที่มีโครงสร้างของเมตริกส์พาริตี้เป็นแบบสุ่ม

3.2 รหัสแอลดีพีซีแบบอาร์เรย์ (Array Codes)

รหัสแอลดีพีซีแบบอาร์เรย์ถูกสร้างขึ้นครั้งแรกในปี ค.ศ. 2000 (2543) โดย J. Fan [3] โดยมีโครงสร้างเมตริกส์พาริตี้เช็คเป็นแบบอาร์เรย์ จึงช่วยแก้ปัญหาความซับซ้อนในการสร้างเมตริกส์พาริตี้ อีกทั้งยังมีสมรรถนะที่ใกล้เคียงกับรหัสแอลดีพีซีที่มีโครงสร้างของเมตริกส์พาริตี้เป็นแบบสุ่ม สำหรับรหัสอาร์เรย์ (Array codes) อธิบายได้ด้วยพารามิเตอร์ 3 ค่าได้แก่ จำนวนเฉพาะ p และจำนวนเต็ม j และ k โดยที่ $j,k \le p$ เมตริกส์ที่ได้มีขนาด jp x kp เขียนได้ในรูป

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} \\ \mathbf{I} & \boldsymbol{\alpha} & \boldsymbol{\alpha}^2 & \cdots & \boldsymbol{\alpha}^{k-1} \\ \mathbf{I} & \boldsymbol{\alpha}^2 & \boldsymbol{\alpha}^4 & \cdots & \boldsymbol{\alpha}^{2(k-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbf{I} & \boldsymbol{\alpha}^{j-1} & \boldsymbol{\alpha}^{2(j-1)} & \cdots & \boldsymbol{\alpha}^{(j-1)(k-1)} \end{bmatrix}_{(jp \text{ x } kp)} \tag{3.21}$$

โดยที่ $\mathbf{I}$ คือเมตริกส์เอกลักษณ์และ $\boldsymbol{\alpha}$ คือเมตริกส์สลับตำแหน่งขนาด p x p ซึ่งเกิดจากการเลื่อนแถวหรือหลักไปทางซ้ายหรือขวาของ $\mathbf{I}$ โดยที่กำลังของ $\boldsymbol{\alpha}$ นั้นคือจำนวนครั้งของการเลื่อนแถวของเมตริกส์สลับตำแหน่ง ความยาวคำรหัสที่ได้มีค่าเท่ากับ kp , ความยาวพาริตี้บิตมีค่าเท่ากับ jp และอัตรารหัส R มีค่าเท่ากับ $1-\left(\frac{p \cdot j - j + 1}{p^2}\right)$

ตัวอย่างของการสร้างเมตริกส์ $\boldsymbol{\alpha}$ ขนาด 5 x 5จากเมตริกส์เอกลักษณ์ด้วยวิธีการการเลื่อนแถว และมีคุณสมบัติที่สำคัญมีดังนี้

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \text{ x } 5)} \quad \boldsymbol{\alpha} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}_{(5 \text{ x } 5)} \quad \boldsymbol{\alpha}^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}_{(5 \text{ x } 5)}$$

$$\boldsymbol{\alpha}^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}_{(5 \text{ x } 5)} \quad \boldsymbol{\alpha}^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{(5 \text{ x } 5)} \quad \boldsymbol{\alpha}^5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \text{ x } 5)}$$

สาเหตุที่เมตริกส์ $\boldsymbol{\alpha}$ มีชื่อว่าเมตริกส์สลับตำแหน่งก็เพราะว่าเมื่อคูณกับเมตริกส์ใด ๆ นั้น ผลลัพธ์ที่ได้จะมีค่าเท่ากับเมตริกส์นั้นถูกสลับตำแหน่งนอกจากนี้เมตริกส์ผกผัน $\boldsymbol{\alpha}^{-1}$ ของเมตริกส์สลับตำแหน่ง มีค่าเท่ากับทรานโพส $\boldsymbol{\alpha}^{T}$ ของเมตริกส์สลับตำแหน่ง

นอกจากนี้ J. Fan ยังได้พิสูจน์ให้เห็นว่ารหัสอาร์เรย์ปราศจากไซเคิลขนาดเท่ากับ 4 และรหัสอาร์เรย์สามารถใช้อัลกอริทึมการถอดรหัสได้เช่นเดียวกับรหัสแอลดีพีซีชนิดทั่วไป ด้วยงานวิจัยของ J.Fan นี้เองได้ช่วยแก้ปัญหาข้อด้อยของรหัสแอลดีพีซีในเรื่องของการสร้างเมตริกส์ $\mathbf{H}$ จากการสุ่มข้อมูลศูนย์หนึ่ง การควบคุมจำนวนเลขหนึ่งในแถวและหลัก และการหลีกเลี่ยงไซเคิลขนาดเท่ากับ 4

3.3 รหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ (Modified Array Codes: MAC)

จากงานวิจัยของ T.Richardson [7] ได้กล่าวว่าการเพิ่มประสิทธิภาพในการเข้ารหัสและทำให้การเข้ารหัสมีความซับซ้อนในระดับเชิงเส้น สามารถทำได้โดยการแปลงให้เมตริกส์พาริตี้เช็ค $\mathbf{H}$ มีรูปร่างสามเหลี่ยม ดังนั้นในปี ค.ศ. 2002 (2545) E. Eleftheriou [4] ได้เสนอโครงสร้างของเมตริกส์พาริตี้เช็คสำหรับรหัสแอลดีพีซีแบบอาร์เรย์แบบใหม่ ซึ่งมีชื่อเรียกว่า รหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ โดยใช้วิธีการที่เรียกว่า Cyclic Shift สมรรถนะของรหัสที่ได้ยังมีค่าดีเทียบเท่ากับรหัสแอลดีพีซีที่มีโครงสร้างของเมตริกส์พาริตี้เป็นแบบสุ่ม
เมตริกส์พาริตี้เช็คของรหัสใหม่นี้เขียนได้ในรูปสมการที่ 3.22

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} & \mathbf{I} & \cdots & \cdots & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \boldsymbol{\alpha} & \cdots & \boldsymbol{\alpha}^{j-2} & \boldsymbol{\alpha}^{j-1} & \cdots & \boldsymbol{\alpha}^{k-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \boldsymbol{\alpha}^{2(j-3)} & \boldsymbol{\alpha}^{2(j-2)} & \cdots & \boldsymbol{\alpha}^{2(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \cdots & \mathbf{I} & \boldsymbol{\alpha}^{(j-1)} & \cdots & \boldsymbol{\alpha}^{(j-1)(k-j)} \end{bmatrix}_{(jp \times kp)} \qquad (3.22)$$

เมื่อ $\mathbf{0}$ คือเมตริกส์ศูนย์ขนาด $p \times p$ รหัสนี้มีความยาวข้อมูลอินพุตเท่ากับ $(k-j)p$ ความยาวคำรหัสเท่ากับ kp และจำนวนบิตพาริตี้เช็ค เท่ากับ jp อัตรารหัสมีค่าเท่ากับ $(1-j/k)$ เมตริกส์ข้างต้นปราศจากไซเคิลขนาดเท่ากับ 4 มีคุณสมบัติที่ดีในเรื่อง Error Floor ที่ต่ำและสามารถใช้อัลกอริทึมการถอดรหัสเดิม เช่นเดียวกับรหัสแอลดีพีซีชนิดทั่วไป สังเกตว่ารูปแบบสามเหลี่ยมทำให้การกระจายตัวของเลขหนึ่งเปลี่ยนจากแบบคงที่เป็นแบบไม่คงที่

ทำการทรานโพสสมการที่ 3.4 จะได้สมการใหม่เป็นสมการที่ 3.23

$$\mathbf{H}_{(m\times n)}\mathbf{c}^{T}{}_{(n\times 1)} = \mathbf{0}^{T}{}_{(m\times 1)} \tag{3.23}$$

เขียนเมตริกส์ $\mathbf{c}$ ให้อยู่ในรูป Systematic form จะได้สมการหลักที่จะใช้ในการเข้ารหัสสำหรับรหัสแอลดีพีซีแบมอดดิฟายอาร์เรย์

$$\mathbf{H}_{(m\times n)}\left[\frac{\mathbf{p}}{\mathbf{m}}\right]^{\mathrm{T}} = \mathbf{0}^{T}{}_{(m\times 1)} \tag{3.24}$$

ผลที่ได้คือความซับซ้อนในการเข้ารหัสจะลดลงอย่างมากเมื่อเทียบกับสมการในการเข้ารหัสที่ได้กล่าวมาก่อนหน้านี้ เนื่องจากการหาค่าพาริตี้บิตนั้นไม่จำเป็นต้องหาค่าเมตริกส์ผกผัน

ตัวอย่างการเข้ารหัสสำหรับรหัสแอลดีพีซีแบมอดดิฟายอาร์เรย์
กำหนดให้พารามิเตอร์ $p=5$, $j=4$ และ $k=5$ จากสมการที่ 3.24

$$\mathbf{H}_{(20\,x\,25)}\left[\frac{\mathbf{p}_{(20x1)}}{\mathbf{m}_{(5x1)}}\right] = \mathbf{0}_{(20\,x\,1)} \tag{3.25}$$

เมื่อทำการคูณเมตริกส์พาริตี้เช็คกับเมตริกส์คำรหัสจะได้สมการทั้งหมด 20 สมการจากนั้นจึงใช้สมการเหล่านี้ในการหาค่าพาริตี้บิตด้วยวิธีการมอดูโล-2

$$\begin{aligned}
p_{20} + m_3 &= 0 \\
p_{19} + m_2 &= 0 \\
p_{18} + m_1 &= 0 \\
&\vdots \\
&\vdots \\
p_2 + p_7 + p_{12} + p_{17} + m_2 &= 0 \\
p_1 + p_6 + p_{11} + p_{16} + m_1 &= 0
\end{aligned} \tag{3.26}$$

จากสมการ (3.26) แสดงให้เห็นว่าความซับซ้อนในการแก้สมการจะเป็นแบบเชิงเส้นอันเป็นผลมาจากการแปลงให้เมตริกส์พาริตี้เช็ค $\mathbf{H}$ มีรูปร่างสามเหลี่ยม

3.4 รหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ที่มีการสลับบิต (Interleaved Modified Array Codes: IMAC)

วิทยานิพนธ์ฉบับนี้ทำการปรับปรุงเมตริกส์พาริตี้เช็คของรหัสมอดดิฟายอาร์เรย์ ด้วย Quasi-cyclic matrix ภายใต้แนวคิดที่ทำการ cyclic shift ในระดับบิตด้วย Quasi-cyclic matrix ซึ่งเป็นส่วนที่เพิ่มเข้าไปในเมตริกส์พาริตี้เช็คของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ให้กลาย เป็นรหัสแอลดีพีซีแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์ และสามารถอธิบายได้ด้วยพารามิเตอร์ 3 ค่า ได้แก่ จำนวนเฉพาะ p จำนวนเต็ม j และ k โดยที่ $j,k \le p$ เมตริกส์นี้มีขนาด $jp \times kp$ เช่นเดียวกับรหัสมอดดิฟายอาร์เรย์ เมตริกส์พาริตี้เช็คใหม่ที่ได้แสดงได้ในรูป

