การออกแบบและการวิเคราะห์รหัสแอลดีพีซีแบบ q-ary และอัลกอริทึมการถอดรหัส

DESIGN AND ANALYSIS OF Q-ARY LDPC CODES AND THE DECODING ALGORITHMS

เวธิต ภาคย์พิสุทธิ์

WATID PHAKPHISUT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2558

KMITL-2015-EN-D-018-099

การออกแบบและการวิเคราะห์รหัสแอลดีพีซีแบบ q-ary และ อัลกอริทึมการถอดรหัส

DESIGN AND ANALYSIS OF Q-ARY LDPC CODES AND THE DECODING ALGORITHMS

เวธิต ภาคย์พิสุทธิ์
WATID PHAKPHISUT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2558

KMITL-2015-EN-D-018-099

DESIGN AND ANALYSIS OF Q-ARY LDPC CODES AND THE DECODING ALGORITHMS

WATID PHAKPHISUT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2015

KMITL-2015-EN-D-018-099

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การออกแบบและวิเคราะห์รหัสแอลดีพีซีแบบ q-ary และอัลกอริธึมการถอดรหัส
Thesis Title Design and Analysis of q-ary LDPC Codes and the Decoding Algorithms
นักศึกษา นายเวธิต ภาคย์พิสุทธิ์
รหัสประจำตัว 54610134
ปริญญา วิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชา วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.พรชัย ทรัพย์นิธิ
หมายเลขวิทยานิพนธ์ KMITL-2015-EN-D-018-099

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ยุทธพงษ์	รังสรรค์เสรี	
ผศ.ดร.ศรวัฒน์	ชิวปรีชา	
รศ.ดร.ลัญฉกร	วุฒิสิทธิกุลกิจ	
ผศ.ดร.ตุลยา	ลิมปิติ	
รศ.ดร.พรชัย	ทรัพย์นิธิ	

วัน / เดือน/ ปี ที่สอบ วันอังคารที่ 14 กรกฎาคม พ.ศ. 2558 เวลา 13.00-15.00 น.
สถานที่สอบ ณ อาคารเฉลิมพระเกียรติใหม่ HM-304

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 14 กรกฎาคม พ.ศ. 2558

หัวข้อวิทยานิพนธ์ การออกแบบและการวิเคราะห์รหัสแอลดีพีซีแบบ q-ary และอัลกอริทึมการถอดรหัส

นักศึกษา นายเวธิต ภาคย์พิสุทธิ์

รหัสประจำตัว 54610134

ปริญญา วิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

พ.ศ. 2558

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.พรชัย ทรัพย์นิธิ

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้ นำเสนอ การปรับปรุงการออกแบบและการถอดรหัสพาริตี้เช็คความแน่นต่ำหรือรหัสแอลดีพีซี รวมถึง แสดงการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีซีในช่องสัญญาณรบกวนแบบต่างๆ ในส่วนแรกของวิทยานิพนธ์ จะนำเสนอการออกแบบเมทริกซ์พาริตี้เช็คของรหัสแอลดีพีซี โดยประยุกต์ใช้อัลกอริทึมพีอีจีและเมทริกซ์อินเทอร์ลิฟ ทำให้ กราฟแทนเนอร์ของรหัสแอลดีพีซีมีวัฏจักรขนาดสูง ผลการจำลองสมรรถนะแสดงให้เห็นว่าที่อัตราบิตผิดพลาดเท่ากับ 4×10^{-8} รหัสแอลดีพีซีที่นำเสนอใช้อัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนหรือเอสเอ็นอาร์ลดลง 0.12 dB ในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต และ 0.5 dB ในช่องสัญญาณผลตอบสนองบางส่วน ส่วนที่สองของวิทยานิพนธ์ นำเสนอ เทคนิคกระจายความเชื่อมั่นสองทิศทางสำหรับการถอดรหัสแอลดีพีซีในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต เป็นผลให้ รหัสแอลดีพีซีใช้ค่าเอสเอ็นอาร์ลดลง 0.04 dB ที่อัตราเฟรมผิดพลาดเท่ากับ 7×10^{-4} นอกจากนี้ นำเสนอการถอดรหัสแอลดีพีซีสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก โดยใช้ความน่าจะเป็นตัดข้ามของช่องสัญญาณสมมาตรไบนารีในการปรับปรุงข่าวสารที่ออกจากโนดตรวจสอบของกราฟแทนเนอร์ วิธีการถอดรหัสที่นำเสนอนี้ ให้สมรรถนะที่ดีกว่าวิธีการถอดรหัสที่ถูกนำเสนอในงานวิจัยก่อนหน้า โดยที่อัตราบิตผิดพลาดเท่ากับ 2×10^{-5} การถอดรหัสที่นำเสนอใช้ค่าเอสเอ็นอาร์ลดลง 0.3 dB ในส่วนสุดท้ายของวิทยานิพนธ์ นำเสนอการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ในช่องสัญญาณผลตอบสนองบางส่วน ผลการวิเคราะห์แสดงให้เห็นว่ารหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ที่ได้รับการออกแบบและให้สมรรถนะสูงในช่องสัญญาณ PR1 อาจให้สมรรถนะต่ำในช่องสัญญาณ PR2 ลำดับสุดท้าย นำเสนอการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีเมื่อทำการถอดรหัสแบบสองมิติ ในระบบบันทึกข้อมูลเชิงแม่เหล็กที่มีค่าเอสเอ็นอาร์ของแทร็กแตกต่างกัน

Thesis	Design and Analysis of q-ary LDPC codes and the Decoding Algorithms
Student	Mr.Watid Phakphisut
Student ID.	54610134
Degree	Doctor of Engineering
Program	Electrical Engineering
Year	2015
Thesis Advisor	Assoc.Prof.Dr.Pornchai Supnithi

ABSTRACT

In this thesis, we present the research work on the design and decoding algorithm of low-density parity-check (LDPC) codes and its theoretical performance analysis. In the first part, we propose the construction of LDPC codes using a progressive edge-growth (PEG) algorithm and an interleaving matrix to minimize the number of cycles in Tanner graph. Simulation results show that the proposed LDPC code outperforms the existing LDPC codes in an additive white Gaussian noise (AWGN) channel and a partial response (PR) channel. The SNR gains of about 0.12 dB and 0.5 dB at the bit error rate (BER) equal to 4×10^{-8} are achieved for the AWGN and PR channels, respectively. In the second part, we propose a bi-directional belief-propagation for LDPC decoder in AWGN channel. The SNR gain of the proposed decoder compared with the existing decoder is about 0.04 dB at the frame error rate (FER) of 7×10^{-4}. In addition, we propose the decoding algorithm of LDPC codes in the bit patterned media recording modeled as a binary symmetric channel (BSC) with an additive white Gaussian noise (AWGN) channel. We modify check node computation that takes into account the crossover probability obtained from the BSC channel. At the BER of 2×10^{-5}, the SNR gain of the proposed decoder over the existing decoder is about 0.05 dB when the crossover probability value is 5×10^{-3}. Finally, the theoretical performances of LDPC codes over finite fields GF(q) in PR channels are analyzed. We use the extrinsic information transfer (EXIT) charts to predict the decoding threshold. The theoretical analyses show that the good codes over GF(q) in PR1 may not perform well in PR2 channel. In addition, we analyze the theoretical performance of two-dimensional LDPC codes in magnetic recording system with unequal SNRs.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ ขอมอบให้ บิดามารดาและครอบครัวที่ผมรัก ความรักและความอบอุ่นที่มีให้เป็นกำลังใจที่ยอดเยี่ยมสำหรับการทำงานวิจัย ขอบคุณบิดา ผู้เป็นแบบอย่างในการทำงานและเป็นเสาหลักของครอบครัว ขอบคุณมารดา ผู้ให้ความสุขและคอยดูแลทุกคนในครอบครัว ขอบคุณน้องชาย สำหรับความห่วงใยและเสียงหัวเราะตลอดมา

ขอขอบคุณอาจารย์พรชัย ทรัพย์นิธิ ซึ่งเป็นที่ปรึกษาในระดับปริญญาโทและเอก ผู้คอยผลักดันและให้กำลังใจในการทำงาน อีกทั้งเป็นแบบอย่างแก่ผมสำหรับการทำงานและการใช้ชีวิต ขอบคุณอาจารย์ยุทธพงษ์ รังสรรค์เสรี ซึ่งเป็นที่ปรึกษาในระดับปริญญาตรี สำหรับความห่วงใยและคำชี้แนะที่มีให้แก่ผม ขอบคุณอาจารย์ทุกท่านที่ผมเคยร่ำเรียนมา แม้ผมจะไม่ได้กล่าวไว้ในที่นี้ แต่ผมยังคงรำลึกถึงท่านทุกคน

ขอบคุณ พี่ เพื่อน และน้องทุกคน สำหรับความทุกข์และความสุขที่มี ตลอดระยะเวลา 10 ปีในลาดกระบัง

ขอบคุณ โครงการปริญญาเอกกาญจนาภิเษก (คปก.) และสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง สำหรับทุนการศึกษาและความรู้ที่ผมได้รับ

เวธิต ภาคย์พิสุทธิ์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

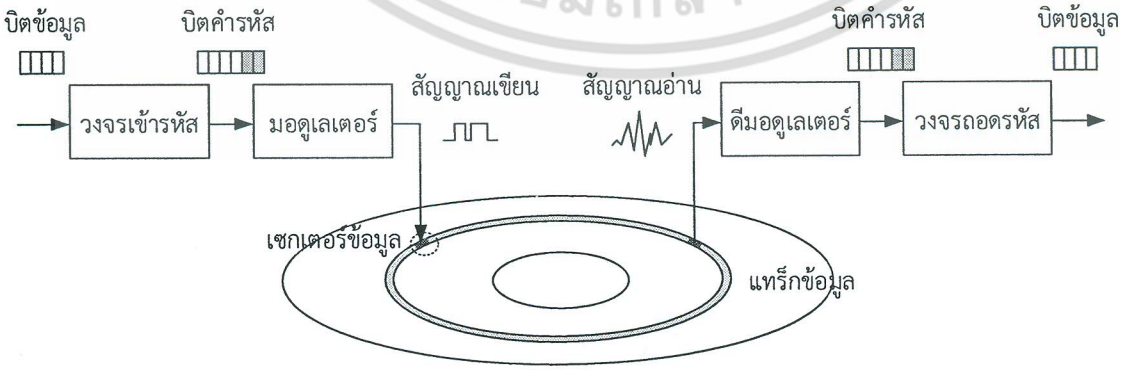
รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

ปัจจุบัน ความต้องการพื้นที่จัดเก็บข้อมูลดิจิตอลมีแนวโน้มเพิ่มสูงขึ้น ส่งผลให้ ระบบบันทึกข้อมูลเชิงแม่เหล็ก (magnetic recording system) ซึ่งเป็นเทคโนโลยีจัดเก็บข้อมูลที่ใช้ในอุตสาหกรรมฮาร์ดดิสก์ไดร์ฟ (hard disk drive) มีความจำเป็นต้องพัฒนาให้มีความหนาแน่นเชิงพื้นที่ (areal density) เพิ่มขึ้น อย่างไรตาม การเพิ่มความหนาแน่นเชิงพื้นที่ ส่งผลให้ความผิดพลาดของข้อมูลสูงขึ้น เนื่องจาก ความผิดเพี้ยนของสัญญาณ การลดทอนของสัญญาณ และการแทรกสอดระหว่างสัญลักษณ์ (intersymbol interference, ISI) ดังนั้น การประมวลผลสัญญาณของระบบบันทึกข้อมูลเชิงแม่เหล็กจึงเข้ามามีบทบาทสำคัญในการกู้คืนสัญญาณและลดอัตราบิตผิดพลาดของข้อมูลที่อ่านจากสื่อบันทึก (media) ทั้งนี้ ระบบบันทึกข้อมูลเชิงแม่เหล็กสามารถพิจารณาได้เป็นระบบสื่อสารชนิดหนึ่ง ดังรูปที่ 1.1 ซึ่งประกอบไปด้วย ช่องสัญญาณ (channel) หรือสื่อบันทึกข้อมูล มอดูเลเตอร์ (modulator) ดีมอดูเลเตอร์ (demodulator) วงจรเข้ารหัส (encoder) และวงจรถอดรหัส (decoder) โดยวงจรมอดูเลเตอร์ทำหน้าที่แปลงบิตข้อมูลให้อยู่ในรูปคลื่นกระแสไฟฟ้าเขียน (write current waveform) ก่อนป้อนไปยังหัวเขียนเพื่อทำการบันทึกข้อมูลลงในสื่อบันทึก และวงจรเข้ารหัสและถอดรหัสทำหน้าที่ลดอัตราบิตผิดพลาดของข้อมูล ปัจจุบัน รหัสพาริตี้เช็คความหนาแน่นต่ำหรือรหัสแอลดีพีซี (low-density parity-check code, LDPC) [1] ซึ่งจัดเป็นรหัสแก้ไขความผิดพลาดของข้อมูลชนิดหนึ่ง ได้รับความนิยมอย่างมากในการประยุกต์ใช้งานในระบบการบันทึกข้อมูลเชิงแม่เหล็ก เนื่องจาก รหัสแอลดีพีซีให้สมรรถนะการแก้ไขความผิดพลาดข้อมูลเข้าใกล้ขีดจำกัดของแชนนอน (Shannon limit) [2] ทำให้ วิทยานิพนธ์ฉบับนี้ จึงมุ่งเน้นการออกแบบและพัฒนาสมรรถนะของรหัสแอลดีพีซี



รูปที่ 1.1 ระบบบันทึกข้อมูลเชิงแม่เหล็ก

งานวิจัยในวิทยานิพนธ์ฉบับนี้ แบ่งออกเป็น 2 ส่วน ได้แก่ การปรับปรุงสมรรถนะของการออกแบบรหัสแอลดีพีซีและการปรับปรุงสมรรถนะของการถอดรหัสแอลดีพีซี ในส่วนแรกของงานวิจัยนำเสนอ การออกแบบเมทริกซ์พาริตี้เช็คของรหัสแอลดีพีซี ดังนี้

1. รหัสควอไซไซคลิกวัฏจักรสูง

ปัจจุบัน รหัสแอลดีพีซีแบบควอไซไซคลิกถูกนำมาประยุกต์ใช้งาน เนื่องจากกระบวนการเข้ารหัสมีความซับซ้อนต่ำ โดยทั่วไป สมรรถนะของรหัสแอลดีพีซีจะขึ้นอยู่กับขนาดของวัฏจักรในกราฟแทนเนอร์ [3] ในงานวิจัย [4] จึงนำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก โดยการประยุกต์ใช้อัลกอริทึมพีอีจี (progressive edge-growth algorithm, PEG algorithm) [5] อย่างไรก็ตาม การออกแบบรหัสแอลดีพีซีด้วยอัลกอริทึมพีอีจีจะเกิดปัญหาที่เรียกว่า สถานการณ์ตัวเลือกมาก (multiple choice situation) ทำให้ รหัสแอลดีพีซีที่ได้รับการออกแบบมีวัฏจักรขนาดไม่สูงสุด ทำให้งานวิจัยนี้ นำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกซึ่งมีวัฏจักรขนาดสูงสุด โดยประยุกต์ใช้อัลกอริทึมพีอีจีที่มีการดัดแปลงเพื่อแก้ปัญหาสถานการณ์ตัวเลือกมาก

2. รหัสอินเทอร์ลิฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน

ในระบบบันทึกข้อมูลเชิงแม่เหล็กหรืออุปกรณ์ฮาร์ดดิสก์ จะพบปัญหาการแทรกสอดระหว่างสัญลักษณ์เป็นจำนวนมาก โดยทั่วไป นิยมใช้วงจรถอดรหัสเทอร์โบอีควอไลเซชัน [6] ซึ่งประกอบด้วยวงจรตรวจหาวีเทอร์บิแบบซอฟต์เอาต์พุต (soft-output Viterbi algorithm, SOVA) [7] และวงจรถอดรหัส แอลดีพีซี เพื่อจัดการปัญหาการแทรกสอดระหว่างสัญลักษณ์ที่เกิดขึ้นในระบบบันทึกข้อมูลเชิงแม่เหล็ก ทั้งนี้ การประยุกต์ใช้งานรหัสแอลดีพีซีแบบควอไซไซคลิกและแบบอาร์เรย์ในวงจรถอดรหัสเทอร์โบอีควอไลเซชันจะก่อให้เกิดวัฏจักรเทียม [8] ดังนั้น ในงานวิจัย จึงนำเสนอโครงสร้างรหัสแอลดีพีซีเพื่อลดจำนวนวัฏจักรเทียมในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน นอกจากนี้ โครงสร้างรหัสแอลดีพีซีที่นำเสนอ ยังปราศจากวัฏจักรขนาด 4 ที่ส่งผลกระทบต่อสมรรถนะของการถอดรหัสแอลดีพีซี

3. รหัสโปรโตกราฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน

รหัสโปรโตกราฟ [9] จัดเป็นรหัสแอลดีพีซีแบบควอไซไซคลิกชนิดหนึ่ง ซึ่งเมทริกซ์พาริตี้เช็คสามารถแสดงในรูปของโปรโตกราฟ (protograph) ในงานวิจัย [10, 11] แสดงการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน อย่างไรก็ตาม การวิเคราะห์จะพิจารณาเฉพาะรหัสไบนารีแอลดีพีซีหรือรหัสแอลดีพีซีบนฟิลด์จำกัด $\mathrm{GF}(q)$ เมื่อ $q=2$ ซึ่งปัจจุบันรหัสนอนไบนารีแอลดีพีซีหรือรหัสแอลดีพีซีบนฟิลด์จำกัด $\mathrm{GF}(q)$ เมื่อ $q>2$ [12] กำลังได้รับความสนใจในการประยุกต์ใช้งาน ดังนั้น ในงานวิจัยนี้ จะนำเสนอการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสโปรโตกราฟบนฟิลด์จำกัด $\mathrm{GF}(q)$ ในช่องสัญญาณผลตอบสนองบางส่วน วิธีการที่ได้นำเสนอนี้ สามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีในช่องสัญญาณผลตอบสนองบางส่วนที่ให้สมรรถนะเข้าใกล้ขีดจำกัดของแชนนอน

ในส่วนที่สองของวิทยานิพนธ์ นำเสนอ อัลกอริทึมการถอดรหัสแอลดีพีซีที่ให้สมรรถนะการแก้ไขความผิดพลาดข้อมูลสูง ดังนี้

1. การถอดรหัสกระจายความเชื่อมั่นสองทิศทาง

ในงานวิจัย [13] ได้นำเสนอการถอดรหัสกระจายความเชื่อมั่นสองทิศทางสำหรับอัลกอริทึมเอสบีพี (shuffled belief propagation, SBP) [14] โดยประยุกต์ใช้ข่าวสารที่ได้จากการถอดรหัสที่มีลำดับของการคำนวณข่าวสารแตกต่างกัน ทำให้ สมรรถนะของการถอดรหัสแอลดีพีซีเพิ่มสูงขึ้น อย่างไรก็ตาม การออกแบบวงจรถอดรหัสที่ใช้อัลกอริทึมเอสบีพีจะมีความซับซ้อนสูง ในปัจจุบัน การถอดรหัสแอลดีพีซีด้วยอัลกอริทึมแอลบีพี (layered belief propagation, LBP) [15] ได้รับความนิยมในการประยุกต์ใช้งาน เนื่องจากการออกแบบวงจรมีความซับซ้อนต่ำ ทำให้ในงานวิจัยนี้ สนใจการประยุกต์ใช้ข่าวสารที่ได้จากกระจายความเชื่อมั่นสองทิศทางสำหรับอัลกอริทึมแอลบีพี นอกจากนี้ ในงานวิจัย จะแสดงการวิเคราะห์สมรรถนะทางทฤษฎีของการถอดรหัสแอลดีพีซีที่ได้นำเสนอ

2. การถอดรหัสสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

ในระบบบันทึกข้อมูลเชิงแม่เหล็กแบบบิตแพทเทิร์น (bit patterned media recording) [16] กระบวนการบันทึกอาจเกิดปัญหาที่เรียกว่า การเขียนผิดพลาด (written-in error) [17] ซึ่งเกิดจากตำแหน่งของหัวเขียนไม่ตรงกับตำแหน่งของไอแลนด์เชิงแม่เหล็ก (magnetic island) ส่งผลให้เกิดความผิดพลาดในการบันทึกข้อมูล ทั้งนี้ สามารถจำลองเหตุการณ์เขียนและอ่านข้อมูลในสื่อบันทึกด้วยแบบจำลองช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก โดยทั่วไป วงจรถอดรหัสแอลดีพีซีได้รับการออกแบบสำหรับช่องสัญญาณรบกวนเกาส์สีขาวบวก ดังนั้น ในงานวิจัยนี้ จึงนำเสนอขั้นตอนการถอดรหัสแอลดีพีซีสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก โดยค่าความน่าจะเป็นตัดข้าม (crossover probability) ของช่องสัญญาณสมมาตรไบนารีจะถูกนำมาใช้ในการคำนวณข่าวสารที่ออกจากโนดตรวจสอบในกราฟแทนเนอร์ (Tanner graph)

3. การถอดรหัสสองมิติ

ในระบบบันทึกข้อมูลเชิงแม่เหล็ก ข้อมูลจะถูกบันทึกลงในเซกเตอร์ข้อมูล (data sector) ของสื่อบันทึกตามแนวเส้นรอบวงซึ่งเรียกว่าแทร็ก (track) ดังรูปที่ 1.1 คำรหัสที่ได้จากการเข้ารหัสแอลดีพีซีจะถูกบันทึกลงในเซกเตอร์เดียวกันและแทร็กเดียวกัน โดยทั่วไป แทร็กต่างๆ ในสื่อบันทึกจะมีอัตราส่วนกำลังของสัญญาณต่อกำลังของสัญญาณรบกวน หรือ ค่าเอสเอ็นอาร์แตกต่างกัน อันเนื่องมาจาก ขนาดของแทร็กที่แตกต่างกัน การใช้หัวอ่านจำนวนหลายหัว เป็นต้น ดังนั้น ในงานวิจัยนี้ จึงนำเสนอรหัสแอลดีพีซีแบบสองมิติ ซึ่งคำรหัสจะถูกแบ่งและบันทึกลงในแทร็กที่แตกต่างกัน เป็นผลให้ ในกระบวนการถอดรหัส บิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์สูงสามารถช่วยบิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์ต่ำ โดยงานวิจัย จะแสดงการวิเคราะห์สมรรถนะทางทฤษฎีของการถอดรหัสแบบสองมิติ โดยวิธีการวิเคราะห์ที่นำเสนอนี้ สามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีแบบสองมิติที่ให้สมรรถนะการแก้ไขความผิดพลาดสูง

วิทยานิพนธ์ฉบับนี้ประกอบไปด้วยเนื้อหาจำนวน 7 บท ในบทที่ 1 แนะนำรายละเอียดและงานวิจัยของวิทยานิพนธ์ บทที่ 2 อธิบายแบบจำลองของช่องสัญญาณที่ใช้จำลองสมรรถนะของรหัสแอลดีพีซี เช่น ช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต ช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก และ ช่องสัญญาณผลตอบสนองบางส่วนซึ่งนิยมใช้จำลองระบบบันทึกข้อมูลเชิงแม่เหล็ก ในส่วนสุดท้าย เกี่ยวข้องกับทฤษฎีข่าวสาร ซึ่งอธิบายปริมาณข่าวสารสูงสุดที่สามารถส่งผ่านช่องสัญญาณหรือเรียกว่าความจุช่องสัญญาณ นอกจากนี้ การคำนวณปริมาณข่าวสารยังถูกใช้ในการประเมินสมรรถนะทางทฤษฎีของรหัสแอลดีพีซี บทที่ 3 อธิบายพื้นฐานของรหัสแอลดีพีซี ได้แก่ ประเภทของรหัสแอลดีพีซี คุณสมบัติพื้นฐานของรหัสแอลดีพีซี การเข้ารหัสแอลดีพีซี รวมถึง การออกแบบรหัสแอลดีพีซีที่ได้รับความสนใจในปัจจุบัน บทที่ 4 อธิบายวิธีการถอดรหัสแอลดีพีซีกรณีฟิลด์จำกัดมีค่าใดๆ โดยแสดงการคำนวณในรูปของความน่าจะเป็นและอัตราส่วนความน่าจะเป็นแบบล็อก ในส่วนสุดท้าย อธิบายวิธีการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีซี ในบทที่ 5 และ 6 อธิบายงานวิจัยที่นำเสนอในวิทยานิพนธ์ โดยงานวิจัยแบ่งออกเป็น 2 ส่วน ได้แก่ การปรับปรุงสมรรถนะของการออกแบบรหัสแอลดีพีซี (บทที่ 5) และ การปรับปรุงสมรรถนะของการถอดรหัสแอลดีพีซี (บทที่ 6) และในบทสุดท้ายอธิบายผลสรุปของงานวิจัย

บทที่ 2
ช่องสัญญาณและความจุช่องสัญญาณ

ในบทนี้ กล่าวถึงช่องสัญญาณและความจุช่องสัญญาณ ซึ่งเป็นพื้นฐานสำคัญของงานวิจัยในวิทยานิพนธ์ ลำดับแรกเป็นการอธิบายประเภทของช่องสัญญาณ เช่น ช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก (cascade of binary symmetric channel with binary-input additive white Gaussian noise channel) และช่องสัญญาณผลตอบสนองบางส่วน (partial response channel) ซึ่งนิยมใช้ในจำลองกระบวนการเขียนและอ่านของระบบบันทึกข้อมูลเชิงแม่เหล็ก นอกจากนี้ แสดงการคำนวณอัตราส่วนความน่าจะเป็นแบบล็อก (Log Likelihood Ratios) ของสัญญาณที่ได้รับจากช่องสัญญาณ ลำดับต่อมา เกี่ยวข้องกับทฤษฎีข่าวสารซึ่งอธิบายปริมาณข่าวสารสูงสุดที่สามารถส่งผ่านช่องสัญญาณหรือเรียกว่าความจุช่องสัญญาณ อีกทั้งยังถูกใช้ในการประเมินสมรรถนะขีดสุดของรหัสแก้ไขความผิดพลาด

2.1 แบบจำลองช่องสัญญาณ

กำหนดให้สัญญาณไบนารีลำดับที่ i แทนด้วยสัญลักษณ์ $v_i \in \{0,1\}$ ถูกส่งผ่านช่องสัญญาณรบกวน และ y_i คือสัญญาณที่ได้รับจากช่องสัญญาณ ในภาครับจำเป็นต้องตรวจหาสัญญาณไบนารีที่ถูกส่งผ่านช่องสัญญาณ โดยทั่วไป นิยมตัดสินใจเลือกสัญญาณไบนารีที่ให้ความน่าจะเป็นอะโพสเทอริ-ออริ (a posteriori probability) มากสุด ทั้งนี้ เพื่อให้ความน่าจะเป็นของการตัดสินใจผิดพลาดมีค่าต่ำสุด โดยทั่วไป ความน่าจะเป็นอะโพสเทอริออริ นิยมแสดงในรูปอัตราส่วนความน่าจะเป็นแบบล็อก[1] หรือค่าแอลแอลอาร์ (Log Likelihood Ratios, LLR) ดังนี้

$$L(v_i \mid y_i) = \log\left(\frac{P(v_i = 0 \mid y_i)}{P(v_i = 1 \mid y_i)}\right) \tag{2.1}$$

ความสัมพันธ์ระหว่างอัตราส่วนความน่าจะเป็นแบบล็อกกับความน่าจะเป็นแสดงได้ดังนี้

$$P(v_i = 0 \mid y_i) = \frac{e^{L(v_i|y_i)}}{1 + e^{L(v_i|y_i)}} \tag{2.2}$$

$$P(v_i = 1 \mid y_i) = \frac{e^{-L(v_i|y_i)}}{1 + e^{-L(v_i|y_i)}} \tag{2.3}$$

[1]วิทยานิพนธ์ฉบับนี้ ลอการิทึมธรรมชาติแทนด้วยสัญลักษณ์ทางคณิตศาสตร์ คือ log

เมื่อภาครับทำการคำนวณอัตราส่วนความน่าจะเป็นแบบล็อก $L(v_i \mid y_i)$ เสร็จสิ้น จะทำการตัดสินใจเลือกสัญญาณไบนารี $\hat{v}_i = 0$ เมื่อ $L(v_i \mid y_i)$ มีค่ามากกว่าศูนย์ ในทางกลับกัน กรณีความน่าจะเป็นแบบล็อก $L(v_i \mid y_i)$ มีค่าน้อยกว่าศูนย์ จะทำการตัดสินใจเลือกสัญญาณไบนารี $\hat{v}_i = 1$ จากกฎของเบย์ (Bayes' rule) ทำให้ สมการที่ 2.1 เขียนใหม่ได้เป็น

$$L(v_i \mid y_i) = \log\left(\frac{P(y_i \mid v_i = 0)P(v_i = 0)}{P(y_i \mid v_i = 1)P(v_i = 1)}\right) = L\left(y_i \mid v_i\right) + L(v_i) \tag{2.4}$$

เมื่อ $L\left(y_i \mid v_i\right)$ คือ อัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับจากช่องสัญญาณ และ $L(v_i)$ คือ อัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณไบนารีที่ถูกส่ง ซึ่งสามารถคำนวณจากวงจรถอดรหัสในภาครับ

2.1.1 ช่องสัญญาณสมมาตรไบนารี

สำหรับช่องสัญญาณสมมาตรไบนารี (binary symmetric channel, BSC) สัญญาณไบนารี $v_i \in \{0,1\}$ ซึ่งมีความน่าจะเป็น $P(v_i = 0) = P(v_i = 1) = 1/2$ จะถูกเปลี่ยนระดับสัญญาณด้วยความน่าจะเป็นตัดข้าม (crossover probability) p_{BSC} ดังรูปที่ 2.1 โดยความน่าจะเป็นของสัญญาณที่ได้รับ y_i เมื่อส่งสัญญาณ v_i มีค่าเท่ากับ

$$P(y_i = 0 \mid v_i = 1) = P(y_i = 1 \mid v_i = 0) = p_{BSC} \tag{2.5}$$

$$P(y_i = 0 \mid v_i = 0) = P(y_i = 1 \mid v_i = 1) = 1 - p_{BSC} \tag{2.6}$$

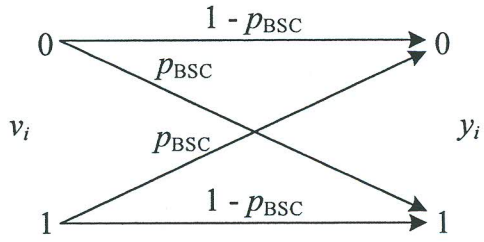
ดังนั้น ความน่าจะเป็นของสัญญาณที่ได้รับ y_i เมื่อส่งสัญญาณ $v_i = 0$ และ $v_i = 1$ มีค่าเท่ากับ

$$P(y_i \mid v_i = 1) = (1 - p_{BSC})^{y_i}(p_{BSC})^{1-y_i} \tag{2.7}$$

$$P(y_i \mid v_i = 0) = (p_{BSC})^{y_i}(1 - p_{BSC})^{1-y_i} \tag{2.8}$$

ทำให้ อัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับจากช่องสัญญาณคำนวณได้จาก

$$L(y_i \mid v_i) = \log\frac{P(y_i \mid v_i = 0)}{P(y_i \mid v_i = 1)} = (1 - 2y_i)\log\left(\frac{1 - p_{BSC}}{p_{BSC}}\right) \tag{2.9}$$



รูปที่ 2.1 แบบจำลองช่องสัญญาณสมมาตรไบนารี

2.1.2 ช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต

สำหรับช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต (binary-input additive white Gaussian noise channel, BI-AWGN channel) กำหนดให้สัญญาณไบนารี $v_i \in \{0,1\}$ ซึ่งมีความน่าจะเป็น $P(v_i = 0) = P(v_i = 1) = 1/2$ ถูกปรับระดับเป็นสัญญาณส่ง $x_i \in \{-1,1\}$ โดยมีสมการความสัมพันธ์ คือ $x_i = 2v_i - 1$ ทำให้สัญญาณที่ได้รับจากช่องสัญญาณคำนวณได้จาก

$$y_i = x_i + n_i \tag{2.10}$$

เมื่อ n_i คือสัญญาณรบกวนที่มีฟังก์ชันความหนาแน่นความน่าจะเป็นแบบปรกติ (normal probability density function) ซึ่งมีค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ σ^2 ซึ่งสามารถเขียนฟังก์ชันความหนาแน่นความน่าจะเป็นของสัญญาณที่ได้รับ y_i ได้ดังนี้

$$p(y_i \mid x_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y_i - x_i)^2}{2\sigma^2} \right) \tag{2.11}$$

อัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับจากช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต คำนวณด้วยสมการดังต่อไปนี้

$$L(y_i \mid x_i) = \log \frac{p(y_i \mid x_i = -1)}{p(y_i \mid x_i = 1)} = -\frac{2y_i}{\sigma^2} \tag{2.12}$$

สำหรับช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต การวัดคุณภาพของช่องสัญญาณนิยมแสดงอยู่ในรูปอัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนหรือเอสเอ็นอาร์ (signal-to-noise ratio, SNR) มีหน่วยเป็นเดซิเบล (decibel, dB) ดังนี้

$$SNR = 10\log_{10}\left(\frac{1}{R}\frac{E_b}{N_0} \right) \quad (dB) \tag{2.13}$$

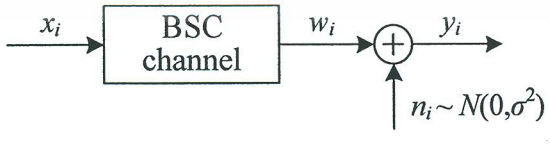
เมื่อ E_b คือ ค่าเฉลี่ยกำลังของสัญญาณส่ง พิจารณาสัญญาณส่ง $x_i \in \{-1,1\}$ ฉะนั้น ค่าเฉลี่ยกำลังในที่นี้จึงมีเท่ากับ $E_b = 1$ และสัญญาณรบกวนเกาส์สีขาวมีความหนาแน่นสเปกตรัมกำลัง (power spectral density, PSD) แบบสองด้านเท่ากับ $N_0 / 2 = \sigma^2$ กรณีที่มีการเข้ารหัสแก้ไขความผิดพลาดจะทำให้ค่าเฉลี่ยกำลังของสัญญาณส่งสูงขึ้น เนื่องจากข้อมูลที่ถูกเข้ารหัสมีความยาวบิตเพิ่มขึ้น กำหนดให้อัตรารหัส R คือ อัตราส่วนของจำนวนบิตของข้อมูลต่อจำนวนบิตของข้อมูลที่ถูกเข้ารหัส ดังนั้น กรณีไม่มีการเข้ารหัสจะทำให้อัตรารหัสเท่ากับ $R = 1$ และอัตรารหัสมีค่าเป็น $0 < R \leq 1$ เสมอ

2.1.3 ช่องสัญญาณเรียงต่อ

การสื่อสารผ่านช่องสัญญาณชนิดหนึ่ง อาจมีส่วนประกอบของสัญญาณรบกวน การลดทอนสัญญาณ และอื่นๆ ภายในช่องสัญญาณ อย่างไรก็ตาม สามารถพิจารณาช่องสัญญาณดังกล่าวเป็นช่องสัญญาณเรียงต่อ (cascade of channels) ตัวอย่างเช่น ระบบบันทึกข้อมูลเชิงแม่เหล็กแบบบิตแพทเทิรน (bit patterned media recording) [16] กระบวนการบันทึกข้อมูลอาจเกิดปัญหาที่เรียกว่า การเขียนผิดพลาด (written-in error) [17] ซึ่งเกิดจากตำแหน่งของหัวเขียนไม่ตรงกับตำแหน่งบิตแม่เหล็กที่ต้องการเขียน ส่งผลให้เกิดความผิดพลาดของข้อมูลที่บันทึก ความผิดพลาดในกระบวนการบันทึกนี้ สามารถจำลองได้ด้วยช่องสัญญาณสมมาตรไบนารี และกระบวนการอ่านสัญญาณอ่านกลับ (readback signal) จะได้รับผลกระทบของสัญญาณรบกวนที่มีฟังก์ชันความหนาแน่นความน่าจะเป็นแบบปรกติตามสมการที่ 2.11

รูปที่ 2.2 แสดงแบบจำลองช่องสัญญาณที่ประกอบด้วยช่องสัญญาณสัญญาณสมมาตรไบนารีและช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต ฟังก์ชันความหนาแน่นความน่าจะเป็นของสัญญาณที่ได้รับ y_i สามารถคำนวณได้จาก [18]

$$p(y_i \mid x_i) = (1 - p_{\text{BSC}}) \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y_i - x_i)^2}{2\sigma^2} \right) + p_{\text{BSC}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y_i + x_i)^2}{2\sigma^2} \right) \quad (2.14)$$



รูปที่ 2.2 แบบจำลองช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

กำหนดให้สัญญาณไบนารี $x_i \in \{-1,1\}$ อัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับจากช่องสัญญาณสามารถคำนวณได้จาก

$$L(y_i|x_i) = \log\left(\frac{(1-p_{\text{BSC}})e^{-\frac{2y_i}{\sigma^2}} + p_{\text{BSC}}}{(1-p_{\text{BSC}}) + p_{\text{BSC}}e^{-\frac{2y_i}{\sigma^2}}}\right) \tag{2.15}$$

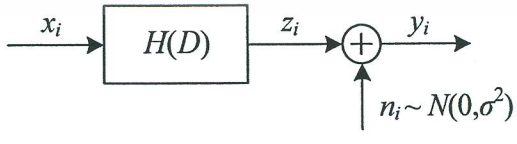
การวัดคุณภาพของช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวกจะขึ้นอยู่กับ ความน่าจะเป็นตัดข้าม p_{BSC} ของช่องสัญญาณสมมาตรไบนารี และค่าเอสเอ็นอาร์ของช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุตซึ่งคำนวณจากสมการที่ 2.13

2.1.4 ช่องสัญญาณความจำ

แบบจำลองช่องสัญญาณในหัวข้อที่ผ่านมา อาจกล่าวได้ว่า เป็นช่องสัญญาณไร้ความจำ (memoryless channel) เนื่องจากเอาต์พุตของช่องสัญญาณ ณ ปัจจุบันขึ้นอยู่กับอินพุตปัจจุบันเท่านั้น โดยไม่ขึ้นอยู่กับอินพุตในอดีตและอนาคต อย่างไรก็ตาม โดยทั่วไป ช่องสัญญาณอาจมีปัญหาการแทรกสอดระหว่างสัญลักษณ์ (intersymbol interference, ISI) ตัวอย่างเช่น ระบบบันทึกข้อมูลเชิงแม่เหล็ก และระบบสื่อสารไร้สายซึ่งสามารถพิจารณาเป็นช่องสัญญาณความจำ รูปที่ 2.3 แสดงแบบจำลองช่องสัญญาณผลตอบสนองบางส่วน (partial response channel, PR channel) [19,20] ซึ่งเป็นแบบจำลองสำหรับช่องสัญญาณเชิงเส้นที่ค่าสัมประสิทธิ์ทุกตัวเป็นจำนวนเต็ม โดยช่องสัญญาณ $H(D)$ กำหนดโดย

$$H(D) = \sum_{k=0}^{N} h_k D^k \tag{2.16}$$

เมื่อ h_k คือสัมประสิทธิ์ลำดับที่ k ของช่องสัญญาณ และ D คือตัวดำเนินการหน่วงเวลา ซึ่งในช่องสัญญาณมีตัวดำเนินการหน่วงเวลาจำนวน N ตัว



รูปที่ 2.3 แบบจำลองช่องสัญญาณผลตอบสนองบางส่วน

สำหรับระบบบันทึกข้อมูลเชิงแสง ช่องสัญญาณ $H(D)$ เขียนได้ดังต่อไปนี้ [21]

$$H(D) = (1+D)^n \tag{2.17}$$

เมื่อ n คือจำนวนเต็มที่มีค่ามากกว่าหรือเท่ากับหนึ่ง กรณีที่ $n=1$ จะเรียกช่องสัญญาณพีอาร์วัน (class-1 partial response channel, PR1 channel) และ $n=2$ เรียกช่องสัญญาณพีอาร์ทู (class-2 partial response channel, PR2 channel)

สำหรับระบบบันทึกข้อมูลเชิงแม่เหล็กแบบแนวนอน ช่องสัญญาณ $H(D)$ เขียนได้ดังนี้ [22]

$$H(D) = (1-D)(1+D)^n \tag{2.18}$$

เมื่อ n คือจำนวนเต็มที่มีค่ามากกว่าหรือเท่ากับศูนย์ กรณีที่ $n=0$ เรียกว่า ช่องสัญญาณผลตอบสนองบางส่วนแบบไดโค้ด (dicode partial response channel) และ $n=1$ เรียกว่า ช่องสัญญาณแบบพีอาร์โฟร์ (class-4 partial response channel, PR4 channel) และ $n=2$ เรียกว่า ช่องสัญญาณอีพีอาร์โฟร์ (extended partial response channel, EPR4 channel) และ $n=3$ เรียกว่า ช่องสัญญาณอีอีพีอาร์โฟร์ (extended-extended partial response channel, EEPR4 channel) เป็นต้น

สัญญาณเอาต์พุตของช่องสัญญาณ $H(D)$ หาได้จากการทำคอนโวลูชันระหว่างสัญญาณอินพุตและสัมประสิทธิ์ของช่องสัญญาณ ดังนั้น สัญญาณที่ได้รับจากช่องสัญญาณผลตอบสนองบางส่วนสามารถคำนวณได้จาก

$$y_i = \sum_{k=0}^{N} x_{i-k} h_k + n_i \tag{2.19}$$

พิจารณาสัญญาณที่ถูกส่ง $x_i \in \{-1,1\}$ ดังนั้น การวัดคุณภาพของช่องสัญญาณผลตอบสนองบางส่วนในรูปของอัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนจะคำนวณโดยใช้สมการต่อไปนี้

$$SNR = 10\log_{10}\left(\frac{1}{R}\frac{\sum_{k=0}^{N}|h_k|^2}{N_0}\right) \quad (dB) \tag{2.20}$$

2.2 การวัดปริมาณข่าวสาร

กำหนดให้ตัวแปรสุ่ม X ประกอบไปด้วยสัญลักษณ์ $\{x_1, x_2, \ldots, x_M\}$ เมื่อ M คือจำนวนสัญลักษณ์ทั้งหมด โดยแต่ละสัญลักษณ์มีความน่าจะเป็นในการเกิดเท่ากับ $\{P(x_1), P(x_2), \ldots, P(x_M)\}$ และ $\sum_{i=1}^{M} P(x_i) = 1$ ดังนั้นปริมาณข่าวสาร I_i ของสัญลักษณ์ x_i คำนวณได้จาก

$$I_i = \log_2\left(\frac{1}{P(x_i)}\right) \quad \text{(บิต)} \tag{2.21}$$

เมื่อสัญลักษณ์ x_i มีความน่าจะเป็นต่ำจะทำให้ปริมาณข่าวสารที่วัดได้มีค่าสูง ซึ่งปริมาณข่าวสารที่วัดได้จะมีค่ามากกว่าหรือเท่ากับศูนย์เสมอ หรือ $I_i \geq 0$

2.2.1 เอนโทรปีและข่าวสารร่วม

เอนโทรปี (entropy) เป็นการวัดปริมาณข่าวสารของตัวแปรสุ่ม X ซึ่งคำนวณได้จากค่าเฉลี่ยปริมาณข่าวสาร I_i ของสัญลักษณ์ ดังนี้

$$H(X) = \mathrm{E}\left[\log_2\left(\frac{1}{P(x_i)}\right)\right] = \sum_i P(x_i)\log_2\left(\frac{1}{P(x_i)}\right) \quad \text{(บิตต่อสัญลักษณ์)} \tag{2.22}$$

ทั้งนี้ อาจกล่าวได้ว่า เอนโทรปีเป็นการวัดความไม่แน่นอนของตัวแปรสุ่ม กรณีตัวแปรสุ่มมีความไม่แน่นอนสูงจะทำให้ปริมาณข่าวสารที่วัดได้มีค่าสูง ตัวอย่างเช่น กรณีต้นทางส่งข้อมูลไบนารีสัญลักษณ์ 0 และ 1 โดยมีความน่าจะเป็นในการส่งแต่ละสัญลักษณ์เท่ากัน เอนโทรปีของข้อมูลจะมีค่าเท่ากับ 1 บิตต่อสัญลักษณ์ ซึ่งมีค่ามากกว่าการส่งข้อมูลที่มีความน่าจะเป็นแต่ละสัญลักษณ์ไม่เท่ากันหรือความไม่แน่นอนของสัญลักษณ์มีค่าน้อย

เมื่อต้นทางส่งตัวแปรสุ่ม X ผ่านช่องสัญญาณรบกวน และ Y คือตัวแปรสุ่มที่ได้รับจากช่องสัญญาณ ดังนั้น เอนโทรปีเงื่อนไข (conditional entropy) หรือความไม่แน่นอนของตัวแปรสุ่ม X เมื่อกำหนดให้แปรสุ่ม Y คำนวณได้จาก

$$H(X \mid Y) = \mathrm{E}\left[\log_2\left(\frac{1}{P(x_i \mid y_j)}\right)\right] = \sum_i \sum_j P(x_i, y_j)\log_2\left(\frac{1}{P(x_i \mid y_j)}\right) \tag{2.23}$$

กรณีช่องสัญญาณปราศจากสัญญาณรบกวน จะทำให้เอนโทรปีที่ได้รับจากช่องสัญญาณจะมีค่าเท่ากับ $H(X)$ อย่างไรก็ตาม กรณีช่องสัญญาณประกอบด้วยสัญญาณรบกวน เอนโทรปีที่ได้รับหรือข่าวสารร่วม (mutual information) จะมีค่าเท่ากับ

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \quad (2.24)$$

ทั้งนี้ อาจกล่าวได้ว่า เมื่อทำการวัดความไม่แน่นอนของตัวแปรสุ่ม X ที่ถูกส่งผ่านช่องสัญญาณจากตัวแปรสุ่ม Y ข่าวสารร่วมจะบ่งบอกความไม่แน่นอนของตัวแปรสุ่ม X ที่ลดลงเมื่อส่งผ่านช่องสัญญาณ ในทางกลับกันข่าวสารร่วมบ่งบอกความไม่แน่นอนที่ลดลงของตัวแปรสุ่ม Y เมื่อทำการวัดความไม่แน่นอนของตัวแปรสุ่ม Y จากตัวแปรสุ่ม X

2.2.2 ความจุช่องสัญญาณ

สำหรับการสื่อสารผ่านช่องสัญญาณ กำหนดให้ตัวแปรสุ่ม X คืออินพุตของช่องสัญญาณซึ่งประกอบไปด้วยสัญลักษณ์ $\{x_1, x_2, \ldots, x_M\}$ และมีความหนาแน่นความน่าจะเป็นเท่ากับ $p(x)$ และตัวแปรสุ่ม Y คือ เอาต์พุตของช่องสัญญาณ ดังนั้น สามารถหาฟังก์ชันความหนาแน่นความน่าจะเป็น $p(x)$ ที่ทำให้ข่าวสารร่วมในสมการที่ 2.24 มีค่าสูงสุด โดยเรียกค่าข่าวสารร่วมสูงสุดว่า ความจุช่องสัญญาณ (channel capacity) ดังนี้

$$C = \max_{p(x)} I(X;Y) \qquad \text{(บิตต่อสัญลักษณ์)} \quad (2.25)$$

กรณีช่องสัญญาณมีคุณสมบัติสมมาตร (symmetric) ข่าวสารร่วมจะมีค่าสูงสุด เมื่อความหนาแน่นความน่าจะเป็น $p(x)$ จะมีการกระจายตัวแบบสม่ำเสมอ

ความจุช่องสัญญาณ สามารถอธิบายประสิทธิภาพของสื่อสารผ่านช่องสัญญาณ โดยแสดงในรูปเอนโทรปีสูงสุดหรือปริมาณข่าวสารสูงสุดที่สามารถส่งผ่านช่องสัญญาณ มีหน่วยเป็นบิตต่อสัญลักษณ์ ดังนั้น การเข้ารหัสข้อมูลไบนารีด้วยอัตรารหัส R (นิยาม อัตรารหัส คือ อัตราส่วนของจำนวนบิตของข้อมูลต่อจำนวนบิตของข้อมูลที่ถูกเข้ารหัส) ทำให้ปริมาณข้อมูลเฉลี่ยเท่ากับ R บิตต่อสัญลักษณ์ จะต้องมีค่าน้อยกว่าหรือเท่ากับความจุช่องสัญญาณเสมอ หรือ $R \le C$ ถึงจะสามารถส่งข้อมูลปริมาณ R บิตต่อสัญลักษณ์ ผ่านช่องสัญญาณรบกวนได้

2.2.2.1 ความจุช่องสัญญาณสมมาตรไบนารี

สำหรับช่องสัญญาณสมมาตรไบนารี สามารถคำนวณข่าวสารร่วมได้ ดังนี้

$$H(X;Y) = H(Y) - H(Y|X) \quad (2.26)$$

เมื่อความไม่แน่นอนของตัวแปรสุ่ม Y เมื่อกำหนดให้ ตัวแปรสุ่ม X คำนวณได้จาก

$$H(Y|X)=\sum_i\sum_j P(y_j|x_i)P(x_i)\log_2\left(\frac{1}{P(y_j|x_i)}\right) \tag{2.27}$$