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I}\omega & \mathbf{I}\omega^2 & \mathbf{I}\omega^3 & \cdots & \mathbf{I}\omega^j \\ \mathbf{0} & \mathbf{I} & \alpha\omega & \alpha^2\omega^2 & \alpha^3\omega^3 & \cdots & \alpha^{(k-2)}\omega^j \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \alpha^2\omega^2 & \alpha^4\omega^3 & \cdots & \alpha^{2(k-3)}\omega^j \\ \vdots & \vdots & \vdots & \mathbf{I} & \alpha^3\omega^3 & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I} & \cdots & \alpha^{(j-1)}\omega^{(k-j)} \end{bmatrix}_{(jp \times kp)} \tag{3.27}$$

จากสมการที่ (3.26) โครงสร้างของเมตริกส์พาริตี้เช็ค $\mathbf{H}$ ที่ได้ยังคงรูปร่างสามเหลี่ยมทำให้ประสิทธิภาพในการเข้ารหัสยังคงเดิม เมตริกส์ $\mathbf{0}$, α และ $\mathbf{I}$ มีคุณสมบัติเช่นเดียวกับมอดดิฟายอาร์เรย์ ความยาวข้อมูลอินพุตเท่ากับ $(k-j)p$ ความยาวคำรหัสเท่ากับ kp และจำนวนพาริตี้เช็คเท่ากับ jp อัตรารหัสมีค่าเท่ากับ $(1-j/k)$

โดยที่ ω คือเมตริกส์ Quasi-cyclic matrix ที่สร้างขึ้นจากเมตริกส์ $\mathbf{I}$ โดยทำการเลื่อนเป็นวงกลม (cyclic shift) กับทุกแถวของเมตริกส์ $\mathbf{I}$ ตัวอย่าง Quasi-cyclic matrix ที่สร้างจากเมตริกส์ $\mathbf{I}$ ขนาด 5 x 5 แสดงดังสมการที่ 3.27

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)} \rightarrow \quad \omega = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)} \tag{3.27}$$

คุณสมบัติที่สำคัญของเมตริกส์ Quasi-cyclic ขนาด $n \times n$ มีดังนี้

1) เมื่อทำการยกกำลังเท่ากับขนาดของเมตริกส์จะมีค่าเท่ากับตัวมันเองกล่าวคือ

$$\boldsymbol{\omega}^{n} = \boldsymbol{\omega} \tag{3.28}$$

$$\boldsymbol{\omega}^{5} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)} \rightarrow \boldsymbol{\omega} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)}$$

2) เมื่อทำการยกกำลัง Quasi-cyclic matrix เท่ากับขนาดของเมตริกส์ลบหนึ่งจะมีค่าเท่ากับเมตริกส์เอกลักษณ์ กล่าวคือ

$$\boldsymbol{\omega}^{n-1} = \mathbf{I} \tag{3.29}$$

$$\boldsymbol{\omega}^{4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)} \rightarrow \mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)}$$

3) รหัสแอลดีพีซีที่นำเสนอมีชื่อว่า อินเตอร์ลีฟมอดดิฟายอาร์เรย์ เนื่องจากเมื่อนำ Quasi-cyclic matrix $\boldsymbol{\omega}$ คูณกับเมตริกส์ใดๆ นั้นผลลัพธ์ที่ได้คือเมตริกส์นั้นถูกอินเตอร์ลีฟ

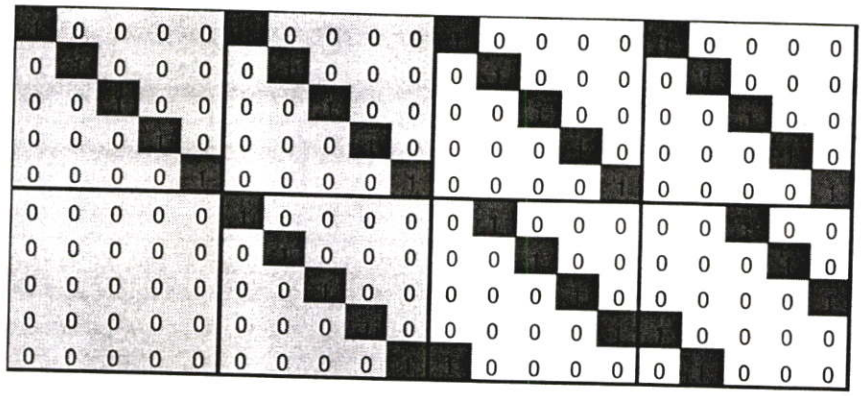
$$\boldsymbol{\alpha} \cdot \boldsymbol{\omega} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}_{(5 \times 5)} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(5 \times 5)} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}_{(5 \times 5)}$$

ตัวอย่าง เมตริกส์พาริตี้เช็คสำหรับรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

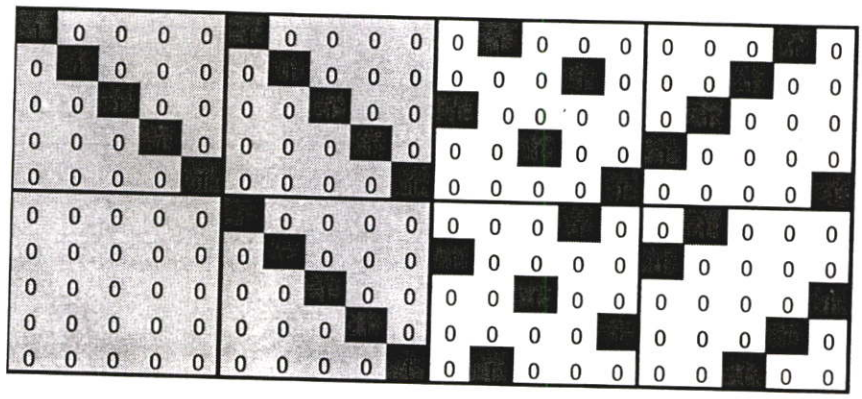
กำหนดให้พารามิเตอร์ $p = 5$, $j = 2$ และ $k = 4$ จากสมการที่ 3.22 และ 3.25 เมตริกส์พาริตี้เช็คที่ได้คือ

$$\begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \boldsymbol{\alpha} & \boldsymbol{\alpha}^2 \end{bmatrix}_{(2\times 4)} \rightarrow \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I}\boldsymbol{\omega} & \mathbf{I}\boldsymbol{\omega}^2 \\ \mathbf{0} & \mathbf{I} & \boldsymbol{\alpha}\boldsymbol{\omega} & \boldsymbol{\alpha}^2\boldsymbol{\omega}^2 \end{bmatrix}_{(2\times 4)}$$

รูปที่ 3.9 แสดงการเปรียบเทียบโครงสร้างของเมตริกส์พาริตี้เช็คสำหรับรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ที่ได้จากการกำหนดค่าพารามิเตอร์ข้างต้น



(ก) รหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์



(ข) รหัสแอลดีพีซีแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์

รูปที่ 3.9 แสดงโครงสร้างของเมตริกส์พาริตี้เช็คสำหรับรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

เมื่อพิจารณาโครงสร้างของเมตริกส์พาริตี้เช็คในรูป (ก) และ (ข) พบว่าตำแหน่งของเลขหนึ่งในหลักที่หนึ่งถึงสิบมีค่าเหมือนกันอันเนื่องมาจากตำแหน่งเหล่านี้ไม่มีการคูณด้วย Quasi-cyclic matrix จึงไม่มีความแตกต่างระหว่างรหัสมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ในขณะที่ตำแหน่งของเลขหนึ่งในหลักที่สิบเอ็ดถึงยี่สิบมีค่าต่างกันคือเมตริกส์นั้นถูกอินเตอร์ลีฟ อันสืบเนื่องมาจากผลกระทบจากการถูกคูณด้วย Quasi-cyclic matrix

จำนวนของเลขหนึ่งในแต่ละแถวและแต่ละหลักของรหัสทั้งสองแบบมีค่าเท่ากัน แต่รหัสทั้งสองแบบปราศจากไซเคิลเท่ากับ 4

จากโครงสร้างเมตริกส์ของเมตริกส์พาริตี้เช็คในรูป (ก) และ (ข) รหัสมอดดิฟายอาร์เรย์และอินเตอร์ลีฟมอดดิฟายอาร์เรย์จะได้ความสัมพันธ์เป็นสมการ และในแต่ละสมการจะบอกความสัมพันธ์แต่ละบิต ระหว่างบิตสัญลักษณ์และบิตเช็คจำนวน 10 สมการ ดังตารางที่ 3.1

ตารางที่ 3.1 สมการที่ได้จากเมตริกส์พาริตี้เช็คสำหรับรหัสแอลดีพีซี แบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

มอดดิฟายอาร์เรย์	อินเตอร์ลีฟมอดดิฟายอาร์เรย์
$c_1 + c_6 + c_{11} + c_{16}$	$c_1 + c_6 + c_{12} + c_{19}$
$c_2 + c_7 + c_{12} + c_{17}$	$c_2 + c_7 + c_{14} + c_{18}$
$c_3 + c_8 + c_{13} + c_{18}$	$c_3 + c_8 + c_{11} + c_{17}$
$c_4 + c_9 + c_{14} + c_{19}$	$c_4 + c_9 + c_{13} + c_{16}$
$c_5 + c_{10} + c_{15} + c_{20}$	$c_5 + c_{10} + c_{15} + c_{20}$
$c_6 + c_{12} + c_{18}$	$c_6 + c_{14} + c_{17}$
$c_7 + c_{13} + c_{19}$	$c_7 + c_{11} + c_{16}$
$c_8 + c_{14} + c_{20}$	$c_8 + c_{13} + c_{20}$
$c_9 + c_{15} + c_{16}$	$c_9 + c_{15} + c_{19}$
$c_{10} + c_{11} + c_{17}$	$c_{10} + c_{12} + c_{18}$

ตารางที่ 3.1 แสดงสมการที่ได้จากในแต่ละโหนดเช็คของมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ในแต่ละสมการของโหนดเช็คจะประกอบด้วยตำแหน่งของโหนดสัญลักษณ์ที่เหมือนกัน และต่างกันระหว่างรหัสมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ดังเช่นในโหนดเช็คที่ 1 ประกอยด้วยโหนดสัญลักษณ์ที่มีค่าเหมือนกัน คือ c_1 และ c_6 อันเนื่องมาจากตำแหน่งเหล่านี้ไม่มีการคูณด้วย Quasi-cyclic matrix และโหนดสัญลักษณ์ที่มีค่าต่างกันคือรหัสมอดดิฟายอาร์เรย์จะประกอบด้วยโหนดสัญลักษณ์ c_{11}, c_{16} ในขณะที่อินเตอร์ลีฟมอดดิฟายอาร์เรย์ประกอบด้วยโหนดสัญลักษณ์ c_{12}, c_{19} อันสืบเนื่องมาจากผลกระทบจากการถูกคูณด้วย Quasi-cyclic matrix ซึ่งความต่างนี้เองจะมีผลทำให้ Tanner กราฟที่ได้ของรหัสทั้งสองแบบมีค่าต่างกัน และเหตุที่ขั้นตอนการถอดรหัสจะอาศัยโครงสร้าง Tanner กราฟมาช่วยในการถอดรหัสจึงมีความเป็นไปได้ที่สมรรถนะอัตราความผิดพลาดบิตของรหัสมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์จะมีค่าที่ต่างกัน ซึ่งจะทำการเปรียบเทียบผลการจำลองสมรรถนะการทำงานในบทต่อไป

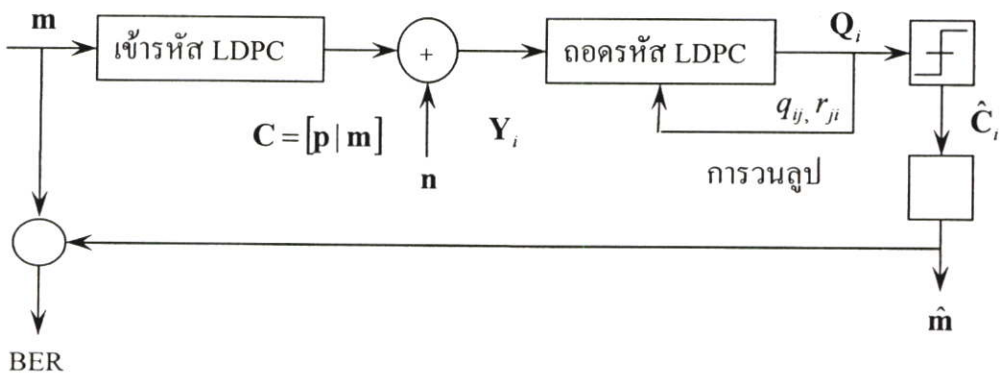
ในบทที่ 3 ได้อธิบายถึงรหัสแอลดีพีซีที่ใช้โครงสร้างแบบสุ่มในการสร้างเมตริกส์พาริตี้เช็ค ข้อเสียที่พบในการสร้างเมตริกส์พาริตี้ จากนั้นรหัสแอลดีพีซีที่ใช้การเข้ารหัสด้วยเมตริกส์พาริตี้เช็คแบบมีโครงสร้างเป็นแบบอาร์เรย์ ซึ่งถูกพัฒนาขึ้นมาเพื่อแก้ปัญหาความซับซ้อนในการสร้างเมตริกส์พาริตี้ของรหัสแอลดีพีซีแบบสุ่ม ในตอนท้ายเพื่อเพิ่มสมรรถนะของอัตราความผิดพลาดบิตของข้อมูลที่ภาครับให้สูงขึ้น ได้นำเสนอรหัสแอลดีพีซีแบบอาร์เรย์ที่มีการสลับบิตของข้อมูลในเมตริกส์พาริตี้เช็ค ซึ่งเป็นหลักการใหม่ที่นำเสนอในวิทยานิพนธ์นี้ ในบทที่ 4 จะนำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์สำหรับการประยุกต์ใช้งานในระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยจะเน้นรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์และ อินเตอร์ลีฟมอดดิฟายอาร์เรย์ที่เหมาะสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

บทที่ 4
การหาค่าสมรรถนะของระบบ

ในบทนี้นำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์ สำหรับการประยุกต์ใช้งานในระ บบบันทึกข้อมูลเชิงแม่เหล็ก โดยจะเน้นรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ (MAC) และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ (IMAC) โดยจะกล่าวถึงพารามิเตอร์ที่ใช้ในการจำลองระบบ และผลที่ได้จากการจำลองระบบ และการหาค่าพารามิเตอร์ที่เหมาะสมสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็ก

4.1 แบบจำลองที่ใช้ในการจำลองระบบ

แบบจำลองที่ใช้ในการจำลองเพื่อหาค่าสมรรถนะของระบบแสดงดังรูปที่ 4.1 โดยจะเป็นการพิจารณาอัตราความผิดพลาดบิตข้อมูลของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์



รูปที่ 4.1 แบบจำลองสมรรถนะการถอดรหัสแบบวนซ้ำ

เมื่อ

m คือ เวกเตอร์ข้อมูลอินพุตขนาด $p \cdot (k - j)$

C คือ เวกเตอร์คำรหัสขนาด $p \cdot k$

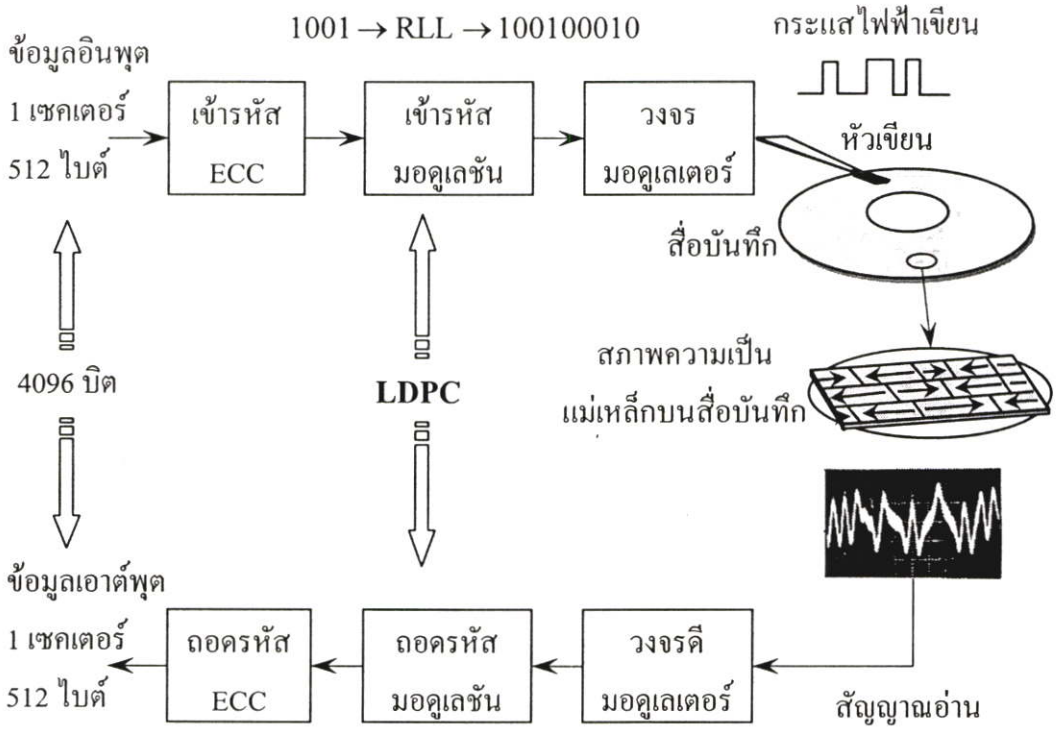
n คือ เวกเตอร์สัญญาณรบกวนเกาส์แบบขาวที่มีสเปกตรัมกำลังงานเท่ากับ $\frac{N_0}{2}$ *W/Hz*

$\mathbf{Y}_i$ คือ เวกเตอร์สัญญาณที่ได้รับผ่านช่องสัญญาณ

อัตราส่วนต่อสัญญาณสัญญาณรบกวนสำหรับบิตข้อมูลคือ $\frac{E_b}{N_o} = \frac{1}{R} \cdot \frac{E_c}{N_o}$ เมื่อ E_c เป็นพลังงานเฉลี่ยของบิตรหัส E_b คือ พลังงานเฉลี่ยของบิตข้อมูล

หมายเหตุ อัตราความผิดพลาดบิตถูกคำนวณจนกว่าจะได้บิตผิดพลาดรวมเท่ากับ 1000 ในแต่ละอัตราส่วนต่อสัญญาณสัญญาณรบกวนรหัส หรือจำนวนบล็อกในการส่งข้อมูลมากกว่าหรือเท่ากับ 1,000,000 บล็อก

4.2 พารามิเตอร์ที่ใช้ในการจำลองระบบ



รูปที่ 4.2 แบบจำลองระบบบันทึกข้อมูลเชิงแม่เหล็ก

แบบจำลองระบบบันทึกข้อมูลเชิงแม่เหล็กแสดงดังรูปที่ 4.2 โดยมีหลักการทำงานดังนี้

1) รหัสแก้ไขข้อผิดพลาด (ECC: error correcting code) มีหน้าที่ในการแก้ไขข้อผิดพลาดที่เกิดขึ้นในระบบ โดยที่รหัส RS (Reed Solomon) ซึ่งเป็นรหัสบล็อกเชิงเส้นชนิดหนึ่งจะเป็น ECC ประเภทหนึ่งที่นิยมใช้ในมากในระบบบันทึกข้อมูลเชิงแม่เหล็กตั้งแต่อดีตจนถึงปัจจุบัน ทั้งนี้ก็เพราะว่ารหัส RS นั้นมีความสามารถในการแก้ไข้ข้อผิดพลาดแบบหลายบิตติดกันได้ อย่างมีประสิทธิภาพ

2) วงจรเข้ารหัสมอดูเลชัน (Modulation Encoder) จะทำหน้าที่ได้หลายแบบได้แก่ทำให้ส่วนประกอบไฟฟ้ากระแสตรงหมดไป หรือทำให้เหลือน้อยที่สุด ช่วยเพิ่มระยะห่างของบิตเปลี่ยน

สถานะ (Transition bit) ที่จะเขียนลงไปในสื่อบันทึก และช่วยลดผลกระทบของการแทรกสอดระหว่างสัญญลักษณ์ (ISI: Inter Symbol Interference) โดยที่รหัสที่นิยมใช้คือ RLL (run-length limited) ซึ่งเป็นรหัสบล็อกเชิงเส้นชนิดหนึ่ง ซึ่งถูกกำหนดด้วยพารามิเตอร์ 4 ตัว คือ m,n,d และ k เมื่อ m คือความยาวบิตข้อมูล n คือความยาวบิตคำรหัส d คือเลขจำนวนเต็มที่กำหนดจำนวนที่น้อยที่สุดของบิตศูนย์ที่อยู่ระหว่างบิตหนึ่ง ซึ่งทำให้บิตหนึ่งสองบิตอยู่ห่างกันเพื่อลดผลกระทบของการแทรกสอดระหว่างสัญญลักษณ์ ในขณะที่ k คือเลขจำนวนเต็มที่กำหนดจำนวนที่มากที่สุดของบิตศูนย์ที่อยู่ระหว่างบิตหนึ่ง ซึ่งจะช่วยรับประกันว่าลำดับข้อมูลที่เขียนลงไปบนสื่อบันทึกจะมีบิตเปลี่ยนสถานะเกิดขึ้อย่างสม่ำเสมอเพียงพอ เพื่อที่จะทำให้ระบบไทมมิ่งริคัฟเวอะรีสามารถทำงานได้อย่างมีประสิทธิภาพ อัตรารหัส $R = m/n \leq 1$ โดยที่อัตรารหัสที่ใช้จะมีค่าประมาณ 8/9 (0.89) หรือสูงกว่า

3) วงจรมอดูเลเตอร์ (Modulator) จะทำหน้าที่แปลงข้อมูลให้อยู่ในรูปคลื่นกระแสไฟฟ้าสี่เหลี่ยมที่เรียกกันว่ากระแสไฟฟ้าเขียน (write current) จากนั้นกระแสไฟฟ้าเขียนจะถูกป้อนไปยังขดลวดของหัวเขียนทำให้เกิดสนามแม่เหล็ก เพื่อที่จะทำให้สื่อบันทึก ณ บริเวณนั้นมีสภาพความเป็นแม่เหล็กตามทิศทางที่ต้องการ