ข่าวสารร่วมจะมีค่าสูงสุดเมื่อความน่าจะเป็น $P(x=0)=P(x=1)=1/2$ ทำให้

$$\begin{aligned}H(Y|X)=&-\left(\frac{1}{2}P(y=0|x=0)\log_2 P(y=0|x=0)+\frac{1}{2}P(y=1|x=0)\log_2 P(y=1|x=0)+\right.\\&\left.\frac{1}{2}P(y=1|x=1)\log_2 P(y=1|x=1)+\frac{1}{2}P(y=0|x=1)\log_2 P(y=0|x=1)\right)\\=&-\left(p_{\text{BSC}}\log_2 p_{\text{BSC}}+(1-p_{\text{BSC}})\log_2(1-p_{\text{BSC}})\right)\end{aligned}$$

กำหนดให้ฟังก์ชัน $\mathcal{H}(p_{\text{BSC}})=-\left(p_{\text{BSC}}\log_2 p_{\text{BSC}}+(1-p_{\text{BSC}})\log_2(1-p_{\text{BSC}})\right)$ เนื่องจากเอนโทรปี $H(Y)=1$ ดังนั้น ความจุช่องสัญญาณมีค่าเท่ากับ

$$C_{\text{BSC}}=1-\mathcal{H}(p_{\text{BSC}}) \tag{2.28}$$

2.2.2.2 ความจุช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต

กำหนดให้สัญญาณไบนารี $x\in\{-1,1\}$ มีความน่าจะเป็น $P(x=0)=P(x=1)=1/2$ ถูกส่งผ่านช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต และสัญญาณ y คือสัญญาณที่ได้รับจากช่องสัญญาณในรูปที่ 2.3 ดังนั้น สามารถคำนวณหาความน่าจะเป็นของสัญญาณที่ได้รับจาก

$$\begin{aligned}p(y)&=p(y|x=1)P(x=1)+p(y|x=-1)P(x=-1)\\&=\frac{1}{2}p(y|x=1)+\frac{1}{2}p(y|x=-1)\end{aligned} \tag{2.29}$$

เมื่อ $p(y|x=\pm1)$ คือ ฟังก์ชันความหนาแน่นความน่าจะเป็นตามสมการที่ 2.11 ทำให้

$$p(y)=\frac{1}{\sqrt{8\pi\sigma^2}}\left(\exp\left(-\frac{(y-1)^2}{2\sigma^2}\right)+\exp\left(-\frac{(y+1)^2}{2\sigma^2}\right)\right) \tag{2.30}$$

ดังนั้น เอนโทรปีของสัญญาณ y ที่ได้รับจากช่องสัญญาณมีค่าเป็น

$$H(Y)=-\int_{-\infty}^{\infty}p(y)\log_2 p(y)dy \tag{2.31}$$

เอนโทรปีเงื่อนไขของสัญญาณที่ได้รับ y เมื่อกำหนดให้สัญญาณที่ถูกส่ง x สามารถคำนวณได้จากเอนโทรปีของสัญญาณรบกวน n ดังนี้

$$H(Y|X) = H(X+N|X) = H(N|X) = H(N) \tag{2.32}$$

โดยเอนโทรปีของสัญญาณรบกวน $n \sim (0,\sigma^2)$ เท่ากับ

$$\begin{aligned} H(N) &= -E\left[\log_2\left(\frac{1}{\sqrt{2\pi\sigma^2}}e^{\left(\frac{n^2}{2\sigma^2}\right)}\right)\right] \\ &= -\log_2\left(\frac{1}{\sqrt{2\pi\sigma^2}}\right) + \left(\frac{E\left[n^2\right]}{2\sigma^2}\right)\log_2(e) \\ &= -\log_2\left(\frac{1}{\sqrt{2\pi\sigma^2}}\right) + \left(\frac{\sigma^2}{2\sigma^2}\right)\log_2(e) \\ &= \frac{1}{2}\log_2\left(2\pi e\sigma^2\right) \end{aligned} \tag{2.33}$$

แทนค่าสมการ 2.28 และ 2.29 ในสมการที่ 2.22 ดังนั้น ความจุช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต จะมีค่าเท่ากับ

$$C_{\text{AWGN}} = -\int_{-\infty}^{\infty} p(y)\log_2 p(y)dy - \frac{1}{2}\log_2\left(2\pi e\sigma^2\right) \tag{2.34}$$

เมื่อ $p(y)$ หาได้จากสมการ 2.28 รูปที่ 2.4 แสดงความจุช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต โดยอัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนหาได้จากสมการที่ 2.11 กำหนดให้ อัตรารหัสในสมการมีค่าเท่ากับ $R = C_{AWGN}$ ในที่นี้จะพบว่าเมื่ออัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนสูงขึ้น จะทำให้ความจุช่องสัญญาณสูงขึ้นหรือสามารถส่งปริมาณข้อมูลเฉลี่ย (บิตต่อสัญลักษณ์) ได้สูงขึ้น ในที่นี้ เมื่อกำหนดให้ปริมาณข้อมูลเฉลี่ยหรืออัตรารหัสมีค่าใดๆ จะสามารถคำนวณหาอัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนต่ำสุดที่ทำให้การส่งข้อมูลปริมาณ R บิตต่อสัญลักษณ์ ผ่านช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุตปราศจากความผิดพลาด หรือเรียกว่าขีดจำกัดของแชนนอน (Shannon limit) ดังตารางที่ 2.1

ตารางที่ 2.1 ขีดจำกัดของแชนนอน

อัตรารหัส R	$SNR_{Shannon\ limit}$ (dB)
0.1	-1.277
0.3	-0.618
0.5	0.188
0.7	1.272
0.9	3.199

2.2.2.3 ความจุช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

พิจารณาช่องสัญญาณเรียงต่อดังรูปที่ 2.2 ซึ่งมีฟังก์ชันความหนาแน่นความน่าจะเป็นของสัญญาณที่ได้รับ y เมื่อกำหนดให้สัญญาณที่ถูกส่ง x ตามสมการที่ 2.14 เมื่อนำไปแทนค่าในสมการที่ 2.29 จะได้

$$p(y)=\frac{1}{\sqrt{8\pi\sigma^2}}\left(p_{\mathrm{BSC}}\exp\left(-\frac{(y_i-1)^2}{2\sigma^2}\right)+(p_{\mathrm{BSC}}-1)\exp\left(-\frac{(y_i+1)^2}{2\sigma^2}\right)+\right.$$
$$\left.(p_{\mathrm{BSC}}-1)\exp\left(-\frac{(y_i-1)^2}{2\sigma^2}\right)+p_{\mathrm{BSC}}\exp\left(-\frac{(y_i+1)^2}{2\sigma^2}\right)\right) \tag{2.35}$$

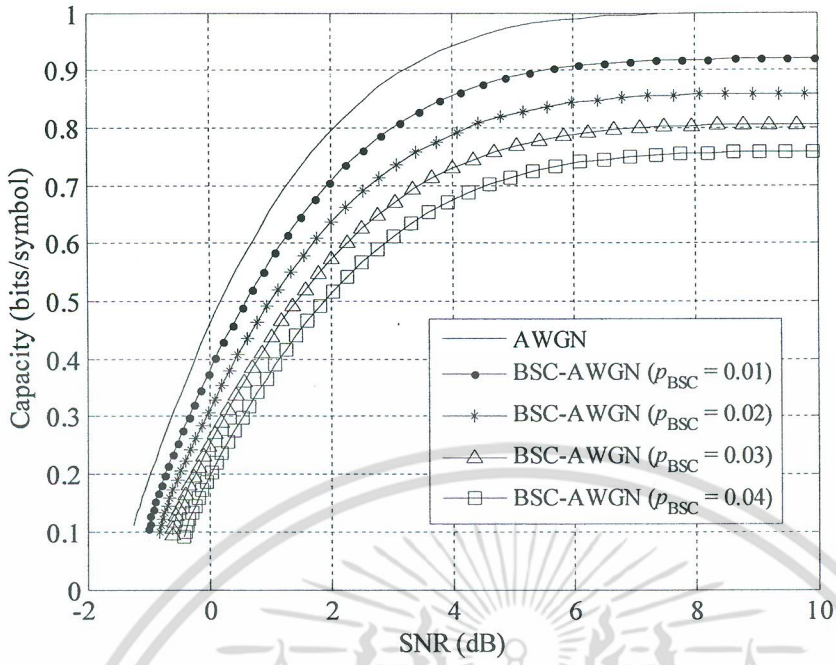
และเอนโทรปีเงื่อนไขคำนวณได้จาก

$$\begin{aligned}H(Y|X)&=-E\left[\log_2 p(y|x)\right]\\&=-\sum_{x=\pm1}\frac{1}{2}\int_{-\infty}^{\infty}p(y|x)\log_2 p(y|x)\\&=-\int_{-\infty}^{\infty}p(y|x)\log_2 p(y|x)\end{aligned} \tag{2.36}$$

ดังนั้น ความจุของช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวกหาได้จาก

$$C_{\mathrm{BSC}\rightarrow\mathrm{AWGN}}=-\int_{-\infty}^{\infty}p(y)\log_2 p(y)dy+\int_{-\infty}^{\infty}p(y|x)\log_2 p(y|x)dy \tag{2.37}$$

เมื่อ $p(y)$ และ $p(y|x)$ คือความหนาแน่นความน่าจะเป็นในสมการที่ 2.35 และ 2.14 ตามลำดับ รูปที่ 2.4 แสดงความจุช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก จากรูปจะเห็นได้ว่าเมื่อค่าความน่าจะเป็นตัดข้าม p_{BSC} เพิ่มสูงขึ้นจะทำให้ความจุช่องสัญญาณลดลง



รูปที่ 2.4 ความจุช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

นอกจากนี้ สำหรับค่าความน่าจะเป็นตัดข้าม p_{BSC} ใดๆ เมื่อทำการเพิ่มค่าเอสเอ็นอาร์จะทำให้ความจุช่องสัญญาณเพิ่มขึ้น อย่างไรก็ตามความจุช่องสัญญาณจะมีค่าน้อยกว่า 1 บิตต่อสัญลักษณ์ เนื่องจากเมื่อพิจารณาช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก กรณีช่องสัญญาณสมมาตรไบนารีที่มีค่าความน่าจะเป็นตัดข้ามอยู่ในช่วง $0 < p_{\text{BSC}} < 1$ จะทำให้เอนโทรปีที่ได้รับน้อยกว่าหนึ่ง $H(V) < 1$ ดังนั้น เมื่อนำข่าวสารส่งผ่านช่องสัญญาณถัดไปทำให้เอนโทรปีที่ได้รับจากช่องสัญญาณจะมีค่าเท่ากับ $H(Y) \le H(V)$ เสมอ

2.2.2.4 ความจุช่องสัญญาณผลตอบสนองบางส่วน

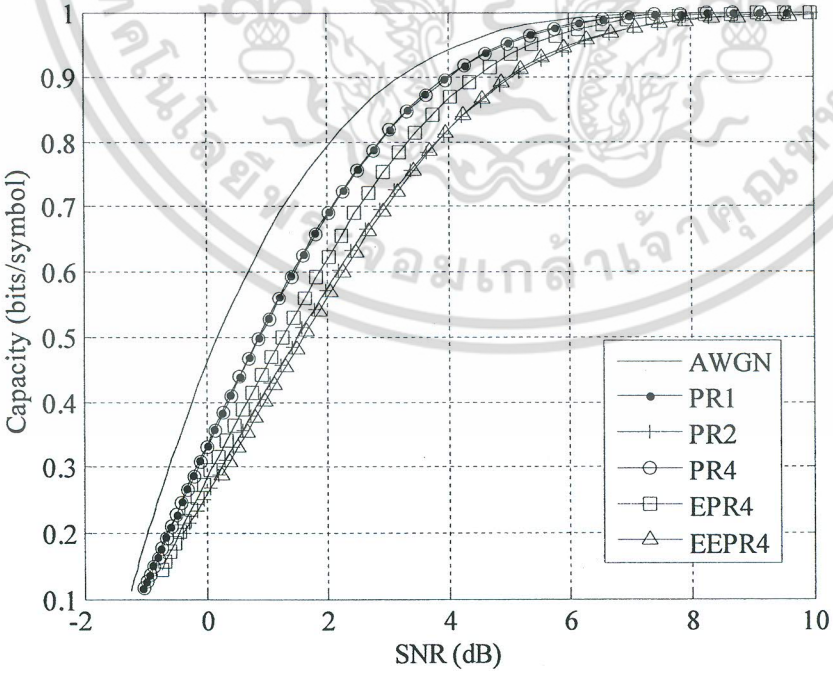
กำหนดให้ $\mathbf{x} = (x_1, x_2, \ldots, x_\tau)$ คือ สัญญาณไบนารีอินพุต และ $\mathbf{y} = (y_1, y_2, \ldots, y_\tau)$ คือ สัญญาณเอาต์พุตของช่องสัญญาณผลตอบสนองบางส่วนดังรูปที่ 2.3 ความจุช่องสัญญาณมีค่าเท่ากับ $I(X|Y) = H(Y) - H(Y|X)$ เมื่อเอนโทรปีเงื่อนไข $H(Y|X)$ คำนวณได้จาก $H(N)$ ตามสมการที่ 2.33 ในงานวิจัย [23] นำเสนอการคำนวณเอนโทรปี $H(Y)$ จากการทำซ้ำไปข้างหน้า (forward recursion) ของวงจรตรวจหาบีซีเจอาร์ [24] กำหนดให้ $\alpha(m)$ คือผลลัพธ์ของการทำซ้ำไปข้างหน้าที่สถานะ m ดังนั้นความน่าจะเป็นของสัญญาณที่ได้รับ $\mathbf{y}$ หาได้จากผลรวมของ $\alpha(m)$ เมื่อ m มีค่าใดๆ เขียนเป็นสมการได้ดังนี้

$$p(\mathbf{y}) = \sum_{m} \alpha(m) \tag{2.38}$$

จากทฤษฎี Shannon-McMillan-Breimann [25] จะได้

$$H(Y) = \lim_{\tau=\infty}\left(-\frac{1}{\tau}\log_2 p(\mathbf{y})\right) \tag{2.39}$$

ดังนั้นเอนโทรปี $H(Y)$ สามารถหาได้ด้วยการจำลองมอนติคาร์โล (Monte Carlo) โดยหาความน่าจะเป็น $p(\mathbf{y})$ จากกระบวนการทำซ้ำไปข้างหน้า (forward recursion) ในวงจรตรวจหาบีซีเจอาร์ จากนั้นทำการคำนวณเอนโทรปี $H(Y)$ ด้วยสมการที่ 2.39 ผลการคำนวณความจุช่องสัญญาณผลตอบสนองบางส่วนแสดงได้ดังรูปที่ 2.5 โดยค่าเอสเอ็นอาร์สามารถคำนวณได้จากสมการที่ 2.20 และอัตรารหัสในสมการมีค่าเท่ากับ $R = C_{AWGN}$ จากรูปสังเกตได้ว่า เมื่อค่าเอสเอ็นอาร์เท่ากับ -1 dB ถึง 8 dB ความจุช่องสัญญาณของช่องสัญญาณผลตอบสนองบางส่วนจะมีค่าต่ำกว่าความจุช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต โดยช่องสัญญาณผลตอบสนองบางส่วนแบบพีอาร์วันและพีอาร์โฟร์ ซึ่งเขียนในรูปสมการได้เป็น $H(D) = 1 + D$ และ $H(D) = 1 - D^2$ ตามลำดับ จะมีความจุช่องสัญญาณเท่ากัน เช่นเดียวกับช่องสัญญาณผลตอบสนองบางส่วนแบบพีอาร์ทูและอีอีพีอาร์โฟร์ ซึ่งเขียนในรูปสมการได้เป็น $H(D) = 1 + 2D + D^2$ และ $H(D) = 1 + 2D - 2D^3 - D^4$ ตามลำดับ จะมีความความจุช่องสัญญาณเท่ากัน นอกจากนี้ ช่องสัญญาณผลตอบสนองบางส่วนแบบพีอาร์ทูและอีอีพีอาร์โฟร์ จะมีความจุช่องสัญญาณต่ำสุดเมื่อเทียบกับช่องสัญญาณผลตอบสนองแบบพีอาร์วัน พีอาร์โฟร์ และอีพีอาร์โฟร์



รูปที่ 2.5 ความจุช่องสัญญาณผลตอบสนองบางส่วน

2.2.3 ขอบเขตความผิดพลาด

ในหัวข้อที่ผ่านมา กล่าวถึง ความจุช่องสัญญาณหรือปริมาณข่าวสารสูงสุดที่สามารถส่งผ่านช่องสัญญาณโดยปราศจากความผิดพลาดของข้อมูล ดังนั้น เมื่อปริมาณข่าวสารมีค่ามากกว่าความจุช่องสัญญาณจะทำให้เกิดความผิดพลาดของข้อมูล นิยามความผิดพลาดด้วยอัตราบิตผิดพลาด P_b มีค่าเท่ากับ อัตราส่วนจำนวนบิตผิดพลาดต่อจำนวนบิตข้อมูล ในกรณีนี้ สามารถคำนวณอัตราบิตผิดพลาด P_b ด้วยแบบจำลองดังรูปที่ 2.6 เมื่อกำหนดให้ข่าวสารที่ได้รับปราศจากความผิดพลาด แต่การเข้ารหัสบีบอัดข้อมูลแบบสูญเสีย (lossy compression) ก่อให้เกิดอัตราบิตผิดพลาด P_b

รูปที่ 2.6 การเข้ารหัสบีบอัดข้อมูลแบบสูญเสียและเชื่อมต่อกับการเข้ารหัสแก้ไขความผิดพลาด

กำหนดให้ การเข้ารหัสบีบอัดข้อมูลมีอัตรารหัสเท่ากับ R_s และรหัสแก้ไขความผิดพลาดมีอัตรารหัสคือ R_c ดังนั้น อัตรารหัสของระบบคำนวณได้จาก $R = R_c / R_s$ การเข้ารหัสบีบอัดข้อมูลแบบสูญเสียที่มีอัตราบิตผิดพลาด P_b สามารถคำนวณความจุหรืออัตรารหัสสูงสุดได้จากทฤษฎีความจุช่องสัญญาณแบบสูญเสีย (rate distortion theory) [25] ดังนี้

$$R_s = 1 - \mathcal{H}(P_b) \tag{2.40}$$

เมื่อฟังก์ชัน $\mathcal{H}(.)$ คือฟังก์ชันคำนวณเอนโทรปีในสมการที่ 2.28 หรือพิจารณาการสูญเสียด้วยแบบจำลองช่องสัญญาณสมมาตรไบนารี ดังนั้น เมื่อกำหนดให้ปริมาณข่าวสารที่ต้องการส่งผ่านช่องสัญญาณ R บิตต่อสัญลักษณ์ และอัตราบิตผิดพลาด P_b จะสามารถคำนวณความจุหรืออัตรารหัสสูงสุด R_c ของช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต จากความสัมพันธ์

$$R = \frac{R_c}{1 - \mathcal{H}(P_b)} \tag{2.41}$$

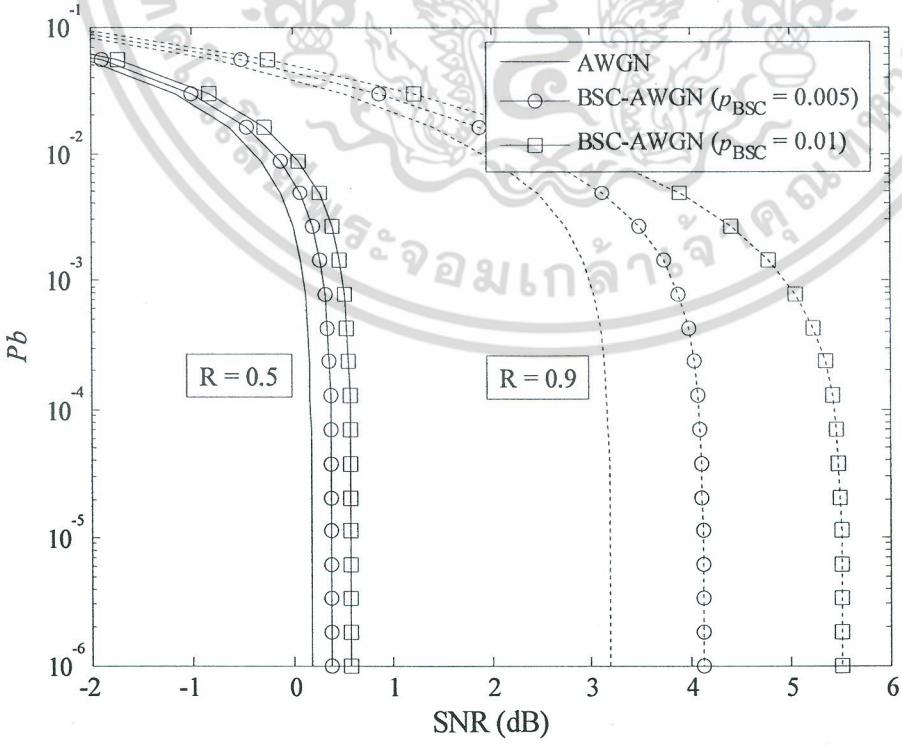
จากสมการที่ 2.34 ทำให้

$$R_c = C_{\text{AWGN}}(\sigma) \tag{2.42}$$

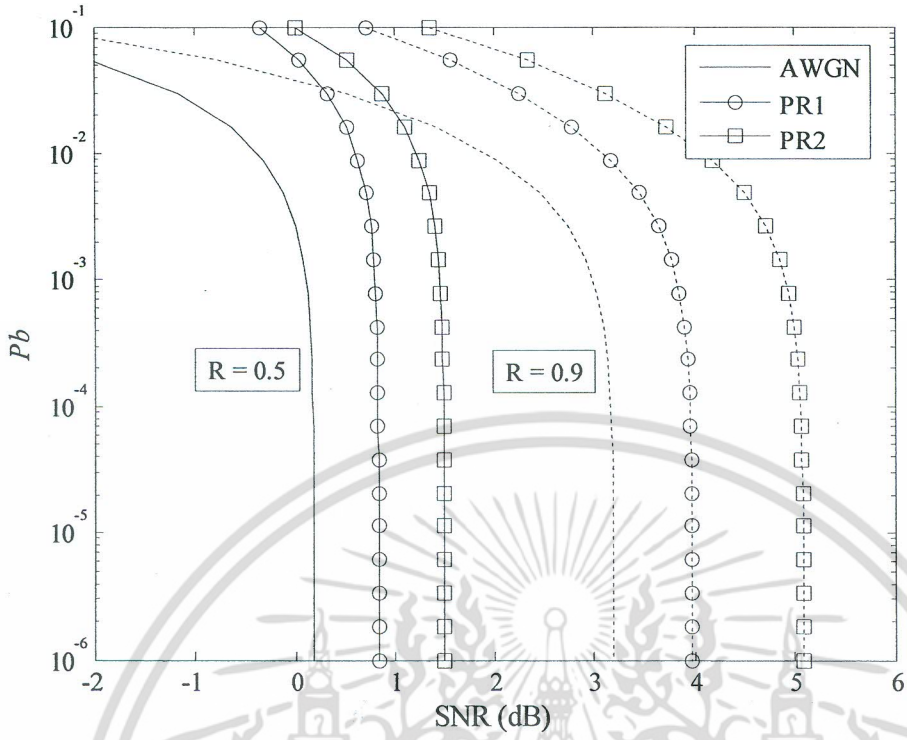
เมื่อ σ คืออินพุตของฟังก์ชันการคำนวณความจุช่องสัญญาณ

ดังนั้น จากสมการที่ 2.41 และ 2.42 จะสามารถคำนวณหา σ ซึ่งทำให้ข่าวสารที่ต้องการส่งปริมาณ R บิตต่อสัญลักษณ์ ก่อให้เกิดอัตราบิตผิดพลาด P_b รูปที่ 2.7 แสดงอัตราบิตผิดพลาด P_b ของช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต โดยอัตรารหัสเท่ากับ 0.5 และ 0.9 จะแทนด้วยเส้นทึบและเส้นประ ตามลำดับ สังเกตได้ว่า เมื่ออัตราบิตผิดพลาดลดลง จะทำให้อัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนเข้าใกล้ขีดจำกัดของแชนนอนในตารางที่ 2.1 นอกจากนี้ในรูปมีการเปรียบเทียบอัตราบิตผิดพลาดกับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก เมื่อค่าเอสเอ็นอาร์เท่ากับ -2 ถึง -1 dB และ -2 ถึง 1 dB สำหรับอัตรารหัสเท่ากับ 0.5 และ 0.9 ตามลำดับ ค่าความน่าจะเป็นตัดข้ามส่งผลต่อให้อัตราบิตผิดพลาดสูงขึ้นเล็กน้อย อย่างไรก็ตามเมื่อค่าเอสเอ็นอาร์เพิ่มสูงขึ้น ค่าความน่าจะเป็นตัดข้ามส่งผลให้อัตราบิตผิดพลาดสูงขึ้นมาก โดยเฉพาะอัตรารหัส 0.9 เมื่อพิจารณาที่อัตราบิตผิดพลาดเท่ากับ 1×10^{-6} สำหรับค่าความน่าจะเป็นตัดข้ามเท่ากับ 0.05 และ 0.01 เอสเอ็นอาร์ที่ต้องการจะเพิ่มขึ้น 0.932 dB และ 2.32 dB ตามลำดับ

สำหรับช่องสัญญาณผลตอบสนองบางส่วน ขอบเขตความผิดพลาดแสดงได้ดังรูปที่ 2.8 โดยช่องสัญญาณผลตอบสนองบางส่วนแบบพีอาร์ทู จะมีอัตราบิตผิดพลาดสูงกว่าช่องสัญญาณแบบพีอาร์วันและช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต พิจารณาที่อัตราบิตผิดพลาดเท่ากับ 1×10^{-6} สำหรับอัตรารหัสเท่ากับ 0.5 เอสเอ็นอาร์จะเพิ่มขึ้น 0.6467 dB และ 1.306 dB สำหรับช่องสัญญาณแบบพีอาร์วันและพีอาร์ทู กรณีอัตรารหัสเท่ากับ 0.9 เอสเอ็นอาร์เพิ่มขึ้น 0.777 dB และ 1.887 dB ตามลำดับ



รูปที่ 2.7 ขอบเขตความผิดพลาดของช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก



รูปที่ 2.8 ขอบเขตความผิดพลาดของช่องสัญญาณผลตอบสนองบางส่วน

บทที่ 3
รหัสพาริตี้เช็คความหนาแน่นต่ำ

รหัสพาริตี้เช็คความหนาแน่นต่ำหรือรหัสแอลดีพีซี (low-density parity-check codes, LDPC codes) [1] จัดเป็นรหัสแก้ไขความผิดพลาดชนิดหนึ่งในระบบสื่อสารดิจิตอล ซึ่งถูกนำเสนอในปี ค.ศ. 1962 โดย Robert Gallager ในงานวิจัยได้นำเสนอรหัสบล็อกเชิงเส้นชนิดหนึ่งซึ่งจำนวนเลขหนึ่งในเมทริกซ์พาริตี้เช็ค มีจำนวนน้อยเมื่อเทียบกับขนาดของเมทริกซ์พาริตี้เช็ค อย่างไรก็ตามรหัสแอลดีพีซีไม่ได้รับความสนใจมากนักในช่วงเวลาดังกล่าว จนกระทั่งในปี ค.ศ. 1997 ได้มีงานวิจัยของ David Mackay [2] ที่พบว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานเข้าใกล้ลิมิตของแชนนอน (Shannon limit) นอกจากนี้ งานวิจัยของ Thomas J. Richardson [28] ยังแสดงให้เห็นถึงความจุช่องสัญญาณที่ได้จากรหัสแอลดีพีซีมีค่าเข้าใกล้ทฤษฎีของแชนนอน

ในบทนี้ จะกล่าวถึงพื้นฐานของรหัสแอลดีพีซี ได้แก่ เมทริกซ์กำเนิดและเมทริกซ์พาริตี้เช็ค วิธีการเข้ารหัสของรหัสแอลดีพีซี คุณลักษณะและการจำแนกประเภทของรหัสแอลดีพีซี สุดท้ายจะอธิบายวิธีการออกแบบรหัสแอลดีพีซีที่ถูกนำเสนอโดย Robert Gallager และ David Mackay รวมถึงการออกแบบรหัสแอลดีพีซีที่ได้รับความนิยมในปัจจุบัน

3.1 เมทริกซ์กำเนิดและเมทริกซ์พาริตี้เช็ค

รหัสแอลดีพีซีจัดเป็นรหัสบล็อกเชิงเส้นชนิดหนึ่ง ซึ่งบิตข้อมูลไบนารีจะถูกแบ่งออกเป็นบล็อกที่มีขนาดเท่ากัน โดยแต่ละบล็อกข้อมูลจะมีบิตข้อมูลเป็นจำนวน K บิต จากนั้นบล็อกข้อมูลในรูปของเวกเตอร์ $\mathbf{u}=(u_1,u_2,\ldots,u_K)$ จะถูกเข้ารหัส เพื่อให้ได้ข้อมูลชุดใหม่เรียกว่าคำรหัส (codeword) ขนาด N บิต เขียนในรูปของเวกเตอร์ได้เป็น $\mathbf{v}=(v_1,v_2,\ldots,v_N)$ ซึ่งคำรหัสนี้จะประกอบไปด้วยข้อมูลจำนวน K บิต และบิตพาริตี้ (parity bits) จำนวน $N-K$ บิต ดังนั้นปริมาณข้อมูลเฉลี่ยในคำรหัสหรืออัตรารหัส (code rate) มีค่าเท่ากับ

$$R=\frac{K}{N} \tag{3.1}$$

โดยอัตรารหัสจะมีค่าเป็น $0<R\leq 1$ เสมอ คุณสมบัติของรหัสบล็อกเชิงเส้นที่สำคัญ คือ การบวกแบบโมดูโล 2 (modulo-2) ของ 2 คำรหัส จะได้คำรหัสอื่นเสมอ และต้องมีคำรหัสซึ่งทุกบิตมีค่าเป็นศูนย์อยู่ด้วยเนื่องจากผลบวกระหว่างคำรหัสใดๆ กับตัวมันเองจะได้คำรหัสที่ทุกบิตมีค่าเป็นศูนย์

จากคุณสมบัติของรหัสบล็อกเชิงเส้น [29] ทำให้รหัสบล็อกเชิงเส้นมีเวกเตอร์คำรหัสขนาด $1\times N$ ที่อิสระต่อกันจำนวน K คำ ได้แก่ $\mathbf{g}_1,\mathbf{g}_2,\ldots,\mathbf{g}_K$ โดยคำรหัสเวกเตอร์ $\mathbf{v}$ ใดๆ สามารถคำนวณได้จากผลรวมเชิงเส้นของเวกเตอร์คำรหัส ดังสมการต่อไปนี้

$$\mathbf{v}=u_1\mathbf{g}_1+u_2\mathbf{g}_2+\cdots+u_K\mathbf{g}_K=\mathbf{u}\cdot\mathbf{G} \tag{3.2}$$

เมื่อ $\mathbf{u}$ คือเวกเตอร์ข้อมูล และ $\mathbf{G}$ คือเมทริกซ์กำเนิด (generator matrix) ขนาด $K\times N$ ดังนี้

$$\mathbf{G}=\begin{bmatrix}\mathbf{g}_1\\ \mathbf{g}_2\\ \vdots\\ \mathbf{g}_K\end{bmatrix}=\begin{bmatrix}g_{1,1} & g_{1,2} & \cdots & g_{1,N}\\ g_{2,1} & g_{2,2} & \cdots & g_{2,N}\\ \vdots & \vdots & \ddots & \vdots\\ g_{K,1} & g_{K,2} & \cdots & g_{K,N}\end{bmatrix} \tag{3.3}$$

ดังนั้น กระบวนการเข้ารหัสของรหัสบล็อกเชิงเส้นเพื่อให้ได้คำรหัสเวกเตอร์ $\mathbf{v}$ สามารถหาได้จากการคูณกันของเวกเตอร์ข้อมูล $\mathbf{u}$ กับเมทริกซ์กำเนิด $\mathbf{G}$ ตามสมการที่ 3.2 สำหรับรหัสบล็อกเชิงเส้นใดๆ จะมีรหัสดูเอิล (dual code) ที่มีเวกเตอร์คำรหัสขนาด $1\times N$ เป็นอิสระต่อกันจำนวน $N-K$ คำ ได้แก่ $\mathbf{h}_1,\mathbf{h}_2,\ldots,\mathbf{h}_{N-K}$ เขียนอยู่ในรูปเมทริกซ์ได้ดังนี้

$$\mathbf{H}=\begin{bmatrix}\mathbf{h}_1\\ \mathbf{h}_2\\ \vdots\\ \mathbf{h}_{N-K}\end{bmatrix}=\begin{bmatrix}h_{1,1} & h_{1,2} & \cdots & h_{1,N}\\ h_{2,1} & h_{2,2} & \cdots & h_{2,N}\\ \vdots & \vdots & \ddots & \vdots\\ h_{N-K,1} & h_{N-K,2} & \cdots & h_{N-K,N}\end{bmatrix} \tag{3.4}$$

ในที่นี้จะเรียกเมทริกซ์ $\mathbf{H}$ ว่าเมทริกซ์พาริตี้เช็ค (parity check matrix) ซึ่งคำรหัสทุกคำในรหัสดูเอิล (dual code) จะตั้งฉากกับคำรหัสทุกคำในรหัสบล็อกเชิงเส้นเสมอ ดังนั้น เมื่อนำเมทริกซ์กำเนิด $\mathbf{G}$ คูณกับเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ ในรูปทรานสโพสจะได้

$$\mathbf{G}\cdot\mathbf{H}^{\mathrm{T}}=\mathbf{0} \tag{3.5}$$

และถ้า $\mathbf{v}$ เป็นคำรหัสคำหนึ่งในรหัสบล็อกเชิงเส้นแล้ว $\mathbf{v}$ จะต้องตั้งฉากกับเวกเตอร์ $\mathbf{h}$ ทุกตัว นั่นคือ

$$\mathbf{v}\cdot\mathbf{H}^{\mathrm{T}}=\mathbf{0} \tag{3.6}$$

กำหนดให้ $\hat{\mathbf{v}}$ คือเวกเตอร์คำรหัสที่ได้รับจากช่องสัญญาณรบกวน ดังนั้น กรณีคำรหัสที่ได้รับปราศจากความผิดพลาดจะทำให้ $\hat{\mathbf{v}} \cdot \mathbf{H}^{\mathrm{T}} = \mathbf{0}$ และกรณีคำรหัสเกิดความผิดพลาดจะทำให้ $\hat{\mathbf{v}} \cdot \mathbf{H}^{\mathrm{T}} \neq \mathbf{0}$

โดยทั่วไป สมรรถนะของรหัสใดๆ จะเพิ่มขึ้นเมื่อระยะห่างต่ำสุด (minimum distance) มีค่าสูง หรือมีจำนวนบิตที่แตกต่างกันระหว่าง 2 คำรหัสสูง สำหรับรหัสบล็อกเชิงเส้น ระยะห่างต่ำสุดจะเพิ่มขึ้นเมื่อจำนวนเลขหนึ่งในเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ เพิ่มขึ้น อย่างไรก็ตาม รหัสพาริตี้เช็คความหนาแน่นต่ำหรือรหัสแอลดีพีซี การเพิ่มจำนวนเลขหนึ่งในเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ จะส่งผลต่อสมรรถนะของการถอดรหัส อีกทั้งยังทำให้กระบวนการถอดรหัสมีความซับซ้อนเพิ่มขึ้น ดังนั้น รหัสแอลดีพีซีจึงนิยามด้วยรหัสบล็อกเชิงเส้นที่จำนวนเลขหนึ่งในเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ มีจำนวนน้อย

3.1.1 การเข้ารหัสเชิงระบบ

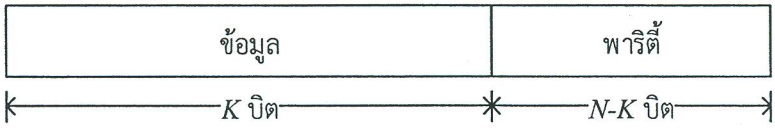
โดยทั่วไป เพื่อให้ง่ายต่อการแยกบิตข้อมูลและบิตพาริตี้ จึงนิยมจัดคำรหัสให้อยู่ในรูปของรหัสเชิงระบบ (systematic format) ดังรูปที่ 3.1 คำรหัสที่อยู่ในรูปของรหัสเชิงระบบจะประกอบไปด้วยส่วนที่เป็นข้อมูล K บิต และส่วนพาริตี้จำนวน $N-K$ บิต เรียงต่อกัน ดังนั้นเพื่อให้ได้คำรหัสในรูปรหัสเชิงระบบ การเข้ารหัสต้องกระทำผ่านเมทริกซ์กำเนิดที่มีลักษณะดังต่อไปนี้

$$\mathbf{G}_{sys} = \begin{bmatrix} \mathbf{I} & \mathbf{G}_{\mathrm{P}} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & g_{1,1} & g_{1,2} & \cdots & g_{1,N-K} \\ 0 & 1 & 0 & 0 & g_{2,1} & g_{2,2} & \cdots & g_{2,N-K} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & g_{K,1} & g_{K,2} & \cdots & g_{K,N-K} \end{bmatrix} \tag{3.7}$$

เมื่อ $\mathbf{I}$ คือเมทริกซ์เอกลักษณ์ สำหรับเมทริกซ์พาริตี้เช็คของรหัสเชิงระบบจะมีลักษณะดังต่อไปนี้

$$\mathbf{H}_{sys} = \begin{bmatrix} \mathbf{H}_{\mathrm{P}} & \mathbf{I} \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,N-K} & 1 & 0 & \cdots & 0 \\ h_{2,1} & h_{2,2} & \cdots & h_{2,N-K} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{N-K,1} & h_{N-K,2} & \cdots & h_{N-K,N-K} & 0 & 0 & \cdots & 1 \end{bmatrix} \tag{3.8}$$

โดยเมทริกซ์ $\mathbf{H}_{\mathrm{P}}$ จะมีค่าเท่ากับทรานสโพสของเมทริกซ์ $\mathbf{G}_{\mathrm{P}}$ เสมอ ทั้งนี้ สังเกตได้ว่า เมื่อกำหนดให้เมทริกซ์กำเนิดในรูปรหัสเชิงระบบจะสามารถคำนวณหาเมทริกซ์พาริตี้เช็คได้โดยง่าย ในทางกลับกันเมื่อกำหนดให้เมทริกซ์พาริตี้เช็คอยู่ในรูปรหัสเชิงระบบจะสามารถคำนวณหาเมทริกซ์กำเนิดได้



รูปที่ 3.1 รูปแบบของรหัสเชิงระบบ

การออกแบบรหัสแอลดีพีซีเกี่ยวข้องกับการออกแบบเมทริกซ์พาริตี้เช็ค ดังนั้น เมื่อทำการออกแบบเมทริกซ์พาริตี้เช็คเสร็จสิ้น การเข้ารหัสเชิงระบบสามารถกระทำได้โดยการแปลงเมทริกซ์พาริตี้เช็คเป็นเมทริกซ์กำเนิด ทั้งนี้อาจใช้เทคนิคการกำจัดเกาส์เซียน (Gaussian elimination) ร่วมกับการสลับหลักในการแปลงเมทริกซ์พาริตี้เช็คให้อยู่ในรูปเมทริกซ์พาริตี้เช็คเชิงระบบตามสมการที่ 3.8 ดังนั้น จากสมการที่ 3.2 คำรหัสที่ได้จากการเข้ารหัสเชิงระบบจะมีค่าเท่ากับ

$$v_i = \begin{cases} u_i & , \quad 1 \le i < K \\ u_0 g_{1,i} + u_1 g_{2,i} + \cdots + u_K g_{K,i} & , \quad K+1 \le i < N \end{cases} \tag{3.9}$$

3.1.2 การเข้ารหัสความซับซ้อนเชิงเส้น

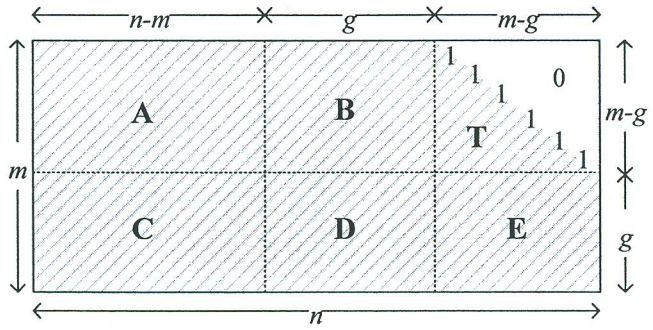
การเข้ารหัสเชิงระบบในหัวข้อที่ผ่านมา จำเป็นต้องใช้เทคนิคการกำจัดเกาส์เซียนเพื่อทำให้เมทริกซ์พาริตี้เช็คมีลักษณะตามสมการที่ 3.8 ก่อนทำการแปลงเป็นเมทริกซ์กำเนิดเพื่อทำการเข้ารหัส อย่างไรก็ตามการใช้เทคนิคการกำจัดเกาส์เซียนจะทำให้เมทริกซ์พาริตี้เช็คมีความหนาแน่นเพิ่มขึ้นทำให้ความซับซ้อนในการเข้ารหัสสูง โดยความซับซ้อนในการเข้ารหัสจะเพิ่มขึ้นเป็น $O(N^2)$ เมื่อ N คือความยาวของคำรหัส ในงานวิจัยของ Thomas J. Richarson [30] จึงได้นำเสนอวิธีการเข้ารหัสสำหรับเมทริกซ์พาริตี้เช็คมากเลขศูนย์ โดยวิธีการนี้ความซับซ้อนของการเข้ารหัสจะเพิ่มขึ้นแบบเชิงเส้นหรือ $O(N)$ การเข้ารหัสที่ถูกนำเสนอจะเริ่มจากการพิจารณาเมทริกซ์พาริตี้เช็คออกเป็นเมทริกซ์ย่อยดังต่อไปนี้

$$\mathbf{H} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{T} \\ \mathbf{C} & \mathbf{D} & \mathbf{E} \end{bmatrix} \tag{3.10}$$

จากนั้นใช้วิธีการสลับแถวหรือหลักเพื่อให้เมทริกซ์ $\mathbf{T}$ ขนาด $(m-g)\times(m-g)$ มีลักษณะเป็นเมทริกซ์สามเหลี่ยมล่างดังรูปที่ 3.2 ในที่นี้ความซับซ้อนของการเข้ารหัสจะขึ้นอยู่กับค่า g ที่เกิดขึ้น กล่าวคือ เมื่อค่า g มีค่าน้อยก็จะทำให้การเข้ารหัสมีความซับซ้อนต่ำ ในที่นี้จะพบว่าปริมาณเลขหนึ่งในเมทริกซ์พาริตี้เช็คจะยังคงเดิม

ลำดับต่อไปเป็นการทำให้เมทริกซ์ $\mathbf{E}$ กลายเป็นเมทริกซ์ศูนย์ด้วยวิธีการกำจัดเกาส์เซียนซึ่งเขียนสมการได้เป็น

$$\mathbf{H}' = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ -\mathbf{E}\mathbf{T}^{-1} & \mathbf{I} \end{bmatrix} \mathbf{H} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{T} \\ -\mathbf{E}\mathbf{T}^{-1}\mathbf{A} + \mathbf{C} & -\mathbf{E}\mathbf{T}^{-1}\mathbf{B} + \mathbf{D} & \mathbf{0} \end{bmatrix} \tag{3.11}$$



รูปที่ 3.2 เมทริกซ์สามเหลี่ยมล่างสำหรับการเข้ารหัสความซับซ้อนเชิงเส้น

กำหนดให้เวกเตอร์คำรหัสอยู่ในรูป $\mathbf{v}=[\mathbf{u}\quad \mathbf{p}_1\quad \mathbf{p}_2]$ เมื่อ $\mathbf{u}$ คือเวกเตอร์ข้อมูลขนาด $1\times n-m$ และ $\mathbf{p}_1$ คือเวกเตอร์พาริตี้ส่วนที่หนึ่งขนาด $1\times g$ และ $\mathbf{p}_2$ คือเวกเตอร์พาริตี้ส่วนที่สอง ขนาด $1\times(m-g)$ จากสมการที่ 3.6 เขียนใหม่ได้เป็น $\mathbf{Hv}^T=\mathbf{0}$ ทำให้ เมื่อแทนค่าเมทริกซ์พาริตี้เช็คในสมการที่ 3.11 จะได้

$$\mathbf{Au}^T+\mathbf{Bp}_1^T+\mathbf{Tp}_2^T=\mathbf{0} \tag{3.12}$$

$$(-\mathbf{ET}^{-1}\mathbf{A}+\mathbf{C})\mathbf{u}^T+(-\mathbf{ET}^{-1}\mathbf{B}+\mathbf{D})\mathbf{p}_1^T=\mathbf{0} \tag{3.13}$$

กำหนดให้ $\phi=-\mathbf{ET}^{-1}\mathbf{B}+\mathbf{D}$ ดังนั้น เวกเตอร์พาริตี้ส่วนที่หนึ่งคำนวณได้จาก

$$\mathbf{p}_1^T=-\phi^{-1}(-\mathbf{ET}^{-1}\mathbf{A}+\mathbf{C})\mathbf{u}^T \tag{3.14}$$

กรณีที่ไม่สามารถหาอินเวอร์สของ ϕ ให้ทำสร้างเมทริกซ์ $\mathbf{T}$ ในขั้นตอนแรกใหม่อีกครั้ง สำหรับเวกเตอร์พาริตี้ส่วนที่สองคำนวณได้จาก

$$\mathbf{p}_2^T=-\mathbf{T}^{-1}(\mathbf{Au}^T+\mathbf{Bp}_1^T) \tag{3.15}$$

3.1.3 การเข้ารหัสควอไซไซคลิก

การเข้ารหัสพาริตี้เช็คความหนาแน่นต่ำที่กล่าวมาในข้างต้น จำเป็นต้องใช้วงจรการบวกและคูณ ในหัวข้อนี้จะอธิบายการเข้ารหัสควอไซไซคลิก (quasi-cyclic) [31] ซึ่งมีความซับซ้อนต่ำและเหมาะกับการประยุกต์ใช้งาน โดยกระบวนการเข้ารหัสควอไซคลิกจะใช้เพียงชิฟต์รีจิสเตอร์ (shift-registers) ที่มีการป้อนกลับเนื่องจากคำรหัสมีลักษณะหมุนวน (cyclic) กล่าวคือ เมื่อนำคำรหัสหนึ่งมาทำการเลื่อนบิตแบบวนกลับแล้ว ผลลัพธ์ที่ได้จะเป็นคำรหัสด้วยเสมอ อย่างไรก็ตามเมทริกซ์พาริตี้เช็คจะต้องมีลักษณะดังนี้

$$\mathbf{H}_{\mathrm{QC}}=\begin{bmatrix}\mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,t}\\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,t}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{A}_{c,1} & \mathbf{A}_{c,2} & \cdots & \mathbf{A}_{c,t}\end{bmatrix} \tag{3.16}$$

เมื่อ $c\le t$ และ $\mathbf{A}_{i,j}$ คือเมทริกซ์เซอร์คิวแลนท์ (circulant matrix) ขนาด $b\times b$ ที่มีจำนวนเลขหนึ่งในแต่ละแถวหรือหลักเท่ากับ w โดยในแต่ละแถวของเมทริกซ์เซอร์คิวแลนท์เกิดจากการเลื่อนแถวที่อยู่ด้านบนหนึ่งครั้ง ตัวอย่างเช่น เมทริกซ์พาริตี้เช็คที่มีเมทริกซ์เซอร์คิวแลนท์ขนาด 5×5 ดังนี้

$$\mathbf{H}=\left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
1&0&0&0&0&0&0&0&0&1&0&0&1&1&0&0&0&1&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&1&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1\\
0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&0&0\\
\hline
0&1&0&0&0&1&1&0&0&0&1&0&0&0&0&0&1&1&0&0\\
0&0&1&0&0&0&1&1&0&0&0&1&0&0&0&0&0&1&1&0\\
0&0&0&1&0&0&0&1&1&0&0&0&1&0&0&0&0&0&1&1\\
0&0&0&0&1&0&0&0&1&1&0&0&0&1&0&1&0&0&0&1\\
1&0&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1&0&0&0
\end{array}\right]$$

พิจารณาเวกเตอร์คำรหัส $\mathbf{v}=(\mathbf{v}_1,\mathbf{v}_2,\ldots\mathbf{v}_t)$ ซึ่งสามารถแบ่งเป็นเวกเตอร์ย่อย $\mathbf{v}_j$ ขนาด $1\times b$ จากความสัมพันธ์ $\mathbf{v}\cdot\mathbf{H}^{\mathrm{T}}=\mathbf{0}$ สังเกตได้ว่าเวกเตอร์ย่อย $\mathbf{v}_j$ จะเกี่ยวข้องกับเมทริกซ์เซอร์คิวแลนท์ $\mathbf{A}_{i,j}$ ทุกแถวของเมทริกซ์พาริตี้เช็ค และเมื่อนำเวกเตอร์ย่อย $\mathbf{v}_j$ มาทำการเลื่อนแบบวนกลับจากซ้ายไปขวา l ครั้ง แทนด้วยสัญลักษณ์ $\mathbf{v}_j^{(l)}$ จะพบว่า $\mathbf{v}_j^{(0)}=\mathbf{v}_j^{(n)}=\mathbf{v}_j$ เมื่อ $n=cb$ กล่าวคือเมื่อทำการเลื่อนเวกเตอร์ย่อยเป็นจำนวนครั้งเท่ากับจำนวนแถวในเมทริกซ์พาริตี้เช็ค ผลลัพธ์ที่ได้คือเวกเตอร์ย่อยตัวเดิม ดังนั้น เมทริกซ์พาริตี้เช็คที่มีลักษณะแบบควอไซไซคลิก การสร้างคำรหัสใดๆ เกิดจากการเลื่อนเวกเตอร์ย่อยทุกตัวเป็นจำนวน l ครั้ง เขียนในรูปสมการได้เป็น $\mathbf{v}=(\mathbf{v}_1^{(l)},\mathbf{v}_2^{(l)},\ldots\mathbf{v}_t^{(l)})$