4.2.1 แนวทางการกำหนดพารามิเตอร์ที่ใช้ในการจำลองระบบ

จากแบบจำลองระบบบันทึกข้อมูลเชิงแม่เหล็กแสดงดังรูปที่ 4.2 ระบบบันทึกข้อมูลเชิงแม่เหล็กโดยทั่วไปจะทำการเขียนข้อมูลเป็นบล็อก ซึ่งบล็อกดังกล่าวจะเรียกว่า เซคเตอร์ หนึ่งบล็อก หรือหนึ่งเซคเตอร์จะมีขนาดเท่ากับ 512 ไบต์ หรือประมาณ 4096 บิต ในขณที่รหัสแอลดีพีซีจะกำหนดให้ทำหน้าที่เป็นรหัสแก้ไขข้อผิดพลาด โด ยวางในตำแหน่งแทนที่ของวงจรเข้ารหัสมอดูเลชัน ซึ่งอัตรารหัสที่ใช้ในระบบบันทึกข้อมูลเชิงแม่เหล็กจะอยู่ที่ 8/9 (0.89) หรือสูงกว่า อัตราบิตผิดพลาดของข้อมูลที่ยอมรับได้ ณ ตำแหน่งนี้อยู่ที่ 10^{-5}

ด้วยเหตุนี้วิทยานิพนธ์ฉบับนี้ นำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์ที่ความยาวคำรหัสประมาณ 4096 บิต และอัตรารหัส มากกว่าหรือเท่ากับ 0.89 อัตราบิตผิดพลาดของข้อมูลที่ยอมรับได้อยู่ที่ 10^{-5} ซึ่งสอดคล้องกับระบบบันทึกข้อมูลเชิงแม่เหล็ก

4.3 สมรรถนะของระบบ

ในการจำลองสมรรถนะของระบบจะพิจารณาในสามหัวข้อดังนี้

1) การเปรียบเทียบสมรรถนะของอัตราความผิดพลาดบิตข้อมูลของรหัสแอลดีพีซีแบบมอดดิอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

2) สมรรถนะของอัตราความผิดพลาดบิตต่อจำนวนรอบการวนลูปที่อัตรารหัสสูง

3) การหาค่าพารามิเตอร์ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง

4.3.1 การเปรียบเทียบสมรรถนะของอัตราความผิดพลาดบิตข้อมูลของรหัสแอลดีพีซีแบบมอดดิอาร์เรย์และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

สำหรับรหัสอาร์เรย์แบบมอดดิฟายอาร์เรย์และ อินเตอร์ลีฟมอดดิฟายอาร์เรย์ อธิบายได้ด้วยพารามิเตอร์ 3 ค่าได้แก่ จำนวนเฉพาะ p และจำนวนเต็ม j และ k โดยที่ $j \le k \le p$ ความยาวข้อมูลอินพุตเท่ากับ $p(k-j)$ ความยาวคำรหัสเท่ากับ kp จำนวนพาริตี้เช็คเท่ากับ jp และอัตรารหัสมีค่าเท่ากับ $(1-j/k)$

การออกแบบจะเริ่มจากกำหนดค่าอัตรารหัส และความยาวคำรหัสที่ต้องการ ซึ่งในที่นี้จะกำหนดค่าประมาณ 4,000-4,100 บิต ในขณะที่อัตรารหัสจะออกแบบตั้งแต่อัตรารหัสปานกลางไปจนถึงอัตรารหัสสูง คือ 0.5-0.92 (เพื่อเปรียบเทียบสมรรถนะการทำงานกับรหัสมอดดิฟายอาร์เรย์) ตารางที่ 4.1 แสดงค่าที่ได้จากการออกแบบ

ตารางที่ 4.1 พารามิเตอร์ที่ใช้ในการจำลองระบบรหัสแอลดีพีซีแบบอาร์เรย์

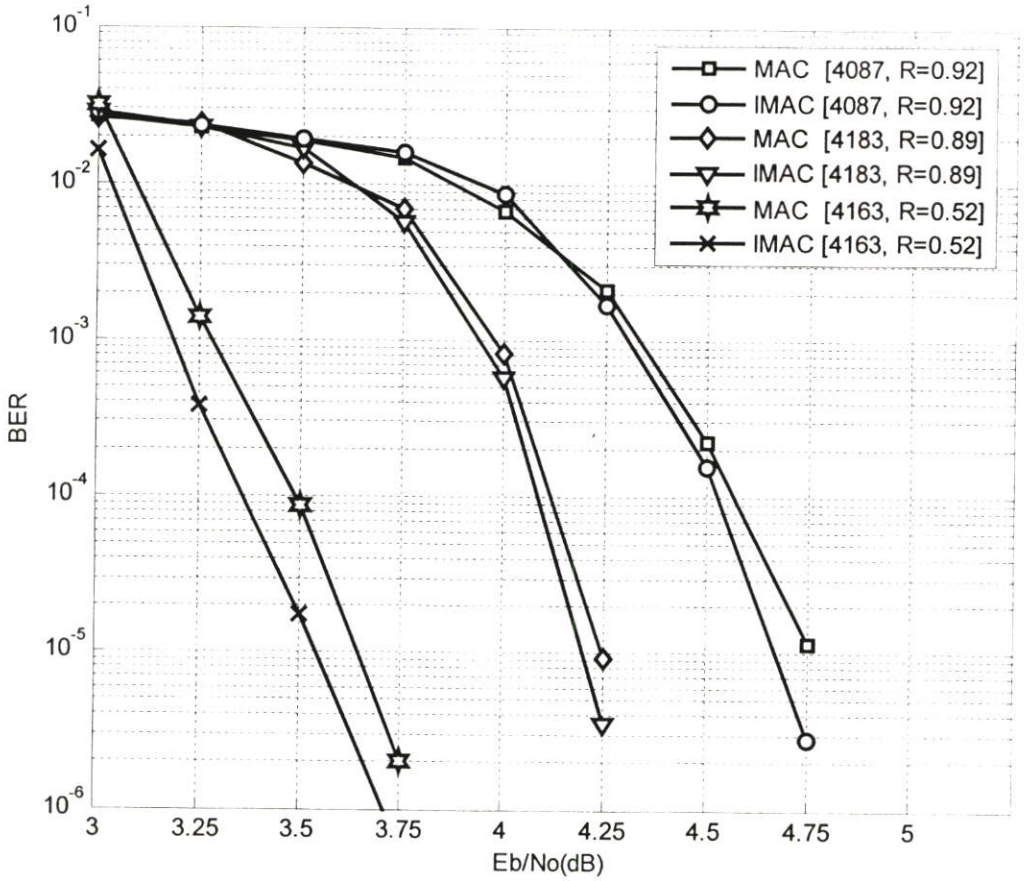
พารามิเตอร์	MAC	IMAC	MAC	IMAC	MAC	IMAC
j	5	←	5	←	11	←
k	61	←	47	←	23	←
p	67	←	89	←	181	←
อัตรารหัส $(1-j/k)$	0.92	←	0.89	←	0.52	←
ข้อมูลอินพุต $p(k-j)$	3,752	←	3,738	←	2,172	←
พาริตี้บิต jp	335	←	445	←	1,991	←
คำรหัส kp	4,087	←	4,183	←	4,163	←
รอบการวนลูป	30	←	←	←	←	←

จากตารางที่ 4.1 จะพบว่าที่อัตรารหัสสูงค่า j จะมีขนาดเล็กเมื่อเทียบกับค่าพารามิเตอร์ k และ p แต่เมื่ออัตรารหัสลดลงค่า j และ p จะสูงขึ้นขณะที่ k ลดลง

ในรูปที่ 4.3 แสดงถึงตัวอย่างผลของการจำลองระบบที่ได้จากการออกแบบค่าพารามิเตอร์ในตารางที่ 4.1 กับแบบจำลองการทำงานในรูปที่ 4.1 โดยผลการจำลองเป็นการเปรียบเทียบสมรรถนะของอัตราความผิดพลาดบิตข้อมูลระหว่างรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ที่ความยาวคำรหัส 4,000-4,100 บิต กับอัตรารหัสจำนวน 3 แบบ คือ 0.52, 0.89 และ 0.92 ที่จำนวนรอบการวนลูปเท่ากับ 30 รอบ

จากผลของอัตราความผิดพลาดข้อมูลเมื่อพิจารณาจากอัตรารหัสจะพบว่า ที่อัตรารหัส 0.92 จะมีค่าสมรรถนะต่ำกว่าที่อัตรารหัส 0.89 และ 0.52 ตามลำดับ โดยพารามิเตอร์ที่มีความแตกต่างกันคือค่า p ซึ่งค่า p จะแปรผกผันกับอัตรารหัส กล่าวคือถ้าอัตรารหัสสูงค่า p จะต่ำถ้า

อัตรารหัสต่ำ ค่า p จะสูง ตามที่สมรรถนะของการถอดรหัสจะขึ้นกับระยะห่างต่ำสุดของคำรหัส ดังนั้นจึงมีความเป็นไปได้ว่า รหัสที่มีค่า p ค่อนข้างสูงจะเป็นรหัสที่มีค่าระยะห่างต่ำสุดของคำรหัสมากกว่ารหัสที่มีค่า p ที่ต่ำกว่า พิจารณาสมรรถนะอัตราความผิดพลาดบิตข้อมูลระหว่างรหัสมอดดิฟายอาร์เรย์ และ อินเตอร์ลีฟมอดดิฟายอาร์เรย์ จะพบว่ารหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์ จะมีค่าอัตราความผิดพลาดบิตข้อมูลดีกว่าในทุกอัตรารหัส โดยจะมีค่าที่ดีกว่าในทุกอัตราส่วนต่อสัญญาณสัญญาณรบกวน สำหรับอัตรารหัส 0.52 ในขณะที่อัตรารหัส 0.89 และ 0.92 อัตราความผิดพลาดบิตจะต่ำกว่าที่อัตราส่วนต่อสัญญาณสัญญาณรบกวน เท่ากับ 4.25 dB และ 4.75 dB ตามลำดับ



รูปที่ 4.3 แสดงสมรรถนะของอัตราความผิดพลาดบิตข้อมูลของรหัสแอลดีพีซีแบบมอดดิอาร์เรย์และอินเตอร์ลีฟมอดดิฟายอาร์เรย์

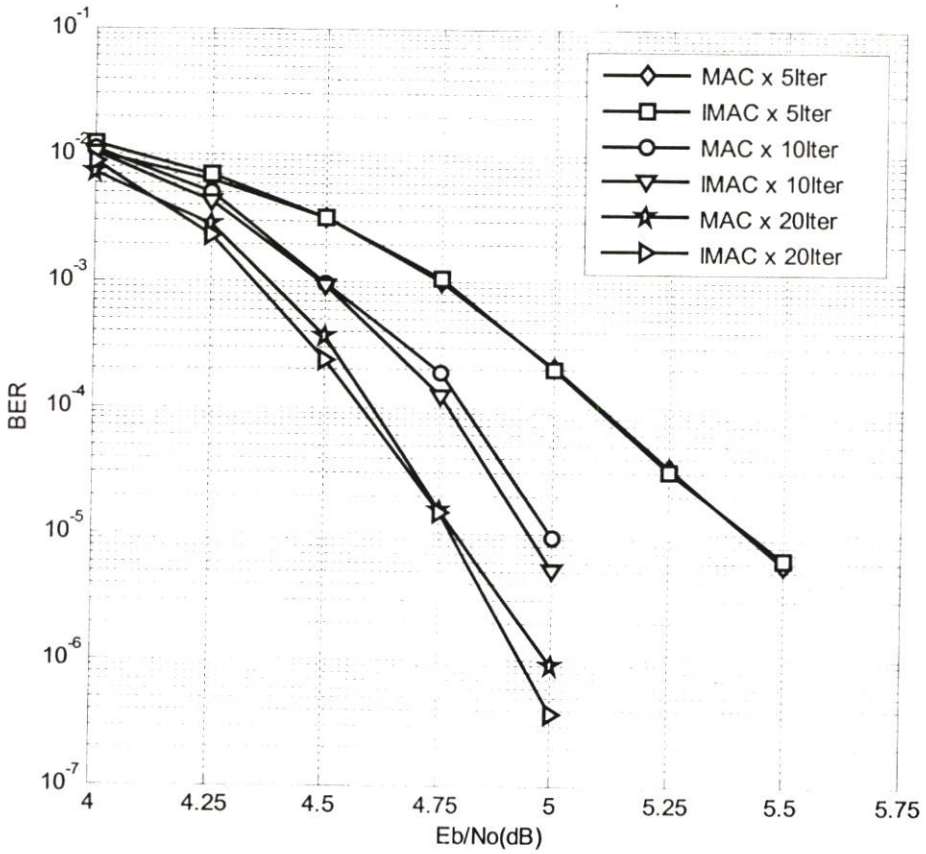
4.3.2 สมรรถนะของอัตราความผิดพลาดบิตต่อจำนวนรอบการวนลูปที่อัตรารหัสสูง