3.2 คุณลักษณะของรหัสพาริตี้เช็คความหนาแน่นต่ำ

ในหัวข้อนี้จะอธิบายคุณลักษณะของรหัสพาริตี้เช็คความหนาแน่นต่ำที่เกี่ยวข้องกับงานวิจัย ได้แก่ การกระจายตัว ฟีลด์จำกัด และวัฏจักร ซึ่งส่งผลต่อสมรรถนะการแก้ไขความผิดพลาดของรหัสพาริตี้เช็คความหนาแน่นต่ำ นอกจากนี้ คุณลักษณะการกระจายตัวและฟีลด์จำกัดยังถูกนำมาใช้ในการแยกประเภทของรหัสพาริตี้เช็คความหนาแน่นต่ำอีกด้วย

3.2.1 การกระจายตัว

รหัสแอลดีพีซี นิยามด้วยเมทริกซ์พาริตี้เช็คที่มีจำนวนเลขหนึ่งน้อยเมื่อเทียบกับขนาดของเมทริกซ์ สามารถจำแนกการกระจายตัวของเลขหนึ่งได้ 2 ลักษณะ ได้แก่ การกระจายตัวแบบสม่ำเสมอ และการกระจายตัวแบบไม่สม่ำเสมอ รหัสแอลดีพีซีที่ถูกนำเสนอครั้งแรกโดย Robert Gallager [1] จะมีลักษณะการกระจายตัวแบบสม่ำเสมอ นิยมเรียกรหัสประเภทนี้ว่ารหัสแอลดีพีซีแบบสม่ำเสมอ (regular LDPC codes) สำหรับรหัสแอลดีพีซีแบบไม่สม่ำเสมอ (irregular LDPC codes) ได้รับการนำเสนอโดย Thomas J. Richarson [32] จะมีการกระจายตัวแบบไม่สม่ำเสมอและเมื่อทำการออกแบบการกระจายตัวของเลขหนึ่งเป็นอย่างดีแล้ว รหัสแอลดีพีซีแบบไม่สม่ำเสมอให้สมรรถนะที่สูงกว่ารหัสแอลดีพีซีแบบสม่ำเสมอ

3.2.1.1 รหัสแอลดีพีซีแบบสม่ำเสมอ

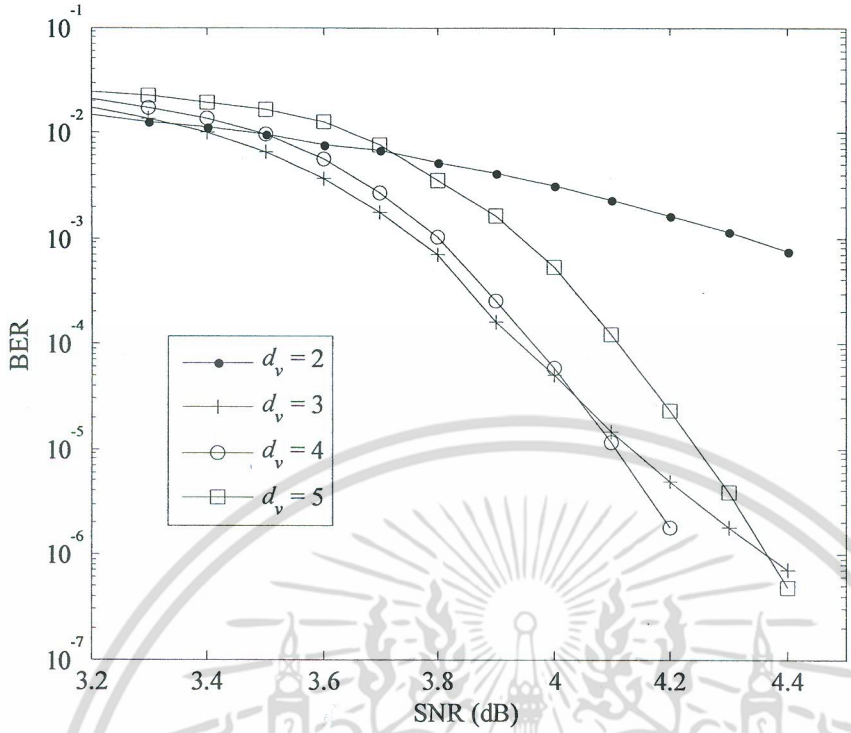
เมทริกซ์พาริตี้เช็คซึ่งมีการกระจายตัวของเลขหนึ่งแบบสม่ำเสมอ จะมีจำนวนเลขหนึ่งในแต่ละแถวเท่ากับ d_c และจำนวนเลขหนึ่งในแต่ละหลักเท่ากับ d_v กำหนดให้เมทริกซ์พาริตี้เช็คขนาด $M \times N$ ดังนั้นจำนวนเลขหนึ่งทั้งหมดในเมทริกซ์พาริตี้เช็คจะมีค่าเท่ากับ

$$E_{\text{Total}} = Md_c = Nd_v \tag{3.17}$$

ดังนั้น อัตรารหัสของรหัสแอลดีพีซีแบบสม่ำเสมอสามารถคำนวณได้จาก

$$R = \frac{K}{N} = \frac{N-M}{N} = \frac{N - Nd_v / d_c}{N} = 1 - \frac{d_v}{d_c} \tag{3.18}$$

รูปที่ 3.3 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีแบบสม่ำเสมอเมื่อทำการถอดรหัสวนซ้ำ 50 รอบ ในที่นี้ จะใช้อัลกอริทึมพีอีจีในการออกแบบเมทริกซ์พาริตี้เช็ค (รายละเอียดอัลกอริทึมพีอีจีอธิบายในหัวข้อที่ 3.3.2) เมื่อกำหนดให้อัตรารหัส $R = 8/9$ ความยาวของคำรหัส $N = 4608$ บิต และความยาวของบิตข้อมูล $K = 4096$ บิต ซึ่งเท่ากับขนาดข้อมูล 1 เซกเตอร์ในอุปกรณ์ฮาร์ดดิสก์ไดรฟ์โดยทั่วไป เมื่อระยะห่างต่ำสุดมีค่าน้อยจะส่งผลกระทบต่อสมรรถนะของรหัสที่เอสเอ็นอาร์สูง ดังนั้นการเพิ่มจำนวนเลขหนึ่งในแต่ละหลักหรือค่า d_v (ทำให้ระยะห่างต่ำสุดมีค่าสูง) จะทำให้สมรรถนะของรหัสดีขึ้น อย่างไรก็ตาม สำหรับรหัสแอลดีพีซี การเพิ่มค่า d_v ของเมทริกซ์พาริตี้เช็คมากเกินไปจะส่งผลให้สมรรถนะการถอดรหัสแอลดีพีซีลดลง รวมถึงความซับซ้อนในการถอดรหัสจะเพิ่มสูงขึ้น จากรูปแสดงให้เห็นว่ารหัสแอลดีพีซีที่มี $d_v = 3$ ให้สมรรถนะที่ดีกว่ารหัสแอลดีพีซีอื่นๆ เมื่อค่าเอสเอ็นอาร์อยู่ระหว่าง 3.4 ถึง 4 dB หรืออยู่ในช่วงวอเตอร์ฟอลล์ (waterfall region) (ในบทที่ 4 จะอธิบายการวิเคราะห์รหัสแอลดีพีซี ซึ่งจะแสดงให้เห็นว่า รหัสแอลดีพีซีแบบสม่ำเสมอเมื่อ $d_v = 3$ ให้สมรรถนะที่



รูปที่ 3.3 อัตราบิตผิดพลาดของรหัสแอลดีพีซีแบบสม่ำเสมอ

ดีสุดในช่วงวอเตอร์ฟอลล์) สำหรับค่าเอสเอ็นอาร์ที่สูงขึ้นรหัสแอลดีพีซีที่ค่า d_v เท่ากับ 3 จะมีสมรรถนะที่แย่กว่ารหัสแอลดีพีซีที่มี d_v เท่ากับ 4 และ 5 ในที่นี้สามารถอธิบายด้วยระยะห่างต่ำสุดของรหัสบล็อกเชิงเส้น

3.2.1.2 รหัสแอลดีพีซีแบบไม่สม่ำเสมอ

สำหรับเมทริกซ์พาริตี้เช็คที่มีการกระจายตัวของเลขหนึ่งแบบไม่สม่ำเสมอ กำหนดให้ d_c คือจำนวนเลขหนึ่งสูงสุดของแถวหรือน้ำหนักสูงสุดของแถว และ d_v คือจำนวนเลขหนึ่งสูงสุดของหลักหรือน้ำหนักสูงสุดของหลัก การกระจายตัวของเลขหนึ่งจะแสดงอยู่ในรูปพหุนาม ดังนี้

$$\rho(x) = \sum_{i=1}^{d_c} \rho_i x^{i-1} \tag{3.19}$$

$$\lambda(x) = \sum_{i=1}^{d_v} \lambda_i x^{i-1} \tag{3.20}$$

เมื่อ ρ_i คืออัตราส่วนระหว่างจำนวนเลขหนึ่งทั้งหมดในแถวที่มีน้ำหนักเท่ากับ i กับจำนวนเลขหนึ่งทั้งหมดในเมทริกซ์พาริตี้เช็ค และ λ_i คืออัตราส่วนระหว่างจำนวนเลขหนึ่งทั้งหมดในหลักที่มีน้ำหนัก

เท่ากับ i กับจำนวนเลขหนึ่งทั้งหมดในเมทริกซ์พาริตี้เช็ค ทั้งนี้ ผลรวมของอัตราส่วนในพหุนามจะเท่ากับ $\sum_{i=1}^{d_c}\rho_i = 1$ และ $\sum_{i=1}^{d_c}\lambda_i = 1$ ตัวอย่างเช่น

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{3.21}$$

จะมีพหุนามการกระจายตัว คือ $\rho(x) = \frac{4}{19}x^3 + \frac{15}{19}x^4$ และ $\lambda(x) = \frac{12}{19}x + \frac{3}{19}x^2 + \frac{4}{19}x^3$

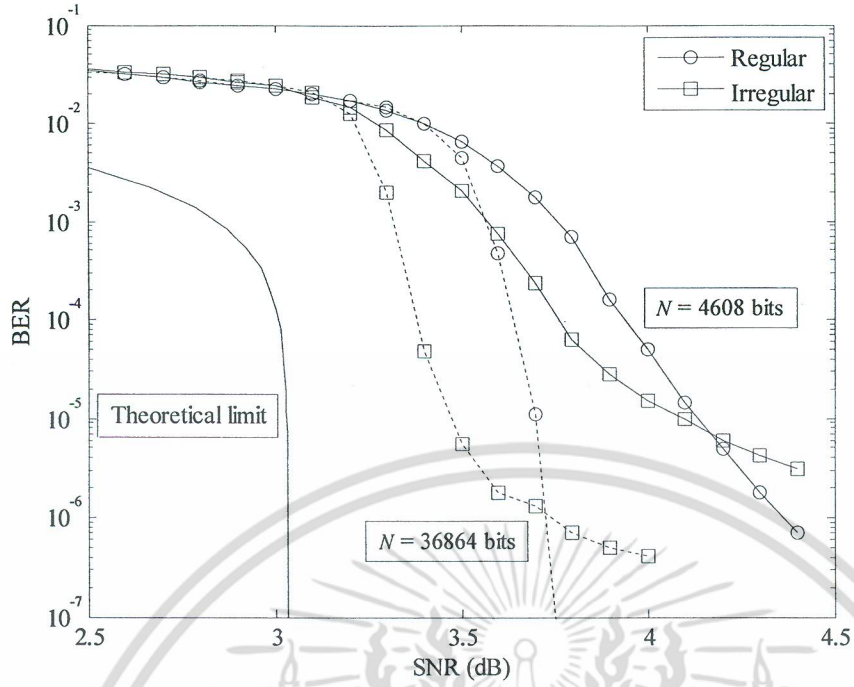
ทำให้ จำนวนเลขหนึ่งทั้งหมดในเมทริกซ์พาริตี้เช็คมีค่าเท่ากับ

$$E_{\text{Total}} = \frac{M}{\sum_{i=1}^{d_c}\rho_i / i} = \frac{N}{\sum_{i=1}^{d_v}\lambda_i / i} \tag{3.22}$$

ดังนั้น อัตรารหัสของรหัสแอลดีพีซีแบบไม่สม่ำเสมอจะมีค่าเป็น

$$R = \frac{K}{N} = \frac{N-M}{N} = 1 - \frac{\sum_{i=1}^{d_c}\rho_i / i}{\sum_{i=1}^{d_v}\lambda_i / i} \tag{3.23}$$

รูปที่ 3.4 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีแบบสม่ำเสมอซึ่งมี $d_v = 3$ เปรียบเทียบกับรหัสแอลดีพีซีแบบไม่สม่ำเสมอซึ่งมีพหุนามการกระจายตัวคือ $\lambda(x) = 0.1570x + 0.3430x^2 + 0.0363x^5 + 0.0591x^6 + 0.2793x^8 + 0.1252x^9$ และ $\rho(x) = 0.1277x^{34} + 0.8723x^{35}$ โดยกำหนดให้อัตรารหัส $R = 8/9$ และใช้อัลกอริทึมพีอีจี (รายละเอียดอัลกอริทึมพีอีจีอธิบายในหัวข้อ 3.3.2) จำนวนการถอดรหัสวนซ้ำเท่ากับ 50 รอบ พิจารณารหัสแอลดีพีซีเมื่อความยาวของคำรหัสเท่ากับ $N = 4608$ บิต จะพบว่ารหัสแอลดีพีซีแบบไม่สม่ำเสมอให้สมรรถนะที่ดีกว่าแอลดีพีซีแบบสม่ำเสมอ (ในบทที่ 4 จะแสดงการวิเคราะห์สมรรถนะของรหัสแอลดีพีซีแบบไม่สม่ำเสมอ โดยจะพบว่ารหัสแอลดีพีซีแบบไม่คงให้สมรรถนะที่ดีกว่ารหัสแอลดีพีซีแบบสม่ำเสมอ) เมื่อทำการเพิ่มความยาวคำรหัสเท่ากับ $N = 36864$ บิต (ในอุปกรณ์ฮาร์ดดิกส์สมัยใหม่ความยาวเซกเตอร์ข้อมูลจะเพิ่มขึ้น) จะสังเกตได้ว่ารหัสแอลดีพีซีแบบสม่ำเสมอและไม่สม่ำเสมอจะมีสมรรถนะที่ดีขึ้น ทั้งนี้ เนื่องจากการเพิ่มความยาวคำรหัสหรือขนาดของเมทริกซ์พาริตี้เช็ค โดยที่ปริมาณเลขหนึ่งในเมทริกซ์ยังคงเท่าเดิมจะทำให้ระยะห่าง



รูปที่ 3.4 อัตราบิตผิดพลาดของรหัสแอลดีพีซีแบบไม่สม่ำเสมอ

ต่ำสุด (minimum distance) เพิ่มสูงขึ้น [1] นอกจากนี้ จะสังเกตได้ว่ารหัสแอลดีพีซีแบบไม่สม่ำเสมอมีสมรรถนะที่เข้าใกล้ลิมิตของแชนนอน (รายละเอียดการคำนวณหาลิมิตของแชนนอนอธิบายในบทที่ 2) เมื่อค่าเอสเอ็นอาร์เท่ากับ 3.4 ถึง 4 dB รหัสแอลดีพีซีแบบไม่สม่ำเสมอจะเกิดความผิดพลาดต่ำสุด (error floor) โดยทั่วไป ความผิดพลาดต่ำสุดของรหัสแอลดีพีซีแบบไม่สม่ำเสมอจะเกิดจากโนดตัวแปรดีกรี 2 (รายละเอียดของโนดตัวแปรจะอธิบายในหัวข้อถัดไป) ดังนั้นการออกแบบรหัสแอลดีพีซีแบบไม่สม่ำเสมอจะต้องควบคุมจำนวนของโนดตัวแปรดีกรี 2 เพื่อให้เกิดความผิดพลาดต่ำสุดที่อัตราบิตผิดพลาดต่ำสุด นอกจากนี้ การเกิดเซตสต็อป (stopping set) [33] ในกราฟแทนเนอร์ จะส่งผลให้เกิดความผิดพลาดต่ำสุดในรหัสแอลดีพีซีแบบสม่ำเสมอและไม่สม่ำเสมอได้เช่นกัน

3.2.2 ฟิลด์จำกัด

กำหนดให้ฟิลด์จำกัด (finite field) หรือฟิลด์กาลัวส์ (Galois field) คือเซ็ตที่มีสมาชิกหรืออิลิเมนท์เป็นจำนวนจำกัด นอกจากนี้ กระบวนการบวก ลบ คูณ และหารระหว่างอิลิเมนท์ ผลลัพธ์ที่ได้จะเท่ากับอิลิเมนท์ที่อยู่ในเซ็ตเสมอ ตัวอย่างเช่น ฟิลด์จำกัดไบนารี ซึ่งมีอิลิเมนท์จำนวนตัว 2 ตัว ได้แก่ 0 และ 1 การบวกและคูณแบบมอดูโล 2 ระหว่างอิลิเมนท์ ผลลัพธ์ที่ได้จะเท่ากับ 0 และ 1 เสมอ สำหรับการลบและหาร ผลลัพธ์สามารถคำนวณได้จากการหาย้อนกลับของผลลัพธ์การบวกและการคูณ โดยทั่วไปนิยมใช้สัญลักษณ์ GF(2) แทนฟิลด์จำกัดไบนารี สำหรับฟิลด์จำกัดไบนารีส่วนขยาย (extension field) แทนด้วยสัญลักษณ์ $GF(2^p)$ เมื่อ p เป็นจำนวนเต็มที่มากกว่าศูนย์ [29]

ตัวอย่างเช่น กรณี $p=2$ จะเท่ากับฟิลด์จำกัดไบนารีส่วนขยาย GF(4) ซึ่งมีอิลิเมนท์จำนวนตัว 4 ตัว ได้แก่ 0, 1, 2 และ 3 ผลลัพธ์ของการบวกและคูณระหว่างอิลิเมนท์แสดงดังตารางที่ 3.1 ทั้งนี้ อาจพิจารณาอิลิเมนท์ของฟิลด์จำกัดไบนารีส่วนขยาย GF(4) ด้วยค่าไบนารีจำนวน 2 บิต ตัวอย่างเช่น อิลิเมนท์ที่มีค่าเท่ากับ 2 สามารถแสดงด้วยค่าไบนารี 10 และอิลิเมนท์เท่ากับ 3 แทนด้วยไบนารี 11 ดังนั้นผลลัพธ์การบวกแบบมอดูโล 2 จึงมีค่าเท่ากับ 01 หรืออิลิเมนท์เท่ากับ 1 ของฟิลด์จำกัดไบนารีส่วนขยาย GF(4)

ตารางที่ 3.1 การบวกและการคูณในฟิลด์จำกัด GF(4)

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

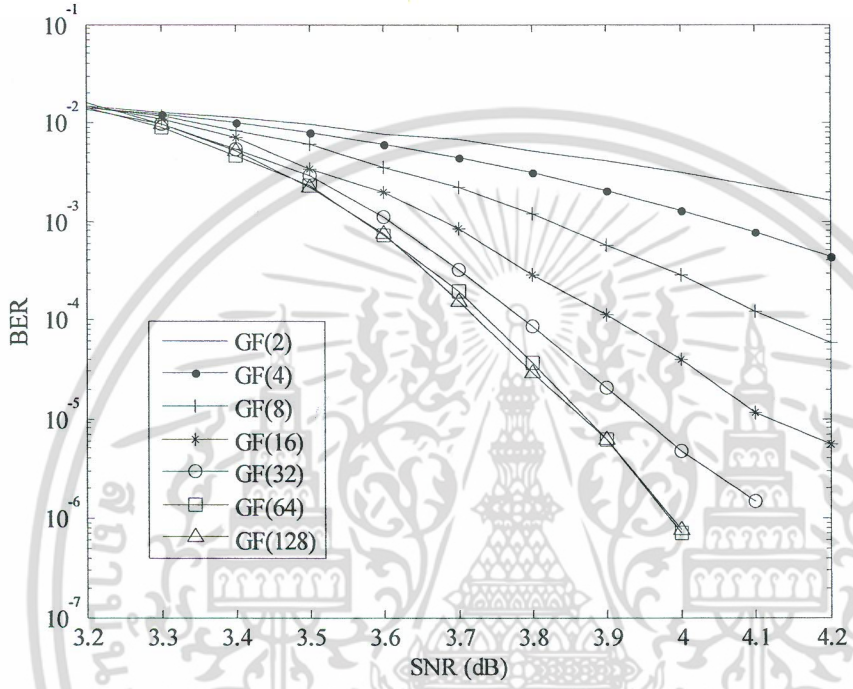
×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

ในงานวิจัยของ David Mackay [12] ได้นำเสนอรหัสแอลดีพีซีบนฟิลด์จำกัดไบนารีส่วนขยายแทนด้วยสัญลักษณ์ GF(q) เมื่อ $q=2^p$ และ p เป็นจำนวนเต็มที่มากกว่าศูนย์ นอกจากนี้ยังแสดงให้เห็นถึงสมรรถนะของรหัสแอลดีพีซีที่เพิ่มขึ้นเมื่อฟิลด์จำกัดมีค่า q สูงขึ้น โดยทั่วไป นิยมเรียกรหัสแอลดีพีซีเมื่อ $q=2$ ว่ารหัสไบนารีแอลดีพีซี (binary LDPC codes) และเรียกรหัสนอนไบนารีแอลดีพีซี (nonbinary LDPC codes) เมื่อฟิลด์จำกัด $q>2$ พิจารณารหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ที่มีอิลิเมนท์ของฟิลด์จำกัดจำนวน q ตัว ได้แก่ $0,1,\ldots,q-1$ ดังนั้นเวกเตอร์คำรหัส $\mathbf{v}$ ที่ได้จากการเข้ารหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) จะต้องมีอิลิเมนท์อยู่ในฟิลด์จำกัดด้วยหรือ $v_i \in \{0,1,\ldots,q-1\}$ เช่นเดียวกับเมทริกซ์กำเนิด $g_{i,j} \in \{0,1,\ldots,q-1\}$ และเมทริกซ์พาริตี้เช็ค $h_{i,j} \in \{0,1,\ldots,q-1\}$ ตัวอย่างเช่น รหัสแอลดีพีซีแบบนอนไบนารีบนฟิลด์จำกัด GF(4) ที่มีเมทริกซ์พาริตี้เช็ค คือ

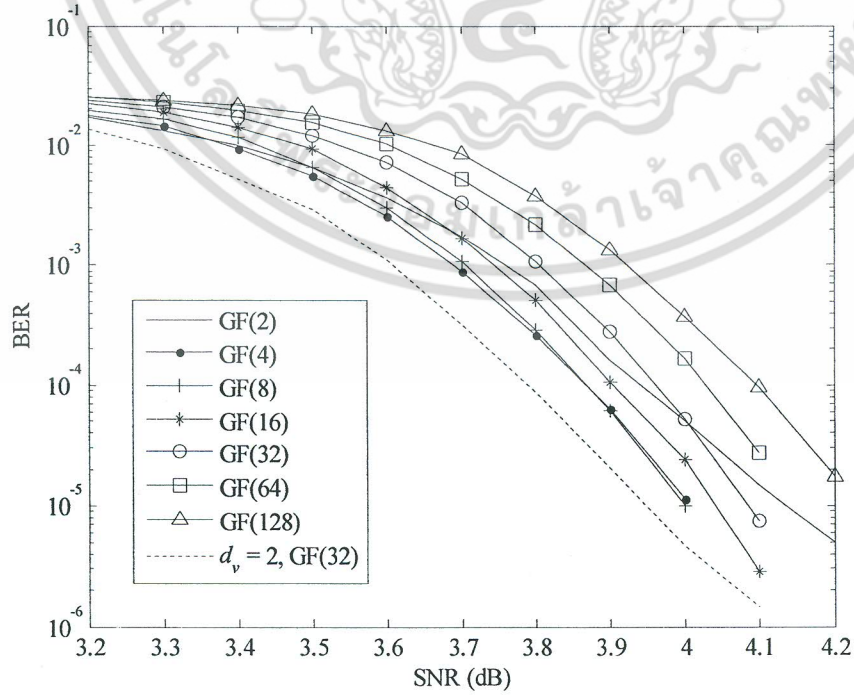
$$\mathbf{H}=\begin{bmatrix}3 & 0 & 1 & 2 & 0 & 0\\ 1 & 3 & 0 & 2 & 1 & 0\\ 0 & 0 & 2 & 0 & 3 & 1\end{bmatrix} \tag{3.24}$$

กำหนดให้ข้อมูลไบนารี $\mathbf{u}=[1\,0\,1\,1\,0\,0]$ หรือเท่ากับข้อมูลบนฟิลด์จำกัด $\mathbf{u}=[2\,3\,0]$ ดังนั้น คำรหัสที่ได้จากการเข้ารหัสจะมีค่าเท่ากับ $\mathbf{v}=[2\,3\,0\,3\,1\,3]$ หรือข้อมูลไบนารี $\mathbf{v}=[1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,1\,1]$ (ใช้วิธีการเข้ารหัสเชิงระบบหรือการเข้ารหัสความซับซ้อนเชิงเส้นในหัวข้อที่ 3.1.1 และ 3.1.2 โดยกระบวนการบวกหรือคูณต้องอยู่บนฟิลด์จำกัด GF(4) เท่านั้น) ทั้งนี้ สังเกตได้ว่าการออกแบบรหัส

นอนไบนารีแอลดีพีซีจะต้องทำให้เมทริกซ์พาริตี้เช็คมีอิลิเมนท์อยู่ในฟิลด์จำกัด อย่างไรก็ตาม นิยมออกแบบเมทริกซ์พาริตี้เช็คบนฟิลด์จำกัด GF(2) ก่อน หลังจากนั้น ทำการสุ่มค่าอิลิเมนท์ในฟิลด์จำกัดลงในตำแหน่งที่ไม่เป็นศูนย์ในเมทริกซ์พาริตี้เช็ค รูปที่ 3.5 แสดงอัตราบิตผิดพลาดของรหัสไบนารีและนอนไบนารีแอลดีพีซีเมื่อใช้ $d_v = 2$ อัตรารหัสเท่ากับ $R = 8/9$ ความยาวของคำรหัสประมาณ $N = 4608$ บิต และจำนวนการถอดรหัสวนซ้ำเท่ากับ 50 รอบ



รูปที่ 3.5 อัตราบิตผิดพลาดของรหัสนอนไบนารีแอลดีพีซีเมื่อ $d_v = 2$



รูปที่ 3.6 อัตราบิตผิดพลาดของรหัสนอนไบนารีแอลดีพีซีเมื่อ $d_v = 3$

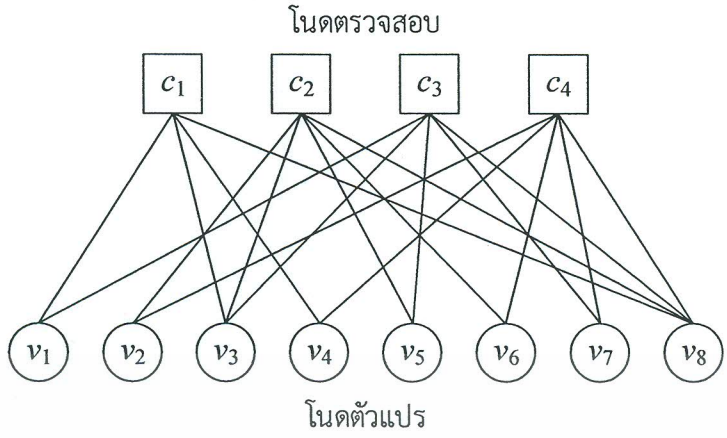
จากรูปสังเกตได้ว่าเมื่อค่าของฟิลด์จำกัดเพิ่มสูงขึ้น จะทำให้สมรรถนะเพิ่มขึ้นตามลำดับ สำหรับรหัสแอลดีพีซีที่มี $d_v = 3$ แสดงในรูปที่ 3.6 สมรรถนะของรหัสจะสูงขึ้นเมื่อทำการเพิ่มค่าของฟิลด์จำกัดจนกระทั่งฟิลด์จำกัดมีค่าเท่ากับ GF(8) หลังจากนั้น การเพิ่มค่าฟิลด์จำกัดจะทำให้สมรรถนะของรหัสลดลง นอกจากนี้ รหัสนอนไบนารีแอลดีพีซีบนฟิลด์จำกัด GF(32) เมื่อ $d_v = 2$ จะให้สมรรถนะที่ดีกว่ารหัสแอลดีพีซีเมื่อใช้ $d_v = 3$ บนฟิลด์จำกัดใดๆ ในงานวิจัยส่วนหนึ่งของวิทยานิพจน์ฉบับนี้จะแสดงการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีซีบนฟิลด์จำกัด รายละเอียดอยู่ในบทที่ 5

3.2.3 กราฟแทนเนอร์และวัฏจักร

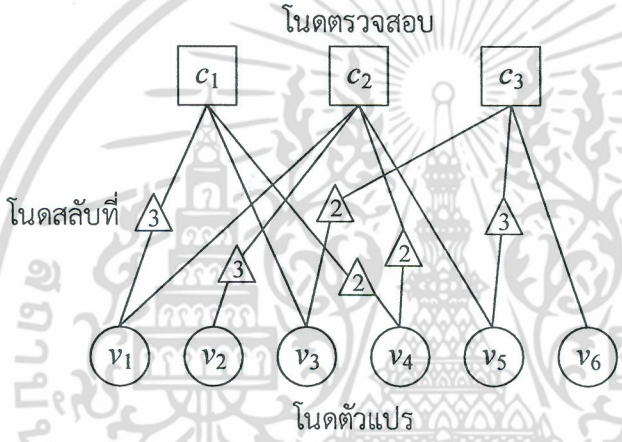
หลังจากรหัสแอลดีพีซีได้รับการนำเสนอเป็นระยะเวลา 20 ปี Robert Tanner [3] ได้ศึกษาการใช้กราฟอธิบายกระบวนการถอดรหัสแอลดีพีซี โดยกราฟที่นำเสนอนี้ เรียกว่า กราฟแทนเนอร์ (Tanner Graph) ซึ่งจัดว่าเป็นกราฟไบพาร์ไทต์ (Bipartite Graph) ชนิดหนึ่ง ที่ประกอบด้วยกลุ่มโนดจำนวน 2 กลุ่มที่ใช้อธิบายความสัมพันธ์ของคำรหัสและเมทริกซ์พาริตี้เช็คในสมการที่ 3.6 โดยกลุ่มโนดตัวแปร (variable node) ได้แก่ $v_1, v_2, \ldots, v_N$ เป็นตัวแทนของบิตคำรหัสจำนวน N บิต และกลุ่มโนดตรวจสอบ (check node) ได้แก่ $c_1, c_2, \ldots, c_{N-K}$ เป็นตัวแทนของแถวในเมทริกซ์พาริตี้เช็คจำนวน $N-K$ แถว กลุ่มโนดทั้งสองจะถูกเชื่อมเข้าด้วยกันตามความสัมพันธ์ของคำรหัสและเมทริกซ์พาริตี้เช็ค ตัวอย่างเช่น พิจารณาเมทริกซ์พาริตี้เช็คในสมการที่ 3.21 เมื่อกำหนดให้เวกเตอร์คำรหัสเท่ากับ $\mathbf{v} = [v_1, v_2, \ldots, v_8]$ ดังนั้น

$$\mathbf{H}.\mathbf{v}^T = \begin{bmatrix} v_1 + v_3 + v_4 + v_8 \\ v_2 + v_3 + v_5 + v_6 + v_8 \\ v_1 + v_3 + v_5 + v_7 + v_8 \\ v_2 + v_4 + v_6 + v_7 + v_8 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{3.25}$$

และสามารถเขียนกราฟแทนเนอร์ได้ดังรูปที่ 3.7 ซึ่งประกอบไปด้วยโนดตรวจสอบจำนวน 4 โนด ได้แก่ c_1, c_2, c_3, c_4 แทนแถวในเมทริกซ์พาริตี้เช็คจำนวน 4 แถว และโนดตัวแปรจำนวน 8 โนด ได้แก่ $v_1, v_2, \ldots, v_8$ แทนบิตคำรหัสจำนวน 8 บิต นอกจากนี้ โนดตัวแปร v_1, v_3, v_4, v_8 มีเส้นเชื่อมไปยังโนดตรวจสอบ c_1 บ่งบอกถึงผลรวมของบิตคำรหัส v_1, v_3, v_4, v_8 จะมีค่าเท่ากับศูนย์ สอดคล้องกับสมการ $v_1 + v_3 + v_4 + v_8 = 0$ ด้านบน และเส้นเชื่อมจากโนดตรวจสอบ c_2 ไปยังโนดตัวแปร v_2, v_3, v_5, v_6, v_8 อธิบายสมการ $v_2 + v_3 + v_5 + v_6 + v_8 = 0$



รูปที่ 3.7 กราฟแทนเนอร์ของรหัสไบนารีแอลดีพีซี



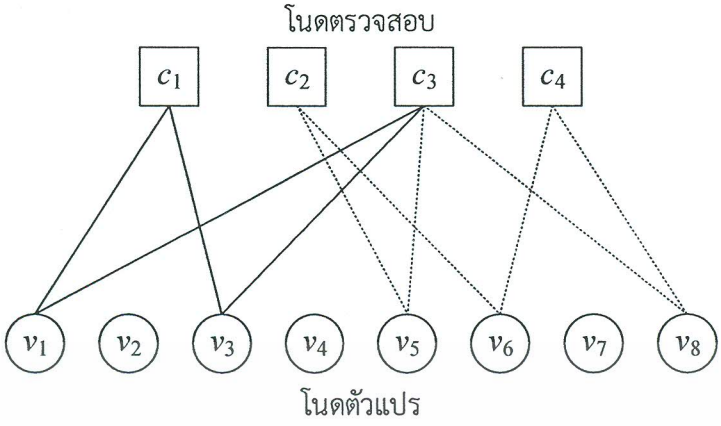
รูปที่ 3.8 กราฟแทนเนอร์ของรหัสนอนไบนารีแอลดีพีซี

สำหรับรหัสแอลดีพีซีแบบนอนไบนารี พิจารณาเมทริกซ์พาริตี้เช็คในสมการที่ 3.24 และกำหนดให้เวกเตอร์คำรหัสเท่ากับ $\mathbf{v}=[v_1, v_2, \ldots, v_6]$ ดังนั้น

$$\mathbf{H}.\mathbf{v}^T = \begin{bmatrix} 3v_1 + v_3 + 2v_4 \\ v_1 + 3v_2 + 2v_4 + v_5 \\ 2v_3 + 3v_5 + v_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \tag{3.26}$$

โดยสามารถเขียนกราฟแทนเนอร์ได้ดังรูปที่ 3.8 สังเกตได้ว่า โนดสลับที่แสดงการคูณบิตคำรหัสด้วยค่าในฟิลด์จำกัด เช่น โนดตัวแปร v_1 และ v_4 เชื่อมต่อกับโนดสลับที่ (permutation node) ก่อนทำการเชื่อมไปยังโนดตรวจสอบ c_1 เพื่อให้ได้ความสัมพันธ์ตามสมการ $3v_1 + v_3 + 2v_4 = 0$

ในบทถัดไปจะอธิบายกระบวนการถอดรหัสแอลดีพีซี โดยจะพบว่ากระบวนการถอดรหัสแอลดีพีซีจะเป็นการส่งความน่าจะเป็นของบิตคำรหัสไปตามเส้นทางในกราฟแทนเนอร์ ตัวอย่างเช่น ในรูปที่ 3.7 ความน่าจะเป็นของบิตคำรหัส v_1 สามารถคำนวณได้จากความน่าจะเป็นของบิตคำรหัส

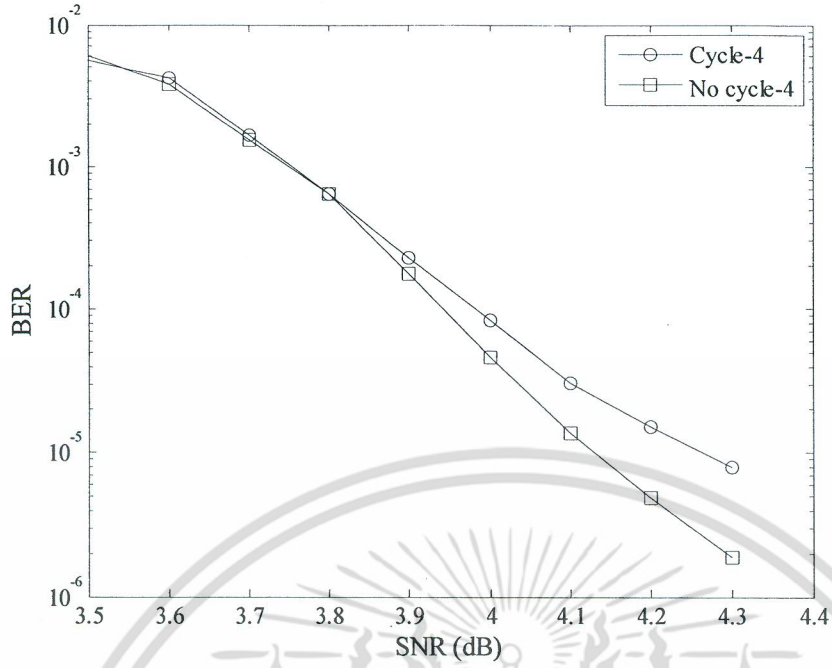


รูปที่ 3.9 วัฏจักรขนาด 4 และ 6

v_3, v_4, v_8 เนื่องจากกระบวนการถอดรหัสแอลดีพีซีมีการทำงานแบบวนซ้ำ ดังนั้น บิตคำรหัส v_1 ที่คำนวณได้ในตอนต้นก็ถูกใช้คำนวณบิตคำรหัส v_3 และบิตคำรหัส v_3 จะถูกใช้คำนวณบิตคำรหัส v_1 อีกครั้ง พิจารณาเส้นทางการส่งข่าวสารของโนด v_1 และ v_3 ในรูปที่ 3.9 จะสังเกตได้ว่าความน่าจะเป็นของบิตคำรหัส v_1 ถูกส่งออกไปและย้อนกลับมาที่บิตคำรหัส v_1 อีกครั้ง เช่นเดียวกับบิตคำรหัส v_3 โดยคิดเป็นจำนวนเส้นเชื่อมเท่ากับ 4 เส้น ในที่นี้ จะเรียกว่า วัฏจักรขนาด 4 (cycle-4) สำหรับวัฏจักรขนาด 6 (cycle-6) ข่าวสารจากโนดตัวแปรจะถูกส่งออกไปและกลับมายังโนดเดิมโดยใช้เส้นเชื่อมเท่ากับ 6 เส้น แสดงดังรูปที่ 3.9 โดยวัฏจักรที่สั้นที่สุดในกราฟแทนเนอร์จะเรียกว่าเกิร์ธ (girth) วัฏจักรที่เกิดขึ้นนี้จะส่งผลต่อสมรรถนะของการถอดรหัสแอลดีพีซี รูปที่ 3.10 แสดงสมรรถนะของรหัสแอลดีพีซีที่มีวัฏจักรขนาด 4 และรหัสแอลดีพีซีที่ปราศจากวัฏจักรขนาด 4 เมื่อกำหนดให้รหัสแอลดีพีซีมีอัตรารหัส $R = 8/9$ ความยาวของคำรหัส $N = 4608$ บิต ความยาวของบิตข้อมูล $K = 4096$ บิต และใช้จำนวนการถอดรหัสวนซ้ำ 50 รอบ จากรูปจะสังเกตได้ว่ารหัสแอลดีพีซีที่ปราศจากวัฏจักรขนาด 4 ให้อัตราบิตผิดพลาดต่ำกว่ารหัสแอลดีพีซีที่มีวัฏจักรขนาด 4

3.3 การออกแบบรหัสพาริตี้เช็คความหนาแน่นต่ำ

ในหัวข้อนี้จะอธิบายวิธีการออกแบบรหัสพาริตี้เช็คความหนาแน่นต่ำ โดยยกตัวอย่างวิธีการออกแบบที่ได้รับความนิยมและเกี่ยวข้องกับวิทยานิพนธ์ฉบับนี้ การออกแบบรหัสแอลดีพีซีจะเกี่ยวข้องกับการออกแบบเมทริกซ์พาริตี้เช็ค ซึ่งสามารถจำแนกการออกแบบได้เป็นสองประเภท ได้แก่ การออกแบบเชิงสุ่มและการออกแบบเชิงโครงสร้าง สำหรับการออกแบบเชิงสุ่ม ตำแหน่งเลขหนึ่งในเมทริกซ์พาริตี้เช็คจะไม่สามารถคาดการณ์ล่วงหน้าได้ ตัวอย่างเช่น อัลกอริทึมแมคเคย์ และอัลกอริทึมพีอีจี สำหรับการออกแบบเชิงโครงสร้าง ตำแหน่งเลขหนึ่งในเมทริกซ์พาริตี้เช็คจะถูกกำหนดไว้อย่างชัดเจน ตัวอย่างเช่น รหัสกาลาเกอร์ และรหัสอาร์เรย์



รูปที่ 3.10 อัตราบิตผิดพลาดของรหัสแอลดีพีซีกรณีมีวัฏจักรขนาด 4

3.3.1 อัลกอริทึมแมคเคย์

ภายหลังจากรหัสแอลดีพีซีถูกนำเสนอเป็นระยะเวลา 35 ปี David Mackay ได้ตีพิมพ์งานวิจัยใน [2] ซึ่งส่งผลต่องานวิจัยที่มีต่อรหัสแอลดีพีซี โดยงานวิจัยนี้แสดงให้เห็นว่ารหัสแอลดีพีซีที่มีเมทริกซ์พาริตี้เช็คเป็นเมทริกซ์มากเลขศูนย์ จะส่งผลให้สมรรถนะเข้าใกล้ลิมิตของแชนนอนเช่นเดียวกับรหัสเทอร์โบที่ถูกนำเสนอโดย Claude Berrou, Alain Glavieux, และ รศ.ดร. ปัญญา ธิติมัชฌิมา [34] การออกแบบเมทริกซ์พาริตี้เช็คด้วยอัลกอริทึมแมคเคย์จะมีลักษณะเชิงสุ่ม แตกต่างจากเมทริกซ์พาริตี้เช็คเชิงโครงสร้างที่ถูกนำเสนอโดย Robert Gallager วิธีการออกแบบเมทริกซ์พาริตี้เช็คด้วยอัลกอริทึมแมคเคย์สามารถจำแนกได้ 6 แบบ โดยเรียงจากวิธีที่มีความซับซ้อนต่ำไปยังความซับซ้อนสูง [35] ดังนี้

1) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ โดยการสุ่มจำนวนเลข 1 ในแต่ละหลักไม่จำเป็นต้องเท่ากับ t
2) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ โดยการสุ่มจำนวนเลข 1 ในแต่ละหลักมีค่าเท่ากับ t
3) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ โดยการสุ่มจำนวนเลข 1 ในแต่ละหลักมีค่าเท่ากับ t และทำให้จำนวนเลขหนึ่งในแต่ละแถวมีการกระจายตัวแบบสม่ำเสมอเท่าที่เป็นไปได้
4) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ ด้วยวิธีที่ 3 และทำให้ปราศจากวัฏจักรขนาด 4
5) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ ด้วยวิธีที่ 3 และทำให้วัฏจักรขนาดมีค่าสูง
6) สร้างเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ ด้วยวิธีที่ 5 โดยเมทริกซ์พาริตี้เช็คมีลักษณะ $\mathbf{H}=[\mathbf{H}_1\ \mathbf{H}_2]$ ซึ่งเมทริกซ์ย่อย $\mathbf{H}_2$ ขนาด $(N-K)\times(N-K)$ สามารถหาอินเวอร์สได้

รหัสแอลดีพีซีที่ออกแบบเมทริกซ์พาริตี้เช็คด้วยวิธีที่ 1-5 สามารถใช้เทคนิคการกำจัดเกาส์เซียนเพื่อทำให้เมทริกซ์พาริตี้เช็คอยู่ในลักษณะเชิงระบบดังหัวข้อที่ 3.1.1 สำหรับการออกแบบเมทริกซ์พาริตี้เช็คด้วยวิธีที่ 6 สามารถเข้ารหัสผ่านเมทริกซ์กำเนิดซึ่งคำนวณได้จาก $\mathbf{G}=[\mathbf{I}\ \ (\mathbf{H}_2)^{-1}\mathbf{H}_1]$

3.3.2 อัลกอริทึมพีอีจี

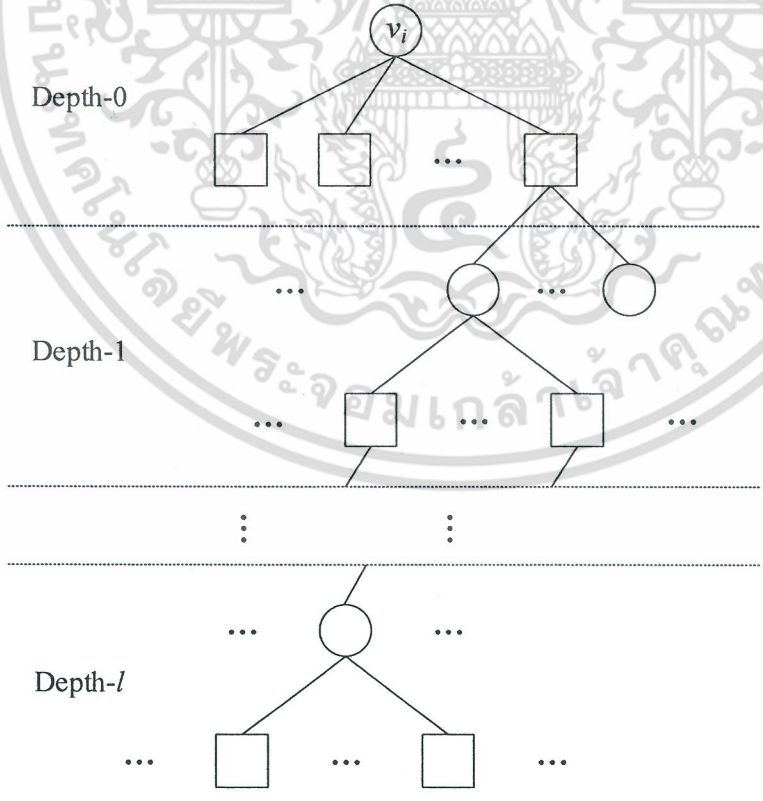
วัฏจักรที่เกิดขึ้นภายในกราฟแทนเนอร์ เกิดจากการส่งผ่านข่าวสารจากโนดตัวแปรใดๆ ไปและกลับมายังโนดตัวแปรเดิมในกระบวนการถอดรหัส ดังนั้นการออกแบบรหัสให้วัฏจักรมีความยาวสูงจะทำให้การถอดรหัสมีประสิทธิภาพดังที่อธิบายในหัวข้อที่ 3.2.3 ในงานวิจัย [5] ได้นำเสนอการออกแบบรหัสแอลดีพีซีเชิงสุ่มที่ทำให้วัฏจักรมีความยาวสูง โดยการใช้อัลกอริทึมขยายขอบแบบก้าวหน้าหรืออัลกอริทึมพีอีจี (progressive edge-growth algorithm, PEG algorithm) พิจารณาข่าวสารหรือเส้นทางจากโนดตัวแปรหนึ่งไปยังโนดตรวจสอบต่างๆในกราฟแทนเนอร์ สามารถแสดงด้วยแผนภาพต้นไม้ดังรูปที่ 3.11 เมื่อกำหนดให้โนดตัวแปรแทนด้วยวงกลมและโนดตรวจสอบแทนด้วยสี่เหลี่ยม โดยจะพบว่าระยะทางจากโนดตัวแปร v_i ไปยังโนดตรวจสอบทุกโนดในกราฟแทนเนอร์จะทำให้แผนภาพต้นไม้มีระดับความลึกที่ l (Depth-l) ซึ่งจะทำให้ความยาววัฏจักรของโนดตัวแปร v_i มีค่าเท่ากับ $2(l+1)$ ตัวอย่างเช่น ในรูปที่ 3.7 เมื่อทำการวาดแผนภาพต้นไม้จากโนดตัวแปร v_1 ไปยังโนดตรวจสอบต่างๆ ในกราฟแทนเนอร์ จะทำให้แผนภาพต้นไม้มีความลึกระดับที่ 1 ซึ่งก่อให้เกิดวัฏจักรขนาด 4