หัวข้อ 4.3.2 จะแสดงสมรรถนะของอัตราความผิดพลาดบิตข้อมูลของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ต่อผลกระทบของอัตราความผิดพลาดบิตข้อมูลกับจำนวนรอบในการวนลูป

กำหนดค่าอัตรารหัสโดยใช้พารามิเตอร์ j , k และ p เท่ากับ 5, 61 และ 67 ตามลำดับ ความยาวคำรหัส 4,087 บิต ความยาวข้อมูลอินพุตเท่ากับ 3,752 บิต จำนวนพาริตี้บิตเท่ากับ 335 บิต และอัตรารหัสมีค่าเท่ากับ 0.92 ทำการปรับค่าจำนวนรอบการวนลูปที่ 5, 10 และ 20 ตามลำดับ ตารางที่ 4.2 แสดงค่าที่ใช้ในการจำลองการทำงานระบบ

ตารางที่ 4.2 พารามิเตอร์ที่ใช้ในการจำลองระบบรหัสแอลดีพีซีแบบอาร์เรย์ต่อผลกระทบของอัตราความผิดพลาดบิตข้อมูลกับจำนวนรอบในการวนลูป

พารามิเตอร์	MAC	IMAC
j	5	←
k	61	←
p	67	←
อัตรารหัส $(1-j/k)$	0.92	←
ข้อมูลอินพุต $p(k-j)$	3,752	←
พาริตี้บิต jp	335	←
คำรหัส kp	4,087	←
รอบการวนลูป	5 /10 /20	←



รูปที่ 4.4 แสดงสมรรถนะของอัตราความผิดพลาดบิตข้อมูลต่อจำนวนรอบการวนลูป

ผลของอัตราความผิดพลาดบิตระหว่างรหัสมอดดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ พบว่าที่จำนวนรอบการวนลูปเท่ากับ 5 จะไม่มีความแตกต่างของอัตราความผิดพลาดบิตข้อมูลระหว่างรหัสทั้งสองแบบ ในขณะที่เมื่อจำนวนรอบการวนลูปเพิ่มขึ้นเป็น 10 และ 20 จะเห็นความแตกต่างของอัตราความผิดพลาดบิตของรหัสทั้งสองแบบ โดยรหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์จะมีค่าอัตราความผิดพลาดบิตข้อมูลดีกว่า

4.2.3 การหาค่าพารามิเตอร์ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง

จากผลการทดลองในข้อที่ 4.3.1 ซึ่งตั้งสมมุติฐานที่ว่ามีความเป็นไปได้ว่า รหัสที่มีค่า p ค่อนข้างสูงจะเป็นรหัสที่มีค่าระยะห่างต่ำสุดของคำรหัสมากกว่ารหัสที่มีค่า p ที่ต่ำกว่า ดังนั้นในหัวข้อนี้จะเป็นการหาค่าพารามิเตอร์ p ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง โดยจะทำการจำลองผลกระทบของขนาดพารามิเตอร์ p ต่ออัตราความผิดพลาดบิตข้อมูลกับรหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์

การออกแบบจะเริ่มจากกำหนดค่าอัตรารหัสไว้ที่ 0.89 และกำหนดความยาวคำรหัสที่ใกล้เคียงกันจำนวน 3 ค่า แต่มีค่าพารามิเตอร์ p ที่ต่างกัน ตารางที่ 4.3 แสดงค่าที่ได้จากการออกแบบ

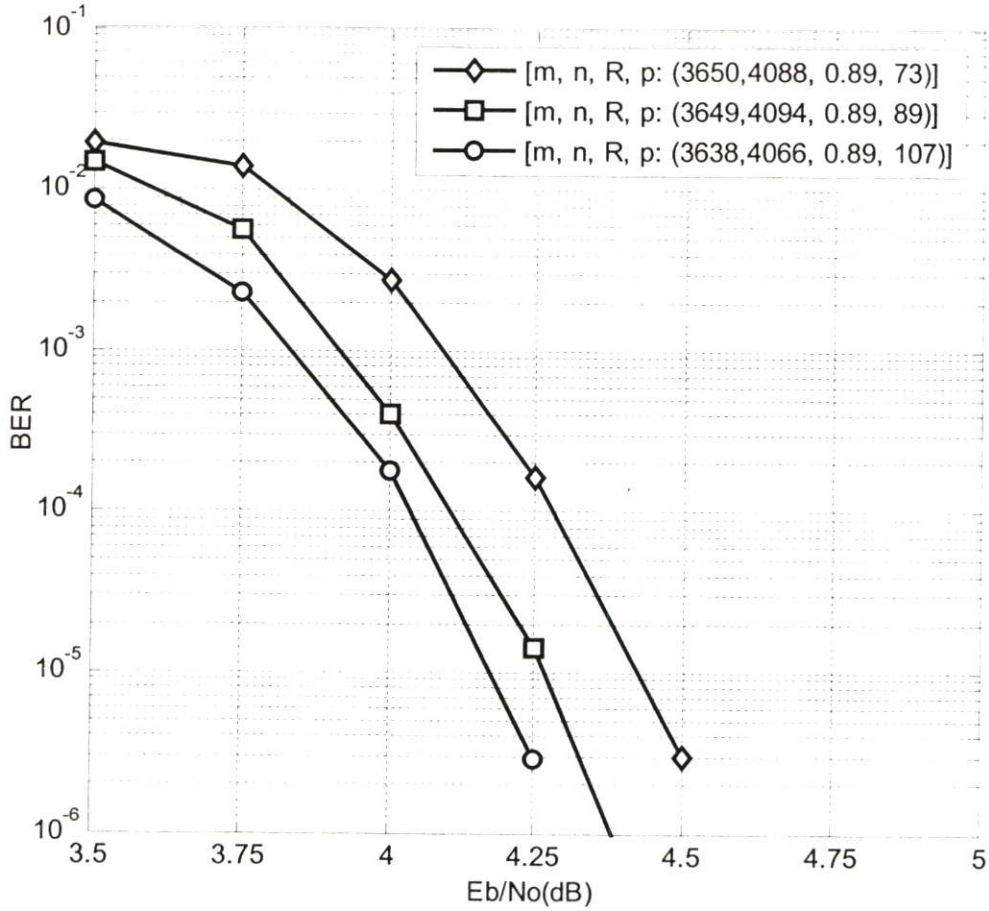
ตารางที่ 4.3 การหาค่าพารามิเตอร์ p ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง

พารามิเตอร์	IMAC		
j	4	5	6
k	38	46	56
p	107	89	73
อัตรารหัส $(1-j/k)$	0.89	0.89	0.89
ข้อมูลอินพุต $p(k-j)$	3,638	3,649	3,650
พาริตี้บิต jp	428	445	438
คำรหัส kp	4,066	4,094	4,088
รอบการวนลูป	30	←	←

จากตารางที่ 4.3 จะพบว่าค่า p จะแปรผกผันกับค่า k ที่รหัสที่มีค่า p ค่อนข้างสูงค่า k จะต่ำ ในขณะที่ค่า p ต่ำลงค่า k จะสูงขึ้น

ในรูปที่ 4.5 แสดงถึงผลการจำลองผลกระทบของขนาดพารามิเตอร์ p ต่ออัตราความผิดพลาดบิตข้อมูลกับรหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์

จากผลของอัตราความผิดพลาดข้อมูลจะพบว่าขนาดของพารามิเตอร์ p มีผลต่อสมรรถนะอัตราความผิดพลาดบิตข้อมูลอย่างชัดเจน เมื่อพิจารณาจากค่า p เท่ากับ 73 พบว่าจะมีค่าอัตราความผิดพลาดข้อมูลที่สูงกว่า รหัสที่ใช้ค่า p เท่ากับ 89 และ 107 ในทุกอัตราส่วนต่อสัญญาณสัญญาณรบกวน โดยที่รหัสที่มีค่า p เท่ากับ 107 จะให้ค่าอัตราอัตราความผิดพลาดบิตข้อมูลที่ต่ำที่สุด และเมื่อพิจารณาค่าอัตราความผิดพลาดบิตข้อมูลที่ 3×10^{-6} อัตราขยายการเข้ารหัสที่พารามิเตอร์ p เท่ากับ 107 จะต่ำกว่าที่พารามิเตอร์ p เท่ากับ 89 และ 73 ประมาณ 0.1 dB และ 0.25 dB ตามลำดับ



รูปที่ 4.5 การจำลองผลกระทบของขนาดพารามิเตอร์ p ต่ออัตราความผิดพลาดบิตข้อมูล

ในบทที่ 4 ได้ทำการออกแบบรหัสแอลดีพีซีชนิดอาร์เรย์ทั้งแบบมอดิฟายอาร์เรย์ และอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ที่อัตรารหัส และความยาวคำรหัสสอดคล้องกับระบบบันทึกข้อมูลเชิงแม่เหล็ก และจำลองสมรรถนะของอัตราความผิดพลาดบิตข้อมูลต่อจำนวนรอบการวนลูปที่อัตรารหัสสูง ผลการทดลองแสดงให้เห็นว่าอัตราความผิดพลาดบิตข้อมูลของรหัสแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์มีค่าต่ำกว่าในกรณีของรหัสมอดดิฟายอาร์เรย์ ซึ่งมีความเหมาะสมที่จะนำไป

อัตรารหัสสูง ผลการทดลองแสดงให้เห็นว่าอัตราความผิดพลาดบิตข้อมูลของรหัสแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์มีค่าต่ำกว่าในกรณีของรหัสมอดดิฟายอาร์เรย์ ซึ่งมีความเหมาะสมที่จะนำไปใช้งานต่อแต่จำเป็นจะต้องทำการทดลองเพิ่มเติมบนช่องสัญญาณแบบเสมือนจริง จากนั้น ทำการจำลองผลกระทบของขนาดพารามิเตอร์ p ต่ออัตราความผิดพลาดบิตข้อมูลกับรหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์ภายใต้สมมุติฐานที่ว่ารหัสที่มีค่า p สูงจะเป็นรหัสที่มีค่าระยะห่างต่ำสุดของคำรหัสมากกว่ารหัสที่มีค่า p ที่ต่ำกว่า จากผลการทดลองพบว่าขนาดของพารามิเตอร์ p มีผลต่อสมรรถนะอัตราความผิดพลาดบิตข้อมูลอย่างชัดเจน จึงเชื่อได้ว่ารหัสที่มีค่า p ค่อนข้างสูงจะเป็นรหัสที่มีค่าระยะห่างต่ำสุดของคำรหัสมากกว่ารหัสที่มีค่า p ที่ต่ำกว่า ซึ่งสามารถใช้เป็นแนวทางในการหาค่าพารามิเตอร์ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง

บทที่ 5
สรุปผลการวิจัย และข้อเสนอแนะ

เทคนิคในการเข้ารหัสช่องสัญญาณที่ใช้อัลกอริทึมในการถอดรหัสแบบวนซ้ำ กำลังเป็นเทคนิคที่กำลังได้รับความสนใจในการประยุกต์ใช้เป็นรหัสในการแก้ไขความผิดพลาด ของข้อมูลสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็กแทนที่ระบบปัจจุบันที่กำลังใช้งานอยู่ อันเนื่องมาจากสมรรถนะอัตราความผิดพลาดบิตข้อมูลของรหัสที่ใช้การถอดรหัสแบบวนซ้ำ ดีกว่ารหัสที่ใช้การถอดรหัสแบบไม่วนซ้ำ

รหัสเทอร์โบ และรหัสแอลดีพีซีก็เป็นรหัสแก้ไขความผิดพลาดที่ใช้อัลกอริทึมในการถอดรหัสแบบวนซ้ำ ซึ่งมีสมรรถนะการทำงานที่เข้าใกล้ลิมิตของแชนนอล อย่างไรก็ดีมีงานวิจัยหลายฉบับได้วิเคราะห์ว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานที่ดีกว่ารหัสเทอร์โบที่ ขนาดความยาวคำรหัสสูง ตัวอย่างเช่นงานวิจัยของ Richardson T.J [7]

วิทยานิพนธ์ฉบับนี้นำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์ สำหรับการประยุกต์ ใช้งานในระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยเน้นรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ของ E. Eleftheriou [4] ที่มีคุณสมบัติที่ระบบบันทึกข้อมูลเชิงแม่เหล็กต้องการ เช่น มี Error floor ที่ต่ำ ปราศจากไซเคิลขนาดเท่ากับ 4 และความสามารถในการแก้ไขความผิดพลาดแบบหลายบิตติดกัน (burst error) [11] และนำเสนอรหัสมอดดิฟายอาร์เรย์ที่เรียกว่า อินเตอร์ลีฟมอดดิฟายอาร์เรย์ซึ่งเป็นหลักการใหม่ที่นำเสนอ แต่ยังคงสามารถใช้โครงสร้างการถอดรหัสแบบเดียวกับรหัสแอลดีพีซีแบบทั่วไปได้ อีกทั้งยังคงคุณสมบัติที่ดีของรหัสมอดดิฟายอาร์เรย์ เช่น มี Error floor ที่ต่ำและปราศจากไซเคิลขนาดเท่ากับ 4 จากนั้นนำเสนอการออกแบบรหัสแอลดีพีซีแบบอาร์เรย์ที่ความยาวคำรหัสประมาณ 4096 บิต และอัตรารหัสสูง ซึ่งสอดคล้องกับระบบบันทึกข้อมูลเชิงแม่เหล็ก จากผลการจำลองสรรถนะการทำงานพบว่าค่าอัตราความผิดพลาดบิตข้อมูลของรหัสแบบอินเตอร์ลีฟมอดดิฟายอาร์เรย์ ต่ำกว่าในกรณีรหัสมอดดิฟายอาร์เรย์ตั้งแต่อัตรารหัสปานกลางไปจนถึงอัตรารหัสสูงบนช่องสัญญาณรบกวนเกาส์แบบขาว จากนั้นทำการหาค่าพารามิเตอร์ที่เหมาะสมสำหรับรหัสแอลดีพีซีแบบอาร์เรย์ที่อัตรารหัสสูง

ในงานวิจัยต่อไปจึงควรจะเป็นการศึกษาการทำงานของรหัสแอลดีพีซีแบบมอดดิฟายอาร์เรย์ และรหัสอินเตอร์ลีฟมอดดิฟายอาร์เรย์บนช่องสัญญาณแบบเสมือนจริง (Realistic magnetic recording channel model) ของระบบบันทึกข้อมูลเชิงแม่เหล็กที่ใช้การบันทึกข้อมูลแบบแนวตั้ง ซึ่งเป็นระบบบันทึกข้อมูลแบบล่าสุด ซึ่งจะมีปัญหาในเรื่องการแทรกสอดระหว่างสัญลักษณ์ และสัญญาณรบกวนบนสื่อบันทึก (media noise) จึงจำเป็นที่จะต้องพิจารณาการทำงานร่วมกันระหว่างรหัสช่องสัญญาณและตัวอิควอไลซ์แบบเทอร์โบ (Turbo equalizer)

บรรณานุกรม

[1] C. Berrou, A. Glanvieux and P. Thitimajshima, "**Near Shannon limit error-correcting coding and decoding: Turbo Codes**," in Proc. IEEE Intl. Conf, pp. 1064-1070, May 1993.

[2] D.J.C. Mackey and R. Neal "**Near Shannon limit performance of low density parity check codes**," Electronics Letters, vol.33, pp. 457-458, Mar 1997.

[3] J. L. Fan, "**Array codes as low-density parity-check codes**," in Proc. 2nd Int. Symp. Turbo Codes, Best, France, pp 543-546, Sep 2000.

[4] E. Eleftheriou and S. Olcer, "**Low-density parity check codes for digital subscriber lines**," Proc. 2002 Int. Conf. on Comm., pp.1752-1757., April – May, 2002.

[5] R. Gallager, "**Low-density parity-check codes**," IRE Trans. Information Theory, pp. 21-28, Jan 1962

[6] R. M. Tanner, "**A recursive approach to low complexity codes**," IEEE Trans. Information Theory, pp.533-547, Sept. 1981.

[7] Richardson T.J., Shokrollahi MA, Urbanke R.L. "**Design of capacity-approaching irregular low-density parity-check codes**," Information Theory IEEE Trans.volume 47, pp.619-637, Feb 2001.

[8] M. Chai and A. Ventura, **"Design and Performace evaluation of some high-rate irregular low-density parity-check codes**," Proc. 2001 IEEE GlobeCom Conf., pp. 990 –994, Nov. 2001.

[9] M. Yang and W. E. Ryan, "**Lowering the error rate floors of moderate-length high rate LDPC codes,"** Proc. 2003 Int. Symp. On Inf. Theory, Jun-July 2003.

[10] Oenning, T.R.; Jaekyun Moon "**Low density parity check coding for magnetic recording channels with media noise**" IEEE International Conference, pp.2189-2193, June 2001.

[11] ผศ.ดร.พรชัย ทรัพย์นิธิ, "การสื่อสารดิจิตอล," คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, พ.ศ. 2549

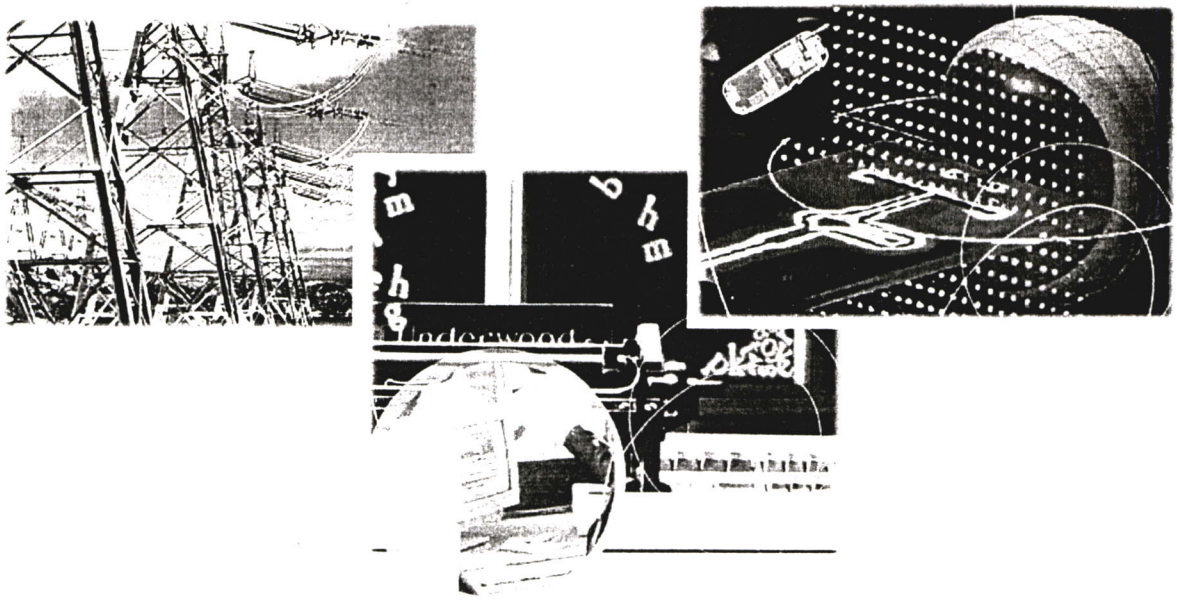
[12] ดร.ปิยะ โควินท์ทวีวัฒน์, "การประมวลสัญญาณสำหรับการจัดเก็บข้อมูลดิจิตอล," คณะวิทยาศาสตร์ และเทคโนโลยี มหาลัยราชภัฏนครปฐม, พ.ศ. 2550

ภาคผนวก

ภาคผนวก ก

บทความที่ได้รับการตีพิมพ์เผยแพร่

1. W. Singhaudom, S. Noppanakeepong, P. Supnithi, "**Design of High-Rate Modified Array Codes for Magnetic Recording System**," ECTI-CON 2007, Chiang Rai, Thailand, May 9-12, 2007.

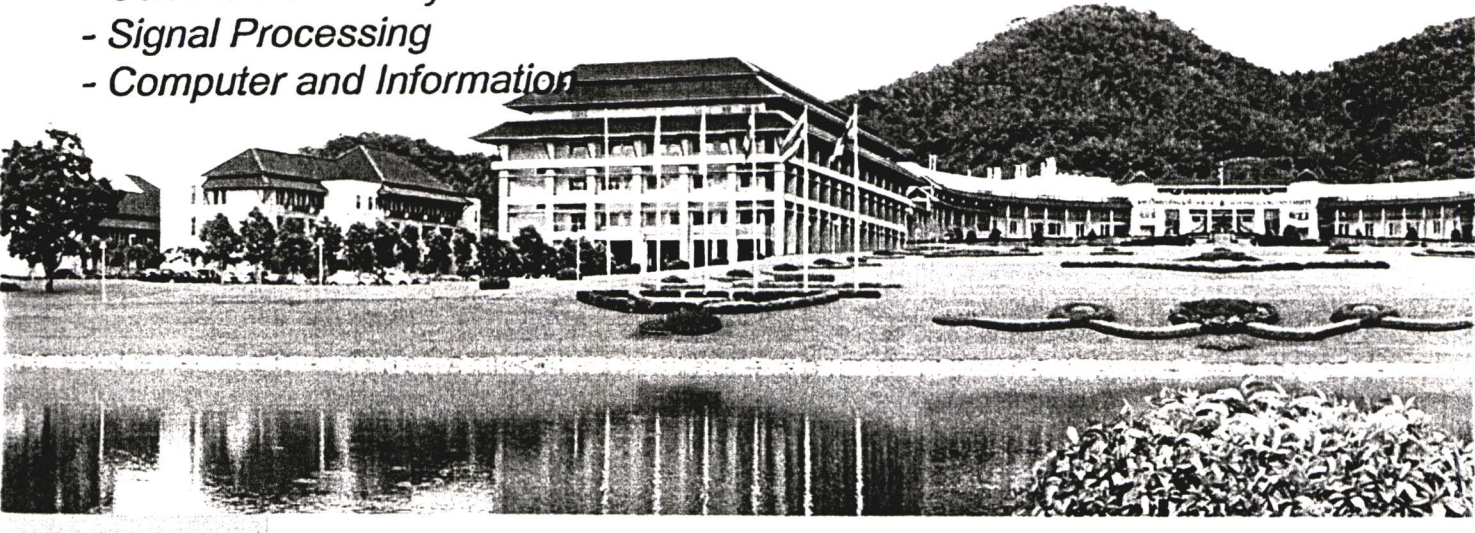


ECTI-CON 2007

Mae Fah Luang University, Chiang Rai, Thailand
May 9-12, 2007

VOLUME 1
- *Circuits and Systems*
- *Control Engineering*
- *Electrical Power Engineering*
- *Other Related Fields*

VOLUME 2
- *Communication Systems*
- *Signal Processing*
- *Computer and Information*



ECTI Association

IEEE THAILAND SECTION

NECTEC a member of NSTDA

WD Western Digital

Design of High-Rate Modified Array Codes for Magnetic Recording System

W. Singhaudom, S. Noppanakeepong, P. Suphithi,
Faculty of Engineering, and Research Center for Communications and Information Technology (ReCCIT)
and I/U CRC in Data Storage Technology and Applications
King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bankok 10520, THAILAND
Email: s5061230@kmitl.ac.th, knsuthic@kmitl.ac.th, ksupornc@kmitl.ac.th

***Abstract*- In applying iterative decoding methods to magnetic recording systems, the high-rate code must be considered. This paper presents design of high-rate Modified Array Codes, a type of Low Density Parity Check (LDPC) Codes, that have been known to possess many advantages required in magnetic recording system such as low error floor, capability of detecting and correcting burst error.**

***Index Terms*- Modified Array Codes, Low-density parity-check codes, high-rate codes, Magnetic recording.**

I. INTRODUCTION

Iterative decoding techniques of error correcting codes in magnetic recording system have been of great interest to replace the conventional error correcting codes. Turbo codes and Low Density Parity Check Codes (LDPC) utilize iterative decoding method which shows performance results close to the Shannon limit [1], [2]. However, many researches found that LDPC codes have better outperform Turbo codes for large block size such as [9].

In magnetic recording systems, higher-rate codes must be considered. One reason is that the internal clock rates of read channels inversely scale with code rate. A low code rate, therefore, means a large disadvantage in practice in hardware design. Furthermore, due to thermal instabilities in the media at high area densities, it may not be possible to reliably record at the higher symbol densities required by low code rates [4].

Recently, a type of LDPC codes coined "Modified Array Codes" is proposed [7] for use in communication system for medium code rate. The code is shown to have performance similar to regular/irregular LDPC codes, but possess attractive properties such as simple encoding, low error floor and capability of detecting and correcting burst error.

In this paper, we present a design of Modified Array Codes for high-rate applications such as magnetic recoding system. We show two sets of codes for block sizes common in magnetic recording systems. The effect of permutation matrix size is studied and together with iterative processing, coding gain is achieved.

II. LOW-DENSITY PARITY CHECK (LDPC) CODES

An LDPC code is a binary linear block code defined by a spare parity check matrix. It can be represented by the Bipartite Graph [5]. Suppose that a parity-check matrix **H** has n columns and m rows, and the codeword consists of n bits, which satisfy m checks, the number of message bits will be $k=(n-m)$, and the rate of code is $R_c = k/n$. The number 1's in the parity check matrix in rows and columns represents an edge between the $i-th$ bit node c_i and the $j-th$ check node f_j.

An example of the parity check matrix **H** of a LDPC code of dimension (m,n) = (3, 7) is shown in Eq. (1).

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}_{m \times n} \quad (1)$$

The Bipartite or Tanner graph representing the LDPC code can be constructed as shown in Fig. 1.

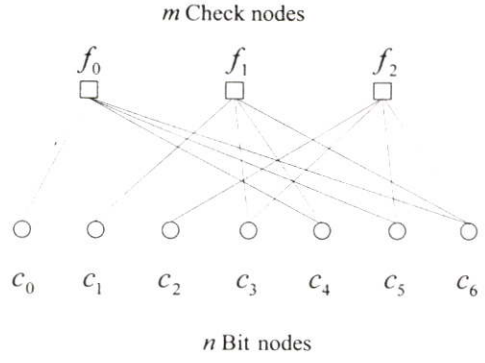


Figure 1. Bipartite or Tanner graph for LDPC code

A disadvantage of general LDPC code is that significant amount of memory is needed to store the parity-check matrix **H** due to long input message bits. An Array Code is a structured LDPC code which solves the memory problem since their parity-check matrix consists of the circulant permutation matrices and the identity matrices. In fact, the required memory for storing them can be reduced by a factor $1/p$, when $p \times p$ circulant permutation matrices are employed. Moreover, Array codes have capability to detecting and correcting burst error [6].

A. Modified Array Codes

To achieve efficient encoding and minimum distance properties, Eleftheriou [7] proposed a new Array Codes which is known as "Modified Array Codes". A parity-check matrix **H** of a modified array codes can be described in terms of the parameter (p, j, k) and has the form

$$\mathbf{H}(p,j,k)\triangleq\begin{bmatrix}\mathbf{I} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} & \cdots & \mathbf{I}\\ \mathbf{0} & \mathbf{I} & \mathbf{P} & \cdots & \mathbf{P}^{(j-2)} & \cdots & \mathbf{P}^{(k-2)}\\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{P}^{2(j-3)} & \cdots & \mathbf{P}^{2(k-3)}\\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots\\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{P}^{(j-1)(k-j)}\end{bmatrix},$$

where p is prime and $j \le k \le p$, $\mathbf{0}$ is the p x p null matrix and $\mathbf{I}$ is the p x p identity matrix. The matrix $\mathbf{P}$ is a p x p circulant permutation matrix which shifts the identity matrix $\mathbf{I}$ to the right once given in Eq. (2). The permutation matrix can be used to shift the multiplied matrix to the right by i times for any integer i, $0 \le i < p$.

$$\mathbf{P}=\begin{bmatrix}0 & 1 & 0 & & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \cdots & 1\\ 1 & 0 & 0 & & 0\end{bmatrix} \qquad (2)$$

In [7], it is shown that for a modified array code, the minimum distance $d_{\min} = 6$ for $j = 3$ and $d_{\min} \ge 8$ for j = 4. Efficient encoding is achieved from $\mathbf{H}$ without the need to compute the generator matrix of the code. As the upper triangular form of $\mathbf{H}$, there are no cycles of length 4 in the corresponding Tanner graph.

The Modified Array Codes defined by $\mathbf{H}$ has codeword length $N = k \cdot p$, number of parity bit $M = j \cdot p$ and message block length $K = p \cdot (k - j)$ and finally, code rate is $R = 1 - j/k$.

B. Cycles of Modified Array Codes

To understand the cycle properties of Modified Array Codes, we will consider the following a more general from of a parity check matrix $\mathbf{H}$, i.e.,

$$\mathbf{H}=\begin{bmatrix}\mathbf{P}^{a_0\cdot 0} & \mathbf{P}^{a_0\cdot 1} & \mathbf{P}^{a_0\cdot 2} & \cdots & \mathbf{P}^{a_0\cdot p-1}\\ \mathbf{0} & \mathbf{P}^{a_1\cdot 1} & \mathbf{P}^{a_1\cdot 2} & \cdots & \mathbf{P}^{a_1\cdot p-1}\\ \mathbf{0} & \mathbf{0} & \mathbf{P}^{a_2\cdot 2} & \cdots & \mathbf{P}^{a_2\cdot p-1}\\ \vdots & \vdots & \vdots & \cdots & \cdots\\ \mathbf{0} & \mathbf{0} & \cdots & \cdots & \mathbf{P}^{a_{j-1}\cdot p-1}\end{bmatrix} \qquad (3)$$

A cycle of length 2k exits in the Tanner graph of Modified Array Codes with the parity check matrix $\mathbf{H}$ and block row labels $a_0, a_1, \ldots, a_{j-1}$ if and only if there exists a close path

$$(i_1, j_1), (i_1, j_2), (i_2, j_2), (i_2, j_3), \ldots, (i_k, j_k), (i_k, j_1).$$

The possible cycles in $\mathbf{H}$ is 2k times, and then the length of the cycles in the permutation is described as shown below.

$$\mathbf{P}^{a_{i_1}\cdot j_1}\left(\mathbf{P}^{a_{i_1}\cdot j_2}\right)^{-1}\mathbf{P}^{a_{i_2}\cdot j_2}\left(\mathbf{P}^{a_{i_2}\cdot j_3}\right)^{-1}\cdots\mathbf{P}^{a_{i_k}\cdot j_k}\left(\mathbf{P}^{a_{i_k}\cdot j_1}\right)^{-1}$$

From the result of short cycles properties in [8], the cycles of length 4 depends on the following permutation,

$$\mathbf{P}^{a_{i_1}\cdot j_1}\left(\mathbf{P}^{a_{i_1}\cdot j_2}\right)^{-1}\mathbf{P}^{a_{i_2}\cdot j_2}\left(\mathbf{P}^{a_{i_2}\cdot j_1}\right)^{-1} = \mathbf{P}^{(a_{i_1}-a_{i_2})(j_1-j_2)}$$

which is exact when it is equal to 1. This occurs when $(a_{i_1} - a_{i_2})(j_1 - j_2) \equiv 0$, which is clearly impossible since $i_1 \ne i_2$ and $j_1 \ne j_2$. Hence, there are no cycles of length 4 for Modified Array Codes.

III. THE SUM-PRODUCT ALGORITHM (SPA)

The sum-product algorithm (SPA) is a soft iterative decoding algorithm most commonly used to decode LDPC codes [2-3]. Given that y_i is the i^{th} received channel value corresponding to the i^{th} transmitted codeword c_i. Input of LDPC decoder is in the form of log likelihood ratios (LLRs) $L(c_i) = \log(P(c_i = 0 \mid y_i)/P(c_i = 1 \mid y_i))$.

From Fig 2, the basic operation in the decoding algorithm is shown. In the Tanner graph, the check nodes and bit nodes interchange soft information. Let the variable q_{ij} be the message (information) sent from the i^{th} bit node to j^{th} check node along a connecting edge, and r_{ji} is the message (information) sent from j^{th} check node to the i^{th} bit node along a connection edge. The information q_{ij} is computed based on the values sent from check nodes connecting to the i^{th} bit node excluding the j^{th} bit node.