การออกแบบกราฟแทนเนอร์ด้วยอัลกอริทึมพีอีจี จะเป็นการทำให้โนดตัวแปรต่างๆ มีวัฏจักรขนาดสูง ซึ่งทำได้โดยการสร้างแผนภาพต้นไม้ของโนดตัวแปรและสร้างเส้นเชื่อมจากโนดตัวแปรไปยังโนดตรวจสอบที่อยู่ในความลึกระดับที่ l การสร้างเส้นเชื่อมจะเริ่มจากโนดตัวแปรลำดับที่ 1 ถึงโนดตัวแปรลำดับที่ N ทั้งนี้ การสร้างเส้นเชื่อมให้กับโนดตัวแปรในช่วงเริ่มต้นจะยังไม่ก่อให้เกิดวัฏจักร พิจาราณาได้จากกราฟแทนเนอร์ในรูปที่ 3.7 เมื่อทำการสร้างเส้นเชื่อมให้กับโนดตัวแปรลำดับที่ 1 และ 2 จะยังไม่ก่อให้เกิดวัฏจักร จนกระทั่ง สร้างเส้นเชื่อมให้กับโนดตัวแปรลำดับที่ 3 รายละเอียดอัลกอริทึมพีอีจีแสดงในตารางที่ 3.2 เมื่อกำหนดให้ d_v คือ จำนวนเส้นเชื่อมของโนดตัวแปร สำหรับการออกแบบรหัสแอลดีพีซีแบบไม่สม่ำเสมอด้วยอัลกอริทึมพีอีจีจะต้องกำหนดให้จำนวนเส้นเชื่อมของโนดตัวแปรต่างๆ ไม่เท่ากัน เช่นเดียวกับจำนวนเส้นเชื่อมของโนดตรวจสอบ งานวิจัยส่วนหนึ่งของวิทยานิพนธ์จะนำเสนอการประยุกต์ใช้อัลกอริทึมพีอีจีในการสร้างรหัสแอลดีพีซีแบบควอไซไซคลิกทำให้กระบวนการเข้ารหัสสามารถใช้ชิฟต์รีจิสเตอร์ที่มีการป้อนกลับดังที่อธิบายในหัวข้อ 3.1.3 รายละเอียดการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกด้วยอัลกอริทึมพีอีจีอธิบายในบทที่ 5

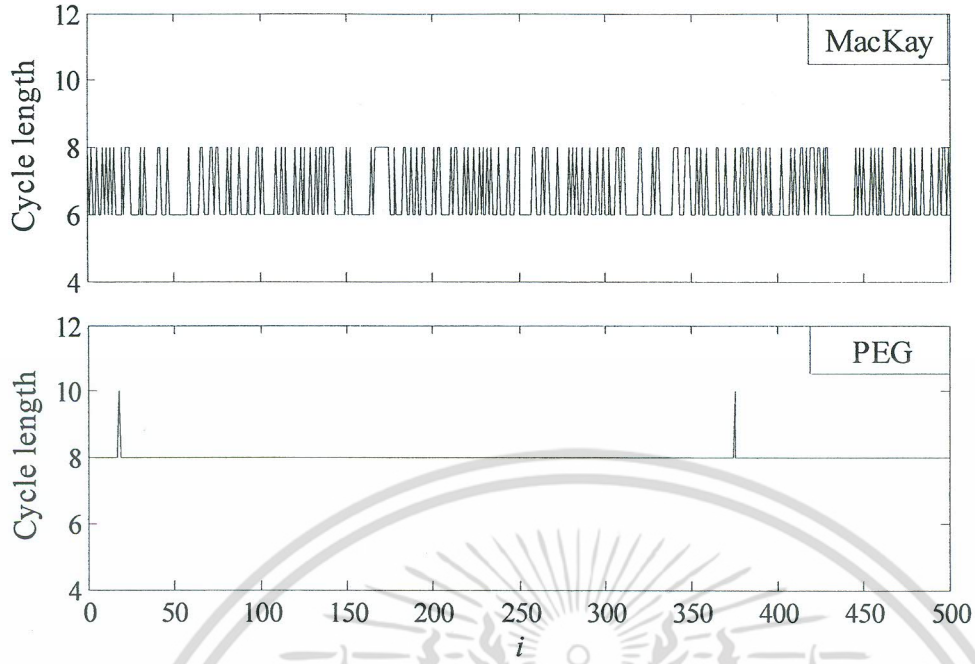
ตารางที่ 3.2 อัลกอริทึมพีอีจี (PEG algorithm)

---

for $i = 1$ **to** N
  for $k = 1$ **to** d_v
    if $k = 1$
      สร้างเส้นเชื่อมจากโนดตัวแปร v_i ไปยังโนดตรวจสอบที่มีเส้นเชื่อมน้อยสุด
    else
      สร้างแผนภาพต้นไม้จากโนดตัวแปร v_i ไปยังโนดตรวจสอบ
      กรณีที่ 1 สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
      สร้างเส้นเชื่อมจากโนดตัวแปร v_i ไปยังโนดตรวจสอบที่อยู่ในความลึก
      ลำดับที่ l ซึ่งจะทำให้โนดตัวแปร v_i เกิดวัฏจักรขนาด $2(l+1)$
      กรณีที่ 2 ไม่สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
      สร้างเส้นเชื่อมจากโนดตัวแปร v_i ไปยังโนดตรวจสอบที่ไม่ได้อยู่ใน
      แผนภาพต้นไม้ ซึ่งจะทำให้โนดตัวแปร v_i ปราศจากวัฏจักร
    end
  end
end



รูปที่ 3.11 แผนภาพต้นไม้ของโนดตัวแปร



รูปที่ 3.12 วัฏจักรของรหัสแอลดีพีซี

รูปที่ 3.12 แสดงความยาววัฏจักรของโนดตัวแปรในรหัสแอลดีพีซี เมื่ออัตรารหัสเท่ากับ $R=0.5$ ความยาวของคำรหัส $N=500$ บิต โดยทำการออกแบบกราฟแทนเนอร์ด้วยอัลกอริทึมแมคเคย์วิธีที่ 4 และอัลกอริทึมพีอีจี จากรูปจะสังเกตได้ว่ากราฟแทนเนอร์ที่ได้จากอัลกอริทึมพีอีจีจะมีวัฏจักรสูงกว่าอัลกอริทึมแมคเคย์วิธีที่ 4 โดยอัลกอริทึมพีอีจีทำให้เกิดวัฏจักรขนาด 8 และ 10 และอัลกอริทึมแมคเคย์จะทำให้เกิดวัฏจักรขนาด 6 และ 8 อย่างไรก็ตาม ขนาดของวัฏจักรที่ได้จากอัลกอริทึมพีอีจีและอัลกอริทึมแมคเคย์จะขึ้นอยู่กับขนาดเมทริกซ์พาริตี้เช็คที่ต้องการสร้างด้วยเช่นกัน

3.3.3 รหัสกาลาเกอร์

รหัสพาริตี้เช็คความหนาแน่นต่ำที่ถูกนำเสนอโดย Robert Gallager จัดเป็นรหัสแอลดีพีซีเชิงโครงสร้าง โดยจำนวนเลขหนึ่งในแต่ละแถวจะมีค่าเท่ากับ d_c และจำนวนเลขหนึ่งในแต่ละหลักมีค่าเท่ากับ d_v ทั้งนี้ เมทริกซ์พาริตี้เช็คจะต้องมีขนาดเท่ากับ $md_v \times md_c$ เมื่อ m เป็นจำนวนเต็มบวกที่มีค่ามากกว่าศูนย์ โดยสามารถแบ่งเมทริกซ์พาริตี้เช็คออกเป็นเมทริกซ์ย่อย $\mathbf{h}$ ขนาด $m \times md_c$ ได้ดังนี้

$$\mathbf{H}=\begin{bmatrix}\mathbf{h}_1\\ \mathbf{h}_2\\ \vdots\\ \mathbf{h}_{d_v}\end{bmatrix} \tag{3.27}$$

เมื่อเลขหนึ่งในเมทริกซ์ย่อย $\mathbf{h}_1$ จะอยู่ในแถวลำดับที่ i และหลักลำดับที่ $(i-1)d_c+1$ ถึง id_c สำหรับเมทริกซ์ย่อยอื่นๆ หาได้จากการหมุนวนแบบสุ่มของหลักในเมทริกซ์ย่อย $\mathbf{h}_1$ อย่างไรก็ตาม กระบวนการหมุนวนจะต้องพยายามหลีกเลี่ยงการเกิดวัฏจักรขนาด 4 ในเมทริกซ์พาริตี้เช็ค ตัวอย่างการออกแบบเมทริกซ์พาริตี้เช็คของรหัสกาลาเกอร์เมื่อ $d_c=6$, $d_v=3$ และ $m=3$ แสดงดังนี้

$$\mathbf{H}=\left[\begin{array}{cccccccccccccccccc}
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
\hdashline
0&0&0&1&0&1&1&0&1&0&0&0&0&0&0&0&1&1\\
0&1&1&0&1&0&0&1&0&0&0&1&0&1&0&0&0&0\\
1&0&0&0&0&0&0&0&0&1&1&0&1&0&1&1&0&0\\
\hdashline
0&0&1&0&0&0&1&0&1&0&1&1&1&0&0&1&0&0\\
0&1&0&1&0&1&0&1&0&0&0&0&0&0&1&0&1&0\\
1&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1
\end{array}\right]$$

3.3.4 รหัสอาร์เรย์

โครงสร้างแบบรหัสอาร์เรย์ (array codes) [36] เป็นที่รู้จักอย่างกว้างขวางสำหรับรหัสแก้ไขความผิดพลาดจำพวกรหัสรีดโซโลมอน[2] (Reed-Solomon Code) [37] เนื่องจากโครงสร้างแบบรหัสอาร์เรย์ ให้สมรรถนะสูงในการแก้ไขความผิดพลาดแบบเบิรสต์ (burst errors) ในงานวิจัย [38] ได้ทำการศึกษาโครงสร้างรหัสอาร์เรย์สำหรับรหัสพาริตี้เช็คความหนาแน่นต่ำ โดยแสดงให้เห็นว่าโครงสร้างรหัสอาร์เรย์ สามารถประยุกต์ใช้งานกับกระบวนการถอดรหัสพาริตี้เช็คความหนาแน่นต่ำ นอกจากนี้รหัสอาร์เรย์ยังปราศจากวัฏจักรขนาด 4 เมทริกซ์พาริตี้เช็คของรหัสอาร์เรย์แสดงได้ดังนี้

$$\mathbf{H}=\begin{bmatrix}
\mathbf{I} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I}\\
\mathbf{I} & \boldsymbol{\alpha} & \boldsymbol{\alpha}^2 & \cdots & \boldsymbol{\alpha}^{(k-1)}\\
\mathbf{I} & \boldsymbol{\alpha}^2 & \boldsymbol{\alpha}^4 & \cdots & \boldsymbol{\alpha}^{2(k-1)}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
\mathbf{I} & \boldsymbol{\alpha}^{j-1} & \boldsymbol{\alpha}^{2(j-1)} & \cdots & \boldsymbol{\alpha}^{(j-1)(k-1)}
\end{bmatrix} \qquad (3.28)$$

เมื่อ $\mathbf{I}$ คือเมทริกซ์เอกลักษณ์ (identity matrix) และ $\boldsymbol{\alpha}$ คือเมทริกซ์เรียงลำดับ (permutation matrix) ขนาด $p\times p$ เมื่อ p คือจำนวนเฉพาะ เมทริกซ์เรียงลำดับสร้างได้จากการเลื่อนแถวหรือหลักไปทางซ้ายหรือขวาของเมตริกซ์เอกลักษณ์ เป็นจำนวนครั้งตามเลขชี้กำลังของเมทริกซ์เรียงลำดับ ตัวอย่างเช่น เมทริกซ์เอกลักษณ์และเมทริกซ์เรียงลำดับขนาดเท่ากับ 5×5

[2]รหัสรีด-โซโลมอน (Reed-Solomon Code) [37] เป็นรหัสแก้ไขความผิดพลาดชนิดหนึ่งที่นิยามด้วยรหัสบล็อกเชิงเส้นแบบนอนไบนารี

$$\mathbf{I}=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix} \quad \boldsymbol{\alpha}=\begin{bmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\end{bmatrix} \quad \boldsymbol{\alpha}^2=\begin{bmatrix}0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\end{bmatrix}$$

$$\boldsymbol{\alpha}^3=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\end{bmatrix} \quad \boldsymbol{\alpha}^4=\begin{bmatrix}0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix} \quad \boldsymbol{\alpha}^5=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

อย่างไรก็ตาม กระบวนการเข้ารหัสอาร์เรย์จะมีความซับซ้อนสูงเนื่องจากจำเป็นต้องใช้เทคนิคการกำจัดเกาส์เซียนซึ่งทำให้เมทริกซ์พาริตี้เช็คมีความหนาแน่นเพิ่มขึ้น ดังนั้นในงานวิจัย [39] ได้นำเสนอการแปลงเมทริกซ์พาริตี้เช็คให้มีลักษณะสามเหลี่ยมบน โดยลำดับแรกจะทำการหมุนวนเมทริกซ์ย่อยในสมการที่ 3.28 ให้เมทริกซ์เอกลักษณ์อยู่ในแนวเส้นทแยงมุมดังนี้

$$\mathbf{H}=\begin{bmatrix}\mathbf{I}&\mathbf{I}&\mathbf{I}&\cdots&\mathbf{I}&\mathbf{I}&\cdots&\mathbf{I}\\ \boldsymbol{\alpha}^{(k-1)}&\mathbf{I}&\boldsymbol{\alpha}&\cdots&\boldsymbol{\alpha}^{(j-2)}&\boldsymbol{\alpha}^{(j-1)}&\cdots&\boldsymbol{\alpha}^{(k-2)}\\ \boldsymbol{\alpha}^{2(k-2)}&\boldsymbol{\alpha}^{2(k-1)}&\mathbf{I}&\cdots&\boldsymbol{\alpha}^{2(j-3)}&\boldsymbol{\alpha}^{2(j-2)}&\cdots&\boldsymbol{\alpha}^{2(k-3)}\\ \vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ \boldsymbol{\alpha}^{(j-1)(k-j+1)}&\boldsymbol{\alpha}^{(j-1)(k-j+2)}&\cdots&\cdots&\mathbf{I}&\boldsymbol{\alpha}^{(j-1)}&\cdots&\boldsymbol{\alpha}^{(j-1)(k-j)}\end{bmatrix} \tag{3.29}$$

จากนั้นทำการเปลี่ยนเมทริกซ์ย่อยด้านซ้ายให้กลายเป็นเมทริกซ์ศูนย์ ทำให้เมทริกซ์พาริตี้เช็คจะอยู่ในลักษณะสามเหลี่ยมบนซึ่งสามารถใช้วิธีการเข้ารหัสความซับซ้อนเชิงเส้นในหัวข้อที่ 3.1.2 และเรียกเมทริกซ์พาริตี้เช็คนี้ว่ารหัสมอดดิฟายอาร์เรย์ (modified array codes) ดังนี้

$$\mathbf{H}=\begin{bmatrix}\mathbf{I}&\mathbf{I}&\mathbf{I}&\cdots&\mathbf{I}&\mathbf{I}&\cdots&\mathbf{I}\\ \mathbf{0}&\mathbf{I}&\boldsymbol{\alpha}&\cdots&\boldsymbol{\alpha}^{(j-2)}&\boldsymbol{\alpha}^{(j-1)}&\cdots&\boldsymbol{\alpha}^{(k-2)}\\ \mathbf{0}&\mathbf{0}&\mathbf{I}&\cdots&\boldsymbol{\alpha}^{2(j-3)}&\boldsymbol{\alpha}^{2(j-2)}&\cdots&\boldsymbol{\alpha}^{2(k-3)}\\ \vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\cdots&\mathbf{I}&\boldsymbol{\alpha}^{(j-1)}&\cdots&\boldsymbol{\alpha}^{(j-1)(k-j)}\end{bmatrix} \tag{3.30}$$

รหัสมอดดิฟายอาร์เรย์ที่ได้นี้จะปราศจากวัฏจักรขนาด 4 อย่างไรก็ตาม การประยุกต์ใช้รหัสมอดดิฟายอาร์เรย์ในช่องสัญญาณผลตอบสนองบางส่วนจะก่อให้เกิดวัฏจักรขนาด 4 เทียมขึ้นมา ในงานวิจัยส่วนหนึ่งของวิทยานิพนธ์นี้ จะแสดงการปรับปรุงรหัสมอดดิฟายอาร์เรย์สำหรับช่องสัญญาณผลตอบสนองบางส่วน รายละเอียดอยู่ในบทที่ 5

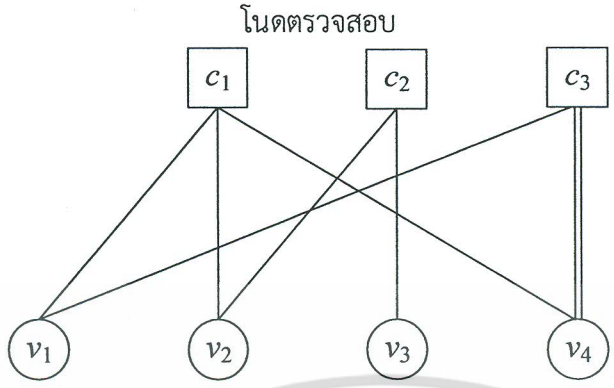
3.3.5 รหัสโปรโตกราฟ

รหัสโปรโตกราฟ (protograph code) [9] ได้รับความนิยมอย่างมากในปัจจุบัน เนื่องจากการวิเคราะห์สมรรถนะของรหัสโปรโตกราฟสามารถกระทำได้โดยง่าย (อธิบายในบทที่ 4) นอกจากนี้ยังมีความสะดวกในการสร้างเมทริกซ์พาริตี้เช็คขนาดใดๆ จากรหัสโปรโตกราฟที่ได้รับการออกแบบเป็นอย่างดี รหัสโปรโตกราฟนิยามด้วยกราฟแทนเนอร์ขนาดเล็กที่เรียกว่าโปรโตกราฟ ประกอบไปด้วยโนดตัวแปรและโนดตรวจสอบ โดยเส้นเชื่อมระหว่างโนดตัวแปรและโนดตรวจสอบสามารถมีได้มากกว่าหนึ่งเส้น ต่างจากกราฟแทนเนอร์ที่มีเส้นเชื่อมได้เพียงหนึ่งเส้นเท่านั้น ตัวอย่างเช่น โปรโตกราฟในรูปที่ 3.13 ที่ประกอบไปด้วยโนดตรวจสอบจำนวน 3 โนด ได้แก่ c_1, c_2, c_3 และโนดตัวแปรจำนวน 4 โนด ได้แก่ v_1, v_2, v_3, v_4 โดยมีเส้นเชื่อมระหว่างโนดตรวจสอบ c_3 และโนดตัวแปร v_4 จำนวน 2 เส้น โปรโตกราฟในรูปที่ 3.13 สามารถเขียนในรูปของเมทริกซ์ฐาน ดังนี้

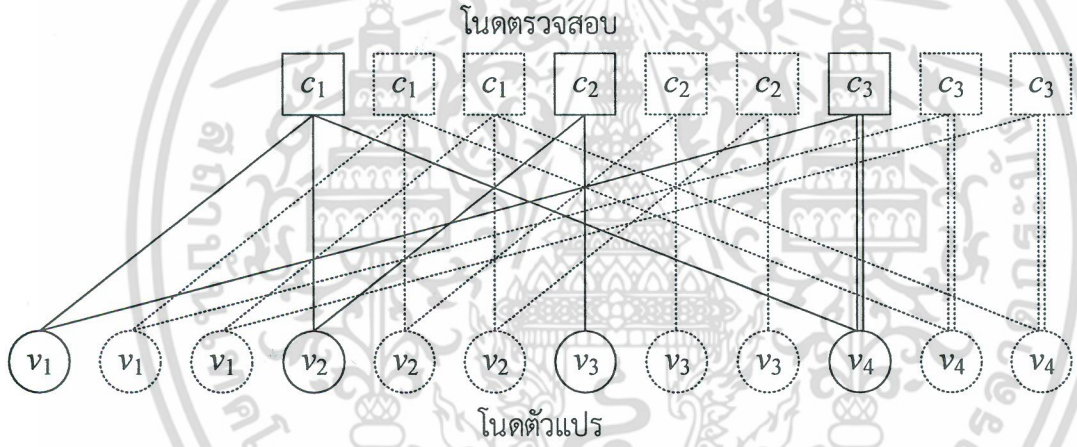
$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \end{bmatrix} \tag{3.31}$$

โดยที่อิลิเม้นท์ในเมทริกซ์ฐาน $b_{j,i}$ แสดงจำนวนเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i และโนดตรวจสอบลำดับที่ j การสร้างกราฟแทนเนอร์จากโปรโตกราฟจะกระทำผ่านกระบวนการที่เรียกว่าการคัดลอกและการหมุนวน รูปที่ 3.14 แสดงโปรโตกราฟที่ถูกคัดลอกจำนวน 3 ชุด โดยการคัดลอกนี้จะทำให้จำนวนโนดตัวแปรเพิ่มขึ้นเป็น 12 โนด และโนดตรวจสอบเท่ากับ 9 โนด จากนั้น ทำการหมุนวนเส้นเชื่อมของโนดตรวจสอบภายในชุดเดียวกันดังรูปที่ 3.15 ทั้งนี้การหมุนวนต้องไม่ก่อให้เกิดวัฏจักรขนาด 4 ในกราฟ และจะสังเกตได้ว่าเส้นเชื่อมระหว่างโนดตัวแปรและโนดตรวจสอบมีเพียงหนึ่งเส้นเท่านั้น กล่าวคือ เมื่อทำการคัดลอกและการหมุนวนโปรโตกราฟ ผลลัพธ์ที่ได้คือกราฟแทนเนอร์ของรหัสแอลดีพีซีที่มีลักษณะควอไซไซคลิก ทำให้สามารถใช้วิธีการเข้ารหัสในหัวข้อที่ 3.1.3 กราฟแทนเนอร์ที่ได้ในรูปที่ 3.13 สามารถเขียนในรูปเมทริกซ์พาริตี้เช็คได้ดังนี้

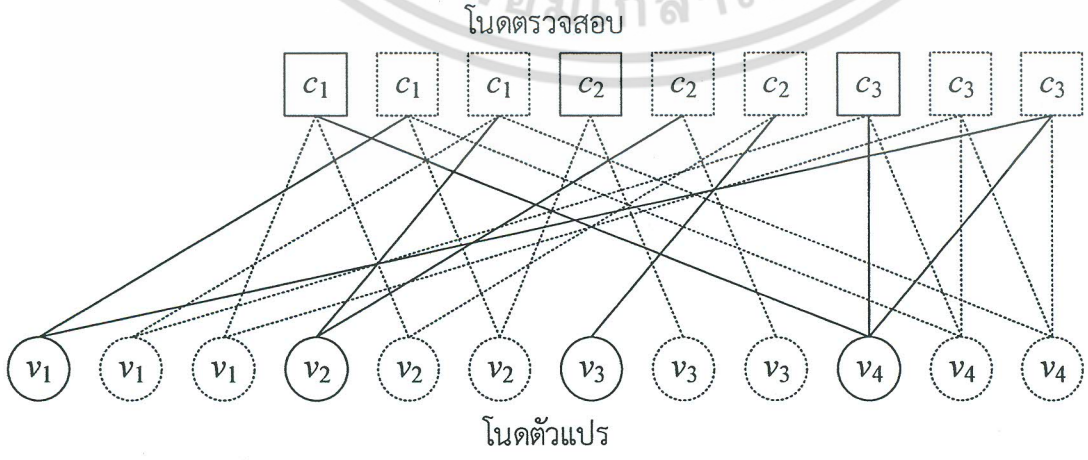
$$\mathbf{H} = \left[\begin{array}{ccc:ccc:ccc:ccc} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hdashline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right] \tag{3.32}$$



รูปที่ 3.13 โปรโตกราฟ



รูปที่ 3.14 การคัดลอกของโปรโตกราฟ



รูปที่ 3.15 การหมุนวนของโปรโตกราฟ

นอกจากนี้ จะสังเกตได้ว่า รหัสแอลดีพีซีแบบควอไซไซคลิกใดๆ สามารถเขียนอยู่ในรูปโปรโตกราฟได้เช่นกัน งานวิจัยส่วนหนึ่งของวิทยานิพนธ์ จะแสดงวิธีการวิเคราะห์สมรรถนะของรหัสโปรโตกราฟเมื่อฟิลด์จำกัดมีค่าใดๆ ภายใต้ช่องสัญญาณรบกวนเกาส์สีขาวบวกและช่องสัญญาณผลตอบสนองบางส่วน นอกจากนี้ สามารถนำวิธีการวิเคราะห์ไปประยุกต์ใช้ในการออกแบบรหัสโปรโตกราฟที่มีสมรรถนะสูงได้ รายละเอียดอธิบายในบทที่ 5

บทที่ 4
อัลกอริทึมการถอดรหัสและการวิเคราะห์สมรรถนะ

ในบทนี้ จะอธิบายวิธีการถอดรหัสพาริตี้เช็คความหนาแน่นต่ำหรือรหัสแอลดีพีซี ซึ่งมีลักษณะการทำงานแบบวนซ้ำ ตามที่ได้กล่าวไว้ในบทที่ผ่านมา กระบวนการถอดรหัสแอลดีพีซีจะใช้อัลกอริทึมที่เรียกว่าอัลกอริทึมซัมโปรดักส์ (sum-product algorithm) หรือ อัลกอริทึมกระจายความเชื่อมั่น (belief propagation algorithm) หลังจากนั้น จะอธิบายวิธีการเรียงลำดับข่าวสารหรือความเชื่อมั่นของกระบวนการถอดรหัสแอลดีพีซี ซึ่งได้รับความนิยมในการประยุกต์ใช้งานกับวงจรถอดรหัสแอลดีพีซีในปัจจุบัน และส่วนสุดท้ายของบทนี้ แสดงการวิเคราะห์สมรรถนะของรหัสแอลดีพีซีในทางทฤษฎี โดยจะพบว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานที่เข้าใกล้ขีดจำกัดของแชนนอน

4.1 อัลกอริทึมกระจายความเชื่อมั่นแบบความน่าจะเป็น

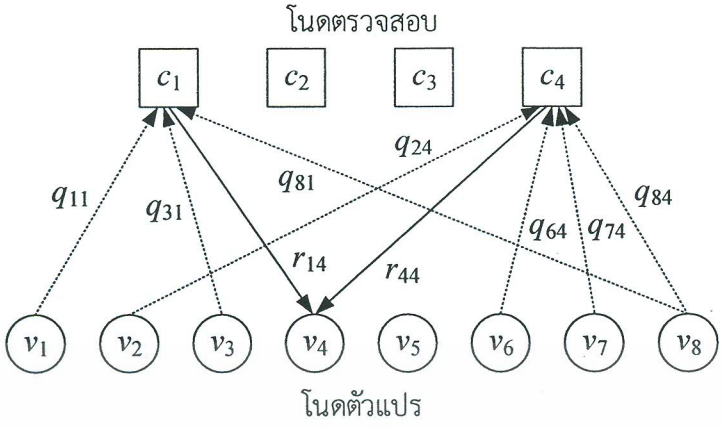
อัลกอริทึมกระจายความเชื่อมั่นของกระบวนการถอดรหัสแอลดีพีซี เป็นการแลกเปลี่ยนข่าวสารระหว่างโนดตัวแปรและโนดตรวจสอบในกราฟแทนเนอร์จำนวนหลายครั้ง (รายละเอียดกราฟแทนเนอร์อธิบายในหัวข้อที่ 3.2.3) ทำให้กระบวนการถอดรหัสแอลดีพีซีมีลักษณะการทำงานแบบวนซ้ำ ในที่นี้ ข่าวสารที่ถูกส่งจากโนดตัวแปรและโนดตรวจสอบจะอยู่ในรูปความเชื่อมั่นหรือความน่าจะเป็นของคำรหัสที่ถูกส่งผ่านช่องสัญญาณ พิจารณารหัสแอลดีพีซีบนฟิลด์จำกัด $\mathrm{GF}(q)$ ที่มีเวกเตอร์คำรหัส $v_i \in \{0,1,\ldots,q-1\}$ และเมทริกซ์พาริตี้เช็ค $h_{i,j} \in \{0,1,\ldots,q-1\}$ สามารถจำแนกอัลกอริทึมกระจายความเชื่อมั่นของรหัสแอลดีพีซีได้เป็น 2 กรณี ดังนี้

4.1.1 กรณีฟิลด์จำกัด GF(2)

สำหรับรหัสไบนารีแอลดีพีซีหรือรหัสแอลดีพีซีบนฟิลด์จำกัด GF(2) ซึ่งมีเวกเตอร์คำรหัส $v_i \in \{0,1\}$ และเมทริกซ์พาริตี้เช็ค $H_{i,j} \in \{0,1\}$ พิจารณากราฟแทนเนอร์ในรูปที่ 3.7 (บทที่ 3) โนดตรวจสอบ c_1 มีเส้นเชื่อมไปยังโนดตัวแปร v_1, v_3, v_4, v_8 แสดงถึงผลรวมแบบมอดูโล 2 ของคำรหัสจะมีค่าเท่ากับ

$$v_1 \oplus v_3 \oplus v_4 \oplus v_8 = 0 \tag{4.1}$$

สมมุติให้ บิตรหัส $v_4 = 1$ ดังนั้น บิตรหัสอื่นจะมีค่าที่เป็นไปได้คือ $v_1 = 1, v_3 = 0, v_8 = 0$ หรือ $v_1 = 0, v_3 = 1, v_8 = 0$ หรือ $v_1 = 0, v_3 = 0, v_8 = 1$ หรือ $v_1 = 1, v_3 = 1, v_8 = 1$ พิจารณารูปที่ 4.1 กำหนดให้สัญลักษณ์ r_{i4} คือความน่าจะเป็นของคำรหัส v_4 ซึ่งทำให้สมการ 4.1 เป็นจริง (หรือความน่าจะเป็นของโนดตัวแปร v_4 ที่ได้รับจากโนดตรวจสอบ c_1)



รูปที่ 4.1 ความเชื่อมั่นจากโนดตรวจสอบไปโนดตัวแปร

และสัญลักษณ์ q_{11}, q_{31}, q_{81} คือความน่าจะเป็นของบิตรหัส v_1, v_3, v_8 (หรือความน่าจะเป็นของโนด สัญลักษณ์ v_1, v_3, v_8 ที่ส่งไปยังโนดตรวจสอบ c_1) ดังนั้น ความน่าจะเป็นของโนดตัวแปร v_4 มีค่าเท่ากับ 1 หรือ $r_{14}(1)$ คำนวณจาก

$$r_{14}(1) = q_{11}(1)q_{31}(0)q_{81}(0) + q_{11}(0)q_{31}(1)q_{81}(0) + q_{11}(0)q_{31}(0)q_{81}(1) + q_{11}(1)q_{31}(1)q_{81}(1) \quad (4.2)$$

เนื่องจาก $q_{ij}(0) + q_{ij}(1) = 1$ จัดรูปใหม่จะได้เป็น

$$\begin{aligned} r_{14}(1) &= \big(1-q_{11}(0)\big)q_{31}(0)q_{81}(0) + q_{11}(0)\big(1-q_{31}(0)\big)q_{81}(0) + \\ &\quad q_{11}(0)q_{31}(0)\big(1-q_{81}(0)\big) + \big(1-q_{11}(0)\big)\big(1-q_{31}(0)\big)\big(1-q_{81}(1)\big) \\ &= 1-q_{11}(0)-q_{31}(0)-q_{81}(0)+2q_{11}(0)q_{31}(0)+2q_{11}(0)q_{81}(0)+2q_{31}(0)q_{81}(0) \\ &\quad -4q_{11}(0)q_{31}(0)q_{81}(0) \\ &= \frac{1}{2} + \frac{1}{2}\big(1-2q_{11}(0)\big)\big(1-2q_{31}(0)\big)\big(1-2q_{81}(0)\big) \end{aligned} \quad (4.3)$$

ในกรณีทั่วไป ความน่าจะเป็นของโนดตัวแปร v_i มีค่าเท่ากับ 1 ซึ่งได้รับจากโนดตรวจสอบ c_j เมื่อจำนวนเส้นเชื่อมของโนดตรวจสอบ c_j เป็นเลขคู่ คำนวณจากสมการต่อไปนี้

$$r_{ji}(1) = \frac{1}{2} + \frac{1}{2}\prod_{i' \in V_j \setminus i}\big(1-2q_{i'j}(0)\big) \quad (4.4)$$

เมื่อ $V_j \setminus i$ คือ เซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบ c_j ยกเว้นโนดตัวแปร v_i

พิจารณาโนดตรวจสอบ c_4 ซึ่งมีเส้นเชื่อมไปยังโนดตัวแปร v_2, v_4, v_6, v_7, v_8 เป็นจำนวนคี่ผลรวมแบบมอดูโล 2 ของคำรหัสจะมีค่าเท่ากับ

$$v_2 \oplus v_4 \oplus v_6 \oplus v_7 \oplus v_8 = 0 \tag{4.5}$$

ดังนั้นความน่าจะเป็นของโนดตัวแปร v_4 มีค่าเท่ากับ 1 ซึ่งได้รับจากโนดตรวจสอบ c_4 หรือ $r_{44}(1)$ จะมีค่าเท่ากับ

$$\begin{aligned} r_{44}(1) = {} & q_{21}(1)q_{61}(0)q_{71}(0)q_{81}(0) + q_{21}(0)q_{61}(1)q_{71}(0)q_{81}(0) + q_{21}(0)q_{61}(0)q_{71}(1)q_{81}(0) + \\ & q_{21}(0)q_{61}(0)q_{71}(0)q_{81}(1) + q_{21}(0)q_{61}(1)q_{71}(1)q_{81}(1) + q_{21}(1)q_{61}(0)q_{71}(1)q_{81}(1) + \\ & q_{21}(1)q_{61}(1)q_{71}(0)q_{81}(1) + q_{21}(1)q_{61}(1)q_{71}(1)q_{81}(0) \end{aligned} \tag{4.6}$$

จัดรูปใหม่จะได้เป็น

$$r_{44}(1) = \frac{1}{2} - \frac{1}{2}\big(1-2q_{21}(0)\big)\big(1-2q_{61}(0)\big)\big(1-2q_{71}(0)\big)\big(1-2q_{81}(0)\big) \tag{4.7}$$

ดังนั้น ความน่าจะเป็นของโนดตัวแปร v_i มีค่าเท่ากับ 1 ซึ่งได้รับจากโนดตรวจสอบ c_j เมื่อจำนวนเส้นเชื่อมของโนดตรวจสอบ c_j เป็นเลขคี่ คำนวณจากสมการต่อไปนี้

$$r_{ji}(1) = \frac{1}{2} - \frac{1}{2}\prod_{i' \in V_j \setminus i}\big(1-2q_{i'j}(0)\big) \tag{4.8}$$

เมื่อ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบ c_j ยกเว้นโนดตัวแปร v_i

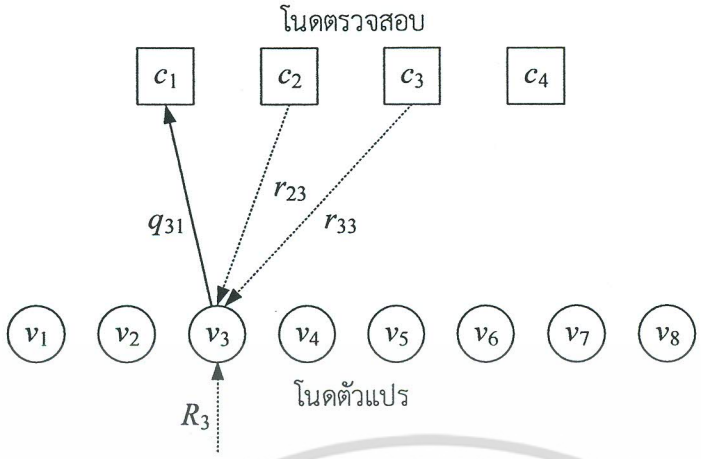
สำหรับความน่าจะเป็นของโนดตัวแปร v_i มีค่าเท่ากับ 0 ซึ่งได้รับจากโนดตรวจสอบ c_j คำนวณจากสมการต่อไปนี้

$$r_{ji}(0) = 1 - r_{ji}(1) \tag{4.9}$$

พิจารณาความน่าจะเป็นหรือความเชื่อมั่นจากโนดตัวแปรไปยังโนดตรวจสอบในรูปที่ 4.2 ความเชื่อมั่นของโนดตัวแปร v_3 ที่ส่งไปยังโนดตรวจสอบ c_1 หรือ q_{31} คำนวณได้ผลคูณของความน่าจะเป็นทั้งหมดที่ได้รับจากโนดตรวจสอบ c_2, c_3 และความน่าจะเป็น R_3 หรือความน่าจะเป็นของโนดตัวแปร v_3 ได้รับจากช่องสัญญาณ ซึ่งมีค่าเท่ากับความน่าจะเป็น $P(y_3 \mid v_3)$ ตามที่ได้อธิบายในบทที่ 2 กำหนดให้ K คือค่าคงที่ซึ่งทำให้ผลรวมความน่าจะเป็น $q_{31}(0) + q_{31}(1) = 1$ ดังนั้น

$$q_{31}(0) = KR_3(0)r_{23}(0)r_{33}(0) \tag{4.10}$$

$$q_{31}(1) = KR_3(1)r_{23}(1)r_{33}(1) \tag{4.11}$$



รูปที่ 4.2 ความเชื่อมั่นจากโนดตัวแปรไปโนดตรวจสอบ

ความเชื่อมั่นจากโนดตัวแปรไปโนดตรวจสอบสามารถเขียนให้อยู่ในรูปสมการทั่วไป ดังนี้

$$q_{ij}(0) = KR_i(0) \prod_{j' \in C_i \setminus j} r_{j'i}(0) \tag{4.12}$$

$$q_{ij}(1) = KR_i(1) \prod_{j' \in C_i \setminus j} r_{j'i}(1) \tag{4.13}$$

เมื่อ $R_i(0) = P(y_i \mid v_i = 0)$ และ $R_i(1) = P(y_i \mid v_i = 1)$ คำนวณจากสมการที่ 2.2 และ 2.3 (บทที่ 2) และ $C_i \setminus j$ คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i ยกเว้นโนดตรวจสอบ c_j

ดังนั้น ความน่าจะเป็นของคำรหัสที่ถูกถอดรหัสด้วยอัลกอริทึมกระจายความเชื่อมั่นมีค่าเป็น

$$Q_i(0) = KR_i(0) \prod_{j' \in C_i} r_{j'i}(0) \tag{4.14}$$

$$Q_i(1) = KR_i(1) \prod_{j' \in C_i} r_{j'i}(1) \tag{4.15}$$

เมื่อ C_i คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i และทำการตัดสินใจคำรหัส $\hat{v}_i$ ที่ถูกส่งผ่านช่องสัญญาณ ดังนี้

$$\hat{v}_i = \begin{cases} 1, & Q_i(0) < Q_i(1) \\ 0, & Q_i(0) > Q_i(1) \end{cases} \tag{4.16}$$

กรณี $Q_i(0) = Q_i(1)$ จะทำการสุ่มเลือกบิตคำรหัสด้วยความน่าจะเป็น $P(\hat{v}_i = 0) = P(\hat{v}_i = 1) = 0.5$

กำหนดให้ M คือจำนวนโนดตรวจสอบและ N คือจำนวนโนดตัวแปรในกราฟแทนเนอร์ ดังนั้น ขั้นตอนการถอดรหัสแอลดีพีซีที่มีจำนวนการวนซ้ำ l_{MAX} ครั้ง แสดงในตารางที่ 4.1

ตารางที่ 4.1 อัลกอริทึมกระจายความเชื่อมั่นแบบความน่าจะเป็นกรณีฟิลด์จำกัด GF(2)

---

for $i=1$ **to** N

คำนวณความเชื่อมั่น $R_i(0)$ และ $R_i(1)$ ของโนดตัวแปรลำดับที่ i ที่ได้รับจากช่องสัญญาณ โดยใช้สมการที่ 2.2 และ 2.3 (บทที่ 2)

end

กำหนดให้ความเชื่อมั่น $r_{ji}(0)=r_{ji}(1)=0.5$ เมื่อ $1\le i\le N$ และ $1\le j\le M$

for $l=1$ **to** l_{MAX}

for $i=1$ **to** N

for all $j\in C_i$

คำนวณความเชื่อมั่น $q_{ij}(0)$ และ $q_{ij}(1)$ จากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j โดยใช้สมการที่ 4.12 และ 4.13

end

end

for $j=1$ **to** M

for all $i\in V_j$

คำนวณความเชื่อมั่น $r_{ji}(0)$ และ $r_{ji}(1)$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.4 (กรณีจำนวนเส้นเชื่อมเป็นเลขคู่) หรือ 4.8 (กรณีจำนวนเส้นเชื่อมเป็นเลขคี่) และสมการที่ 4.9

end

end

end

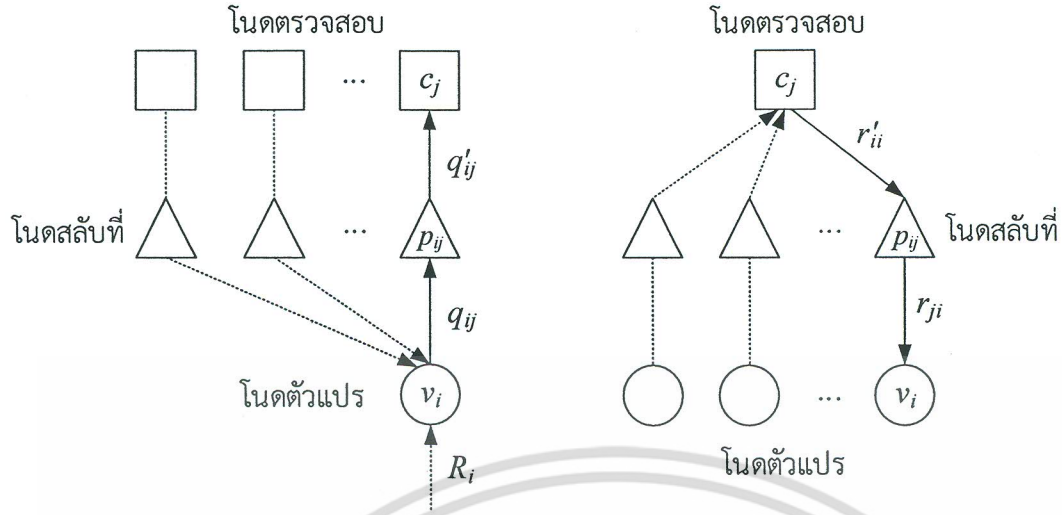
for $i=1$ **to** N

คำนวณความเชื่อมั่น $Q_i(0)$ และ $Q_i(1)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.14 และ 4.15 หลังจากนั้นทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณโดยใช้สมการที่ 4.16

end

4.1.2 กรณีฟิลด์จำกัด GF(q)

สำหรับรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ซึ่งมีเวกเตอร์คำรหัส $v_i\in\{0,1,\ldots,q-1\}$ และเมทริกซ์พาริตี้เช็ค $h_{i,j}\in\{0,1,\ldots q-1\}$ (นิยมเรียกรหัสไบนารีแอลดีพีซีเมื่อ $q=2$ และรหัสนอนไบนารีแอลดีพีซีเมื่อ $q>2$) พิจารณาข่าวสารในกราฟแทนเนอร์ของรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ในรูปที่ 4.3 โดยพบว่าความเชื่อมั่นจากโนดตัวแปร v_i ไปยังโนดตรวจสอบ c_j และความเชื่อมั่นจากโนดตรวจสอบ c_j ไปยังโนดตัวแปร v_i จะผ่านโนดสลับที่ p_{ij} ก่อนเสมอ (โนดสลับที่ p_{ij} แสดงอิลิเมนท์ในเมทริกซ์พาริตี้เช็คที่มีค่ามากกว่าศูนย์ รายละเอียดอธิบายในหัวข้อ 3.2.3)



ก) โนดตัวแปรไปโนดตรวจสอบ ข) โนดตรวจสอบไปโนดตัวแปร

รูปที่ 4.3 ความเชื่อมั่นในกราฟแทนเนอร์ของรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q)

จากหัวข้อที่ผ่านมา สังเกตได้ว่าความเชื่อมั่นที่ส่งออกจากโนดตัวแปรจะมีค่าเท่ากับผลคูณของความเชื่อมั่นทั้งหมดที่ส่งให้โนดตัวแปรตามสมการที่ 4.12 และ 4.13 ดังนั้น สำหรับรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ข่าวสารที่ออกจากโนดตัวแปร v_i ไปยังโนดสลับที่ p_{ij} หรือความน่าจะเป็นที่โนดตัวแปร v_i จะมีค่าเป็น $k=0,1,\ldots q-1$ คำนวณได้จาก

$$q_{ij}(k) = KR_i(k)\prod_{j'\in C_i\setminus j} r_{j'i}(k) \tag{4.17}$$

เมื่อ K คือค่าคงที่ซึ่งทำให้ผลรวมความน่าจะเป็น $\sum_k q_{ij}(k)=1$ และ $C_i \setminus j$ คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i ยกเว้นโนดตรวจสอบ c_j สำหรับความน่าจะเป็น $R_i(k)$ ที่ได้รับจากช่องสัญญาณ สามารถคำนวณได้จากผลคูณความน่าจะเป็นของคำรหัสแบบไบนารีที่ได้รับจากช่องสัญญาณ ตัวอย่างเช่น กรณีฟิลด์จำกัด GF(4) บิตคำรหัส $v_i \in \{0,1,2,3\}$ จะถูกแทนด้วยคำรหัสไบนารี $v_i \in \{0,1\}$ จำนวน 2 บิต ก่อนถูกส่งผ่านช่องสัญญาณ ดังนั้น ความน่าจะเป็นของบิตคำรหัสบนฟิลด์จำกัดจะมีค่าเท่ากับ ผลคูณความน่าจะเป็นของสัญญาณที่ได้รับจากช่องสัญญาณจำนวน 2 บิต ได้แก่

$$R_i(0) = P(y_l \mid v_l = 0)\times P(y_{l+1} \mid v_{l+1} = 0) \tag{4.18}$$

$$R_i(1) = P(y_l \mid v_l = 0)\times P(y_{l+1} \mid v_{l+1} = 1) \tag{4.19}$$

$$R_i(2) = P(y_l \mid v_l = 1)\times P(y_{l+1} \mid v_{l+1} = 0) \tag{4.20}$$

$$R_i(3) = P(y_l \mid v_l = 1)\times P(y_{l+1} \mid v_{l+1} = 1) \tag{4.21}$$

เมื่อ l คือลำดับของบิตคำรหัสไบนารีซึ่งเกี่ยวข้องกับบิตคำรหัสลำดับที่ i บนฟิลด์จำกัด ทั้งนี้สามารถเขียนให้อยู่ในรูปทั่วไปได้ดังนี้

$$R_i(k) = \prod_l P(y_l \mid v_l = 0,1) \tag{4.22}$$

สำหรับความน่าจะเป็นของคำรหัสที่ถูกถอดรหัส สามารถคำนวณได้ ดังนี้

$$Q_i(k) = KR_i(k) \prod_{j' \in C_i} r_{j'i}(k) \tag{4.23}$$

เมื่อ C_i คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i และทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณจาก

$$\hat{v}_i = k \text{ เมื่อ } Q_i(k) = \max\{Q_i(.)\} \tag{4.24}$$

พิจารณากราฟแทนเนอร์ในรูปที่ 3.8 (บทที่ 3) โนดตัวแปร v_5 เชื่อมกับโนดสลับที่ p_{53} ซึ่งมีค่าเท่ากับ 3 จากนั้นเชื่อมกับโนดตรวจสอบ c_3 ทำให้ ข่าวสาร q_{53} จากโนดตัวแปร v_5 จะถูกคูณด้วยค่าคงที่เท่ากับ 3 จากตารางการคูณในตารางที่ 3.1 ทำให้ข่าวสาร q'_{53} ที่ออกจากโนดสลับที่ p_{53} มีค่าเท่ากับ

$$q'_{53}(0) = q_{53}(0) \tag{4.25}$$

$$q'_{53}(1) = q_{53}(2) \tag{4.26}$$

$$q'_{53}(2) = q_{53}(3) \tag{4.27}$$

$$q'_{53}(3) = q_{53}(1) \tag{4.28}$$

จะสังเกตได้ว่าข่าวสาร q'_{ij} เกิดจากการสลับที่ข่าวสาร q_{ij} กำหนดให้ $k = 0,1,\ldots q-1$ ดังนั้น ข่าวสาร q'_{ij} ที่ออกจากโนดสลับที่ p_{ij} ไปยังโนดตรวจสอบ c_j คำนวณได้จาก

$$q'_{ij}(kp_{ij}) = q_{ij}(k) \tag{4.29}$$

และข่าวสาร r_{ji} ที่ออกจากโนดสลับที่ p_{ij} ไปยังโนดสลับตำแหน่ง v_i คำนวณได้จาก

$$r_{ji}(k / p_{ij}) = r'_{ji}(k) \tag{4.30}$$

พิจารณากราฟแทนเนอร์ในรูปที่ 3.8 และการบวกและคูณในตารางที่ 3.1 ความน่าจะเป็น r_{36} จากโนดตรวจสอบ c_3 ไปยังโนดตัวแปร v_6 คำนวณได้จาก

$$r'_{36}(0) = q'_{33}(0)q'_{53}(0) + q'_{33}(1)q'_{53}(1) + q'_{33}(2)q'_{53}(2) + q'_{33}(3)q'_{53}(3) \quad (4.31)$$

$$r'_{36}(1) = q'_{33}(0)q'_{53}(1) + q'_{33}(1)q'_{53}(0) + q'_{33}(2)q'_{53}(3) + q'_{33}(3)q'_{53}(2) \quad (4.32)$$

$$r'_{36}(2) = q'_{33}(0)q'_{53}(2) + q'_{33}(1)q'_{53}(3) + q'_{33}(2)q'_{53}(0) + q'_{33}(3)q'_{53}(1) \quad (4.33)$$

$$r'_{36}(3) = q'_{33}(0)q'_{53}(3) + q'_{33}(1)q'_{53}(2) + q'_{33}(2)q'_{53}(1) + q'_{33}(3)q'_{53}(0) \quad (4.34)$$

จากสมการที่ 4.31 ถึง 4.34 จะได้

$$r'_{36}(0) + r'_{36}(1) + r'_{36}(2) + r'_{36}(3) = \left(q'_{33}(0) + q'_{33}(1) + q'_{33}(2) + q'_{33}(3)\right)\left(q'_{53}(0) + q'_{53}(1) + q'_{53}(2) + q'_{53}(3)\right)$$
$$r'_{36}(0) - r'_{36}(1) + r'_{36}(2) - r'_{36}(3) = \left(q'_{33}(0) - q'_{33}(1) + q'_{33}(2) - q'_{33}(3)\right)\left(q'_{53}(0) - q'_{53}(1) + q'_{53}(2) - q'_{53}(3)\right)$$
$$r'_{36}(0) + r'_{36}(1) - r'_{36}(2) - r'_{36}(3) = \left(q'_{33}(0) + q'_{33}(1) - q'_{33}(2) - q'_{33}(3)\right)\left(q'_{53}(0) + q'_{53}(1) - q'_{53}(2) - q'_{53}(3)\right)$$
$$r'_{36}(0) - r'_{36}(1) - r'_{36}(2) + r'_{36}(3) = \left(q'_{33}(0) - q'_{33}(1) - q'_{33}(2) + q'_{33}(3)\right)\left(q'_{53}(0) - q'_{53}(1) - q'_{53}(2) + q'_{53}(3)\right)$$

หรือเขียนในรูปเมทริกซ์ ดังนี้

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} r'_{36}(0) \\ r'_{36}(1) \\ r'_{36}(2) \\ r'_{36}(3) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} q'_{33}(0) \\ q'_{33}(1) \\ q'_{33}(2) \\ q'_{33}(3) \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} q'_{53}(0) \\ q'_{53}(1) \\ q'_{53}(2) \\ r'_{53}(3) \end{bmatrix} \quad (4.35)$$

เมื่อสัญลักษณ์ $\otimes$ คือการคูณระหว่างอิลิเมนท์ของเมทริกซ์ พิจารณาการแปลงฟูเรียร์แบบเร็ว (fast Fourier transform) โดยใช้เมทริกซ์ฮาดามาร์ด (Hadamard matrix) ดังต่อไปนี้

$$F_{2^a} = \begin{bmatrix} F_{2^{a-1}} & F_{2^{a-1}} \\ F_{2^{a-1}} & -F_{2^{a-1}} \end{bmatrix} \quad (4.36)$$

เมื่อ a คือจำนวนเต็มบวกใดๆ ตัวอย่างเช่น $F_1 = [1]$ และ $F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ ดังนั้น สามารถแสดงสมการที่ 4.35 โดยใช้การแปลงฟูเรียร์แบบเร็วดังนี้

$$F\left(\begin{bmatrix} r'_{36}(0) \\ r'_{36}(1) \\ r'_{36}(2) \\ r'_{36}(3) \end{bmatrix}\right) = F\left(\begin{bmatrix} q'_{33}(0) \\ q'_{33}(1) \\ q'_{33}(2) \\ q'_{33}(3) \end{bmatrix}\right) \otimes F\left(\begin{bmatrix} q'_{53}(0) \\ q'_{53}(1) \\ q'_{53}(2) \\ r'_{53}(3) \end{bmatrix}\right) \tag{4.37}$$

จัดรูปใหม่จะได้

$$\begin{bmatrix} r'_{36}(0) \\ r'_{36}(1) \\ r'_{36}(2) \\ r'_{36}(3) \end{bmatrix} = F^{-1}\left(F\left(\begin{bmatrix} q'_{33}(0) \\ q'_{33}(1) \\ q'_{33}(2) \\ q'_{33}(3) \end{bmatrix}\right) \otimes F\left(\begin{bmatrix} q'_{53}(0) \\ q'_{53}(1) \\ q'_{53}(2) \\ r'_{53}(3) \end{bmatrix}\right)\right) \tag{4.38}$$

เมื่อ F^{-1} คือการแปลงฟูเรียร์ผกผันแบบเร็วหรืออินเวอร์สของเมทริกซ์ฮาร์ดามาร์ด ดังนั้น การคำนวณข่าวสาร r'_{ji} จากโนดตรวจสอบ c_j ไปยังโนดสลับที่ p_{ij} สามารถเขียนอยู่ในรูปทั่วไป ดังนี้

$$r'_{ji}(.) = F^{-1}\left(\prod_{i' \in V_j \setminus i} F\left(q'_{i'j}(.)\right) \right) \tag{4.39}$$

เมื่อ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบ c_j ยกเว้นโนดตัวแปร v_i

ขั้นตอนการถอดรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) โดยใช้อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็น แสดงในตารางต่อไปนี้

ตารางที่ 4.2 อัลกอริทึมกระจายความเชื่อมั่นแบบความน่าจะเป็นกรณีฟีลด์จำกัด GF(q)

---

for $i = 1$ **to** N

คำนวณความเชื่อมั่น $R_i(.)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.22 โดยความน่าจะเป็นของสัญญาณที่ได้รับจากช่องสัญญาณจำนวณจากสมการที่ 2.2 และ 2.3 (บทที่ 2)

end

กำหนดให้ความเชื่อมั่น $r_{ji}(.) = 1/q$ เมื่อ $1 \le i \le N$ และ $1 \le j \le M$

for $l = 1$ **to** l_{MAX}

for $i = 1$ **to** N

for all $j \in C_i$

คำนวณความเชื่อมั่น $q_{ij}(.)$ จากโนดตัวแปรลำดับที่ i ไปยังโนดสลับที่โดยใช้สมการที่ 4.17 จากนั้นคำนวณความเชื่อมั่น $q'_{ij}(.)$ ไปยังโนดตรวจสอบลำดับที่ j โดยใช้สมการที่ 4.29

end

end

for $j=1$ **to** M

for all $i \in V_j$

คำนวณความเชื่อมั่น $r'_{ji}(.)$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดสลับที่โดยใช้สมการที่ 4.39 จากนั้นคำนวณความเชื่อมั่น $r_{ji}(.)$ ไปยังโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.30

end

end

end

for $i=1$ **to** N

คำนวณความเชื่อมั่น $Q_i(.)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.23 หลังจากนั้นทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณโดยใช้สมการที่ 4.24

end

4.2 อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อก

อัลกอริทึมกระจายความเชื่อมั่นแบบความน่าจะเป็นในหัวข้อที่ผ่านมา ไม่เหมาะสมต่อการประยุกต์ใช้งานในวงจรถอดรหัส ทั้งนี้ เนื่องจากอัลกอริทึมมีความซับซ้อนสูง โดยจะพบว่าขั้นตอนการถอดรหัสจะประกอบไปด้วยการคูณเป็นจำนวนมาก อีกทั้งปัญหาการเก็บข้อมูลในรูปความน่าจะเป็นลงในหน่วยความจำ โดยทั่วไป นิยมใช้อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อก ดังต่อไปนี้

4.2.1 กรณีฟิลด์จำกัด GF(2)

กำหนดให้ ข่าวสารในกราฟแทนเนอร์ของรหัสไบนารีแอลดีพีซีอยู่ในรูปอัตราส่วนความน่าจะเป็นแบบล็อก (Log Likelihood Ratios, LLR) ดังนี้

$$L(q_{ij}) = \log\left(\frac{q_{ij}(0)}{q_{ij}(1)}\right) \tag{4.40}$$

$$L(Q_i) = \log\left(\frac{Q_i(0)}{Q_i(1)}\right) \tag{4.41}$$

$$L(r_{ji}) = \log\left(\frac{r_{ji}(0)}{r_{ji}(1)}\right) \tag{4.42}$$

$$L(R_i) = \log\left(\frac{R_i(0)}{R_i(1)}\right) \tag{4.43}$$

อัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโนดตัวแปรไปยังโนดตรวจสอบ คำนวณได้จากการนำสมการที่ 4.12 มาหารด้วย 4.13 ซึ่งจะได้

$$L(q_{ij}) = L(R_i) + \sum_{j' \in C_i \setminus j} L(r_{j'i}) \tag{4.44}$$

และอัตราส่วนความน่าจะเป็นแบบล็อกของคำรหัสที่ได้จากการถอดรหัสหาได้จาก

$$L(Q_i) = L(R_i) + \sum_{j \in C_i} L(r_{j'i}) \tag{4.45}$$

และทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณ ดังนี้

$$\hat{v}_i = \begin{cases} 1\ , & L(Q_i) < 0 \\ 0\ , & L(Q_i) > 0 \end{cases} \tag{4.46}$$

สำหรับอัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโนดตรวจสอบไปยังโนดตัวแปร กรณีเส้นเชื่อมของโนดตรวจสอบเป็นเลขคู่ จากสมการที่ 4.4 ทำการแทน $r_{ji}(1)$ ด้วย $1-r_{ji}(0)$ จะได้

$$1-2r_{ji}(0) = \prod_{i' \in V_j \setminus i} \left(1-2q_{i'j}(0)\right) \tag{4.47}$$

จากความสัมพันธ์ $1-2P(x=0) = -\tanh\left(\frac{1}{2}\log\left(\frac{P(x=0)}{P(x=1)}\right)\right)$ ดังนั้น

$$-\tanh\left(\frac{1}{2}L(r_{ji})\right) = \prod_{i' \in V_j \setminus i}\left(-\tanh\left(\frac{1}{2}L(q_{i'j})\right)\right) \tag{4.48}$$

เนื่องจากเส้นเชื่อมของโนดตรวจสอบเป็นเลขคู่ ทำให้

$$L(r_{ji}) = 2\tanh^{-1}\left(\prod_{i' \in V_j \setminus i} \tanh\left(\frac{1}{2}L(q_{i'j})\right)\right) \tag{4.49}$$

สำหรับการคำนวณกรณีเส้นเชื่อมของโนดตรวจสอบเป็นเลขคี่ จะมีผลลัพธ์เท่ากับสมการที่ 4.49

การคำนวณข่าวสารจากโนดตรวจสอบไปยังโนดตัวแปรโดยใช้สมการที่ 4.49 อาจเกิดปัญหาในการคำนวณฟังก์ชัน $\tanh(.)$ และ $\tanh^{-1}(.)$ ดังนั้น กำหนดให้ $L(q_{ij}) = \alpha_{ij}\beta_{ij}$ โดยที่ $\alpha_{ij} = \text{sign}\{L(q_{ij})\}$ และ $\beta_{ij} = |L(q_{ij})|$ จะได้

$$L(r_{ji}) = \left(\prod_{i' \in V_j \setminus i} \alpha_{i'j} \right) 2\tanh^{-1}\left(\prod_{i' \in V_j \setminus i} \tanh\left(\frac{1}{2}\beta_{i'j} \right) \right)$$
$$= \left(\prod_{i' \in V_j \setminus i} \alpha_{i'j} \right) 2\tanh^{-1} \log^{-1} \sum_{i' \in V_j \setminus i} \log\left(\tanh\left(\frac{1}{2}\beta_{i'j} \right) \right) \quad (4.50)$$

กำหนดให้ $\phi(x) = -\log(\tanh(x/2)) = \log((e^x+1)/(e^x-1))$ และ $\phi(x) = \phi^{-1}(x)$ ที่ $x > 0$ ดังนั้น ข่าวสารในรูปอัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโนดตรวจสอบไปยังโนดตัวแปรเท่ากับ

$$L(r_{ji}) = \left(\prod_{i' \in V_j \setminus i} \alpha_{i'j} \right) \left(\phi\left(\sum_{i' \in V_j \setminus i} \phi(\beta_{i'j}) \right) \right) \quad (4.51)$$

ขั้นตอนการถอดรหัสแอลดีพีซีบนฟีลด์จำกัด GF(2) โดยใช้อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อก แสดงในตารางต่อไปนี้

ตารางที่ 4.3 อัลกอริทึมกระจายความเชื่อมั่นแบบล็อกกรณีฟีลด์จำกัด GF(2)

for $i = 1$ **to** N
  คำนวณความเชื่อมั่น $L(R_i)$ ของโนดตัวแปรลำดับที่ i ที่ได้รับจากช่องสัญญาณ
  โดยใช้สมการในบทที่ 2
end
กำหนดให้ความเชื่อมั่น $L(r_{ji}) = 0$ เมื่อ $1 \le i \le N$ และ $1 \le j \le M$
for $l = 1$ **to** l_{MAX}
  for $i = 1$ **to** N
    for all $j \in C_i$
      คำนวณความเชื่อมั่น $L(q_{ij})$ จากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบ
      ลำดับที่ j โดยใช้สมการที่ 4.44
    end
  end
  for $j = 1$ **to** M
    for all $i \in V_j$
      คำนวณความเชื่อมั่น $L(r_{ji})$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปร
      ลำดับที่ i โดยใช้สมการที่ 4.49 หรือ 4.51
    end
  end
end

for $i=1$ **to** N

คำนวณความเชื่อมั่น $L(Q_i)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.45

หลังจากนั้นทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณโดยใช้สมการที่ 4.46

end

4.2.2 กรณีฟิลด์จำกัด GF(q)

กำหนดให้ ข่าวสารในกราฟแทนเนอร์ของรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) อยู่ในรูปอัตราส่วนความน่าจะเป็นแบบล็อก (Log Likelihood Ratios, LLR) ดังนี้

$$\mathbf{L}(q_{ij})=\left[L_0(q_{ij})\ L_1(q_{ij})\ \ldots\ L_{q-1}(q_{ij})\right]=\left[\log\left(\frac{q_{ij}(0)}{q_{ij}(0)}\right)\ \log\left(\frac{q_{ij}(1)}{q_{ij}(0)}\right)\ \ldots\ \log\left(\frac{q_{ij}(q-1)}{q_{ij}(0)}\right)\right] \quad (4.52)$$

$$\mathbf{L}(Q_i)=\left[L_0(Q_i)\ L_1(Q_i)\ \ldots\ L_{q-1}(Q_i)\right]=\left[\log\left(\frac{Q_i(0)}{Q_i(0)}\right)\ \log\left(\frac{Q_i(1)}{Q_i(0)}\right)\ \ldots\ \log\left(\frac{Q_i(q-1)}{Q_i(0)}\right)\right] \quad (4.53)$$

$$\mathbf{L}(r_{ji})=\left[L_0(r_{ji})\ L_1(r_{ji})\ \ldots\ L_{q-1}(r_{ji})\right]=\left[\log\left(\frac{r_{ji}(0)}{r_{ji}(0)}\right)\ \log\left(\frac{r_{ji}(1)}{r_{ji}(0)}\right)\ \ldots\ \log\left(\frac{r_{ji}(q-1)}{r_{ji}(0)}\right)\right] \quad (4.54)$$

$$\mathbf{L}(R_i)=\left[L_0(R_i)\ L_1(R_i)\ \ldots\ L_{q-1}(R_i)\right]=\left[\log\left(\frac{R_i(0)}{R_i(0)}\right)\ \log\left(\frac{R_i(1)}{R_i(0)}\right)\ \ldots\ \log\left(\frac{R_i(q-1)}{R_i(0)}\right)\right] \quad (4.55)$$

จากสมการที่ 4.17 อัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโนดตัวแปรไปยังโนดตรวจสอบสามารถเขียนในรูปอัตราส่วนความน่าจะเป็นแบบล็อก ดังนี้

$$L_k(q_{ij})=L\left(\frac{q_{ij}(k)}{q_{ij}(0)}\right)=L\left(\frac{KR_i(k)\prod_{j'\in C_i\setminus j}r_{j'i}(k)}{KR_i(0)\prod_{j'\in C_i\setminus j}r_{j'i}(0)}\right)=L_k\left(R_i\right)+\sum_{j'\in C_i\setminus j}L_k(r_{j'i}) \quad (4.56)$$

เมื่อ $k=0,1,2\ldots,q-1$ และความเชื่อมั่นที่ได้จากการถอดรหัสแอลดีพีซีคำนวณได้จาก

$$L_k(Q_i)=L_k\left(R_i\right)+\sum_{j'\in C_i}L_k(r_{j'i}) \quad (4.57)$$

และทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณ ดังนี้

$$\hat{v}_i=k \ \text{ เมื่อ } \ L_k(Q_i)=\max\left\{\mathbf{L}(Q_i)\right\} \quad (4.58)$$

จากสมการที่ 4.29 และ 4.30 จะสังเกตได้ว่า ข่าวสาร q'_{ij} และ r_{ji} ที่ออกจากโนดสลับที่เกิดจากการสลับที่ข่าวสาร q_{ij} และ r'_{ji} ตามลำดับ ดังนั้น กำหนดให้ $k=0,1,\ldots,q-1$ ทำให้

$$L_{kp_{ij}}(q'_{ij}) = L_k(q_{ij}) \tag{4.59}$$

$$L_{k/p_{ij}}(r_{ji}) = L_k(r'_{ji}) \tag{4.60}$$

พิจารณาข่าวสารจากโนดตรวจสอบไปยังโนดสลับที่ในสมการที่ 4.31 และ 4.34 อัตราส่วนความน่าจะเป็นแบบล็อกจะมีค่าเป็น

$$L_3(r'_{36}) = \log\left(\frac{r'_{36}(3)}{r'_{36}(0)}\right) = \log\left(\frac{q'_{33}(0)q'_{53}(3)+q'_{33}(1)q'_{53}(2)+q'_{33}(2)q'_{53}(1)+q'_{33}(3)q'_{53}(0)}{q'_{33}(0)q'_{53}(0)+q'_{33}(1)q'_{53}(1)+q'_{33}(2)q'_{53}(2)+q'_{33}(3)q'_{53}(3)}\right) \tag{4.61}$$

เนื่องจาก $L_k(q_{ij}) = \log\left(\frac{q_{ij}(k)}{q_{ij}(0)}\right)$ เมื่อ $k=0,1,2,\ldots,q-1$ ทำให้

$$\begin{aligned} L_3(r'_{36}) = {} & \log\left(e^{L_0(q'_{33})+L_3(q'_{53})}+e^{L_1(q'_{33})+L_2(q'_{53})}+e^{L_2(q'_{33})+L_1(q'_{53})}+e^{L_3(q'_{33})+L_0(q'_{53})}\right) - \\ & \log\left(e^{L_0(q'_{33})+L_0(q'_{53})}+e^{L_1(q'_{33})+L_1(q'_{53})}+e^{L_2(q'_{33})+L_2(q'_{53})}+e^{L_3(q'_{33})+L_3(q'_{53})}\right) \end{aligned} \tag{4.62}$$

ดังนั้น การคำนวณข่าวสารจากโนดตรวจสอบไปยังโนดสลับที่เขียนในรูปทั่วไปได้ดังนี้

$$L_k(r'_{ji}) = \log\left(\sum_{x=0}^{q-1}\exp\left(\sum_{i'\in V_j\backslash i} L_{k'_{i'}\in\{\text{condition}(x,k)\}}(q_{i'j})\right)\right) - \log\left(\sum_{x=0}^{q-1}\exp\left(\sum_{i'\in V_j\backslash i} L_x(q_{i'j})\right)\right) \tag{4.63}$$

เมื่อ $\{\text{condition}(x,k)\}$ คือ เซตของอิลิเมนท์ในฟิลด์จำกัด $GF(q)$ ซึ่งมีเงื่อนไขที่ทำให้ผลรวม $x+\sum_{i'\in V_j\backslash i}k' = k$ เป็นจริง กำหนดให้ $\max^*(x_1,x_2) = \log(e^{x_1}+e^{x_2})$ (กรณี $\max^*(x_1,x_2,x_3)$ จะมีค่าเท่ากับ $\max^*(\max^*(x_1,x_2),x_3)$) ดังนั้น ข่าวสารจากโนดตรวจสอบไปยังโนดสลับที่ในสมการที่ 4.63 จะมีค่าเท่ากับ

$$L_k(r'_{ji}) = \max^*\left(L_{k'_{i'}\in\{\text{condition}(x,k)\}}(q_{i'j})\right) - \max^*\left(\mathbf{L}(q_{i'j})\right) \tag{4.64}$$

เนื่องจาก $\max^*(x_1,x_2) = \max\{x_1,x_2\} + \log\left(1+e^{-|x_1-x_2|}\right)$ ดังนั้น

$$L_k(r'_{ji}) = \max\left(L_{k'_{i'}\in\{\text{condition}(x,k)\}}(q_{i'j})\right) - \max\left\{\mathbf{L}(q_{i'j})\right\} + K \tag{4.65}$$

เมื่อ K คือค่าคงที่ซึ่งสามารถคำนวณไว้ล่วงหน้า (สมรรถนะของการถอดรหัสจะลดลงเมื่อค่า K ที่ใช้แตกต่างจากค่าที่ถูกต้อง) ทำให้การคำนวณข่าวสารจากโนดตรวจสอบไปยังโนดสลับที่จะใช้เพียงวงจรเปรียบเทียบและวงจรบวกเท่านั้น

อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อก ตามได้อธิบายในข้างต้น จะปราศจากการคูณที่ก่อให้เกิดความซับซ้อนและความไม่เสถียรของวงจรถอดรหัสแอลดีพีซี ขั้นตอนการถอดรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) โดยใช้อัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อก แสดงในตารางต่อไปนี้

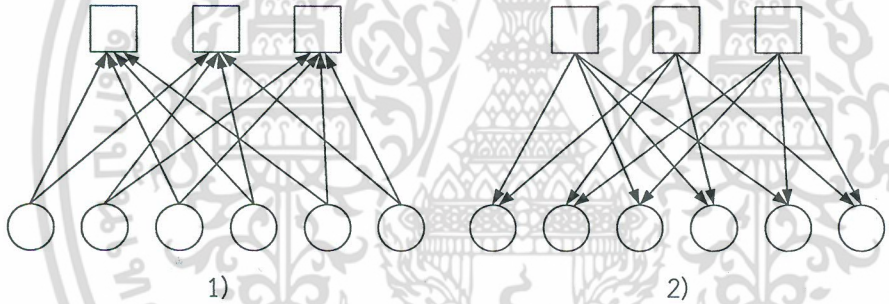
ตารางที่ 4.4 อัลกอริทึมกระจายความเชื่อมั่นแบบล็อกกรณีฟิลด์จำกัด GF(q)

---

for $i=1$ **to** N
  คำนวณความเชื่อมั่น $\mathbf{L}(R_i)$ ของโนดตัวแปรลำดับที่ i จากสัญญาณที่ได้รับจากช่องสัญญาณ
end
กำหนดให้ความเชื่อมั่น $\mathbf{L}(r_{ji})=0$ เมื่อ $1\le i\le N$ และ $1\le j\le M$
for $l=1$ **to** l_{MAX}
  for $i=1$ **to** N
    for all $j\in C_i$
      คำนวณความเชื่อมั่น $\mathbf{L}(q_{ij})$ จากโนดตัวแปรลำดับที่ i ไปยังโนดสลับที่โดยใช้สมการที่ 4.56 จากนั้นคำนวณความเชื่อมั่น $\mathbf{L}(q'_{ij})$ ไปยังโนดตรวจสอบลำดับที่ j โดยใช้สมการที่ 4.59
    end
  end
  for $j=1$ **to** M
    for all $i\in V_j$
      คำนวณความเชื่อมั่น $\mathbf{L}(r'_{ji})$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดสลับที่โดยใช้สมการที่ 4.65 จากนั้นคำนวณความเชื่อมั่น $\mathbf{L}(r_{ji})$ ไปยังโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.60
    end
  end
end
for $i=1$ **to** N
  คำนวณความเชื่อมั่น $\mathbf{L}(Q_i)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.57 หลังจากนั้นทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณโดยใช้สมการที่ 4.58
end

4.3 ลำดับการกระจายความเชื่อมั่น

หัวข้อที่ผ่านมา แสดงขั้นตอนการถอดรหัสแอลดีพีซีด้วยอัลกอริทึมกระจายความเชื่อมั่นหรืออัลกอริทึมบีพี (belief propagation algorithm, BP) โดยจะสังเกตได้ว่า การถอดรหัสแอลดีพีซีเป็นการแลกเปลี่ยนความเชื่อมั่นระหว่างโนดตรวจสอบและโนดตัวแปร รูปที่ 4.4 แสดงการแลกเปลี่ยนความเชื่อมั่นของการถอดรหัสแอลดีพีซีจำนวน 1 รอบ ความเชื่อมั่นในรูปความน่าจะเป็นของบิตคำรหัสถูกคำนวณจากโนดตัวแปรไปยังโนดตรวจสอบตามเส้นทางต่างๆ ในกราฟแทนเนอร์ จากนั้นคำนวณข่าวสารจากโนดตรวจสอบไปยังโนดตัวแปรเป็นอันเสร็จสิ้นกระบวนการถอดรหัสจำนวน 1 รอบ รูปที่ 4.7 แสดงอัตราบิตผิดพลาดของการถอดรหัสแอลดีพีซีด้วยอัลกอริทึมกระจายความเชื่อมั่นหรืออัลกอริทึมบีพี กำหนดให้รหัสแอลดีพีซีมีความยาวของคำรหัส $N = 4608$ บิต อัตรารหัสเท่ากับ $R = 8/9$ และดีกรีของโนดตัวแปร $d_v = 3$ เมื่ออัตราส่วนกำลังสัญญาณส่งต่อสัญญาณรบกวนมีค่าเท่ากับ $\mathrm{SNR} = 4.2$ dB โดยจะสังเกตได้ว่า เมื่อจำนวนการถอดรหัสวนซ้ำเพิ่มขึ้นจะทำให้อัตราบิตผิดพลาดลดลง จนกระทั่งจำนวนการวนซ้ำมากกว่า 35 รอบ อัตราบิตผิดพลาดจะมีลักษณะลู่เข้า (convergent)

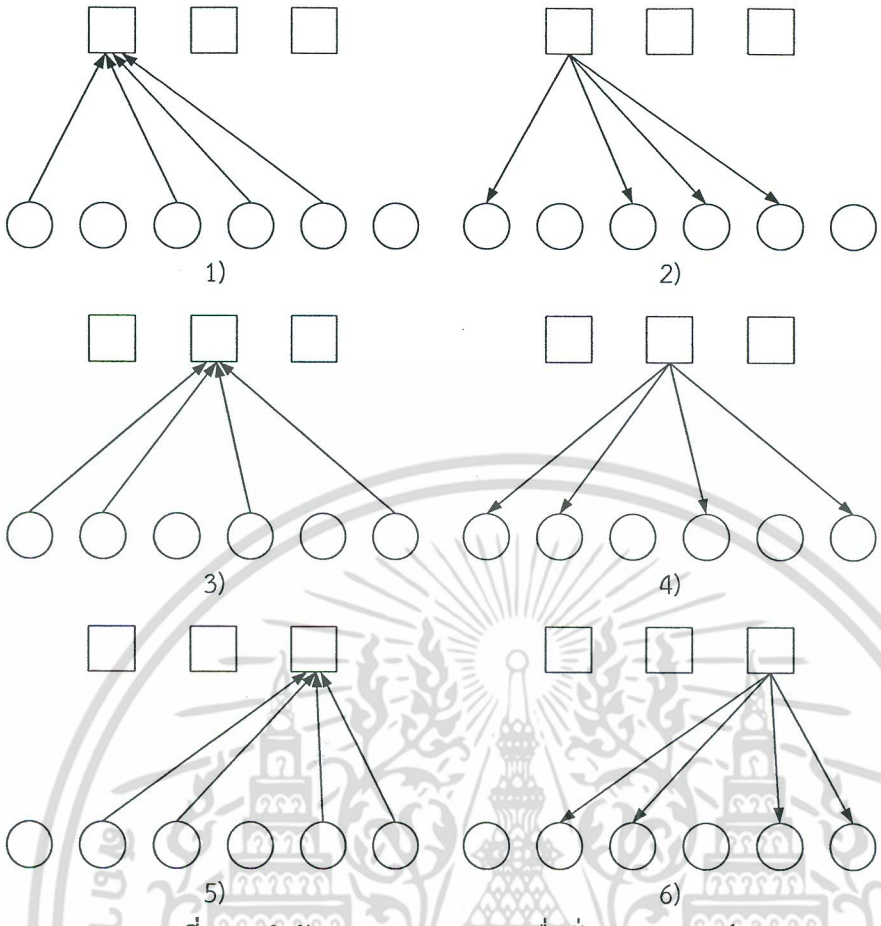


รูปที่ 4.4 ลำดับการกระจายความเชื่อมั่นแบบปรกติ

4.2.1 ลำดับแบบเลเยอร์

4.2.1 ลำดับแบบเลเยอร์

ในงานวิจัย [15] ได้นำเสนอการปรับปรุงลำดับการกระจายความเชื่อมั่นในกระบวนการถอดรหัสแอลดีพีซี เรียกว่า อัลกอริทึมกระจายความเชื่อมั่นแบบเลเยอร์หรืออัลกอริทึมแอลบีพี (layered belief propagation, LBP) พิจารณาลำดับการกระจายความเชื่อมั่นแบบเลเยอร์ในรูปที่ 4.6 ข่าวสารจากโนดตัวแปรจะถูกส่งไปยังโนดตรวจสอบลำดับที่ 1 และโนดตรวจสอบลำดับที่ 1 จะส่งข่าวสารกลับไปยังโนดตัวแปร จากนั้น เริ่มการส่งข่าวสารจากโนดตัวแปรไปยังโนดตรวจสอบลำดับที่ 2 จนกระทั่งโนดตัวแปรและโนดตรวจสอบส่งข่าวสารครบทุกโนด (เท่ากับการถอดรหัสวนซ้ำจำนวน 1 รอบ) โดยสังเกตได้ว่า ลำดับการกระจายข่าวสารของโนดตัวแปรและโนดตรวจสอบถูกปรับเปลี่ยน (กระจายข่าวสารเรียงลำดับตามโนดตรวจสอบ) ต่างจากอัลกอริทึมบีพี ซึ่งโนดตัวแปรจะส่งข่าวสารไปยังโนดตรวจสอบทุกโนดจนครบ หลังจากนั้น ทำการส่งข่าวสารจากโนดตรวจสอบไปยังโนดตัวแปร



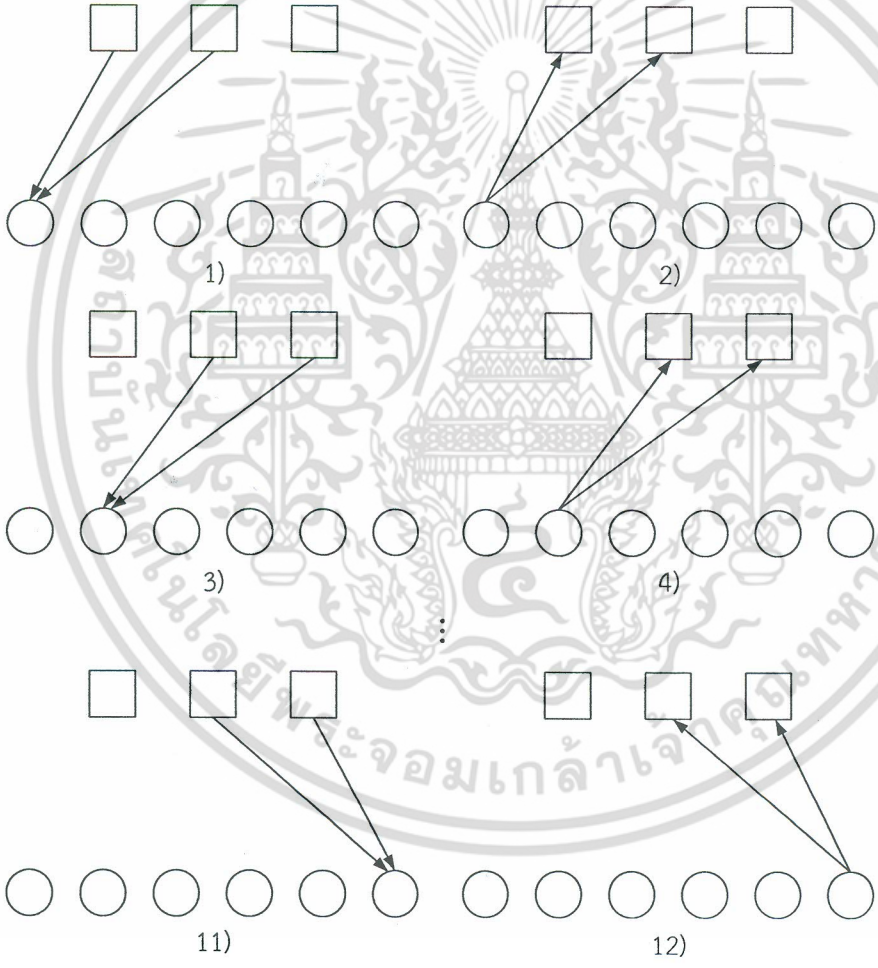
รูปที่ 4.5 ลำดับการกระจายความเชื่อมั่นแบบเลเยอร์

ทั้งนี้ อาจกล่าวได้ว่า อัลกอริทึมแอลบีพีมีความซับซ้อนเท่ากับอัลกอริทึมบีพี เนื่องจากจำนวนข่าวสารที่ถูกคำนวณในกระบวนการถอดรหัสไม่เปลี่ยนแปลง โดยในงานวิจัย [40] แสดงให้เห็นว่าวงจรการถอดรหัสแอลบีพีมีความซับซ้อนใกล้เคียงกับวงจรการถอดรหัสบีพี รูปที่ 4.7 แสดงอัตราบิตผิดพลาดของการถอดรหัสแอลบีพี โดยจะสังเกตได้ว่า การถอดรหัสแบบแอลบีพีจะมีอัตราบิตผิดพลาดที่ต่ำกว่าการถอดรหัสแบบบีพี เมื่อจำนวนการวนซ้ำเท่ากัน นอกจากนี้ การถอดรหัสแบบแอลบีพีจะลู่เข้าที่อัตราบิตผิดพลาดต่ำกว่าการถอดรหัสแบบบีพี ในงานวิจัยส่วนหนึ่งของวิทยานิพนธ์จะนำเสนอวิธีการปรับปรุงการถอดรหัสแอลบีพี ซึ่งมีอัตราบิตผิดพลาดที่ต่ำกว่าการถอดรหัสแบบแอลบีพีเมื่อพิจารณาความซับซ้อนที่เท่ากัน รายละเอียดอธิบายในบทที่ 6

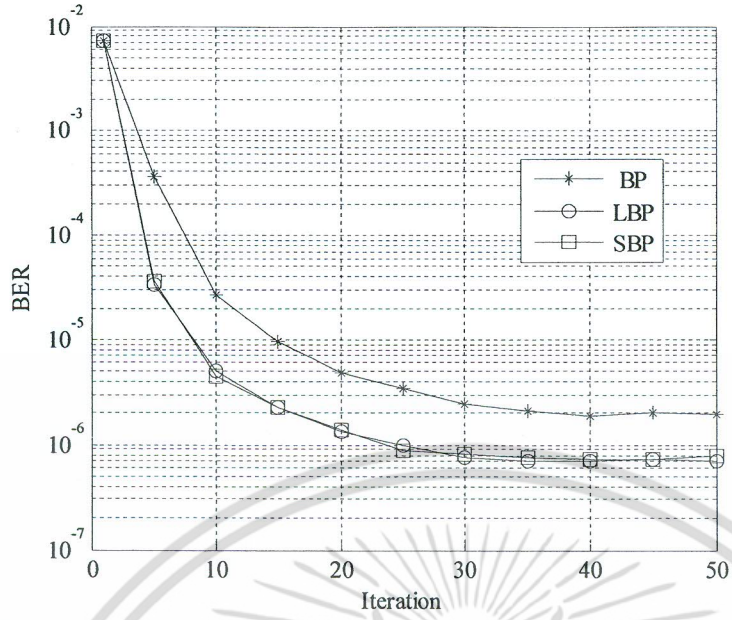
4.2.2 ลำดับแบบชัฟเฟิล

การกระจายข่าวสารเรียงลำดับแบบเลเยอร์ตามที่ได้อธิบายในหัวข้อที่ผ่านมา ข่าวสารถูกส่งแบบเรียงลำดับตามโนดตรวจสอบ จากโนดตรวจสอบลำดับที่หนึ่งไปยังโนดตรวจสอบลำดับสุดท้าย (ลำดับของโนดตรวจสอบที่กระจายข่าวสารจะไม่ส่งผลต่ออัตราบิตผิดพลาดของการถอดรหัส รายละเอียดแสดงในบทที่ 6) สำหรับการกระจายข่าวสารเรียงลำดับแบบชัฟเฟิลหรืออัลกอริทึมกระจายความเชื่อมั่นแบบชัฟเฟิลหรือเอสบีพี (shuffled belief propagation, SBP) [14] ข่าวสารจะถูกส่งแบบ

เรียงลำดับตามโนดตัวแปรดังรูปที่ 4.6 โดยจะสังเกตได้ว่า ขั้นตอนแรกของการถอดรหัสเอสบีพีจะเริ่มจากการส่งข่าวสารจากโนดตรวจสอบไปยังโนดตัวแปร (โดยทั่วไป อัลกอริทึมการถอดรหัสจะเริ่มจากการส่งข่าวสารของโนดตัวแปรไปยังโนดตรวจสอบ) ทำให้การถอดรหัสรอบแรกของอัลกอริทึมเอสบีพีจำเป็นต้องคำนวณข่าวสารจากโนดตัวแปรไปยังโนดตรวจสอบทุกโนดหรือคำนวณข่าวสารตั้งต้นก่อนทำการกระจายข่าวสารแบบเอสบีพี เนื่องจากการคำนวณข่าวสารของโนดตรวจสอบต้องใช้ข่าวสารของโนดตัวแปร รูปที่ 4.7 แสดงให้เห็นว่า อัลกอริทึมเอสบีพีมีอัตราบิตผิดพลาดเท่ากับอัลกอริทึมแอลบีพี อย่างไรก็ตาม การออกแบบวงจรของอัลกอริทึมเอสบีพีจะมีความซับซ้อนมากกว่าอัลกอริทึมแอลบีพี [41]



รูปที่ 4.6 ลำดับการกระจายความเชื่อมั่นแบบชัฟเฟิล



รูปที่ 4.7 อัตราบิตผิดพลาดของการถอดรหัสแอลดีพีซีบีพี เลเยอร์ และชัฟเฟิล

4.4 การวิเคราะห์สมรรถนะ

รหัสพาริตี้เช็คความหนาแน่นต่ำหรือรหัสแอลดีพีซี จัดเป็นรหัสแก้ไขความผิดพลาดข้อมูลที่มีสมรรถนะเข้าใกล้ลิมิตของแชนนอน (Shannon limit) [28] อย่างไรก็ตาม สมรรถนะของรหัสแอลดีพีซีขึ้นอยู่กับการออกแบบเมทริกซ์พาริตี้เช็ค ทั้งนี้ การประเมินสมรรถนะของรหัสแอลดีพีซีสามารถใช้การจำลองหาอัตราบิตผิดพลาดในระบบคอมพิวเตอร์ อย่างไรก็ตาม การประเมินด้วยวิธีดังกล่าวใช้ระยะเวลานาน ดังนั้น การประเมินสมรรถนะของรหัสแอลดีพีซีทางทฤษฎีจึงมีประโยชน์เนื่องจากใช้เวลารวดเร็วและสามารถอธิบายสมรรถนะขีดสุดของรหัสแอลดีพีซีได้ การหาสมรรถนะของรหัสแอลดีพีซีทางทฤษฎีสามารถใช้วิธีการเอ็กซิทชาร์ท (extrinsic information transfer charts, EXIT charts) [42] ซึ่งคำนวณข่าวสารร่วม (รายละเอียดข่าวสารร่วมอธิบายในหัวข้อ 2.2.1) ของข่าวสารที่ออกจากโนดตัวแปรและโนดตรวจสอบในกราฟแทนเนอร์ ผลลัพธ์ของวิธีการเอ็กซิทชาร์ทแสดงให้เห็นถึง อัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนน้อยสุด หรือค่าเทรสโฮลด์[3] (threshold) ซึ่งทำให้การถอดรหัสปราศจากบิตผิดพลาด ในหัวข้อนี้ จะอธิบายเฉพาะวิธีการหาสมรรถนะของรหัสไบนารีแอลดีพีซี สำหรับวิธีการหาค่าเทรสโฮลด์ของรหัสนอนไบนารีแอลดีพีซีจะอธิบายในบทถัดไป

[3]นอกจากนี้ การหาสมรรถนะของรหัสแอลดีพีซีทางทฤษฎีสามารถใช้วิธีการเด็นซิตี้อีโวลูชั่น (density evolution) [28] ซึ่งจะคำนวณค่าเทรสโฮลด์ของการถอดรหัสแอลดีพีซีเช่นเดียวกับวิธีการเอ็กซิทชาร์ท

พิจารณาสัญญาณที่ได้รับจากช่องสัญญาณรบกวนเกาส์สีขาวบวก $y = x + n$ เมื่อ $x \in \{-1, 1\}$ คือข้อมูลที่ถูกส่งผ่านช่องสัญญาณที่มี $P(x = \pm 1) = 1/2$ และ n คือสัญญาณรบกวนที่มีฟังก์ชันความหนาแน่นความน่าจะเป็นแบบปรกติ (normal probability density function) ซึ่งมีค่าเฉลี่ยเท่ากับศูนย์และความแปรปรวนเท่ากับ σ_n^2 ดังนั้น สามารถคำนวณอัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับจากช่องสัญญาณ ดังนี้

$$L(y) = \log \frac{p(y \mid x = +1)}{p(y \mid x = -1)} = \frac{2}{\sigma_n^2} y \tag{4.66}$$

กำหนดให้ข้อมูล $x = 1$ ถูกส่งผ่านช่องสัญญาณ ดังนั้น ค่าเฉลี่ยและความแปรปรวนของอัตราส่วนความน่าจะเป็นแบบล็อกจะมีค่าเท่ากับ

$$\mu = E\left[L(y)\right] = \frac{2}{\sigma_n^2} E(y) = \frac{2}{\sigma_n^2} \tag{4.67}$$

$$\sigma^2 = \mathrm{var}\left[L(y)\right] \frac{4}{\sigma_n^4} \mathrm{var}(y) = \frac{4}{\sigma_n^2} \tag{4.68}$$

จากสมการที่ 4.67 และ 4.68 จะได้

$$\mu = \frac{\sigma^2}{2} \tag{4.69}$$

จากสมการที่ 2.26 (บทที่ 2) ทำให้ ข่าวสารร่วมระหว่างข้อมูล X ที่ถูกส่งผ่านช่องสัญญาณ และอัตราส่วนความน่าจะเป็นแบบล็อก L ที่ได้รับจากช่องสัญญาณ คำนวณได้จาก

$$\begin{aligned} I(X;L) &= H(X) - H(X \mid L) \\ &= 1 - \iint P(x,l) \log_2 \left(\frac{1}{P(x \mid l)} \right) dx dl \\ &= 1 - \iint P(l \mid x) P(x) \log_2 \left(\frac{P(l)}{P(l \mid x) P(x)} \right) dx dl \\ &= 1 - \sum_{x=\pm 1} \frac{1}{2} \int p(l \mid x) \log_2 \left(\frac{p(l \mid x = +1) + p(l \mid x = -1)}{p(l \mid x)} \right) dl \\ &= 1 - \int p(l \mid x = +1) \log_2 \left(1 + \frac{p(l \mid x = -1)}{p(l \mid x = +1)} \right) dl \end{aligned} \tag{4.70}$$

ดังนั้น ข่าวสารร่วมของอัตราส่วนความน่าจะเป็นแบบล็อกที่มีฟังก์ชันความหนาแน่นความน่าจะเป็นแบบปรกติ และมีค่าเฉลี่ย $\mu=\sigma^2/2$ และความแปรปรวน σ^2 คำนวณได้จาก

$$I(X;Y)=J(\sigma)=1-\int\frac{1}{\sqrt{2\pi\sigma^2}}e^{\frac{-(l-\sigma^2/2)^2}{2\sigma^2}}\log_2\left(1+e^{-l}\right)dl \tag{4.71}$$

ทั้งนี้ จะสังเกตได้ว่า การคำนวณข่าวสารร่วมของอัตราส่วนความน่าจะเป็นแบบล็อกจะขึ้นอยู่กับความแปรปรวน σ^2 กำหนดให้ $J(.)$ คือฟังก์ชันการคำนวณข่าวสารร่วม เพื่อความสะดวกสามารถใช้ฟังก์ชันพหุนามแทนฟังก์ชันการคำนวณข่าวสารร่วมในสมการที่ 4.71 ดังนี้ [42]

$$J(\sigma)\approx\begin{cases}a_{J,1}\sigma^3+b_{J,1}\sigma^2+c_{J,1}\sigma, & 0\le\sigma\le1.6363\\ 1-\exp\left(a_{J,2}\sigma^3+b_{J,2}\sigma^2+c_{J,2}\sigma+d_{J,2}\right), & 1.6363<\sigma<10\\ 1, & \sigma\ge10\end{cases} \tag{4.72}$$

เมื่อ

$$a_{J,1}=-0.0421061,\ b_{J,1}=-0.209252,\ c_{J,1}=-0.00640081,$$
$$a_{J,2}=0.00181491,\ b_{J,2}=-0.142675,\ c_{J,2}=-0.0822054,d_{J,2}=0.0549608$$

กำหนดให้ $J^{-1}(.)$ คืออินเวอร์สฟังก์ชันการคำนวณข่าวสารร่วมซึ่งมีฟังก์ชันพหุนาม ดังนี้

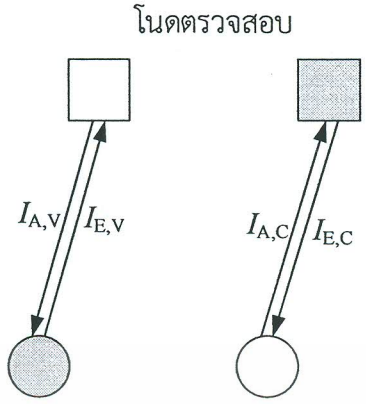
$$J^{-1}(\sigma)\approx\begin{cases}a_{J^{-1},1}I^2+b_{J^{-1},1}I+c_{J^{-1},1}\sqrt{I}, & 0\le I\le0.3646\\ -a_{J^{-1},2}\log\left(b_{J^{-1},2}(1-I)\right)+c_{J^{-1},2}I, & 0.3646<I<1\end{cases} \tag{4.73}$$

เมื่อ

$$a_{J^{-1},1}=1.09542,\quad b_{J^{-1},1}=0.214217,\ c_{J^{-1},1}=2.33727,$$
$$a_{J^{-1},2}=0.706692,\ b_{J^{-1},2}=0.386013,\ c_{J^{-1},2}=-1.75017$$

4.2.1 รหัสแอลดีพีซีแบบสม่ำเสมอและไม่สม่ำเสมอ

กำหนดให้ กราฟแทนเนอร์ของรหัสไบนารีแอลดีพีซีแบบสม่ำเสมอ มีจำนวนเส้นเชื่อมกับโนดตัวแปรเท่ากับ d_v และโนดตรวจสอบเท่ากับ d_c ทำให้อัตรารหัสมีค่าเป็น $R=1-d_v/d_c$ สมมุติให้กราฟแทนเนอร์ปราศจากวัฏจักรและความยาวคำรหัสมีค่าเป็นอนันต์ พิจารณาข่าวสารร่วมในรูปที่ 4.8 เมื่อ $I_{A,V}$ คือ ข่าวสารร่วมที่เข้าไปยังโนดตัวแปร และ $I_{E,V}$ คือ ข่าวสารร่วมที่ออกจากโนดตัวแปร และ $I_{A,C}$ คือ ข่าวสารร่วมที่เข้าไปยังโนดตรวจสอบ และ $I_{E,C}$ คือ ข่าวสารร่วมที่ออกจากโนดตรวจสอบ



รูปที่ 4.8 ข่าวสารร่วมในกราฟแทนเนอร์

จากสมการที่ 4.44 ข่าวสารในรูปอัตราส่วนความน่าจะเป็นแบบล็อกที่ออกจากโนดตัวแปรคำนวณได้จากผลรวมของข่าวสารที่ได้รับจากช่องสัญญาณและโนดตรวจสอบจำนวน $d_v - 1$ โนด ดังนั้น ข่าวสารที่ออกจากโนดตัวแปรจะมีความแปรปรวนเท่ากับ $\sigma^2 = \sigma_{CH}^2 + (d_v - 1)\sigma_A^2$ เมื่อ σ_A^2 คือ ความแปรปรวนของข่าวสารที่ได้รับจากโนดตรวจสอบ และ σ_{CH}^2 คือ ความแปรปรวนของข่าวสารที่ได้รับจากช่องสัญญาณ ดังนั้น ข่าวสารร่วมที่ส่งออกจากโนดตัวแปรคำนวณได้จาก

$$I_{E,V} = J(\sigma) = J\left(\sqrt{(d_v - 1)\sigma_A^2 + \sigma_{CH}^2}\right) \tag{4.74}$$