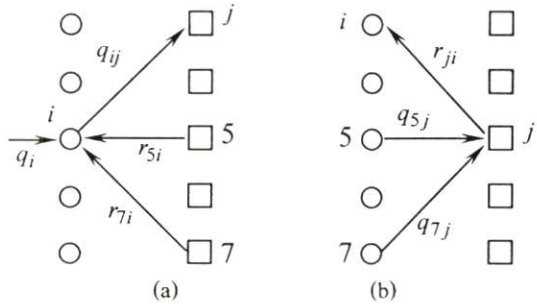


Figure 2. (a) A message is passed from i^{th} bit node to j^{th} check node and (b) A message is passed from the j^{th} check node to the i^{th} bit node.

The Operation of Log-Domain SPA Decoder

The operation of log-domain SPA decoder consists 5 steps, i.e.,

Step 1: Initialization. The LLR value of q_{ij} is set to be equal to the LLR value of the received channel values computed from

$$L(q_{ij}) = L(c_i) = 2y_i/\sigma^2, \qquad (4)$$

where σ^2 is variance of Gaussian noise.

Step 2: Update equation for the message from check nodes to bit nodes given by

$$L(r_{ij}) = \prod_{i' \in V_j \setminus i} \alpha_{i'j} \cdot \phi\left(\sum_{i' \in V_j \setminus i} \phi(\beta_{i'j}) \right), \quad (5)$$

where $\alpha_{ij} = \mathrm{sgn}\{L(q_{ij})\}$, $\beta_{ij} = |L(q_{ij})|$ and define $\phi(x) = \log\{(e^x + 1)/(e^x - 1)\}$ with the base of e. In addition, $V_{j\setminus i}$ represents all the bit nodes except the i^{th} bit node.

Step 3: Update equation for the message from bit node to check node is given by

$$L(q_{ij}) = L(c_i) + \sum_{j' \in C_i \setminus j} L(r_{j'i}) \quad (6)$$

Step 4: For i = 0, 1... n-1, the extrinsic output of decoder is given by

$$L(Q_i) = L(c_i) + \sum_{j \in C_i} L(r_{ji}) \quad (7)$$

Step 5: For i = 0, 1... n-1, the estimated channel input can be computed from

$$\hat{c}_i = \begin{cases} 1, \text{ if } L(Q_i) < 0 \\ 0 \text{ else} \end{cases} \quad (8)$$

If $\hat{\mathbf{c}}\mathbf{H}^t = \mathbf{0}$ or the number of iterations equals the maximum limit, stop, or else, go to Step 2.

IV. Simulation Results and Discussions

The current magnetic recording systems require high code rate such as 8/9 (0.88) and higher and the block size is around 1000 and 4000 bits. In this section, we present the design and performance of modified array codes at high-rate codes with block sizes which are common in magnetic recording systems.

A. Performance results with block size 1100~1300

The Modified Array Codes can be designed by fixing the code rate R and codeword length $N = k \cdot p$ to be around 1,100 – 1,300 bits, and then select p and k respectively. Due to the constraint of high code rates, the parameter j has to be low, given k. The relationship between j and k can be found in Table I. The targeted code rates are in the range of 0.88 – 0.9. Some examples of the designed codes are shown in Table 1.

Table 1: Code parameters with block size 1,100-1,300

j	3	3	3
k	31	29	25
p	37	43	53
$R_c = (1 - j/k)$	0.903	0.897	0.88
Message $p \cdot (k - j)$	1,036	1,118	1,166
Parity bit $j \cdot p$	111	129	159
Block size $k \cdot p$	1,147	1,247	1,325

For high-code rates, it can be observed that the parameter j is small compared with the parameter k. To select the best codes among designed codes, we simulate the performance and compare the results in AWGN channel, but the code rates and code lengths are tailored for magnetic recording systems.. The code performance in terms of the bit error rate (BER) compared with SNR is plotted. In the simulations, we refer to the input signal-to-noise ratio as electronics SNR in AWGN channel and defined it as

$$\left(\frac{E_b}{N_o}\right)_{dB} = \log_{10}\left(\frac{1}{R}\frac{E_c}{N_o}\right),$$

where E_c is the average energy of coded bits, E_b is the average energy of message bits and N_o is noise PSD. Each BER point is computed by using as many data packets as needed to collect at least 1000 error bits. The performance of the targeted block sizes are shown in Fig. 3. Note that the number of iterations in the decoding process is 30. Three modified array codes with code rates of ~0.9 are simulated in this paper. Three different values of p are considered, including 37, 43 and 53. The modified array codes with $p = 37$ has the worst performance than the other two, in particular, at BER = 10^{-5}, the codes with p = 43 and 53 need the SNR of 4.8 and 4.6 dB, which are less than for the code with p = *37*. The size of permutation matrix **P** evidently affects the code performance. It can be seen that performance is improved when the permutation matrix size increases. As the performance of the decoder is determined by the minimum distance of the code, the codes with larger **P** produces higher minimum distance.

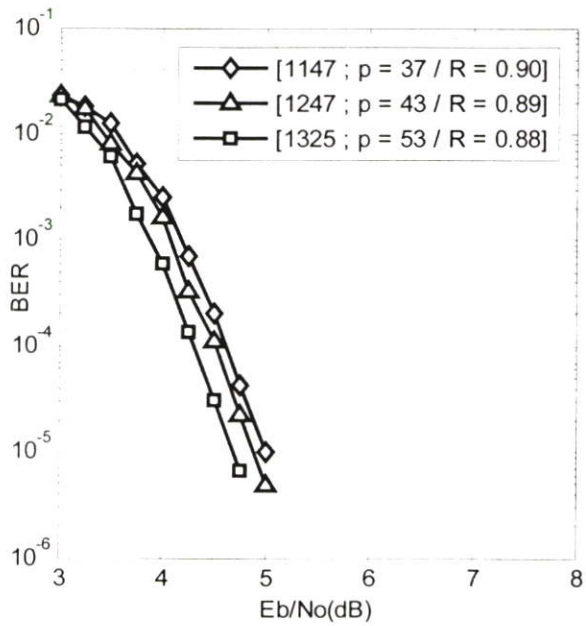


Figure 3. Performance results with block size 1100~1300 with various sizes of permutation matrix (after 30 iterations)

B. Performance results with block size 4000~4100

For this part, we fix the codeword length to be 4,000–4,100 bits, and then adjust the parameter j, k, and p, respectively. The code rate is targeted at 0.89 - 0.92, then the designed codes are shown in Table 2.

Table 2 : Code parameters with block size 4,000-4,100

j	5	5	5
k	61	53	47
p	67	79	89
$R_c = (1 - j/k)$	0.92	0.91	0.89
Message $p \cdot (k - j)$	3,752	3,792	3,738
Parity bit $j \cdot p$	335	395	445
Block size $k \cdot p$	4,087	4,187	4,183

Similar to the result in Fig. 3, the permutation matrix size affects the code performance. Three different values for p are considered, including 67, 79 and 89. The modified array code with p = 67 has the worst performance compared with the other two, in particular, at BER $=10^{-5}$, the code with p = 79 and 89 need 4.5 and 4.25 dB less than that of p = 67 code.

It can be seen that performance is improved when the permutation matrix size increases as well.

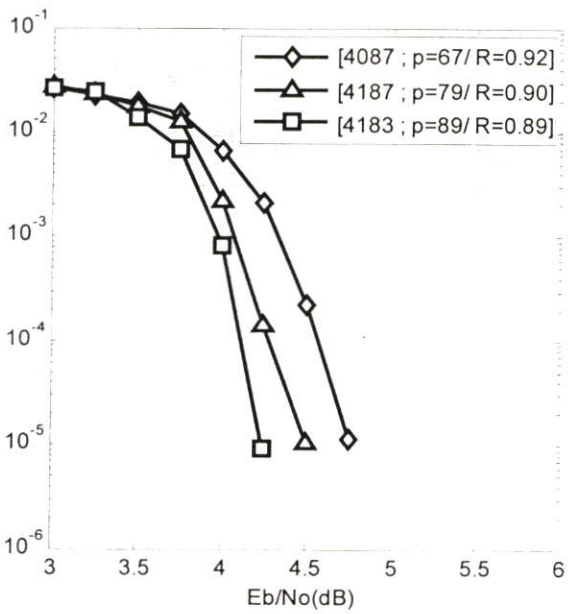


Figure 4. Performance results with block size 4000~4100 with various sizes of permutation matrix (after 30 iterations)

V. Conclusions

The design of high-rate Modified Array Codes at high code rate with block sizes suitable for magnetic recording system is illustrated. For high-rate codes, the simulation shows that the size of permutation matrix affects the code performance with larger p leads to higher minimum distance. This is valid for the both cases of considered block sizes. Modified Array Codes LDPC have been shown to possess suitable properties for magnetic recording system such as low-complexity encoding process, low error floor and capability of detecting and correcting burst. It is, therefore, possible to use the Modified Array Codes together with iterative decoding method, as the error correcting code in the magnetic recording channel. For future works, we plan to evaluate the performance of Modified Array Codes together with turbo equalization in realistic magnetic recording channel model.

References

[1] C. Berrou, A. Glanvieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in Proc. *IEEE Intl. Conf.*, pp. 1064-1070, May 1993.

[2] D.J.C. Mackey and R. Neal "Near Shannon limit performance of low density parity check codes," *Electronics Letters*, vol.33, pp. 457-458, Mar 1997.

[3] R. Gallager, "Low-density parity-check codes," *IRE Trans. Information Theory*, pp. 21-28, Jan 1962.

[4] Oenning, T.R.; Jaekyun Moon "Low density parity check coding for magnetic recording channels with media noise" *IEEE International Conference*, June 2001, pp.2189 -93.

[5] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Information Theory*, pp.533-547, Sept. 1981.

[6] M. Blaum, R. Roth, "New Array Codes for Multiple Phased Burst Correction," *IEEE Trans. Inform. Theory*, vol.39, No.1, Jan 1993, pp 66-77.

[7] E. Eleftheriou and S. Olcer, "Low-density parity check codes for digital subscriber lines," *Proc. 2002 Int. Conf. on Comm.*, pp.1752-1757., April – May, 2002.

[8] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc.* 2nd *Int. Symp. Turbo Codes*, Best, France, Sep 2000, pp 543-546.

[9] Richardson T.J., Shokrollahi MA, Urbanke R.L. "Design of capacity-approaching irregular low-density parity-check codes," *Information Theory IEEE Trans.volume 47*, pp.619-637, Feb 2001.

ประวัติผู้เขียน

ชื่อ	นายวิชาญ สิงห์อุดม
วันเดือนปีเกิด	18 ตุลาคม พ.ศ.2516
สถานที่เกิด	จังหวัดนครราชสีมา
วุฒิการศึกษา	ปริญญาตรี อุตสาหกรรมศาสตร์บัณฑิต(เกียรตินิยม) สาขาวิชาเทคโนโลยีไฟฟ้าอุตสาหกรรม
สถานศึกษา	คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ พ.ศ.2541

ประสบการณ์ทำงาน

2540 ~ 2543	เจ้าหน้าที่ฝ่ายออกแบบและติดตั้งระบบป้องกันอันตราย และผลกระทบจากฟ้าผ่า บริษัทสตาบิลจำกัด
2543 ~ ปัจจุบัน	วิศวกรฝ่ายทดสอบคุณสมบัติทางไฟฟ้าสำหรับฮาร์ดดิสก์ไดร์ฟ บริษัทฟูจิตสึ (ประเทศไทย) จำกัด