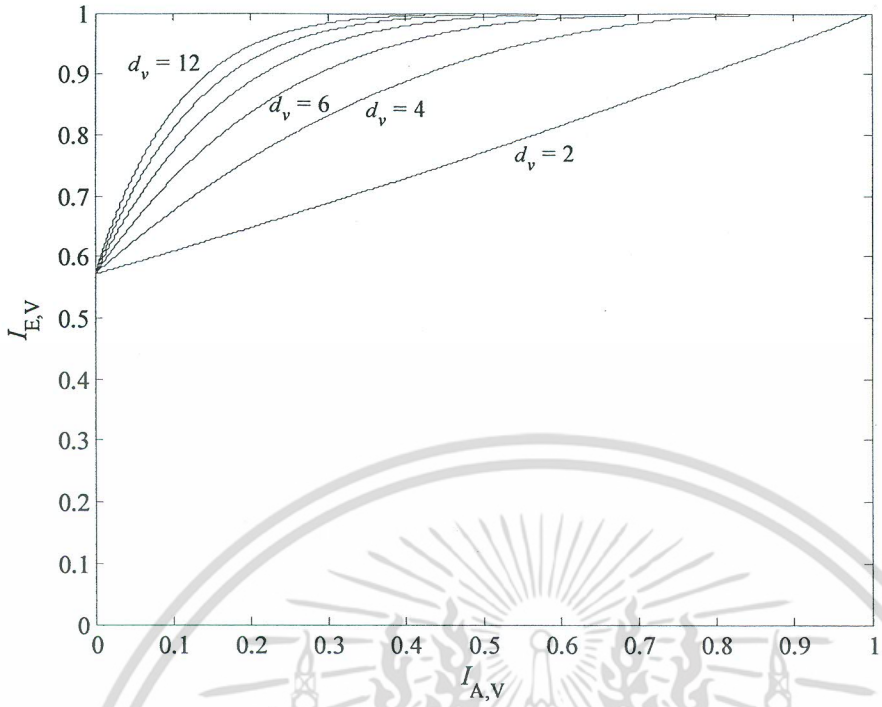
เมื่อ $J(.)$ คือฟังก์ชันข่าวสารร่วมในสมการที่ 4.72 เนื่องจาก $I_{A,V} = J(\sigma_A)$ ดังนั้น

$$I_{E,V} = J\left(\sqrt{(d_v - 1)[J^{-1}(I_{A,V})]^2 + \sigma_{CH}^2}\right) \tag{4.75}$$

เมื่อ $J^{-1}(.)$ คืออินเวอร์สฟังก์ชันข่าวสารร่วมในสมการที่ 4.73 และจากสมการที่ 4.68 และ 2.13 (บทที่ 2) ทำให้ความแปรปรวนของข่าวสารที่ได้รับจากช่องสัญญาณมีค่าเท่ากับ

$$\sigma_{CH}^2 = R\left(8 \times 10^{SNR/10}\right) \tag{4.76}$$

เมื่ออัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนหรือเอสเอ็นอาร์มีหน่วยเป็นเดซิเบล



รูปที่ 4.9 ข่าวสารร่วมที่ออกจากโนดตัวแปร

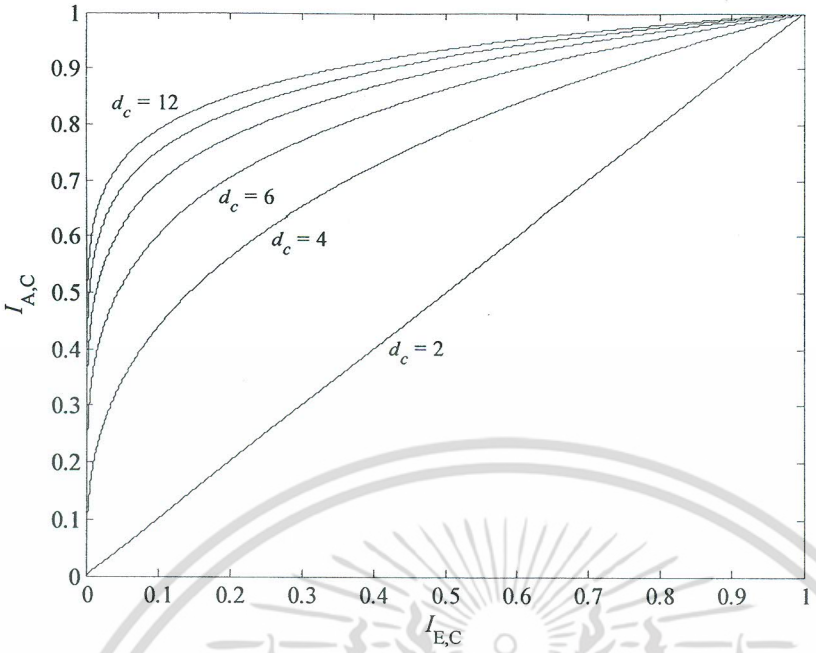
รูปที่ 4.9 แสดงข่าวสารร่วม $I_{E,V}$ ที่ออกจากโนดตัวแปร เมื่อจำนวนเส้นเชื่อมมีค่า d_v =2,4,6,8, 10,12 และค่าเอสเอ็นอาร์เท่ากับ 1.1 dB โดยจะสังเกตได้ว่า เมื่อข่าวสารร่วม $I_{A,V} = 0$ หรือปราศข่าวสารจากโนดตรวจสอบ ข่าวสารร่วม $I_{E,V}$ จะไม่เท่ากับศูนย์ เนื่องจากโนดตัวแปรยังคงได้รับข่าวสารจากช่องสัญญาณ และข่าวสารร่วม $I_{E,V}$ จะมีค่าสูงขึ้นเมื่อค่าข่าวสารร่วม $I_{A,V}$ และจำนวนเส้นเชื่อม d_v เพิ่มขึ้น

สำหรับข่าวสารร่วม $I_{E,C}$ ที่ออกจากโนดตรวจสอบดังรูปที่ 4.8 การคำนวณข่าวสารร่วม $I_{E,C}$ สามารถคำนวณได้จาก การวัดความแปรปรวนของข่าวสารที่ออกจากโนดตรวจสอบโดยวิธีการจำลอง จากนั้นคำนวณข่าวสารร่วมโดยใช้สมการที่ 4.71 อย่างไรก็ตาม ในงานวิจัย [42] ได้แสดงให้เห็นว่า ข่าวสารร่วมระหว่างรหัสพาริตี้เช็คเดี่ยว (single parity-check code, SPC code) ความยาวคำรหัส d_c บิต และอัตรารหัสเท่ากับ $(d_c - 1)/d_c$ กับรหัสทำซ้ำ (repetition code, REP code) ความยาวคำรหัส d_c บิต และอัตรารหัสเท่ากับ $1/d_c$ จะมีความสัมพันธ์ตามสมการต่อไปนี้

$$I_{E,SPC}(I_A, d_c) = 1 - I_{E,REP}(1 - I_A, d_c) \tag{4.77}$$

โนดตรวจสอบและโนดตัวแปรของรหัสแอลดีพีซี สามารถพิจารณาได้เป็นรหัสพาริตี้เช็คเดี่ยวและรหัสทำซ้ำ ตามลำดับ ดังนั้น ข่าวสารร่วมที่ออกจากโนดตรวจสอบจะมีค่าประมาณ

$$I_{E,C} \approx 1 - J\left(\sqrt{(d_c - 1)[J^{-1}(1 - I_{A,C})]^2}\right) \tag{4.78}$$



รูปที่ 4.10 ข่าวสารร่วมที่ออกจากโนดตรวจสอบ

รูปที่ 4.10 แสดงข่าวสารร่วม $I_{E,C}$ ที่ออกจากโนดตรวจสอบ (แกนนอน) เมื่อกำหนดให้ $I_{A,C}$ ที่เข้าไปยังโนดตรวจสอบ (แกนตั้ง) เมื่อจำนวนเส้นเชื่อมเท่ากับ $d_c = 2,4,6,8,10,12$ โดยจะสังเกตได้ว่าค่าข่าวสารร่วม $I_{E,C}$ จะสูงขึ้นเมื่อค่าข่าวสารร่วม $I_{A,C}$ และจำนวนเส้นเชื่อม d_c เพิ่มขึ้น

สำหรับรหัสไบนารีแอลดีพีซีแบบไม่สม่ำเสมอ สมมุติให้ความยาวคำรหัสมีค่าเป็นอนันต์และกราฟแทนเนอร์ปราศจากวัฏจักร โดยเส้นเชื่อมของโนดตัวแปรและโนดตรวจสอบสามารถแสดงอยู่ในรูปพหุนามตามสมการที่ 3.19 และ 3.20 ดังนั้น ข่าวสารร่วมของโนดตัวแปรและโนดตรวจสอบคำนวณได้จาก

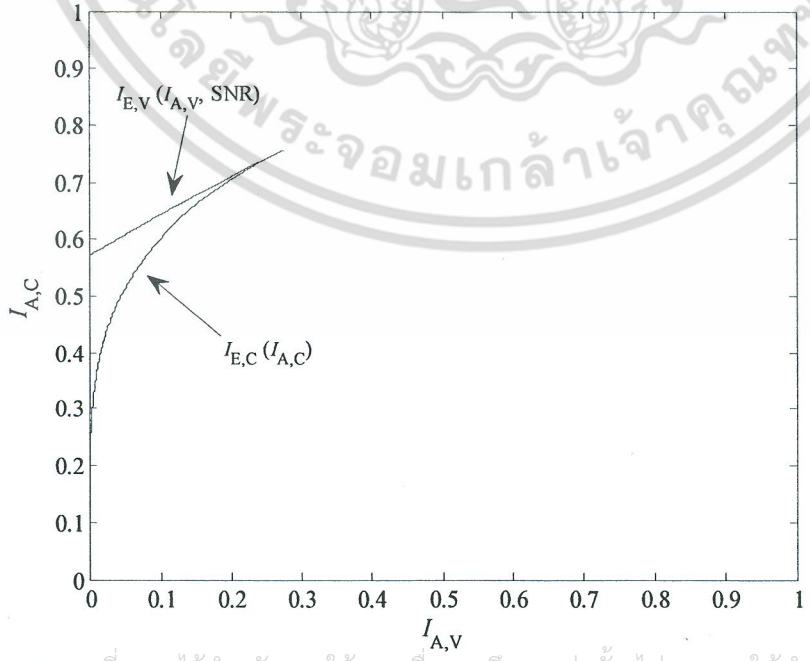
$$I_{E,V}^{\text{inr}} = \sum_{d=1}^{d_v} \lambda_d I_{E,V}(I_{A,V}, d) \tag{4.79}$$

$$I_{E,C}^{\text{inr}} = \sum_{d=1}^{d_v} \rho_d I_{E,C}(I_{A,C}, d) \tag{4.80}$$

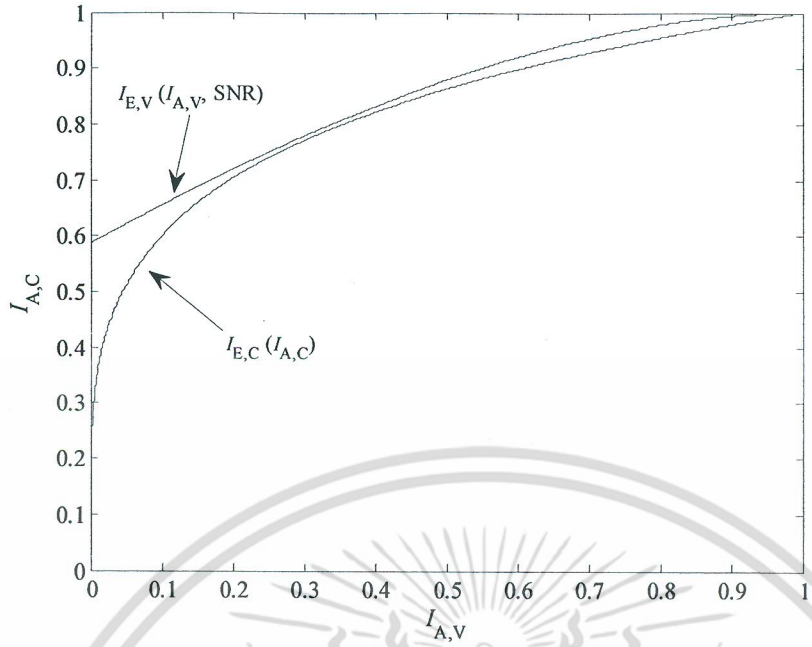
กระบวนการถอดรหัสแอลดีพีซีเป็นการแลกเปลี่ยนข่าวสารระหว่าง โนดตรวจสอบและโนดตัวแปร ดังนั้น ข่าวสารร่วม $I_{E,V}$ ที่ออกจากโนดตัวแปร จะกลายเป็นข่าวสารร่วม $I_{A,C}$ ที่เข้าไปยังโนดตรวจสอบ และข่าวสารร่วม $I_{E,C}$ ที่ออกจากโนดตรวจสอบ จะกลายเป็นข่าวสารร่วม $I_{A,V}$ ที่เข้าไปยังโนดตัวแปร ดังนั้น ข่าวสารร่วมในรูปที่ 4.9 และ 4.10 สามารถนำมาพิจารณาร่วมกัน (แสดงผลในรูปเดียวกัน) ทำให้ สามารถอธิบายการแลกเปลี่ยนข่าวสารของกระบวนการถอดรหัสแอลดีพีซี ผลลัพธ์ที่ได้จะเรียกว่า เอ็กซิทชาร์ท (extrinsic information transfer charts, EXIT charts)

กำหนดให้ รหัสไบนารีแอลดีพีซีแบบสม่ำเสมอที่มีอัตรารหัสเท่ากับ $R=1/2$ จำนวนเส้นเชื่อมของโนดตัวแปรและโนดตรวจสอบเท่ากับ $d_v=3$ และ $d_c=6$ ตามลำดับ เมื่อค่าเอสเอ็นอาร์เท่ากับ 1.1 dB เอ็กซิทชาร์ทแสดงในรูปที่ 4.11 โดยจะสังเกตได้ว่า กราฟมาบรรจบกันเมื่อค่า $I_{A,V}$ และ $I_{A,C}$ เท่ากับ 0.27 และ 0.75 บิตต่อสัญลักษณ์ ตามลำดับ ดังนั้น การถอดรหัสแอลดีพีซีจะไม่สามารถถอดรหัสได้อย่างถูกต้อง เนื่องจากต้นทางส่งข้อมูลไบนารีที่มีปริมาณข่าวสารเท่ากับ 1 บิตต่อสัญลักษณ์ เมื่อทำการเพิ่มค่าเอสเอ็นอาร์เท่ากับ 1.3 dB จะพบว่ากราฟบรรจบกันเมื่อค่า $I_{A,V}$ และ $I_{A,C}$ เท่ากับ 1 ดังรูปที่ 4.12 ในกรณีนี้ รหัสแอลดีพีซีจะทำการถอดรหัสได้อย่างถูกต้อง สำหรับค่าเอสเอ็นอาร์ต่ำสุดซึ่งทำให้กราฟของเอ็กซิตชาร์ทบรรจบกันเมื่อข่าวสารร่วม $I_{A,V}$ และ $I_{A,C}$ มีค่าเท่ากับ 1 จะเรียกว่า **เทรสโฮลด์** (threshold) ซึ่งนิยมใช้อธิบายสมรรถนะขีดสุดของรหัสแอลดีพีซี

ตารางที่ 4.5 แสดงค่าเทรสโฮลด์ของรหัสไบนารีแอลดีพีซีแบบสม่ำเสมอและไม่สม่ำเสมอ เมื่ออัตรารหัสเท่ากับ 8/9 จากตารางจะสังเกตได้ว่ารหัสแอลดีพีซีแบบสม่ำเสมอจะมีค่าเทรสโฮลด์ต่ำสุดเมื่อ $d_v=3$ ซึ่งค่าเทรสโฮลด์ของรหัสแอลดีพีซีห่างจากขีดจำกัดของแชนนอน 0.468 dB (ขีดจำกัดของแชนนอนเท่ากับ 3.034 dB รายละเอียดการคำนวณแสดงในบทที่ 2) สำหรับรหัสแอลพีซีแบบไม่สม่ำเสมอซึ่งมีพหุนามการกระจายตัวคือ $\lambda(x)=0.1570x+0.3430x^2+0.0363x^5+0.0591x^6+0.2793x^8+0.1252x^9$ และ $\rho(x)=0.1277x^{34}+0.8723x^{35}$ จะมีค่าเทรสโฮลด์ต่ำกว่ารหัสแอลดีพีซีแบบสม่ำเสมอ ทั้งนี้ ค่าเทรสโฮลด์ของรหัสแอลพีซีแบบไม่สม่ำเสมอห่างจากขีดจำกัดของแชนนอนเพียง 0.1574 dB สำหรับค่าเทรสโฮลด์ในตารางสามารถอธิบายอัตราบิตผิดพลาดช่วงวอเตอร์ฟอลล์ในรูปที่ 3.3 และ 3.4 (บทที่ 3) สำหรับอัตรารหัสเท่ากับ 1/2 ค่าเทรสโฮลด์ของรหัสไบนารีแอลดีพีซีแบบสม่ำเสมอและไม่สม่ำเสมอแสดงในตารางที่ 4.6 เมื่อพหุนามการกระจายตัวของรหัสแอลดีพีซีแบบไม่สม่ำเสมอแสดงใน [32] กรณี $d_v=50$



รูปที่ 4.11 เอ็กซิทชาร์ทของรหัสแอลดีพีซีเมื่อค่าเอสเอ็นอาร์เท่ากับ 1.1 dB



รูปที่ 4.12 เอ็กซิทชาร์ทของรหัสแอลดีพีซีเมื่อค่าเอสเอ็นอาร์เท่ากับ 1.3 dB

ตารางที่ 4.5 ค่าเทรสโฮลด์ของรหัสไบนารีแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 8/9

(d_v, d_c)	เทรสโฮลด์ (dB)	เทรสโฮลด์ - ขีดจำกัดของแชนนอน (dB)
(2 , 18)	4.723	1.689
(3 , 27)	3.502	0.468
(4 , 36)	3.517	0.483
(5 , 45)	3.653	0.619
$(\lambda_d(x), \rho_d(x))$	3.191	0.157

ตารางที่ 4.6 ค่าเทรสโฮลด์ของรหัสไบนารีแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 1/2

(d_v, d_c)	เทรสโฮลด์ (dB)	เทรสโฮลด์ - ขีดจำกัดของแชนนอน (dB)
(2 , 4)	3.037	2.849
(3 , 6)	1.102	0.914
(4 , 8)	1.534	1.346
(5 , 10)	1.996	1.808
$(\lambda_d(x), \rho_d(x))$	0.219	0.031

4.2.2 รหัสโปรโตกราฟ

การวิเคราะห์รหัสแอลดีพีซีด้วยวิธีการเอ็กซิตชาร์ทในหัวข้อที่ผ่านมา จะสังเกตได้ว่าการวิเคราะห์จะไม่คำนึงถึงวิธีการเชื่อมต่อระหว่างโนดตรวจสอบและโนดตัวแปร หรือตำแหน่งของค่าที่ไม่เป็นศูนย์ในเมทริกซ์พาริตี้เช็ค การวิเคราะห์จะพิจารณาจำนวนเส้นเชื่อมระหว่างโนดตรวจสอบและโนดตัวแปรเท่านั้น ในงานวิจัย [43] ได้นำเสนอการวิเคราะห์รหัสแอลดีพีซีแบบโปรโตกราฟ ซึ่งการวิเคราะห์จะคำนึงถึงการเชื่อมต่อของโนดตรวจสอบและโนดตัวแปรในโปรโตกราฟ (รายละเอียดโปรโตกราฟ อธิบายในหัวข้อ 3.3.5)

กำหนดให้โปรโตกราฟประกอบด้วยโนดตัวแปรจำนวน N โนด โนดตรวจสอบจำนวน M โนด และเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i กับโนดตรวจสอบลำดับที่ j มีจำนวน $b_{j,i}$ เส้น ข่าวสารร่วมจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j สามารถคำนวณได้ ดังนี้

$$I_{\mathrm{E,V}}(j,i) = J\left(\sqrt{\sum_{j'\in C_i\setminus j} b_{j',i}\left[J^{-1}(I_{\mathrm{A,V}}(j',i))\right]^2 + (b_{j,i}-1)\left[J^{-1}(I_{\mathrm{A,V}}(j,i))\right]^2 + \sigma_{\mathrm{CH}}^2}\right) \tag{4.81}$$

เมื่อ $J(.)$ และ $J^{-1}(.)$ คือฟังก์ชันข่าวสารร่วมและอินเวอร์สฟังก์ชันข่าวสารร่วมในสมการที่ 4.72 และ 4.73 ตามลำดับ และ $C_i \setminus j$ คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i ยกเว้นโนดตรวจสอบ c_j และ σ_{CH}^2 คือความแปรปรวนของข่าวสารที่ได้รับจากช่องสัญญาณในสมการที่ 4.76 กรณีรหัสแอลดีพีซีมีการทำพังก์เชอร์ (puncture) หรือบิตคำรหัสบางบิตไม่ได้ถูกส่งผ่านช่องสัญญาณ ซึ่งทำให้อัตรารหัสมีค่าเท่ากับ $R = K/(N-n)$ เมื่อ K คือ จำนวนบิตข้อมูล N คือ จำนวนบิตคำรหัส และ n คือ จำนวนบิตที่ถูกพังก์เชอร์ การถอดรหัสแอลดีพีซีที่มีการทำพังก์เชอร์ โนดตัวแปรที่ถูกพังก์เชอร์จะปราศจากข่าวสารที่ได้รับจากช่องสัญญาณ หรือความแปรปรวน σ_{CH}^2 ในสมการที่ 4.81 เท่ากับศูนย์

สำหรับข่าวสารร่วมจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i คำนวณได้จาก

$$I_{\mathrm{E,C}}(j,i) = 1 - J\left(\sqrt{\sum_{i'\in V_j\setminus i} b_{j,i'}\left[J^{-1}(1-I_{\mathrm{A,C}}(j,i'))\right]^2 + (b_{j,i}-1)\left[J^{-1}(1-I_{\mathrm{A,C}}(j,i))\right]^2}\right) \tag{4.82}$$

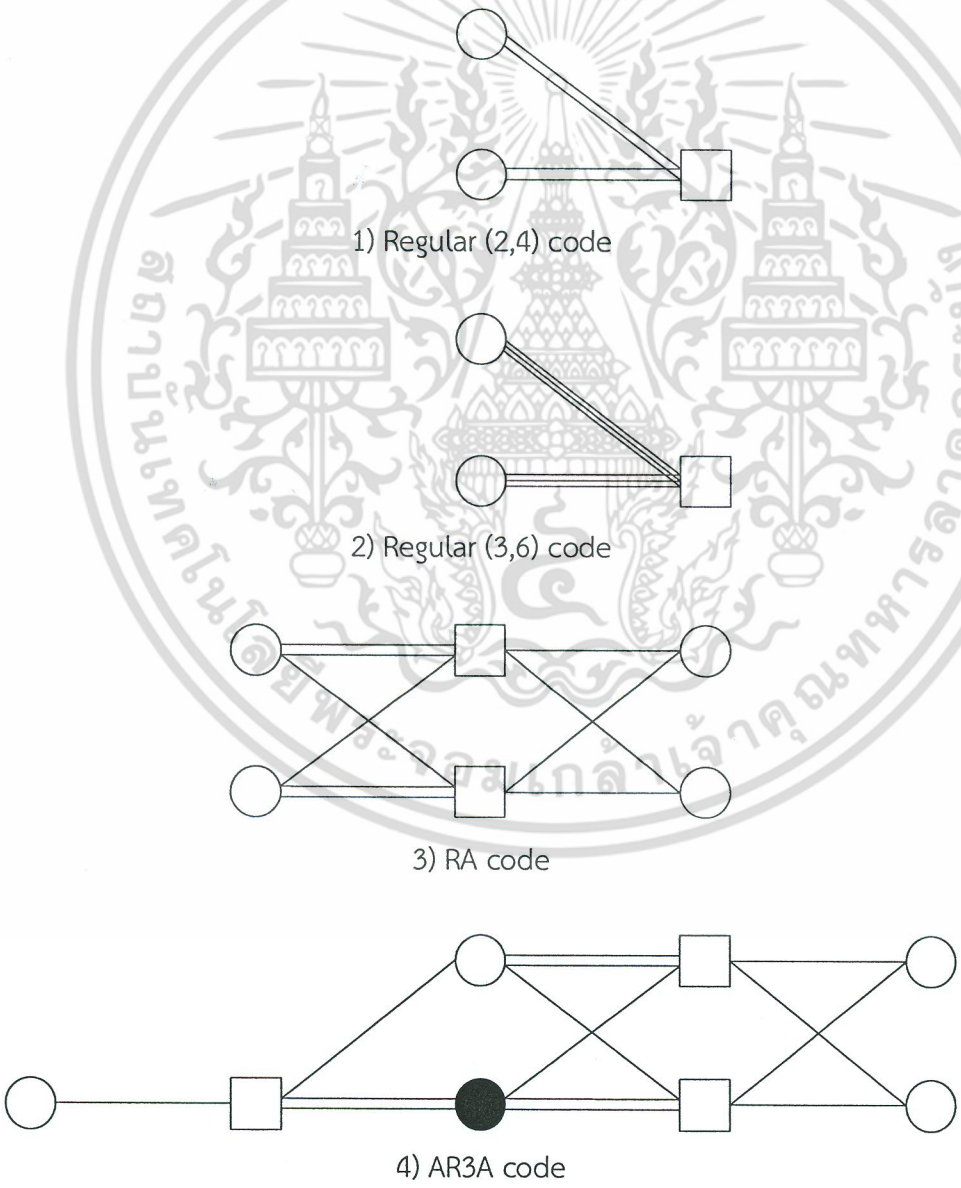
เมื่อ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบ c_j ยกเว้นโนดตัวแปร v_i

คำรหัสที่ได้รับจากการถอดรหัสจะมีข่าวสารร่วมเท่ากับ

$$I_{\mathrm{APP}}(i) = J\left(\sqrt{\sum_{j\in C_i} b_{j',i}\left[J^{-1}(I_{\mathrm{A,V}}(j',i))\right]^2 + \sigma_{\mathrm{CH}}^2}\right) \tag{4.83}$$

เมื่อ C_i คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปร v_i

การวิเคราะห์สมรรถนะของรหัสโปรโตกราฟ จะเริ่มจากกำหนดค่าเอสเอ็นอาร์ของช่องสัญญาณรบกวนเกาส์สีขาวบวก จากนั้นคำนวณข่าวสารร่วมของรหัสแอลดีพีซีโดยใช้สมการที่ 4.81 ถึง 4.83 จนกระทั่ง ข่าวสารร่วมมีค่าคงที่ โดยเทรสโฮลด์ของรหัสโปรโตกราฟจะมีค่าเท่ากับเอสเอ็นอาร์ต่ำสุดที่ทำให้ข่าวสารร่วม $I_{\mathrm{APP}}(i)$ มีค่าเท่ากับ 1 เมื่อ i มีค่าใดๆ รูปที่ 4.13 แสดงรหัสโปรโตกราฟอัตรารหัสเท่ากับ 1/2 ได้แก่ รหัสสม่ำเสมอซึ่งมี $d_v = 3$ และ $d_v = 4$ รหัสอาร์เอ (repeat-accumulate code, RA code) และรหัสเออาร์สามเอ (accumulate repeat-accumulate code, AR3A code) [44] โดยกำหนดให้ สัญลักษณ์สี่เหลี่ยมแทนโนดตรวจสอบ สัญลักษณ์วงกลมสีขาวแทนโนดตัวแปร และวงกลมสีดำแทนโนดตัวแปรที่ถูกพังก์เชอร์



รูปที่ 4.13 ตัวอย่างรหัสโปรโตกราฟ

รหัสโปรโตกราฟในรูปสามารถเขียนเมทริกซ์ฐานได้ ดังนี้

$$\mathbf{B}_{\text{Regular}(2,4)} = [2 \quad 2] \tag{4.84}$$

$$\mathbf{B}_{\text{Regular}(3,6)} = [3 \quad 3] \tag{4.85}$$

$$\mathbf{B}_{\text{RA}} = \begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \end{bmatrix} \tag{4.86}$$

$$\mathbf{B}_{\text{AR3A}} = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 1 & 2 & 1 \end{bmatrix} \tag{4.87}$$

เมื่อเมทริกซ์ฐานของรหัสเออาร์สามเอถูกทำพังก์เชอร์ในหลักที่ 4 (สามารถพิจารณารหัสอาร์เอและรหัสเออาร์สามเอ คือ รหัสไม่สม่ำเสมอชนิดหนึ่ง เนื่องจากเส้นเชื่อมของโนดตรวจสอบและโนดตัวแปรมีจำนวนไม่สม่ำเสมอ) ตารางที่ 4.7 แสดงค่าเทรสโฮลด์ของรหัสโปรโตกราฟ โดยจะสังเกตได้ว่ารหัสโปรโตกราฟแบบสม่ำเสมอ (2,4) และ (3,6) มีค่าเทรสโฮลด์สอดคล้องกับค่าเทรสโฮลด์ของรหัสแอลดีพีซีแบบสม่ำเสมอในตารางที่ 4.6 และรหัสเออาร์สามเอให้ค่าเทรสโฮลด์ต่ำกว่ารหัสสม่ำเสมอ สำหรับการวิเคราะห์ค่าเทรสโฮลด์ของรหัสนอนไบนารีโปรโตกราฟจะอธิบายในบทถัดไป

ตารางที่ 4.7 ค่าเทรสโฮลด์ของรหัสไบนารีโปรโตกราฟเมื่ออัตรารหัสเท่ากับ 1/2

รหัส	เทรสโฮลด์ (dB)	เทรสโฮลด์ - ขีดจำกัดของแชนนอน (dB)
Regular (2,4)	3.037	2.849
Regular (3,6)	1.102	0.914
RA	1.146	0.958
AR3A	0.474	0.286

บทที่ 5
การปรับปรุงสมรรถนะของการออกแบบรหัสแอลดีพีซี

ในบทนี้ จะอธิบายงานวิจัยของวิทยานิพนธ์ที่เกี่ยวข้องกับการออกแบบรหัสแอลดีพีซี ตามที่ได้กล่าวในบทก่อนหน้า การออกแบบรหัสแอลดีพีซีเป็นการออกแบบกราฟแทนเนอร์หรือเมทริกซ์พาริตี้เช็ค ดังนั้น หัวข้อแรกจะนำเสนอการออกแบบกราฟแทนเนอร์ที่มีวัฏจักรสูง รหัสแอลดีพีซีที่ได้จะมีลักษณะควอไซไซคลิก (quasi-cyclic) ทำให้ การเข้ารหัสมีความซับซ้อนต่ำและเหมาะสำหรับการประยุกต์ใช้งาน หัวข้อถัดไป นำเสนอการออกแบบรหัสแอลดีพีซีสำหรับวงจรเทอร์โบอีควอไลเซชั่น (turbo equalization) ซึ่งได้รับความนิยมในการประยุกต์ใช้งานกับระบบบันทึกข้อมูลเชิงแม่เหล็ก และหัวข้อสุดท้าย นำเสนอการวิเคราะห์สมรรถนะทางทฤษฎีรหัสโปรโตกราฟแอลดีพีซีบนฟีลด์จำกัด GF(q) สำหรับช่องสัญญาณผลตอบสนองบางส่วน วิธีการที่ได้นำเสนอนี้ สามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีในช่องสัญญาณผลตอบสนองบางส่วนที่มีสมรรถนะเข้าใกล้ขีดจำกัดของแชนนอน (Shannon limit)

5.1 รหัสควอไซไซคลิกวัฏจักรสูง

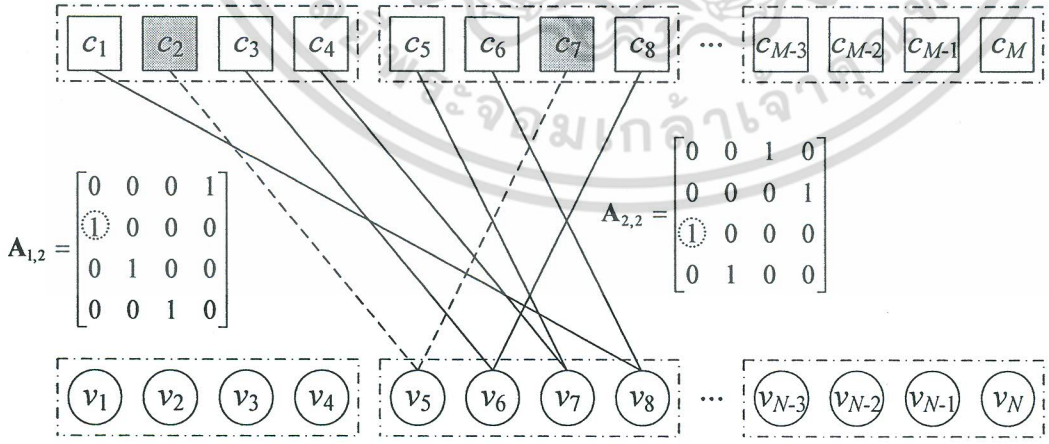
การออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก (quasi-cyclic low-density parity-check codes, QC-LDPC codes) ในหัวข้อที่ 3.1.3 (บทที่ 3) จะทำให้กระบวนการเข้ารหัสมีความซับซ้อนต่ำและเหมาะสมกับการประยุกต์ใช้งาน อย่างไรก็ตาม การออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกให้มีขนาดความยาวคำรหัสและอัตรารหัสตามที่ต้องการมีความยุ่งยาก เนื่องจากการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกจะขึ้นอยู่กับขนาดของไฟไนต์จีโอเมทรี (finite geometry) [29] ดังนั้นในงานวิจัย [4] จึงนำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก โดยการประยุกต์ใช้อัลกอริทึมพีอีจี (progressive edge-growth algorithm, PEG algorithm) (รายละเอียดอัลกอริทึมพีอีจีอธิบายในหัวข้อที่ 3.3.2) ทำให้ การออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกมีความยืดหยุ่นสามารถสร้างรหัสที่มีความยาวคำรหัสและอัตรารหัสตามที่ต้องการ อย่างไรก็ตาม การออกแบบรหัสแอลดีพีซีด้วยอัลกอริทึมพีอีจีจะเกิดปัญหาที่เรียกว่า สถานการณ์ตัวเลือกมาก (multiple choice situation) (อธิบายในลำดับถัดไป) ซึ่งทำให้รหัสแอลดีพีซีที่ได้รับการออกแบบมีวัฏจักรขนาดไม่สูงสุด นอกจากนี้ ในการออกแบบรหัสแอลดีพีซีแต่ละครั้ง วัฏจักรที่ได้จะมีขนาดไม่เท่ากัน ทำให้งานวิจัยส่วนแรกของวิทยานิพนธ์ จะนำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกซึ่งมีวัฏจักรขนาดสูงสุด โดยประยุกต์ใช้อัลกอริทึมพีอีจีที่มีการดัดแปลงเพื่อแก้ปัญหาการเกิดสถานการณ์ตัวเลือกมาก

5.1.1 อัลกอริทึมพีอีจีแบบควอไซไซคลิก

กำหนดให้ รหัสแอลดีพีซีมีเมทริกซ์พาริตี้เช็ค $\mathbf{H}$ ขนาด $M \times N$ ทำให้ ความยาวคำรหัสเท่ากับ N บิต และความยาวบิตพาริตี้เท่ากับ M บิต ทั้งนี้ สามารถแสดงเมทริกซ์พาริตี้เช็คของรหัสแอลดีพีซีด้วยกราฟแทนเนอร์ ซึ่งประกอบไปด้วยโนดตรวจสอบจำนวน M โนด และโนดตัวแปรจำนวน N โนด โดยเส้นเชื่อมระหว่างโนดตรวจสอบและโนดตัวแปรแสดงความสัมพันธ์ของบิตคำรหัสที่ได้จากการเข้ารหัสแอลดีพีซี สำหรับรหัสแอลดีพีซีแบบควอไซไซคลิก จะมีเมทริกซ์พาริตี้เช็คลักษณะดังต่อไปนี้

$$\mathbf{H}_{\mathrm{QC}} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{c,1} & \mathbf{A}_{c,2} & \cdots & \mathbf{A}_{c,t} \end{bmatrix} \tag{5.1}$$

เมื่อ $\mathbf{A}_{i,j}$ คือเมทริกซ์เซอร์คิวแลนท์ (circulant matrix) ขนาด $b \times b$ ซึ่งแต่ละแถวของเมทริกซ์เซอร์คิวแลนท์เกิดจากการเลื่อนแถวที่อยู่ด้านบนแบบวนกลับจำนวนหนึ่งครั้ง หรือการเลื่อนหลักที่อยู่ด้ายซ้ายแบบวนกลับจำนวนหนึ่งครั้ง (ตัวอย่างของเมทริกซ์เซอร์คิวแลนท์แสดงในหัวข้อที่ 3.1.3) ทำให้กราฟแทนเนอร์ของรหัสแอลดีพีซีแบบควอไซไซคลิกมีลักษณะดังรูปที่ 5.1 พิจารณาหลักที่ 1 ของเมทริกซ์เซอร์คิวแลนท์ขนาด 4×4 จะสังเกตได้ว่าหลักที่ 2 เกิดจากการเลื่อนหลักที่อยู่ด้านซ้ายหรือหลักที่ 1 แบบวนกลับจำนวนหนึ่งครั้ง จากนั้น ทำการเลื่อนหลักถัดไปจนกระทั่งถึงหลักที่ 4 โนดตรวจสอบและโนดตัวแปรของกราฟแทนเนอร์แบบควอไซไซคลิก สามารถแบ่งออกได้เป็นกลุ่ม แต่ละกลุ่มประกอบไปด้วยโนดจำนวน 4 โนด และเส้นเชื่อมระหว่างกลุ่มโนดมีลักษณะแบบวนกลับ



รูปที่ 5.1 กราฟแทนเนอร์ของรหัสแอลดีพีซีแบบควอไซไซคลิก

ในงานวิจัย [4] นำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกด้วยอัลกอริทึมพีอีจี ในที่นี้ จะเรียกว่า อัลกอริทึมพีอีจีคิวซี (PEG-QC algorithm) โดยการออกแบบจะเริ่มต้นจากการแบ่งโนดตรวจสอบและโนดตัวแปรออกเป็นกลุ่ม โดยแต่ละกลุ่มจะประกอบไปด้วยโนดจำนวน b โนด ซึ่งเท่ากับขนาดของเมทริกซ์เซอร์คิวแลนท์ในสมการที่ 5.1 โนดตัวแปรลำดับต่ำสุดของกลุ่ม หรือโนดตัวแปร v_5 ในรูปที่ 5.1 จะสร้างเส้นเชื่อมไปยังโนดตรวจสอบโดยใช้อัลกอริทึมพีอีจี กล่าวคือ สร้างแผนภาพต้นไม้จากโนดตัวแปร v_5 ไปยังโนดตรวจสอบใดๆ ที่อยู่นอกกลุ่ม จากนั้นทำการเลือกโนดตรวจสอบที่ไม่ได้อยู่ในแผนภาพต้นไม้ หรือทำการเลือกโนดตรวจสอบที่อยู่ความลึกลำดับที่ l (รายละเอียดแผนภาพต้นไม้อธิบายในหัวข้อที่ 3.3.2) สำหรับโนดตัวแปรอื่นภายในกลุ่ม หรือโนดตัวแปร v_6, v_7, v_8 ในรูปที่ 5.1 จะสร้างเส้นเชื่อมไปยังโนดตรวจสอบด้วยวิธีการหมุนวน (cyclic) เมทริกซ์เซอร์คิวแลนท์ในสมการที่ 5.1 ซึ่งทำให้กราฟแทนเนอร์มีลักษณะแบบวนกลับขั้นตอนการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกด้วยอัลกอริทึมพีอีจีแสดงในตารางที่ 5.1

ตารางที่ 5.1 อัลกอริทึมพีอีจีคิวซี (PEG-QC algorithm)

---

for $i = 1$ **to** t
  for $k = 1$ **to** d_v
    if $k = 1$
      สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i-1)b+1}$ ไปยังโนดตรวจสอบที่มีเส้นเชื่อมน้อยสุด
    else
      สร้างแผนภาพต้นไม้จากโนดตัวแปร $v_{(i-1)b+1}$ ไปยังโนดตรวจสอบ
      กรณีที่ 1 สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
      สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i-1)b+1}$ ไปยังโนดตรวจสอบที่อยู่ในความลึก
      ลำดับที่ l ซึ่งจะทำให้โนดตัวแปร $v_{(i-1)b+1}$ เกิดวัฏจักรขนาด $2(l+1)$
      กรณีที่ 2 ไม่สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
      สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i-1)b+1}$ ไปยังโนดตรวจสอบที่ไม่ได้อยู่ใน
      แผนภาพต้นไม้ ซึ่งจะทำให้โนดตัวแปร $v_{(i-1)b+1}$ ปราศจากวัฏจักร
    end
  end
  for $m = 2$ **to** b
    สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i-1)b+m}$ ไปยังโนดตรวจสอบ $c_{\mathrm{mod}(j+1,b)}$
    เมื่อ j คือ ลำดับของโนดตรวจสอบที่เชื่อมไปยังโนดตัวแปรลำดับที่ $(i-1)b+m$
  end
end

5.1.2 อัลกอริทึมพีอีจีแบบควอไซไซคลิกวัฏจักรสูงสุด

พิจารณาอัลกอริทึมพีอีจีในตารางที่ 3.2 เมื่อ $k>1$ หรือการสร้างเส้นเชื่อมลำดับที่ $2,3,\ldots,d_v$ ของโนดตัวแปร อัลกอริทึมพีอีจีจะทำการสร้างแผนภาพต้นไม้จากโนดตัวแปร v_i ไปยังโนดตรวจสอบต่างๆ ในกราฟแทนเนอร์ ซึ่งจะเกิดเหตุการณ์ 2 แบบ ได้แก่ กรณีที่ 1 สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด และกรณีที่ 2 ไม่สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด สำหรับกรณีที่ 2 นั้นการสร้างเส้นเชื่อมจากโนดตัวแปร v_i ไปยังโนดตรวจสอบที่ไม่ได้อยู่ในแผนภาพต้นไม้ จะทำให้โนดตัวแปร v_i ปราศจากวัฏจักร ต่างจากกรณีที่ 1 ซึ่งการสร้างเส้นเชื่อมจากโนดตัวแปร v_i ไปยังโนดตรวจสอบที่อยู่ในระดับความลึกที่ l จะทำให้โนดตัวแปร v_i เกิดวัฏจักรขนาด $2(l+1)$ อย่างไรก็ตาม การสร้างแผนภาพต้นไม้ของโนดตัวแปรใดๆ ณ ระดับความลึกที่ l มักจะมีโนดตรวจสอบมากกว่า 1 โนด ซึ่งอัลกอริทึมพีอีจีจะใช้การสุ่มเลือกโนดตรวจสอบในระดับความลึกที่ l ทำให้ การสร้างกราฟแทนเนอร์ด้วยอัลกอริทึมพีอีจีในแต่ละครั้ง กราฟแทนเนอร์ที่ได้จะมีวัฏจักรขนาดแตกต่างกัน นอกจากนี้ กราฟแทนเนอร์จะมีวัฏจักรขนาดไม่สูงสุด เนื่องจาก การสุ่มเลือกโนดตรวจสอบในระดับความลึกที่ l อาจไม่ใช่ตัวเลือกที่ดีสุด ในที่นี้ จะเรียกเหตุการณ์นี้ว่า สถานการณ์ตัวเลือกมาก (multiple choice situation)

การประยุกต์ใช้อัลกอริทึมพีอีจีในการสร้างรหัสแอลดีพีซีแบบควอไซไซคลิก ตามที่ได้อธิบายในหัวข้อก่อนหน้า สถานการณ์ตัวเลือกมาก ยังคงเกิดขึ้นในขั้นตอนการสร้างแผนภาพต้นไม้ นอกจากนี้ยังส่งผลกระทบต่อการสร้างกราฟแทนเนอร์ให้มีวัฏจักรสูง เนื่องจากโนดตรวจสอบและโนดตัวแปรถูกแบ่งออกเป็นกลุ่ม ทำให้จำนวนครั้งในการสร้างแผนภาพต้นไม้ลดลง ดังนั้น การสุ่มเลือกโนดตรวจสอบในสถานการณ์ตัวเลือกมาก ควรได้รับการพิจารณาอย่างถี่ถ้วน ในงานวิจัยนี้ จึงนำเสนอการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกที่มีวัฏจักรขนาดสูงสุด โดยเรียกว่า อัลกอริทึมพีอีจีคิวซีแม็ก (PEG-QC-MAX algorithm) โดยการใช้อัลกอริทึมพีอีจีที่มีการแก้ปัญหาสถานการณ์ตัวเลือกมาก

อัลกอริทึมพีอีจีคิวซีแม็กจะเริ่มจากการแบ่งโนดตรวจสอบและโนดตัวแปรออกเป็นกลุ่ม โดยแต่ละกลุ่มจะประกอบไปด้วยโนดจำนวน b โนด โนดตัวแปรลำดับต่ำสุดของกลุ่ม หรือโนดตัวแปรลำดับที่ $(i-1)b+1$ เมื่อ i คือจำนวนเต็มบวกที่มากกว่าศูนย์ จะสร้างเส้นเชื่อมไปยังโนดตรวจสอบโดยใช้อัลกอริทึมพีอีจี สำหรับโนดตัวแปรอื่นภายในกลุ่มจะสร้างเส้นเชื่อมไปยังโนดตรวจสอบด้วยวิธีการหมุนวน อย่างไรก็ตาม เมื่อทำการสร้างเส้นเชื่อมให้กับกลุ่มโนดตัวแปรจำนวน 1 กลุ่มเสร็จสิ้น ให้คำนวณขนาดของวัฏจักรที่เกิดขึ้นและจัดเก็บรูปแบบการเชื่อมต่อของโนด จากนั้น ทำลายเส้นเชื่อมของกลุ่มโนดตัวแปรปัจจุบันหรือโนดตัวแปรลำดับที่ $ib+1$ ถึง $ib+b$ และทำลายเส้นเชื่อมของกลุ่มโนดตัวแปรก่อนหน้าหรือโนดตัวแปรลำดับที่ $(i-1)b+1$ ถึง $(i-1)b+b$ เมื่อทำลายเส้นเชื่อมของกลุ่มโนดเสร็จสิ้น ให้เริ่มต้นการสร้างเส้นเชื่อมใหม่อีกครั้ง ดังนั้น สถานการณ์ตัวเลือกมากที่เกิดขึ้นในอัลกอริทึมพีอีจีจะได้รับการแก้ไขโดยการทำซ้ำ เพื่อหารูปแบบการเชื่อมต่อของโนดตัวแปรที่ก่อให้เกิดวัฏจักรขนาดสูงสุด อัลกอริทึมพีอีจีคิวซีแม็กที่นำเสนอนี้จัดเป็นอัลกอริทึมกรีดดี้ (greedy

algorithm) ประเภทหนึ่ง ซึ่งงานวิจัยจะจำกัดขอบเขตด้วยจำนวนการทำซ้ำสูงสุดเท่ากับ l_{MAX} ครั้ง และการทำลายเส้นเชื่อมของกลุ่มโนดตัวแปรก่อนหน้าจะพิจารณาเฉพาะหนึ่งช่วงเวลาเท่านั้น หรือเฉพาะโนดตัวแปรลำดับที่ $(i-1)b+1$ ถึง $(i-1)b+b$ เท่านั้น รายละเอียดอัลกอริทึมพีอีจีคิวซีแม็กแสดงในตารางที่ 5.2

ตารางที่ 5.2 อัลกอริทึมพีอีจีคิวซีแม็ก (PEG-QC-MAX algorithm)

---

for $i=1$ **to** $t-1$
  for $l=1$ **to** l_{MAX}
    ทำลายเส้นเชื่อมของโนดตัวแปร $v_{(i-1)b+1}$ ถึง v_{ib+b}
    for $a=0$ **to** 1
      for $k=1$ **to** d_v
        if $k=1$
          สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i+a-1)b+1}$ ไปยังโนดตรวจสอบที่มีเส้นเชื่อมน้อยสุด
        else
          สร้างแผนภาพต้นไม้จากโนดตัวแปร $v_{(i+a-1)b+1}$ ไปยังโนดตรวจสอบ
          <u>กรณีที่ 1</u> สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
          สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i+a-1)b+1}$ ไปยังโนดตรวจสอบที่อยู่ในความลึกลำดับที่ l ซึ่งจะทำให้โนดตัวแปร $v_{(i+a-1)b+1}$ เกิดวัฏจักรขนาด $2(l+1)$
          <u>กรณีที่ 2</u> ไม่สามารถสร้างแผนภาพต้นไม้ไปยังโนดตรวจสอบครบทุกโนด
          สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i+a-1)b+1}$ ไปยังโนดตรวจสอบที่ไม่ได้อยู่ในแผนภาพต้นไม้ ซึ่งจะทำให้โนดตัวแปร $v_{(i+a-1)b+1}$ ปราศจากวัฏจักร
        end
      end
      for $m=2$ **to** b
        สร้างเส้นเชื่อมจากโนดตัวแปร $v_{(i+a-1)b+m}$ ไปยังโนดตรวจสอบ $c_{\mathrm{mod}(j+1,b)}$ เมื่อ j คือลำดับของโนดตรวจสอบที่เชื่อมไปยังโนดตัวแปรลำดับที่ $(i+a-1)b+m$
      end
    end
    คำนวณขนาดวัฏจักรของโนดตัวแปร $v_{(i-1)b+1}$ ถึง v_{ib+b} จากนั้นจัดเก็บรูปแบบการเชื่อมต่อระหว่างโนดตรวจสอบกับโนดตัวแปร $v_{(i-1)b+1}$ ถึง v_{ib+b}
  end
  เลือกรูปแบบการเชื่อมต่อระหว่างโนดตรวจสอบกับโนดตัวแปร $v_{(i-1)b+1}$ ถึง v_{ib+b} ซึ่งทำให้วัฏจักรมีความยาวสูงสุด
end

ตารางที่ 5.3 แสดงวัฏจักรของรหัสแอลดีพีซีเมื่อจำนวนเส้นเชื่อมของโนดตัวแปรเท่ากับ 3 และความยาวคำรหัสเท่ากับ 1944 บิต ตามมาตรฐานการสื่อสารไร้สาย IEEE 802.11n [45] โดยสังเกตได้ว่า เมื่ออัตรารหัสสูงขึ้นจะทำให้ขนาดของวัฏจักรเล็กลง เนื่องจากเมทริกซ์พาริตี้เช็คหรือกราฟแทนเนอร์มีขนาดเล็กลงแต่จำนวนเส้นเชื่อมยังคงเท่าเดิม ทำให้วัฏจักรมีขนาดเล็กลงตามลำดับ การออกแบบรหัสแอลดีพีซีด้วยอัลกอริทึมพีอีจี (PEG algorithm) จะทำให้กราฟแทนเนอร์มีวัฏจักรขนาดสูงกว่าการออกแบบกราฟแทนเนอร์ด้วยอัลกอริทึมอื่น อย่างไรก็ตาม รหัสแอลดีพีซีที่ได้จะมีลักษณะเชิงสุ่มซึ่งไม่เหมาะต่อการประยุกต์ใช้งาน สำหรับการออกแบบรหัสแอลดีพีซีควอไซไซคลิกด้วยอัลกอริทึมพีอีจีหรืออัลกอริทึมพีอีจีคิวซี (PEG-QC algorithm) จะก่อให้เกิดวัฏจักรขนาด 6 เนื่องจากปัญหาสถานการณ์ตัวเลือกมากที่เกิดขึ้น สำหรับอัลกอริทึมพีอีจีคิวซีแม็ก (PEG-QC-MAX algorithm) ที่นำเสนอในงานวิจัยนี้ ขนาดวัฏจักรจะสูงกว่าอัลกอริทึมพีอีจีคิวซีและอัลกอริทึมในงานวิจัย [46] ซึ่งใช้ออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก นอกจากนี้ ขนาดวัฏจักรจะมีค่าใกล้เคียงกับอัลกอริทึมพีอีจียกเว้นอัตรารหัส 5/6 ซึ่งอัลกอริทึมพีอีจีคิวซีแม็กมีขนาดวัฏจักรสูงกว่าอัลกอริทึมพีอีจี

ตารางที่ 5.3 วัฏจักรของรหัสแอลดีพีซีเมื่อความยาวคำรหัสเท่ากับ 1944 บิต

อัตรารหัส	วิธีการออกแบบ	จำนวนของวัฏจักร (%)			
		4	6	8	10
1/2	PEG	0	0	0.07	99.93
	PEG-QC	0	2.12	45.55	52.33
	PEG-QC-MAX	0	0	0.06	99.94
	Other codes [46]	0	0	100	0
2/3	PEG	0	0	99.99	0.01
	PEG-QC	0	8.39	91.61	0
	PEG-QC-MAX	0	0	100	0
	Other codes [46]	0	87.50	12.50	0
3/4	PEG	0	0	100	0
	PEG-QC	0	22.70	77.30	0
	PEG-QC-MAX	0	0	100	0
	Other codes [46]	0	90.91	9.09	0
5/6	PEG	0	96.45	3.55	0
	PEG-QC	0	96.26	3.74	0
	PEG-QC-MAX	0	89.50	10.50	0
	Other codes [46]	0	94.12	5.88	0

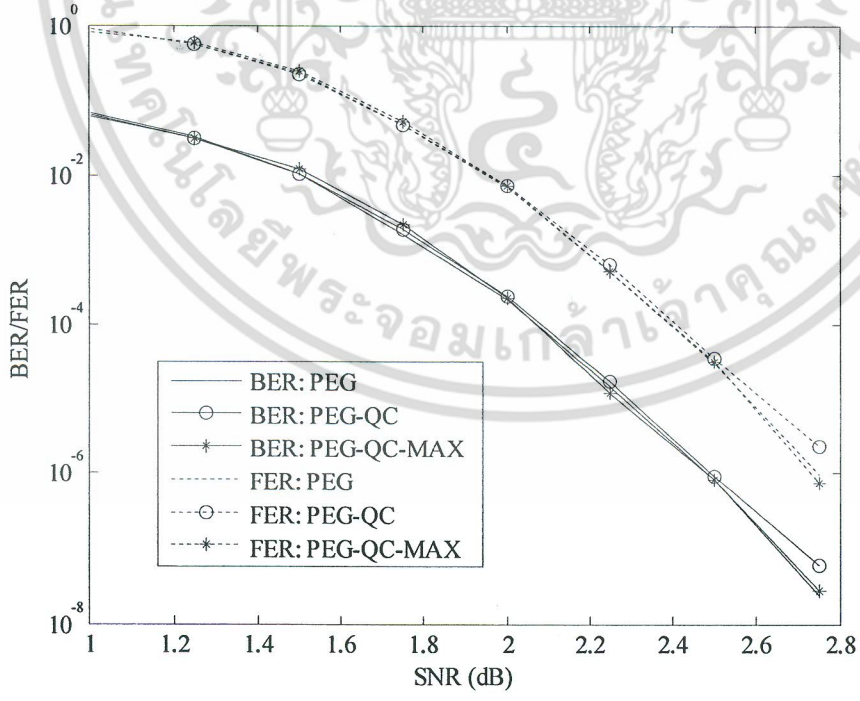
ตารางที่ 5.4 แสดงวัฏจักรของรหัสแอลดีพีซีเมื่อจำนวนเส้นเชื่อมของโนดตัวแปรเท่ากับ 3 และความยาวคำรหัสเท่ากับ 4608 บิต ใกล้เคียงกับเซ็กเตอร์ข้อมูลของอุปกรณ์ฮาร์ดดิสก์ โดยจะสังเกตได้ว่า เมื่อความยาวคำรหัสเพิ่มขึ้นจะทำให้ขนาดวัฏจักรของรหัสแอลดีพีซีเพิ่มขึ้น ทั้งนี้ สามารถอธิบายได้จากขนาดของเมทริกซ์พาริตี้เช็คหรือกราฟแทนเนอร์ที่ใหญ่ขึ้น แต่จำนวนเส้นเชื่อมยังคงเท่าเดิม ส่งผลให้ขนาดของวัฏจักรใหญ่ขึ้นตามลำดับ จากตารางจะเห็นว่า การออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิกโดยใช้อัลกอริทึมพีอีจีคิวซี (PEG-QC algorithm) ยังคงให้วัฏจักรขนาดเล็กกว่าอัลกอริทึมพีอีจี (PEG algorithm) สำหรับอัลกอริทึมพีอีจีคิวซีแม็ก (PEG-QC-MAX) ที่นำเสนอในงานวิจัยนี้ วัฏจักรจะมีขนาดใหญ่กว่าอัลกอริทึมอื่นทุกอัตรารหัส เนื่องจากการออกแบบรหัสแอลดีพีซีด้วยอัลกอริทึมพีอีจีและอัลกอริทึมพีอีจีคิวซียังคงเกิดปัญหาสถานการณ์ตัวเลือกมาก

ตารางที่ 5.4 วัฏจักรของรหัสแอลดีพีซีเมื่อความยาวคำรหัสเท่ากับ 4608 บิต

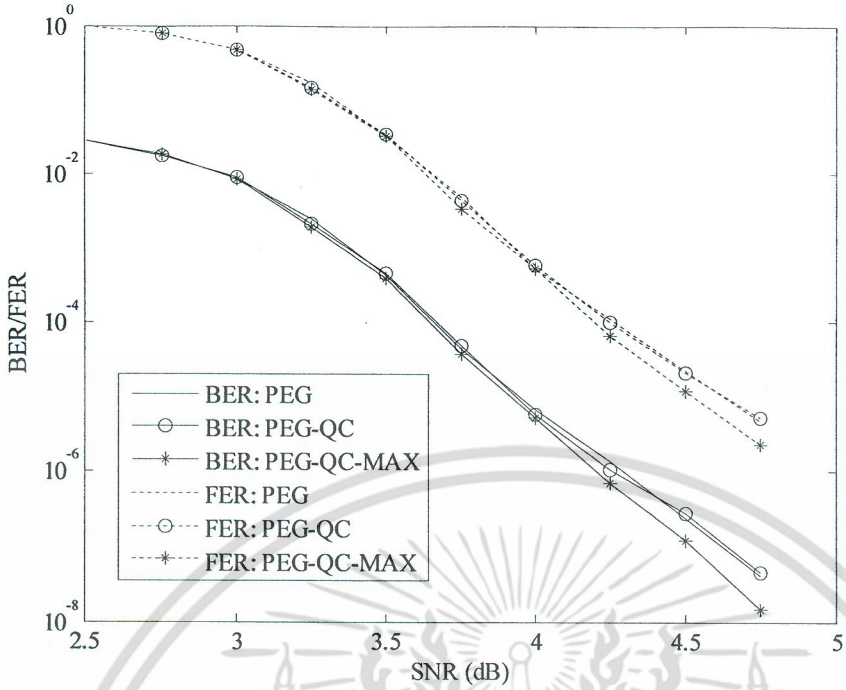
อัตรารหัส	วิธีการออกแบบ	จำนวนของวัฏจักร (%)				
		4	6	8	10	12
1/2	PEG	0	0	0.04	98.47	1.49
	PEG-QC	0	1.93	33.95	63.20	0.92
	PEG-QC-MAX	0	0	0	88.02	11.98
	Other codes [46]	0	0	100	0	0
11/16	PEG	0	0	92.67	7.33	0
	PEG-QC	0	7.28	90.17	2.55	0
	PEG-QC-MAX	0	0	75.57	24.43	0
	Other codes [46]	0	87.36	12.48	0	0
3/4	PEG	0	0	100	0	0
	PEG-QC	0	13.70	86.30	0	0
	PEG-QC-MAX	0	0	100	0	0
	Other codes [46]	0	90.91	9.09	0	0
27/32	PEG	0	0.89	99.11	0	0
	PEG-QC	0	54.09	45.91	0	0
	PEG-QC-MAX	0	0	100	0	0
	Other codes [46]	0	94.44	5.56	0	0

5.1.3 ผลการจำลองสมรรถนะของรหัสควอไซไซคลิกวัฏจักรสูง

รูปที่ 5.2 แสดงอัตราบิตผิดพลาดและอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่ได้รับการออกแบบด้วยอัลกอริทึมพีอีจี พีอีจีคิวซี และพีอีจีคิวซีแม็ก ในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต เมื่อกำหนดให้ อัตรารหัสเท่ากับ 1/2 ความยาวคำรหัสเท่ากับ 1944 บิต และจำนวนการวนซ้ำของถอดรหัสเท่ากับ 25 รอบ จากรูปจะสังเกตได้ว่า รหัสแอลดีพีซีที่ได้รับการออกแบบด้วยอัลกอริทึมพีอีจีและอัลกอริทึมพีอีจีคิวซีแม็ก ให้อัตราบิตผิดพลาดและอัตราเฟรมผิดพลาดต่ำกว่ารหัสแอลดีพีซีที่ออกแบบด้วยอัลกอริทึมพีอีจีคิวซี โดยใช้ค่าเอสเอ็นอาร์ลดลง 0.07 dB ที่อัตราเฟรมผิดพลาดเท่ากับ 3×10^{-6} ทั้งนี้ สามารถอธิบายได้จากขนาดวัฏจักรของรหัสแอลดีพีซีในตารางที่ 5.3 อัลกอริทึมพีอีจีคิวซีมีวัฏจักรขนาด 6, 8 และ 10 ในขณะที่อัลกอริทึมพีอีจีและอัลกอริทึมพีอีจีคิวซีแม็กมีวัฏจักรขนาด 8 และ 10 เท่านั้น รูปที่ 5.3 แสดงอัตราบิตผิดพลาดและอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 5/6 รหัสแอลดีพีซีที่ได้รับการออกแบบด้วยอัลกอริทึมพีอีจีคิวซีแม็กให้สมรรถนะที่ดีสุดเมื่อเทียบกับรหัสแอลดีพีซีแบบอื่น โดยใช้ค่าเอสเอ็นอาร์ลดลง 0.12 dB ที่อัตราเฟรมผิดพลาดเท่ากับ 5×10^{-6} ทั้งนี้ เนื่องจากอัลกอริทึมพีอีจี อัลกอริทึมพีอีจีคิวซี และอัลกอริทึมพีอีจีคิวซีแม็กมีวัฏจักรขนาด 6 จำนวน 96.45% 96.26% และ 89.50% ตามลำดับ และวัฏจักรขนาด 8 จำนวน 3.55% 3.74% และ 10.50% ตามลำดับ ซึ่งจะสังเกตได้ว่าอัลกอริทึมพีอีจีคิวซีแม็กมีขนาดวัฏจักรที่สูงกว่าอัลกอริทึมอื่นๆ



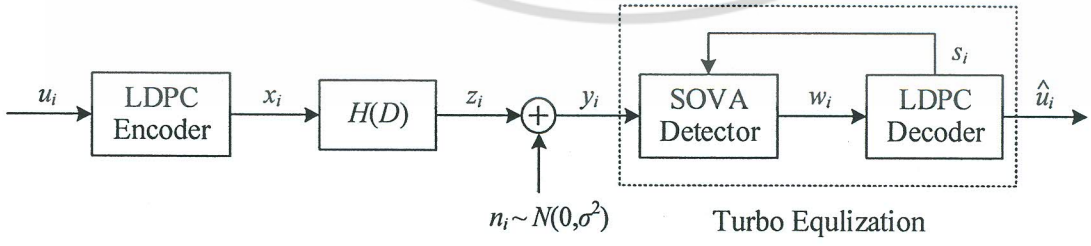
รูปที่ 5.2 อัตราบิตผิดพลาดของรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 1/2



รูปที่ 5.3 อัตราบิตผิดพลาดของรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 5/6

5.2 รหัสอินเทอร์ลิฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน

ระบบบันทึกข้อมูลเชิงแม่เหล็กหรืออุปกรณ์ฮาร์ดดิสก์ จะพบปัญหาการแทรกสอดระหว่างสัญลักษณ์เป็นจำนวนมาก โดยทั่วไป นิยมใช้วงจรถอดรหัสเทอร์โบอีควอไลเซชัน [6] ในการจัดการปัญหาการแทรกสอดระหว่างสัญลักษณ์ของระบบบันทึกข้อมูลเชิงแม่เหล็ก รูปที่ 5.4 แสดงการประยุกต์ใช้งานวงจรถอดรหัสเทอร์โบอีควอไลเซชันในช่องสัญญาณผลตอบสนองบางส่วน ซึ่งนิยมใช้จำลองระบบบันทึกข้อมูลเชิงแม่เหล็ก วงจรถอดรหัสเทอร์โบอีควอไลเซชัน [47] จะประกอบไปด้วยวงจรตรวจหาวิเทอร์บิแบบซอฟต์เอาต์พุต (soft-output Viterbi algorithm, SOVA) [7] และวงจรถอดรหัส แอลดีพีซีซึ่งมีการแลกเปลี่ยนข่าวสารระหว่างวงจรทำให้การถอดรหัสเทอร์โบอีควอไลเซชันมีลักษณะการทำงานแบบวนซ้ำ

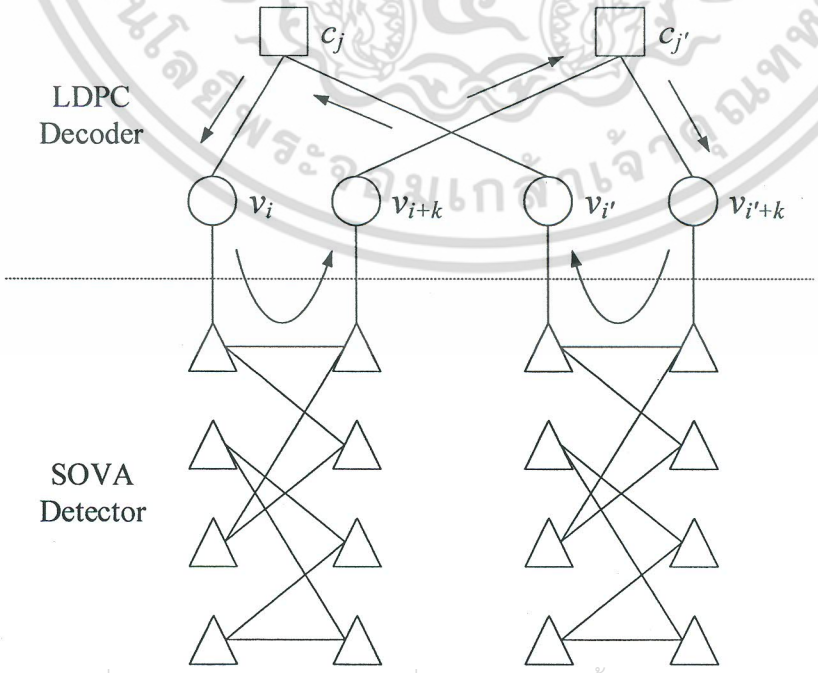


รูปที่ 5.4 วงจรถอดรหัสเทอร์โบอีควอไลเซชัน

โดยทั่วไป การออกแบบรหัสแอลดีพีซีต้องทำให้กราฟแทนเนอร์มีวัฏจักรขนาดสูง อย่างไรก็ตาม การประยุกต์ใช้งานรหัสแอลดีพีซีแบบควอไซไซคลิกและแบบอาร์เรย์ (รายละเอียดอธิบายในบทที่ 3) ในระบบบันทึกข้อมูลเชิงแม่เหล็ก อาจก่อให้เกิดวัฏจักรเทียม (pseudo cycle) [8] ในกระบวนการถอดรหัสเทอร์โบอีควอไลเซชัน พิจารณารหัสแอลดีพีซีแบบควอไซไซคลิกและแบบอาร์เรย์ ซึ่งมีเมทริกซ์เซอร์คิวแลนท์ที่สร้างจากจากการเลื่อนแถวที่อยู่ด้านบนแบบวนกลับ ทำให้ตำแหน่งของเลขหนึ่งในเมทริกซ์พาริตี้เช็คอยู่ในลักษณะทแยงมุม ดังนี้

$$\mathbf{H} = \begin{bmatrix} 1 & & 1 & \\ & 1 & & 1 \end{bmatrix} \tag{5.2}$$

และสามารถเขียนกราฟแทนเนอร์ได้ดังรูปที่ 5.5 เมื่อวงจรถอดรหัสเทอร์โบอีควอไลเซชันทำการแลกเปลี่ยนข่าวสารระหว่างวงจรตรวจหาวิเทอร์บิแบบซอฟต์เอาต์พุตและวงจรถอดรหัสแอลดีพีซี ทำให้ ข่าวสารจากโนดตัวแปร v_i ของวงจรถอดรหัสแอลดีพีซีถูกส่งไปยังโนดเทรลลิสของวงจรตรวจหาวีเทอร์บิแบบซอฟต์เอาต์พุต จากนั้น โนดเทรลลิสจะส่งข่าวสารไปยังโนดตัวแปร v_{i+k} เช่นเดียวกับข่าวสารจากโนดตัวแปร $v_{i'}$ ไปยังโนดตัวแปร $v_{i'+k}$ โดยผ่านโนดเทรลลิส ทั้งนี้ จะสังเกตได้ว่า การแลกเปลี่ยนข่าวสารของวงจรถอดรหัสเทอร์โบอีควอไลเซชันก่อให้วัฏจักรขนาด 4 ในที่นี้จะเรียกว่า วัฏจักรเทียม เนื่องจากวัฏจักรที่เกิดขึ้น ไม่ได้เกิดจากกราฟแทนเนอร์ของรหัสแอลดีพีซี แต่เกิดจากเชื่อมต่อระหว่างวงจรตรวจหาวิเทอร์บิละเอียดกับวงจรถอดรหัสแอลดีพีซี



รูปที่ 5.5 วัฏจักรเทียมในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน

5.2.1 รหัสแรนด้อมอินเทอร์ลิฟอาร์เรย์

ในงานวิจัย [8] นำเสนอรหัสแรนด้อมอินเทอร์ลิฟอาร์เรย์หรือรหัสอาร์ไอเอ (random interleaved array code, RIA code) เพื่อลดจำนวนวัฏจักรเทียมที่เกิดขึ้นในรหัสอาร์เรย์ (รายละเอียดรหัสอาร์เรย์อธิบายในหัวข้อที่ 3.3.4) เมทริกซ์พาริตี้เช็คของรหัสอาร์ไอเอจะอยู่ในรูป $\mathbf{H}=[\mathbf{H}_1\ \mathbf{H}_2]$ ขนาด $(N-K)\times N$ เมื่อ N คือความยาวของบิตคำรหัส และ K คือความยาวของบิตข้อมูล โดยเมทริกซ์ $\mathbf{H}_1$ ขนาด $(N-K)\times K$ เกิดจากการดัดแปลงรหัสอาร์เรย์ ดังนี้

$$\mathbf{H}_1=\begin{bmatrix} \mathbf{I} & \mathbf{I}\boldsymbol{\omega}_g & \mathbf{I}\boldsymbol{\omega}_g^2 & \cdots & \mathbf{I}\boldsymbol{\omega}_g^{(k-j-1)} \\ \mathbf{I} & \boldsymbol{\alpha}\boldsymbol{\omega}_g & \boldsymbol{\alpha}^2\boldsymbol{\omega}_g^2 & \cdots & \boldsymbol{\alpha}^{(k-1)}\boldsymbol{\omega}_g^{(k-j-1)} \\ \mathbf{I} & \boldsymbol{\alpha}^2\boldsymbol{\omega}_g & \boldsymbol{\alpha}^4\boldsymbol{\omega}_g^2 & \cdots & \boldsymbol{\alpha}^{2(k-1)}\boldsymbol{\omega}_g^{(k-j-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I} & \boldsymbol{\alpha}^{j-1}\boldsymbol{\omega}_g & \boldsymbol{\alpha}^{2(j-1)}\boldsymbol{\omega}_g^2 & \cdots & \boldsymbol{\alpha}^{(j-1)(k-1)}\boldsymbol{\omega}_g^{(k-j-1)} \end{bmatrix} \tag{5.3}$$

เมื่อ $\mathbf{I}$ คือเมทริกซ์เอกลักษณ์ (identity matrix) ขนาด $p\times p$ โดยที่ p คือจำนวนเฉพาะ และ $\boldsymbol{\alpha}$ คือเมทริกซ์เรียงลำดับ (permutation matrix) (ตัวอย่างเมทริกซ์เรียงลำดับอธิบายในหัวข้อที่ 3.3.4 (บทที่ 3)) และ $\boldsymbol{\omega}_g$ คือเมทริกซ์สลับตำแหน่ง (interleaving matrix) สร้างได้จากเมทริกซ์เอกลักษณ์ $\mathbf{I}$ ที่ทำการเลื่อนแถวแบบวนกลับเป็นจำนวน g ครั้ง ตัวอย่างของเมทริกซ์สลับตำแหน่งขนาด 5×5 แสดงได้ดังนี้

$$\boldsymbol{\omega}_2=\begin{bmatrix} 0&1&0&0&0 \\ 0&0&0&1&0 \\ 1&0&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&0&1 \end{bmatrix} \qquad \boldsymbol{\omega}_3=\begin{bmatrix} 0&0&1&0&0 \\ 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&1&0&0&0 \\ 0&0&0&0&1 \end{bmatrix}$$

สำหรับเมทริกซ์ $\mathbf{H}_2$ ขนาด $(N-K)\times K$ จะมีลักษณะหมุนวนคล้ายกับเมทริกซ์เรียงลำดับ $\boldsymbol{\alpha}$ โดยมีจำนวนเลขหนึ่งในแต่ละหลักเท่ากับ 3 ตัวอย่างเช่น เมทริกซ์ $\mathbf{H}_2$ ขนาด 10×10 ในสมการที่ 5.4 การเข้ารหัสแรนด้อมอินเทอร์ลิฟอาร์เรย์จะกระทำผ่านเมทริกซ์กำเนิด $\mathbf{G}$ ซึ่งอยู่ในรูป $\mathbf{G}=[\mathbf{I}\ (\mathbf{H}_2^{-1}.\mathbf{H}_1)^T]$ ดังนั้น การออกแบบเมทริกซ์ $\mathbf{H}_2$ จะต้องทำให้อินเวอร์สของเมทริกซ์ $\mathbf{H}_2$ เป็นเมทริกซ์มากเลขศูนย์ (sparse matrix) เพื่อทำให้การเข้ารหัสมีความซับซ้อนต่ำ นอกจากนี้ เมทริกซ์ $\mathbf{H}_2$ ที่ได้รับการออกแบบอาจมีจำนวนแถวไม่สอดคล้องกับเมทริกซ์ $\mathbf{H}_1$ เนื่องจากการออกแบบเมทริกซ์ $\mathbf{H}_1$ อยู่ภายใต้ข้อจำกัดของพารามิเตอร์ p ดังนั้น แถวของเมทริกซ์ $\mathbf{H}_1$ จะต้องถูกตัดทิ้งเพื่อทำให้จำนวนแถวของเมทริกซ์ $\mathbf{H}_1$ และ $\mathbf{H}_2$ มีความสอดคล้องกัน

$$\mathbf{H}_2 = \begin{bmatrix} 1 & & 1 & & & & 1 & & \\ & 1 & & 1 & & & & 1 & \\ & & 1 & & 1 & & & & 1 \\ 1 & & & 1 & & 1 & & & \\ & 1 & & & 1 & & 1 & & \\ & & 1 & & & 1 & & 1 & \\ & & & 1 & & & 1 & & 1 \\ 1 & & & & 1 & & & 1 & \\ & 1 & & & & 1 & & & 1 \end{bmatrix} \tag{5.4}$$

5.2.2 รหัสอินเทอร์ลิฟมอดดิฟายอาร์เรย์

รหัสแรนด้อมอินเทอร์ลิฟอาร์เรย์หรืออาร์ไอเอที่อธิบายในหัวข้อก่อนหน้า การออกแบบเมทริกซ์ $\mathbf{H}_2$ ให้มีขนาดตามที่ต้องการมีความยุ่งยาก เนื่องจากจำเป็นต้องทำให้อินเวอร์สของเมทริกซ์ $\mathbf{H}_2$ เป็นเมทริกซ์มากเลขศูนย์ (sparse matrix) เพื่อทำให้การเข้ารหัสมีความซับซ้อนต่ำ นอกจากนี้ เมทริกซ์ $\mathbf{H}_2$ ยังก่อให้เกิดวัฏจักรขนาด 4 ดังนั้น ในงานวิจัยนี้จะนำเสนอรหัสอินเทอร์ลิฟมอดดิฟายอาร์เรย์หรือรหัสไอแม็ก (interleaved modified array code, IMAC) เพื่อลดจำนวนวัฏจักรเทียมที่เกิดขึ้นในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน อีกทั้งการเข้ารหัสมีความซับซ้อนต่ำ พิจารณาโครงสร้างรหัสแม็ก (modified array code, MAC) ในสมการที่ 3.30 (บทที่ 3) เมื่อทำการคูณเมทริกซ์พาริตี้เช็คของรหัสแม็กด้วยเมทริกซ์สลับตำแหน่ง $\boldsymbol{\omega}_g$ ขนาด $p \times p$ เมื่อ p คือจำนวนเฉพาะ ทำให้

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I}\boldsymbol{\omega}_g & \mathbf{I}\boldsymbol{\omega}_g^2 & \cdots & \mathbf{I}\boldsymbol{\omega}_g^{(j-1)} & \mathbf{I}\boldsymbol{\omega}_g^{(j)} & \cdots & \mathbf{I}\boldsymbol{\omega}_g^{(k-1)} \\ \mathbf{0} & \mathbf{I} & \boldsymbol{\alpha}\boldsymbol{\omega}_g & \cdots & \boldsymbol{\alpha}^{(j-2)}\boldsymbol{\omega}_g^{(j-2)} & \boldsymbol{\alpha}^{(j-1)}\boldsymbol{\omega}_g^{(j-1)} & \cdots & \boldsymbol{\alpha}^{(k-2)}\boldsymbol{\omega}_g^{(k-2)} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \boldsymbol{\alpha}^{2(j-3)}\boldsymbol{\omega}_g^{(j-3)} & \boldsymbol{\alpha}^{2(j-2)}\boldsymbol{\omega}_g^{(j-2)} & \cdots & \boldsymbol{\alpha}^{2(k-3)}\boldsymbol{\omega}_g^{(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \boldsymbol{\alpha}^{(j-1)}\boldsymbol{\omega}_g & \cdots & \boldsymbol{\alpha}^{(j-1)(k-j)}\boldsymbol{\omega}_g^{(k-j)} \end{bmatrix} \tag{5.5}$$

และเรียกโครงสร้างรหัสนี้ว่า รหัสอินเทอร์ลิฟมอดดิฟายอาร์เรย์หรือไอแม็ก (interleaved modified array code, IMAC) กำหนดให้คำรหัสที่ได้จากการเข้ารหัสอยู่ในรูป

$$\mathbf{c} = \left[\mathbf{p}_1\ \mathbf{p}_2\ \ldots\ \mathbf{p}_j\ \mathbf{m}_1\ \mathbf{m}_2\ \ldots\ \mathbf{m}_{(k-j)}\right] \tag{5.6}$$

เมื่อ $\mathbf{p}$ และ $\mathbf{m}$ คือบล็อกพาริตี้และบล็อกข้อมูลขนาด p บิต ตามลำดับ เนื่องจาก $\mathbf{H}\mathbf{c}^T = \mathbf{0}$ ทำให้สมการที่ 5.5 และ 5.6 เขียนใหม่ได้เป็น

$$\begin{bmatrix} \mathbf{I} & \mathbf{I}\omega_g & \mathbf{I}\omega_g^2 & \cdots & \mathbf{I}\omega_g^{(j-1)} & \mathbf{I}\omega_g^{(j)} & \cdots & \mathbf{I}\omega_g^{(k-1)} \\ \mathbf{0} & \mathbf{I} & \boldsymbol{\alpha}\omega_g & \cdots & \boldsymbol{\alpha}^{(j-2)}\omega_g^{(j-2)} & \boldsymbol{\alpha}^{(j-1)}\omega_g^{(j-1)} & \cdots & \boldsymbol{\alpha}^{(k-2)}\omega_g^{(k-2)} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \boldsymbol{\alpha}^{2(j-3)}\omega_g^{(j-3)} & \boldsymbol{\alpha}^{2(j-2)}\omega_g^{(j-2)} & \cdots & \boldsymbol{\alpha}^{2(k-3)}\omega_g^{(k-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \boldsymbol{\alpha}^{(j-1)}\omega_g & \cdots & \boldsymbol{\alpha}^{(j-1)(k-j)}\omega_g^{(k-j)} \end{bmatrix} \begin{bmatrix} \mathbf{p}_1 \\ \vdots \\ \mathbf{p}_j \\ \mathbf{m}_1 \\ \vdots \\ \mathbf{m}_{(k-j)} \end{bmatrix} = \mathbf{0} \quad (5.7)$$

จัดรูปใหม่จะได้

$$\begin{aligned} \mathbf{p}_1 &= \mathbf{p}_2\omega_g + \mathbf{p}_3\omega_g^2 + \ldots + \mathbf{p}_j\boldsymbol{\alpha}^{(j-1)} + \mathbf{m}_1\omega_g^j + \mathbf{m}_2\omega_g^{(j+1)} + \ldots + \mathbf{m}_{k-j}\omega_g^{(k-1)} \\ \mathbf{p}_2 &= \mathbf{p}_3\boldsymbol{\alpha}\omega_g + \mathbf{p}_4\boldsymbol{\alpha}^2\omega_g^2 + \ldots + \mathbf{p}_j\boldsymbol{\alpha}^{(j-2)}\omega_g^{(j-2)} + \mathbf{m}_1\boldsymbol{\alpha}^{(j-1)}\omega_g^{(j-1)} + \ldots + \mathbf{m}_{k-j}\boldsymbol{\alpha}^{(k-2)}\omega_g^{(k-2)} \\ &\vdots \\ \mathbf{p}_{j-1} &= \mathbf{p}_j\boldsymbol{\alpha}^{(j-2)}\omega_g + \mathbf{m}_1\boldsymbol{\alpha}^{2(j-2)}\omega_g^2 + \mathbf{m}_2\boldsymbol{\alpha}^{3(j-2)}\omega_g^3 + \ldots + \mathbf{m}_{k-j}\boldsymbol{\alpha}^{(j-2)(k-j+1)}\omega_g^{(k-j+1)} \\ \mathbf{p}_j &= \mathbf{m}_1\boldsymbol{\alpha}^{(j-1)}\omega_g + \mathbf{m}_2\boldsymbol{\alpha}^{2(j-1)}\omega_g^2 + \ldots + \mathbf{m}_{k-j}\boldsymbol{\alpha}^{(j-1)(k-j)}\omega_g^{(k-j)} \end{aligned} \quad (5.8)$$

ดังนั้นบล็อกพาริตี้ $\mathbf{p}_j$ ของรหัสอินเทอร์ลิฟมอดดิฟายอาร์เรย์หรือไอแม็ก คำนวณได้จาก

$$\mathbf{p}_j = \sum_{i=1}^{k-j} \mathbf{m}_i\boldsymbol{\alpha}^{(j-1)i}\boldsymbol{\omega}^i \quad (5.9)$$

และบล็อกพาริตี้ $\mathbf{p}_l$ เมื่อ $1 \le l < j$ คำนวณได้ดังนี้

$$\mathbf{p}_l = \sum_{i=1}^{j-l} \mathbf{p}_{l+i}\boldsymbol{\alpha}^{(l-1)i}\boldsymbol{\omega}^i + \sum_{i=1}^{k-j} \mathbf{m}_i\boldsymbol{\alpha}^{(l-1)(j-l+i)}\boldsymbol{\omega}^{j-l+i} \quad (5.10)$$

จะสังเกตได้ว่า การคูณด้วยเมทริกซ์ $\boldsymbol{\alpha}$ และ $\boldsymbol{\omega}$ ในสมการที่ 5.9 และ 5.10 จะเท่ากับการหมุนวนเวกเตอร์ $\mathbf{p}$ และ $\mathbf{m}$ ดังนั้น การเข้ารหัสไอแม็กจะใช้เพียงชิฟต์รีจิสเตอร์และวงจรการบวก ต่างจากรหัสอาร์ไอเอที่ต้องใช้วงจรการคูณและการบวก นอกจากนี้ รหัสไอแม็กปราศจากเมทริกซ์ $\mathbf{H}_2$ ที่ก่อให้เกิดวัฏจักรขนาด 4 และมีความซับซ้อนในการออกแบบ ตารางที่ 5.5 แสดงจำนวนวัฏจักรเทียมและวัฏจักรขนาด 4 ของรหัสแม็ก (MAC) ไอแม็ก (IMAC) และอาร์ไอเอ (RIA) ที่อัตรารหัส 0.91 โดยกำหนดให้พารามิเตอร์ p, j, k มีค่าเท่ากับ 89, 4, 46 ตามลำดับ จากตารางจะสังเกตได้ว่ารหัสไอแม็กเมื่อ $g = 3,80$ จะปราศจากวัฏจักรขนาด 4 เช่นเดียวกับรหัสแม็ก อย่างไรก็ตาม รหัสแม็กจะมีวัฏจักรเทียมจำนวนมาก เนื่องจากรหัสแม็กไม่ได้รับการออกแบบสำหรับการใช้งานในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน ตารางที่ 5.6 แสดงจำนวนวัฏจักรเทียมของรหัสไอแม็กและอาร์ไอเอที่อัตรารหัสต่างๆ จากตารางจะเห็นว่ารหัสไอแม็กมีจำนวนวัฏจักรเทียมน้อยกว่ารหัสอาร์ไอเอ

ตารางที่ 5.5 จำนวนวัฏจักรของโครงสร้างรหัสแบบต่างๆ

โครงสร้างรหัส	จำนวนวัฏจักรเทียม	จำนวนวัฏจักรขนาด 4
MAC	360,851	0
IMAC-g2	54,926	84,194
IMAC-g3	23,374	0
IMAC-g80	27,887	0
RIA-g2	49,610	476
RIA-g3	25,969	476
RIA-g80	30,821	476

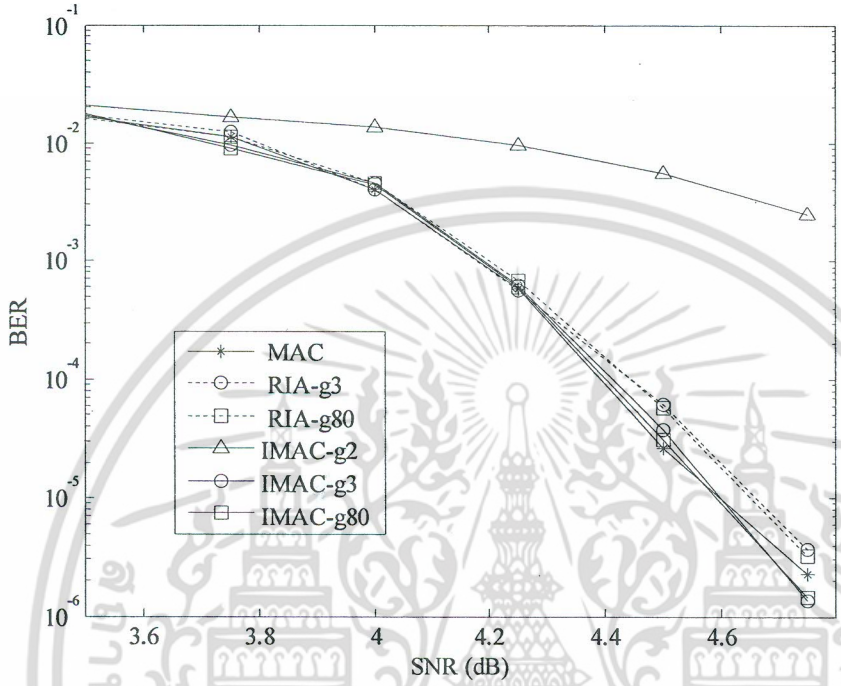
ตารางที่ 5.6 จำนวนวัฏจักรเทียมของรหัสอินเทอร์ลีฟ

อัตรารหัส	(p, j, k)	RIA-g80	IMAC-g80
0.91	(89, 4, 46)	30,821	27,887
0.83	(179, 4, 23)	7,612	4,137
0.67	(353, 4, 12)	9,830	1,059

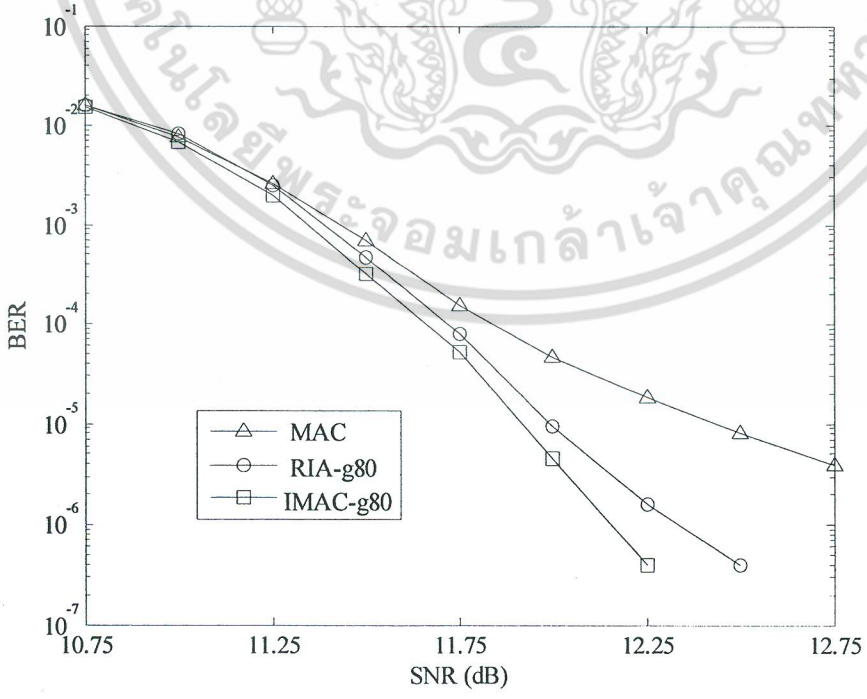
5.2.3 ผลการจำลองสมรรถนะของรหัสอินเทอร์ลีฟ

ในหัวข้อนี้ จะแสดงผลการจำลองอัตราบิตผิดพลาดของรหัสแม็ก ไอแม็ก และอาร์ไอเอ โดยกำหนดให้อัตรารหัสเท่ากับ 0.91 และพารามิเตอร์ p, j, k มีค่าเท่ากับ 89, 4, 46 ตามลำดับ รูปที่ 5.6 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีเมื่อจำนวนการถอดรหัสวนซ้ำเท่ากับ 20 รอบ ในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต จากรูปจะสังเกตได้ว่า รหัสไอแม็ก-g2 มีสมรรถนะแย่สุด เนื่องจากโครงสร้างรหัสก่อให้เกิดวัฏจักรขนาด 4 เป็นจำนวนมาก สำหรับรหัสแม็กและไอแม็ก-g3,80 จะมีสมรรถนะดีสุดเนื่องจากปราศจากวัฏจักรขนาด 4 รูปที่ 5.7 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีในช่องสัญญาณผลตอบสนองบางส่วนแบบ EPR2 ซึ่งมีสมการของช่องสัญญาณคือ $H(D) = 1 + 3D + 3D^2 + D^3$ จะเห็นได้ว่า รหัสแม็กซึ่งมีอัตราบิตผิดพลาดต่ำในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต จะมีอัตราบิตผิดพลาดสูงในช่องสัญญาณผลตอบสนองบางส่วน เนื่องจากรหัสแม็กมีวัฏจักรเทียมเป็นจำนวนมาก สำหรับรหัสไอแม็ก-g80 ที่นำเสนอในงานวิจัยนี้ จะมีอัตราบิตผิดพลาดต่ำสุดเมื่อเทียบกับรหัสแม็กและอาร์ไอเอ โดยที่อัตราบิตผิดพลาดเท่ากับ 4×10^{-7} รหัสไอแม็ก-g80 ใช้ค่าเอสเอ็นอาร์ลดลง 0.25 dB เมื่อเทียบกับรหัสอาร์ไอเอ รูปที่ 5.8 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีในช่องสัญญาณผลตอบสนองบางส่วนแบบ EEPR2 ซึ่งมีสมการของช่องสัญญาณคือ $H(D) = 1 + 4D + 6D^2 + 4D^3 + D^3$ รหัสไอแม็ก-g80 ยังคงให้อัตราบิตผิดพลาด

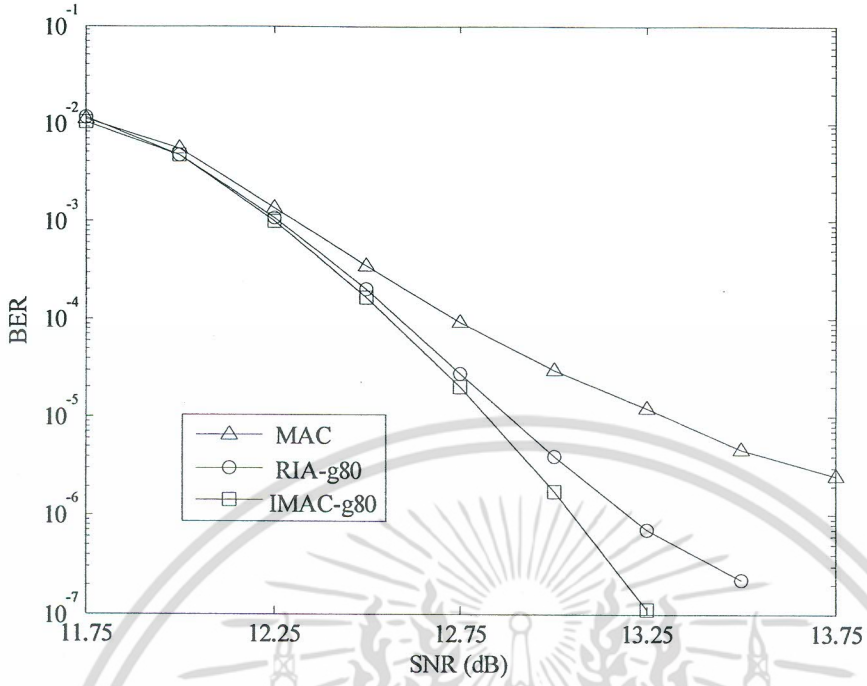
ต่ำสุดเมื่อเทียบกับรหัสแม็กและอาร์ไอเอที่มีจำนวนวัฏจักรเทียมและวัฏจักรขนาด 4 อยู่เป็นจำนวนมาก โดยที่อัตราบิตผิดพลาดเท่ากับ 2×10^{-7} รหัสไอแม็ก-g80 ใช้ค่าเอสเอ็นอาร์ลดลง 0.30 dB เมื่อเทียบกับรหัสอาร์ไอเอ



รูปที่ 5.6 อัตราบิตผิดพลาดของรหัสอินเทอร์ลีฟในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต



รูปที่ 5.7 อัตราบิตผิดพลาดของรหัสอินเทอร์ลีฟในช่องสัญญาณผลตอบสนองบางส่วนแบบ EPR2



รูปที่ 5.8 อัตราบิตผิดพลาดของรหัสอินเทอร์ลีฟในช่องสัญญาณผลตอบสนองบางส่วนแบบ EEPR2

5.3 รหัสโปรโตกราฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน

หัวข้อที่ 3.3.5 (บทที่ 3) อธิบายรหัสโปรโตกราฟ ซึ่งกระบวนการสร้างกราฟแทนเนอร์จะทำให้รหัสโปรโตกราฟมีลักษณะควอไซไซคลิก (quasi-cyclic) ทั้งนี้ อาจกล่าวได้ว่ารหัสแอลดีพีซีแบบควอไซไซคลิกใดๆ สามารถเขียนในรูปเมทริกซ์ฐานของรหัสโปรโตกราฟได้ (เช่นเดียวกับรหัสแอลดีพีซีที่นำเสนอในหัวข้อที่ผ่านมา) ในหัวข้อที่ 4.2.2 (บทที่ 4) แสดงการวิเคราะห์รหัสโปรโตกราฟด้วยวิธีการเอ็กซิตชาร์ท (extrinsic information transfer charts, EXIT charts) โดยจะสังเกตได้ว่าวิธีการวิเคราะห์จะเกี่ยวข้องกับเมทริกซ์ฐานของรหัสโปรโตกราฟ ในงานวิจัย [10, 11] ได้ประยุกต์ใช้วิธีการเอ็กซิตชาร์ท สำหรับการวิเคราะห์และออกแบบรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน อย่างไรก็ตาม การวิเคราะห์จะพิจารณารหัสไบนารีแอลดีพีซีหรือรหัสแอลดีพีซีบนฟีลด์จำกัด $\mathrm{GF}(q)$ เมื่อ $q=2$ เท่านั้น ในหัวข้อที่ 3.2.2 (บทที่ 3) แสดงให้เห็นว่าสมรรถนะของรหัสแอลดีพีซีจะเพิ่มสูงขึ้นเมื่อค่า q เพิ่มขึ้น ทั้งนี้ สมรรถนะของรหัสแอลดีพีซีจะขึ้นอยู่กับปริมาณเลขหนึ่งในเมทริกซ์พาริตี้เช็คหรือจำนวนเส้นเชื่อมในกราฟแทนเนอร์ ดังนั้น ในงานวิจัยนี้จะนำเสนอวิธีการวิเคราะห์รหัสโปรโตกราฟบนฟีลด์จำกัด $\mathrm{GF}(q)$ สำหรับช่องสัญญาณผลตอบสนองบางส่วน โดยประยุกต์ใช้วิธีการเอ็กซิตชาร์ทในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน วิธีการที่ได้นำเสนอนี้ จะแสดงค่าเทรสโฮลด์ของรหัสโปรโตกราฟแบบต่างๆ ซึ่งสามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีในช่องสัญญาณผลตอบสนองบางส่วนที่ให้สมรรถนะเข้าใกล้ขีดจำกัดของแชนนอน

5.3.1 ข่าวสารร่วมของรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q)

สำหรับรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) ข่าวสารในรูปอัตราส่วนความน่าจะเป็นแบบล็อกหรือค่าแอลแอลอาร์ระหว่างโนดตัวแปรและโนดตรวจสอบจะเป็นเวกเตอร์ขนาด $1\times q$ ดังสมการที่ 4.52 และ 4.54 (บทที่ 4) อย่างไรก็ตาม อิลิเมนท์ลำดับที่หนึ่งในเวกเตอร์จะมีค่าเท่ากับ 1 เสมอ ดังนั้น สามารถพิจารณาข่าวสารแอลแอลอาร์เป็นเวกเตอร์ขนาด $1\times q-1$ ในงานวิจัย [48,49] นำเสนอการคำนวณข่าวสารร่วมของรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) เมื่อกำหนดให้อิลิเมนท์ที่ไม่เป็นศูนย์ของเมทริกซ์พาริตี้เช็ค ได้แก่ $1,\ldots,q-1$ มีการกระจายตัวแบบสม่ำเสมอ ทำให้ข่าวสารแอลแอลอาร์ขนาด $1\times q-1$ ระหว่างโนดตรวจสอบกับโนดตัวแปรมีค่าเฉลี่ย $\mathbf{m}$ และความแปรปรวนร่วมเกี่ยว (covariance) $\boldsymbol{\Sigma}$ ดังนี้

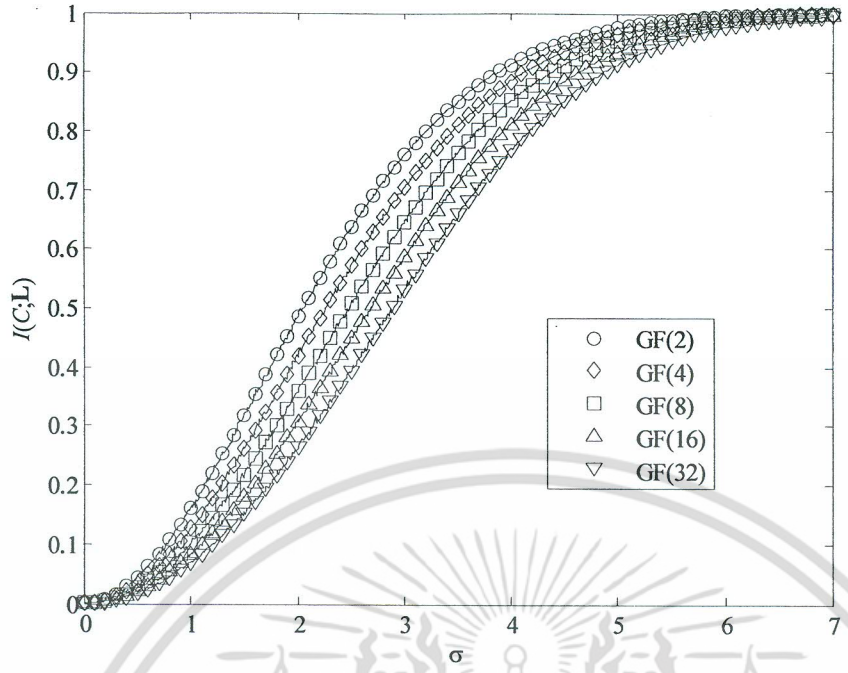
$$\mathbf{m}=\begin{bmatrix}\sigma^2/2\\ \sigma^2/2\\ \vdots\\ \sigma^2/2\end{bmatrix}_{(q-1)\times 1} \qquad \boldsymbol{\Sigma}=\begin{bmatrix}\sigma^2 & \sigma^2/2 & \cdots & \sigma^2/2\\ \sigma^2/2 & \sigma^2 & \cdots & \vdots\\ \vdots & \vdots & \ddots & \sigma^2/2\\ \sigma^2/2 & \cdots & \sigma^2/2 & \sigma^2\end{bmatrix}_{(q-1)\times(q-1)} \tag{5.11}$$

เมื่อค่าฟีลด์จำกัดเท่ากับ $q=2$ หรือรหัสไบนารีแอลดีพีซี ข่าวสารแอลแอลอาร์จะมีค่าเฉลี่ยและความแปรปรวนเท่ากับสมการที่ 4.96 และ 4.68 (บทที่ 4) นอกจากนี้ จะสังเกตได้ว่า ค่าเฉลี่ยและแปรปรวนร่วมเกี่ยวขึ้นอยู่กับความแปรปรวน σ^2 ของข่าวสารแอลแอลอาร์

กำหนดให้คำรหัสที่ได้จากการเข้ารหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) มีค่าเท่ากับศูนย์เสมอ หรือคำรหัสลำดับใดๆ มีค่าเป็น $C=0$ และข่าวสารแอลแอลอาร์ระหว่างโนดตัวแปรและโนดตรวจสอบของรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) คือ $\mathbf{L}=[L_1\ \ldots\ L_{q-1}]$ จากสมการที่ 4.70 (บทที่ 4) ทำให้การคำนวณข่าวสารร่วมระหว่างคำรหัส C และเวกเตอร์แอลแอลอาร์ $\mathbf{L}$ คำนวณได้จากสมการต่อไปนี้

$$I(C;\mathbf{L})=H(C)-H(C|\mathbf{L})=1-E\left[\log_q\left(1+\sum_{i=1}^{q-1}e^{-L_i}\right)|C=0\right] \tag{5.12}$$

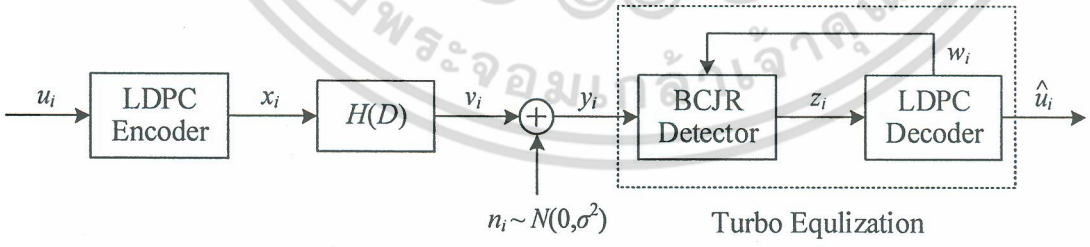
รูปที่ 5.9 แสดงการวัดปริมาณข่าวสารร่วมของข่าวสารแอลแอลอาร์โดยใช้จากการจำลองมอนติคาโล โดยจะสังเกตได้ว่า เมื่อค่าเบี่ยงเบนมาตรฐาน σ ของข่าวสารแอลแอลอาร์สูงขึ้นจะทำให้ข่าวสารร่วม $I(C;\mathbf{L})$ เพิ่มขึ้น และเมื่อค่าฟีลด์จำกัด GF(q) เพิ่มขึ้นจะทำให้ข่าวสารร่วม $I(C;\mathbf{L})$ ลดลง เนื่องจากรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) เวกเตอร์แอลแอลอาร์ $\mathbf{L}$ จะแทนข้อมูลไบนารีจำนวน $\log_2 q$ บิต



รูปที่ 5.9 ข่าวสารร่วมของแอลแอลอาร์

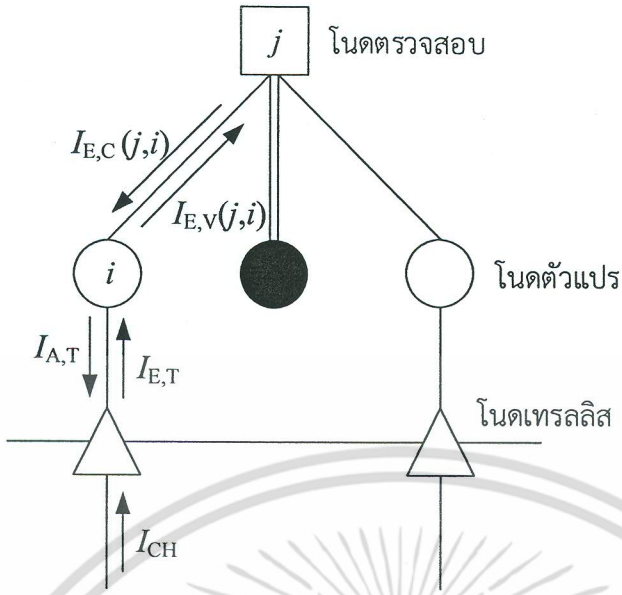
5.3.2 การวิเคราะห์รหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน

การวิเคราะห์และออกแบบรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วนถูกนำเสนอในงานวิจัย [10, 11] อย่างไรก็ตาม การวิเคราะห์จะพิจารณารหัสไบนารีแอลดีพีซีหรือรหัสแอลดีพีซีบนฟีลด์จำกัด GF(q) เมื่อ $q=2$ เท่านั้น ดังนั้น ในงานวิจัยนี้จึงนำเสนอวิธีการวิเคราะห์รหัสโปรโตกราฟบนฟีลด์จำกัด GF(q) สำหรับช่องสัญญาณผลตอบสนองบางส่วน พิจารณาวงจรถอดรหัสเทอร์โบอีควอไลเซชัน[4] ในรูปที่ 5.10 การถอดรหัสจะมีลักษณะการทำงานแบบวนซ้ำ โดยทำการแลกเปลี่ยนข่าวสารระหว่างวงจรถอดรหัสบีซีเจอาร์ [24] และวงจรถอดรหัสแอลดีพีซี



รูปที่ 5.10 วงจรถอดรหัสเทอร์โบอีควอไลเซชัน

[4]ในงานวิจัยส่วนนี้ จะใช้วงจรตรวจหาบีซีเจอาร์แทนวงจรตรวจหาวีเทอร์บิแบบซอฟต์เอาต์พุต เนื่องจากวงจรตรวจหาบีซีเจอาร์จัดเป็นวงจรถอดรหัสเอ็มเอพี (Maximum a posteriori probability decoding, MAP decoding) ซึ่งเหมาะสมต่อการวิเคราะห์หาสมรรถนะขีดสุดของการถอดรหัส

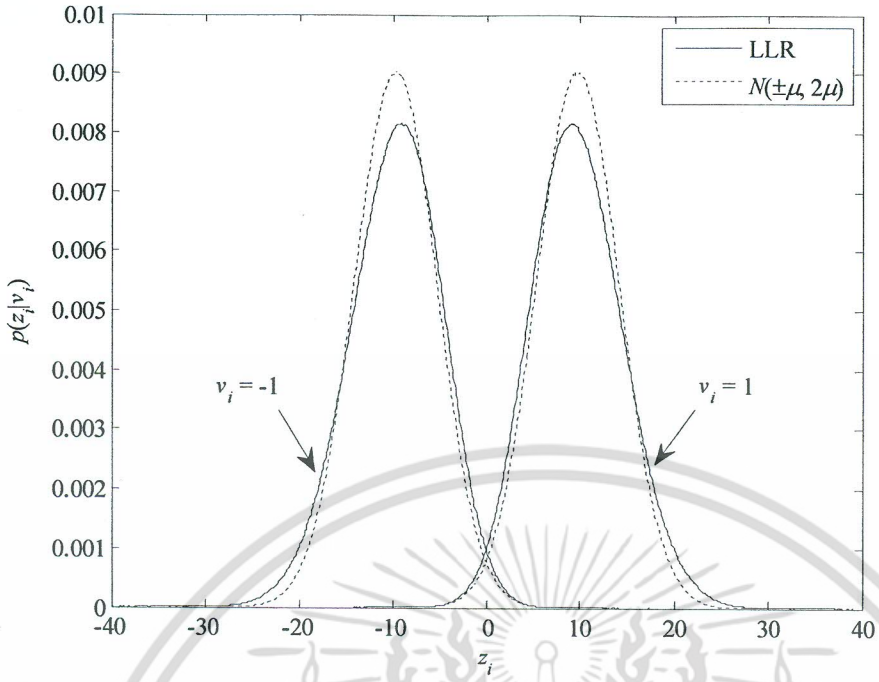


รูปที่ 5.11 ข่าวสารร่วมของวงจรถอดรหัสเทอร์โบอีควอไลเซชัน

การวิเคราะห์รหัสโปรโตกราฟบนฟีลด์จำกัด GF(q) ในช่องสัญญาณผลตอบสนองบางส่วนจะต้องคำนวณข่าวสารร่วมที่ออกจากวงจรตรวจหาบีซีเจอาร์และวงจรถอดรหัสแอลดีพีซี พิจารณาข่าวสารร่วมในรูปที่ 5.11 เมื่อโนดเทรลลิสแทนวงจรตรวจหาบีซีเจอาร์ และโนดตัวแปรและโนดตรวจสอบแทนวงจรถอดรหัสแอลดีพีซี กำหนดให้ I_{CH} คือข่าวสารร่วมที่ได้รับจากช่องสัญญาณ $I_{E,T}$ คือข่าวสารร่วมที่ออกจากโนดเทรลลิสไปยังโนดตัวแปร $I_{A,T}$ คือข่าวสารร่วมที่โนดเทรลลิสได้รับ $I_{E,V}(j,i)$ คือข่าวสารร่วมจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j และ $I_{E,C}(j,i)$ คือข่าวสารร่วมจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i สำหรับโนดตัวแปรที่ถูกทำพังก์เชอร์ (โนดตัวแปรสีดำ) จะไม่ได้รับข่าวสารร่วม $I_{E,T}$ จากโนดเทรลลิส

5.3.2.1 ข่าวสารร่วมของโนดเทรลลิส

พิจารณาวงจรถอดรหัสบีซีเจอาร์ในรูปที่ 5.10 สัญญาณเอาท์พุต z_i ในรูปอัตราส่วนความน่าจะเป็นแบบล็อกหรือค่าแอลแอลอาร์ของวงจรตรวจหาบีซีเจอาร์จะขึ้นอยู่กับสัญญาณ y_i ที่ได้รับจากช่องสัญญาณและสัญญาณ w_i ที่ได้รับจากวงจรถอดรหัสแอลดีพีซี รูปที่ 5.12 แสดงความหนาแน่นความน่าจะเป็นของค่าแอลแอลอาร์ z_i ที่ออกจากวงจรตรวจหาบีซีเจอาร์ (แทนด้วยเส้นทึบ) เมื่อสัญญาณส่ง $v_i = \pm 1$ และค่าแอลแอลอาร์ของสัญญาณ $w_i = \pm 1$ จะสังเกตได้ว่า สัญญาณเอาท์พุต z_i มีความหนาแน่นความน่าจะเป็นแบบปรกติซึ่งมีค่าเฉลี่ยเท่ากับ $\pm\mu$ และความแปรปรวนเท่ากับ σ^2 นอกจากนี้ รูปที่ 5.12 แสดงความหนาแน่นความน่าจะเป็นแบบปรกติซึ่งมีค่าเฉลี่ยเท่ากับ $\pm\mu$ และความแปรปรวนเท่ากับ 2μ (แทนด้วยเส้นประ) ตามคุณสมบัติสัญญาณแอลแอลอาร์ที่ได้รับจากช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุตในสมการที่ 4.68 และ 4.69 (บทที่ 4) โดยจะสังเกตได้ว่าความหนาแน่นความน่าจะเป็นของสัญญาณ z_i ใกล้เคียงกับคุณสมบัติดังกล่าว

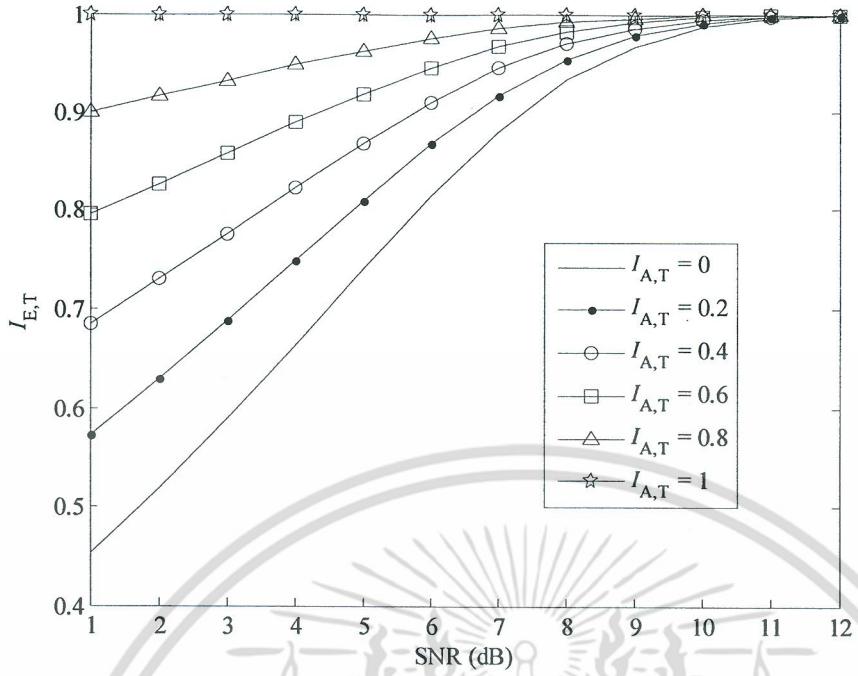


รูปที่ 5.12 ความหนาแน่นความน่าจะเป็นของสัญญาณที่ได้รับจากวงจรตรวจหาบีซีเจอาร์

ดังนั้น จากสมการที่ 4.70 (บทที่ 4) ข่าวสารร่วม $I_{E,T}$ ที่ได้รับจากวงจรตรวจหาบีซีเจอาร์คำนวณได้จากสมการต่อไปนี้

$$I_{E,T} = 1 - E\left[\log_2\left(1+e^{-v_i \cdot z_i}\right)\right] \tag{5.13}$$

เมื่อ z_i คือสัญญาณแอลแอลอาร์ของเอาท์พุตที่ได้รับจากวงจรตรวจหาบีซีเจอาร์ และ v_i คือสัญญาณส่งผ่านช่องสัญญาณในรูปที่ 5.10 โดยกำหนดให้สัญญาณ w_i มีความหนาแน่นความน่าจะเป็นแบบปรกติซึ่งมีค่าเฉลี่ยเท่ากับ $\pm\sigma^2/2$ และความแปรปรวนเท่ากับ σ^2 ซึ่งคำนวณได้จากอินเวอร์สฟังก์ชันการคำนวณข่าวสารร่วม $J_2^{-1}(I_{A,T})$ ในสมการที่ 5.14 รูปที่ 5.13 แสดงข่าวสารร่วม $I_{E,T}$ เมื่อช่องสัญญาณเป็นแบบ PR1 หรือ $H(D)=1+D$ และกำหนดให้ข่าวสารร่วม $I_{A,T}$ ที่ได้รับจากวงจรถอดรหัสแอลดีพีซีมีค่าต่างๆ จากรูปจะสังเกตได้ว่าเมื่ออัตราส่วนกำลังของสัญญาณส่งต่อกำลังของสัญญาณรบกวนหรือค่าเอสเอ็นอาร์เพิ่มขึ้น จะทำให้ข่าวสารร่วม $I_{E,T}$ ที่ได้รับจากวงจรตรวจหาบีซีเจอาร์เพิ่มขึ้น (นิยามค่าเอสเอ็นอาร์แสดงในสมการที่ 2.20 (บทที่ 2)) และเมื่อข่าวสารร่วม $I_{A,T}$ เพิ่มขึ้น จะทำให้ข่าวสารร่วม $I_{E,T}$ ที่ได้รับจากวงจรตรวจหาบีซีเจอาร์เพิ่มขึ้นเช่นกัน และกรณีที่ข่าวสารร่วม $I_{A,T}$ เท่ากับ 1 หรือกรณีค่าเอสเอ็นอาร์เท่ากับ 12 dB จะทำให้ข่าวสารร่วม $I_{E,T}$ เท่ากับ 1 หมายความว่า ข้อมูลที่ออกจากวงจรตรวจหาบีซีเจอาร์เหมือนกับข้อมูลที่ถูกส่งผ่านช่องสัญญาณหรือข้อมูลที่ถูกถอดรหัสปราศจากบิตผิดพลาด



รูปที่ 5.13 ข่าวสารร่วม $I_{E,T}$

5.3.2.2 ข่าวสารร่วมของโนดตัวแปร

ในสมการที่ 4.56 (บทที่ 4) อธิบายการคำนวณค่าแอลแอลอาร์ที่ออกจากโนดตัวแปร โดยจะเห็นว่า ค่าแอลแอลอาร์ที่ออกจากโนดตัวแปรเกิดจากผลรวมของค่าแอลแอลอาร์ที่ได้รับจากโนดตรวจสอบและช่องสัญญาณ สำหรับรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) ค่าแอลแอลอาร์จากโนดตรวจสอบไปยังโนดตัวแปรจะมีค่าเฉลี่ย $\mathbf{m}$ และความแปรปรวนร่วมเกี่ยว $\mathbf{\Sigma}$ ตามสมการที่ 5.11 และสามารถคำนวณข่าวสารร่วมโดยการจำลองมอนติคาโลในสมการที่ 5.12 จากรูปที่ 5.9 จะสังเกตได้ว่าข่าวสารร่วมขึ้นอยู่กับค่าความแปรปรวนของค่าแอลแอลอาร์ ดังนั้น ในงานวิจัยนี้ จะกำหนดให้ $J_q(\sigma)$ คือฟังก์ชันการคำนวณข่าวสารร่วมที่มีอินพุตคือ σ และทำการประมาณข่าวสารร่วมในรูปที่ 5.9 ด้วยสมการพหุนาม ดังนี้

$$J_q(\sigma) \approx \begin{cases} a_{J,q,1}\sigma^3 + b_{J,q,1}\sigma^2 + c_{J,q,1}\sigma + d_{J,q,1}, & 0 \le \sigma \le \sigma_q^* \\ 1 - \exp\left(a_{J,q,2}\sigma^3 + b_{J,q,2}\sigma^2 + c_{J,q,2}\sigma + d_{J,q,2}\right), & \sigma_q^* < \sigma \le 7 \\ 1, & \sigma > 7 \end{cases} \qquad (5.14)$$

เมื่อสัมประสิทธิ์ของพหุนามแสดงในตารางที่ 5.7 นอกจากนี้ กำหนดให้ $J_q^{-1}(I)$ คืออินเวอร์สฟังก์ชันการคำนวณข่าวสารร่วมที่มีอินพุตคือ I ดังนี้

$$J_q^{-1}(I) \approx \begin{cases} 0, & I = 0 \\ a_{J^{-1},q,1}\left(\sqrt{I}\right)^3 + b_{J^{-1},q,1}\left(\sqrt{I}\right)^2 + c_{J^{-1},q,1}\sqrt{I} + d_{J^{-1},q,1}, & 0 < I \le I_q^* \\ a_{J^{-1},q,2}\left(\log(1-I)-I\right)^3 + b_{J^{-1},q,2}\left(\log(1-I)-I\right)^2 & \\ \quad + c_{J^{-1},q,2}\left(\log(1-I)-I\right) + d_{J^{-1},q,2}, & I_q^* < I < 1 \end{cases} \quad (5.15)$$

เมื่อสัมประสิทธิ์ของพหุนามแสดงในตารางที่ 5.8

ตารางที่ 5.7 พารามิเตอร์ของฟังก์ชัน $J_q(\sigma)$

q	2	4	8	16	32
σ_q^*	1.63	1.78	1.93	2.06	2.2
$a_{J,q,1}$	-0.0407	-0.0250	-0.0170	-0.0072	-0.0051
$b_{J,q,1}$	0.2064	0.1594	0.1290	0.0924	0.0786
$c_{J,q,1}$	-0.0053	-0.0082	-0.0106	-0.0022	-0.0045
$d_{J,q,1}$	0.0002	0.0006	0.0010	0.0002	0.0004
$a_{J,q,2}$	0.0016	0.0004	-0.00004	-0.0006	-0.0022
$b_{J,q,2}$	-0.1415	-0.1356	-0.1360	-0.1332	-0.1139
$c_{J,q,2}$	-0.0829	-0.0067	0.0865	0.1677	0.1715
$d_{J,q,2}$	0.0533	0.0080	-0.0751	-0.1728	-0.1848

ตารางที่ 5.8 พารามิเตอร์ของฟังก์ชัน $J_q^{-1}(\sigma)$

q	2	4	8	16	32
I_q^*	0.3637	0.3501	0.3388	0.3248	0.3166
$a_{J^{-1},q,1}$	1.3264	1.8479	2.5716	0.9815	1.6612
$b_{J^{-1},q,1}$	-0.3159	-0.9627	-1.7480	-0.3870	-1.1113
$c_{J^{-1},q,1}$	2.4184	2.9679	3.5278	3.5413	4.0481
$d_{J^{-1},q,1}$	-0.0045	-0.0180	-0.0316	-0.0114	-0.0162
$a_{J^{-1},q,2}$	-0.0021	-0.0030	-0.0043	-0.0063	-0.0095
$b_{J^{-1},q,2}$	-0.0632	-0.0788	-0.0977	-0.1237	-0.1633
$c_{J^{-1},q,2}$	-1.1609	-1.2355	-1.3168	-1.4235	-1.5742
$d_{J^{-1},q,2}$	0.7421	0.8853	1.0251	1.1366	1.2026

สำหรับค่าแอลแอลอาร์จากโนดตัวแปรไปยังโนดเทรลลิส จะคำนวณจากผลรวมของ ค่าแอลแอลอาร์ที่ได้รับจากโนดตรวจสอบ ยกเว้น ค่าแอลแอลอาร์ที่ได้รับจากช่องสัญญาณ (ค่าแอลแอลอาร์จากวงจรถอดรหัสแอลดีพีซีไปยังวงจรตรวจหาบีซีเจอาร์ จะใช้ข่าวสารเอ็กทรินซิต (extrinsic information)) ดังนั้น ค่าแอลแอลอาร์ที่ออกจากโนดตัวแปรไปยังโนดเทรลลิสจะมีความแปรปรวนเท่ากับ ผลรวมความแปรปรวนของค่าแอลแอลอาร์ที่ได้รับจากโนดตรวจสอบ ทำให้ข่าวสารร่วม $I_{\mathrm{A,T}}$ จากโนดตัวแปรไปยังโนดเทรลลิสคำนวณได้จากสมการต่อไปนี้

$$I_{\mathrm{A,T}} = \frac{1}{N}\sum_{j}\left(J_q\left(\sqrt{\sum_{j\in C_i} b_{j',i}\left[J_q^{-1}(I_{\mathrm{E,C}}(j',i))\right]^2}\right)\right) \tag{5.16}$$

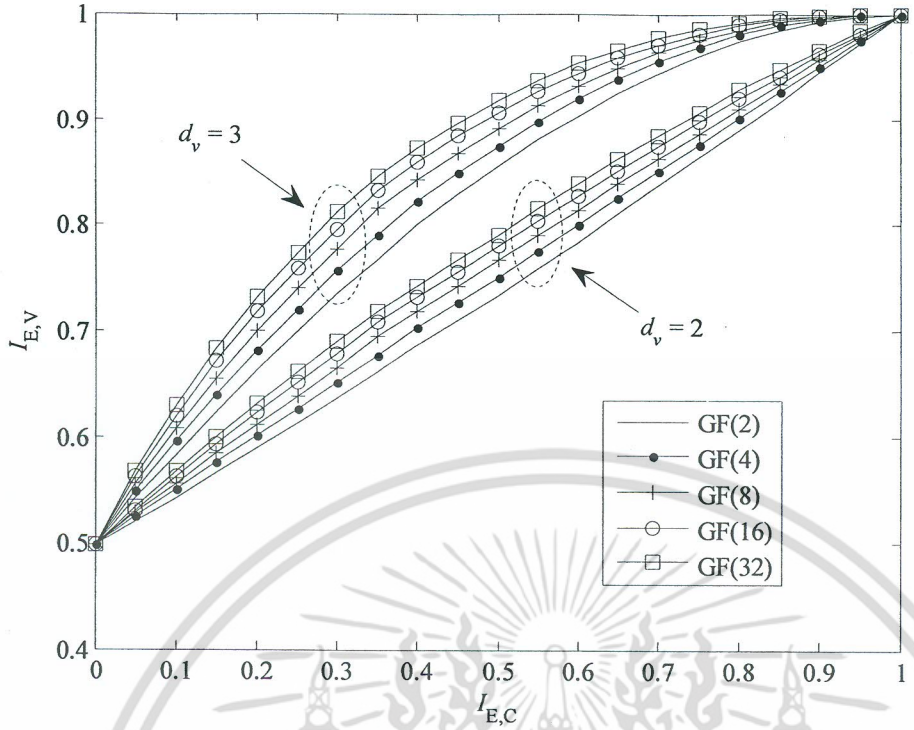
เมื่อ $J_q(.)$ และ $J_q^{-1}(.)$ คือฟังก์ชันข่าวสารร่วมในสมการที่ 5.14 และ 5.15 ตามลำดับ N คือ จำนวนโนดตัวแปร และ $b_{j,i}$ คือจำนวนเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i กับโนดตรวจสอบลำดับที่ j และ C_i คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปรลำดับที่ i

สำหรับค่าแอลแอลอาร์จากโนดตัวแปรไปยังโนดตรวจสอบ จะคำนวณจากผลรวมของค่าแอลแอลอาร์ที่ได้รับจากโนดตรวจสอบและช่องสัญญาณ ในกรณีนี้ ค่าแอลแอลอาร์ที่ได้รับจากช่องสัญญาณ คือ ค่าแอลแอลอาร์จากวงจรตรวจหาบีซีเจอาร์ การคำนวณข่าวสารร่วมจากโนดตัวแปรไปยังโนดตรวจสอบต้องใช้การจำลองมอนติคาโล โดยทำการวัดข่าวสารร่วมที่ออกจากโนดตัวแปรด้วยสมการที่ 5.11 กำหนดให้ $J_R(.)$ คือฟังก์ชันการคำนวณข่าวสารร่วมที่ประมาณได้จากการจำลองมอนติคาโล ดังนั้น ข่าวสารร่วม $I_{\mathrm{E,V}}(j,i)$ จากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j คำนวณได้จาก

$$I_{\mathrm{E,V}}(j,i) = J_R(\sigma_{\mathrm{A}}, \sigma_{\mathrm{E,T}}) \tag{5.17}$$

เมื่อ $\sigma_{\mathrm{E,T}}$ คือค่าเบี่ยงเบนมาตรฐานของค่าแอลแอลอาร์จากวงจรตรวจหาบีซีเจอาร์ (กรณีโนดตัวแปรถูกพังก์เชอร์จะปราศจากค่าแอลแอลอาร์จากวงจรตรวจหาบีซีเจอาร์ หรือค่าความเบี่ยงเบนมาตรฐานเท่ากับ $\sigma_{\mathrm{E,T}} = 0$) อย่างไรก็ตาม ค่าแอลแอลอาร์จากวงจรตรวจหาบีซีเจอาร์จะอยู่บนฟีลด์จำกัด GF(2) ทำให้ การจำลองมอนติคาโล ค่าแอลแอลอาร์บนฟีลด์จำกัด GF(2) จะถูกแปลงเป็นค่าแอลแอลอาร์บนฟีลด์จำกัด GF(q) เพื่อทำการบวกกับค่าแอลแอลอาร์ที่ได้รับจากโนดตรวจสอบซึ่งมีค่าเบี่ยงเบนมาตรฐานเท่ากับสมการที่ 5.18

$$\sigma_{\mathrm{A}} = \sqrt{\sum_{j'\in C_i\setminus j} b_{j',i}\left[J_q^{-1}(I_{\mathrm{E,C}}(j',i))\right]^2 + (b_{j,i}-1)\left[J_q^{-1}(I_{\mathrm{E,C}}(j,i))\right]^2} \tag{5.18}$$



รูปที่ 5.14 ข่าวสารร่วม $I_{E,V}$

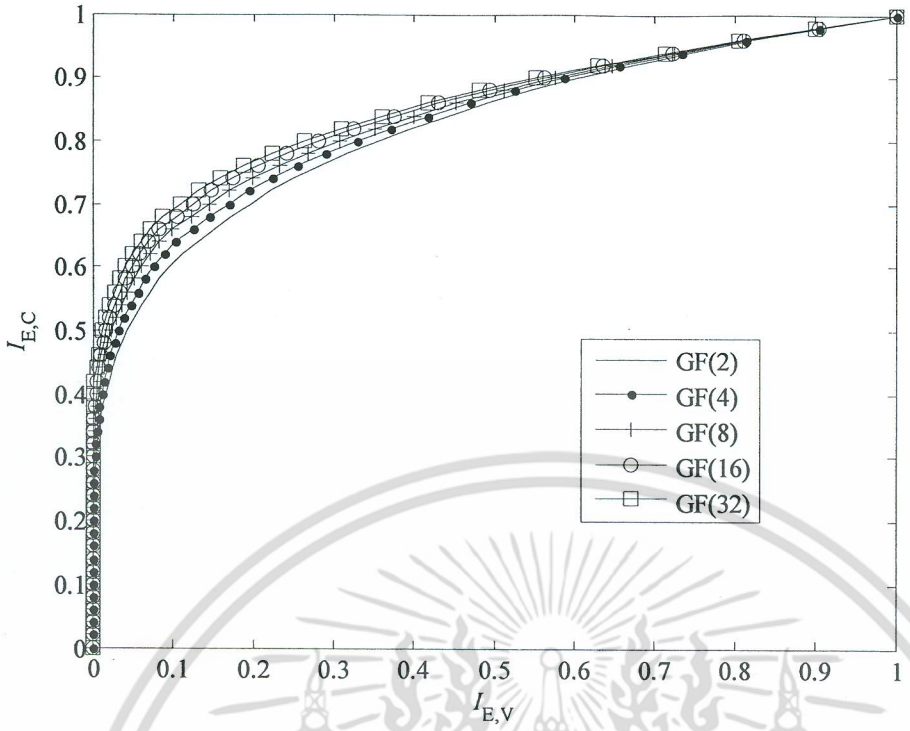
เมื่อ $J_q(.)$ และ $J_q^{-1}(.)$ คือฟังก์ชันข่าวสารร่วมในสมการที่ 5.14 และ 5.15 ตามลำดับ และ $b_{j,i}$ คือจำนวนเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i กับโนดตรวจสอบลำดับที่ j และ $C_i \setminus j$ คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปรลำดับที่ i ยกเว้นโนดตรวจสอบลำดับที่ j

รูปที่ 5.14 แสดงข่าวสารร่วม $I_{E,V}$ ที่ออกจากโนดตัวแปรของรหัสโปรโตกราฟสม่ำเสมอ ซึ่งมี $d_v = 3$ และ $d_v = 4$ โดยเมทริกซ์ฐานของรหัสโปรโตกราฟแสดงในสมการที่ 4.84 และ 4.85 (บทที่ 4) ตามลำดับ และกำหนดให้ข่าวสารร่วมจากโนดเทรลลิสเท่ากับ $I_{E,T} = 0.5$ จากรูปจะสังเกตได้ว่า เมื่อข่าวสารร่วมที่ได้รับจากโนดตรวจสอบเท่ากับ $I_{E,C} = 0$ หรือปราศจากข่าวสารจากโนดตรวจสอบ จะทำให้ข่าวสารร่วมที่ออกจากโนดตัวแปรเท่ากับ $I_{E,V} = 0.5$ และเมื่อข่าวสารร่วมที่ได้รับจากโนดตรวจสอบเพิ่มขึ้น จะทำให้ข่าวสารร่วมที่ออกจากโนดตัวแปรเพิ่มขึ้น นอกจากนี้ เมื่อจำนวนเส้นเชื่อมของโนดตัวแปร d_v เพิ่มขึ้น หรือค่าฟิลด์จำกัด GF(q) เพิ่มขึ้น จะทำให้ข่าวสารร่วมที่ออกจากโนดตัวแปรเพิ่มขึ้นเช่นกัน

5.3.2.3 ข่าวสารร่วมของโนดตรวจสอบ

จากความสัมพันธ์ในสมการที่ 4.77 ทำให้ ข่าวสารร่วม $I_{E,C}(j,i)$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i คำนวณได้จาก

$$I_{E,C}(j,i) = 1 - J_q\left(\sqrt{\sum_{i' \in V_j \setminus i} b_{j,i'}\left[J_q^{-1}(1 - I_{E,V}(j,i'))\right]^2 + (b_{j,i} - 1)\left[J_q^{-1}(1 - I_{E,V}(j,i))\right]^2}\right) \quad (5.19)$$



รูปที่ 5.15 ข่าวสารร่วม $I_{E,C}$

เมื่อ $J_q(.)$ และ $J_q^{-1}(.)$ คือฟังก์ชันข่าวสารร่วมในสมการที่ 5.14 และ 5.15 ตามลำดับ และ $b_{j,i}$ คือ จำนวนเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i กับโนดตรวจสอบลำดับที่ j และ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบลำดับที่ j ยกเว้นโนดตัวแปรลำดับที่ i

รูปที่ 5.15 แสดงข่าวสารร่วม $I_{E,C}$ ที่ออกจากโนดตรวจสอบของรหัสโปรโตกราฟบนฟีลด์จำกัด GF(q) จากรูปจะสังเกตได้ว่า เมื่อข่าวสารร่วมที่ได้รับจากโนดตัวแปรเท่ากับ $I_{E,V} = 0$ หรือปราศจากข่าวสารจากโนดตัวแปร จะทำให้ข่าวสารร่วมที่ออกจากตรวจสอบเท่ากับ $I_{E,C} = 0$ และเมื่อข่าวสารร่วมที่ได้รับจากโนดตัวแปรเพิ่มขึ้นจะทำให้ข่าวสารร่วมที่ออกจากโนดตรวจสอบเพิ่มขึ้น

5.3.2.4 การวิเคราะห์เอ็กซิตชาร์ท

การวิเคราะห์รหัสโปรโตกราฟบนฟีลด์จำกัด GF(q) สำหรับช่องสัญญาณผลตอบสนองบางส่วน จะเริ่มจากกำหนดประเภทของช่องสัญญาณ $H(D)$ และค่าเอสเอ็นอาร์ของช่องสัญญาณ จากนั้นคำนวณข่าวสารร่วมในรูปที่ 5.11 จนกระทั่ง ข่าวสารร่วมมีค่าคงที่ โดยเทรสโฮลด์ของรหัสโปรโตกราฟจะมีค่าเท่ากับเอสเอ็นอาร์ต่ำสุดที่ทำให้ข่าวสารร่วม $I_{APP}(i)$ ในสมการที่ 5.20 มีค่าเท่ากับ 1 เมื่อ i มีค่าใดๆ

$$I_{APP}(i) = J_R(\sigma_A, \sigma_{E,T}) \tag{5.20}$$

โดยที่ $J_R(.)$ คือฟังก์ชันการคำนวณข่าวสารร่วมในสมการที่ 5.17 ในที่นี้ ค่าเบี่ยงเบนมาตรฐาน σ_{A} คำนวณจากสมการต่อไปนี้

$$\sigma_{\mathrm{A}} = \sqrt{\sum_{j' \in C_i} b_{j',i} \left[J_q^{-1}(I_{\mathrm{E,C}}(j',i)) \right]^2} \tag{5.21}$$

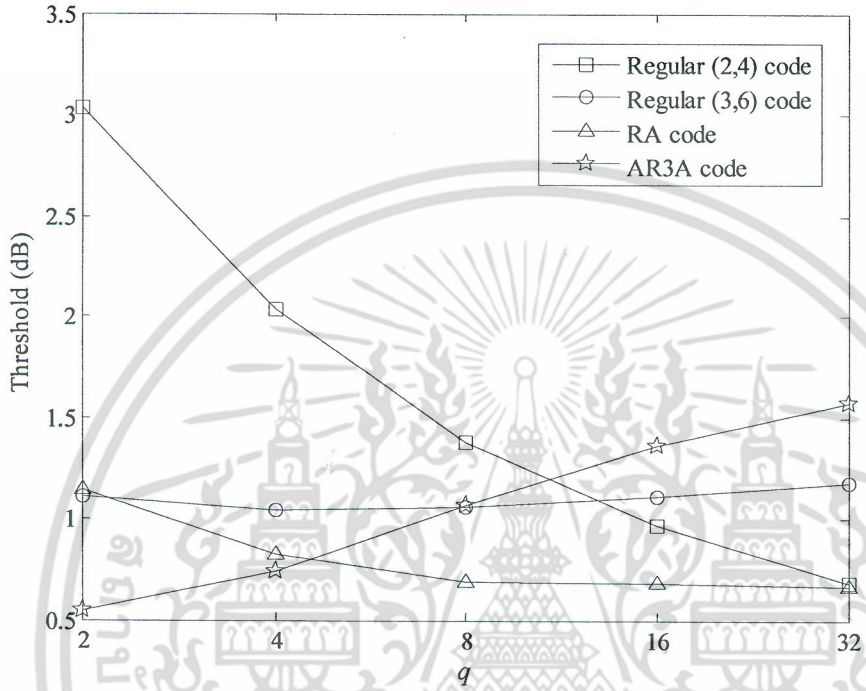
เมื่อ $J_q(.)$ และ $J_q^{-1}(.)$ คือฟังก์ชันข่าวสารร่วมในสมการที่ 5.14 และ 5.15 ตามลำดับ และ $b_{j,i}$ คือ จำนวนเส้นเชื่อมระหว่างโนดตัวแปรลำดับที่ i กับโนดตรวจสอบลำดับที่ j และ C_i คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปรลำดับที่ i

5.3.3 ผลการจำลองสมรรถนะรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน

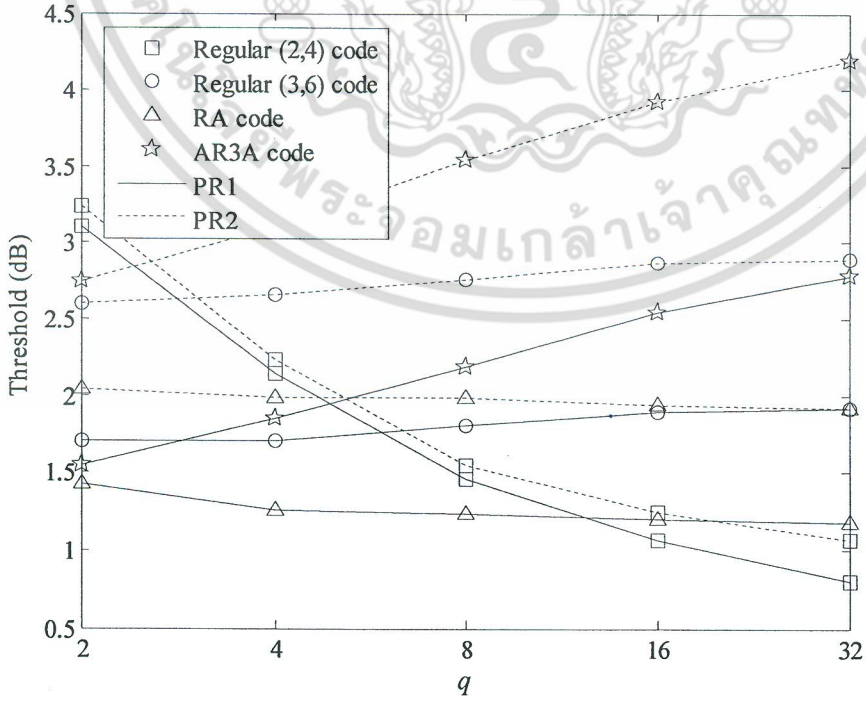
พิจารณารหัสโปรโตกราฟ อัตรารหัสเท่ากับ 1/2 ได้แก่ รหัสสม่ำเสมอซึ่งมี $d_v = 3$ และ $d_v = 4$ รหัสอาร์เอ (repeat-accumulate code, RA code) และรหัสเออาร์สามเอ (accumulate repeat-accumulate code, AR3A code) [44] ซึ่งมีเมทริกซ์ฐานแสดงในสมการที่ 4.84-4.87 (บทที่ 4) รูปที่ 5.16 แสดงค่าเทรสโฮลด์ของรหัสโปรโตกราฟในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต กรณีฟิลด์จำกัด GF(2) รหัสโปรโตกราฟแบบสม่ำเสมอ $d_v = 3$ จะมีค่าเทรสโฮลด์ต่ำกว่ารหัสแบบสม่ำเสมอ $d_v = 2$ สำหรับรหัสเออาร์สามเอซึ่งจัดเป็นรหัสโปรโตกราฟแบบไม่สม่ำเสมอชนิดหนึ่งจะมีค่า เทรสโฮลด์ต่ำกว่ารหัสแบบสม่ำเสมอ และเมื่อฟิลด์จำกัดเพิ่มขึ้น รหัสสม่ำเสมอ $d_v = 2$ จะมีค่าเทรสโฮลด์ลดลง ต่างจากรหัสสม่ำเสมอ $d_v = 3$ ซึ่งค่าเทรสโฮลด์จะลดลงจนกระทั่งฟิลด์จำกัดมีค่าเท่ากับ GF(8) จากนั้นค่าเทรสโฮลด์จะเพิ่มขึ้น ค่าเทรสโฮลด์ของรหัสสม่ำเสมอนี้ สามารถใช้อธิบายอัตราบิตผิดพลาดในรูปที่ 3.5 และ 3.6 (บทที่ 3) จากรูปที่ 5.16 จะสังเกตได้ว่ารหัสเออาร์สามเอมีค่าเทรสโฮลด์ต่ำสุดเมื่อเทียบกับรหัสอื่นๆ เมื่อฟิลด์จำกัดคือ GF(2) และ GF(4) สำหรับฟิลด์จำกัด GF(8) GF(16) และ GF(32) รหัสอาร์เอจะให้ค่าเทรสโฮลด์ต่ำสุด

รูปที่ 5.17 แสดงค่าเทรสโฮลด์ของรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน โดยพบว่า รหัสเออาร์สามเอบนฟิลด์จำกัด GF(2) และ GF(4) ซึ่งมีค่าเทรสโฮลด์ต่ำสุดในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต จะมีค่าเทรสโฮลด์สูงกว่ารหัสอื่นๆ ในช่องสัญญาณผลตอบสนองบางส่วน ดังนั้น รหัสแอลดีพีซีที่ให้สมรรถนะดีในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต อาจจะให้สมรรถนะที่แย่ในช่องสัญญาณผลตอบสนองบางส่วน นอกจากนี้ ช่องสัญญาณผลตอบสนองบางส่วนแบบ PR2 จะทำให้ค่าเทรสโฮลด์ของรหัสต่างๆ สูงกว่าช่องสัญญาณเป็นแบบ PR1 โดยรหัสสม่ำเสมอ $d_v = 3$, รหัสสม่ำเสมอ $d_v = 4$, รหัสอาร์เอ และรหัสเออาร์สามเอ จะมีค่าเทรสโฮลด์เพิ่มขึ้น 0.95, 0.152, 0.716 และ 1.32 dB ตามลำดับ ทำให้ กรณีฟิลด์จำกัด GF(8) รหัสอาร์เอซึ่งมีค่าเทรสโฮลด์ต่ำสุดในช่องสัญญาณ PR1 จะมีเทรสโฮลด์สูงกว่ารหัสสม่ำเสมอ $d_v = 2$ ในช่องสัญญาณ PR2 รูปที่ 5.16 แสดงอัตราเฟรมผิดพลาดของรหัสโปรโตกราฟในช่องสัญญาณ

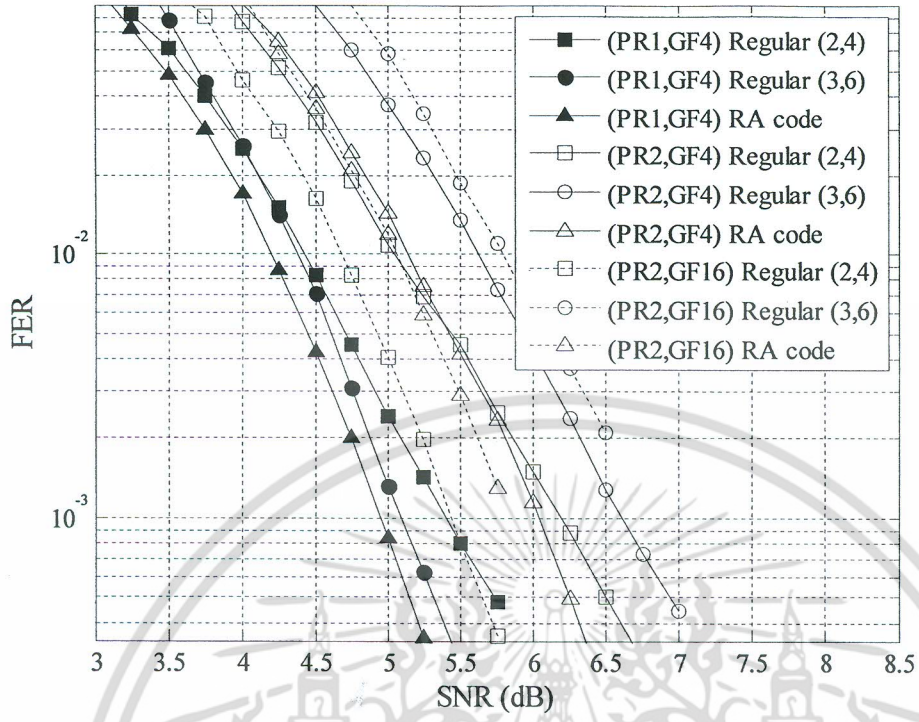
ผลตอบสนองบางส่วน เมื่อกำหนดให้ กรณีฟิลด์จำกัด GF(4) และ GF(16) ใช้จำนวนการคัดลอกของกราฟเท่ากับ 16 และ 8 ครั้ง ตามลำดับ และจำนวนการถอดรหัสวนซ้ำของวงจรถอดรหัสเทอร์โบอีควอไลเซชันและวงจรถอดรหัสแอลดีพีซีเท่ากับ 10 และ 20 รอบ ตามลำดับ อัตราบิตผิดพลาดของรหัสโปรโตกราฟจะสอดคล้องกับค่าเทรสโฮลด์ที่แสดงในรูปที่ 5.18



รูปที่ 5.16 เทรสโฮลด์ของรหัสโปรโตกราฟในช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุต



รูปที่ 5.17 เทรสโฮลด์ของรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน



รูปที่ 5.18 อัตราเฟรมผิดพลาดของรหัสโปรโตกราฟในช่องสัญญาณผลตอบสนองบางส่วน

บทที่ 6
การปรับปรุงสมรรถนะของการถอดรหัสแอลดีพีซี

ในบทนี้ จะอธิบายงานวิจัยของวิทยานิพนธ์ซึ่งเกี่ยวข้องกับการถอดรหัสแอลดีพีซี โดยหัวข้อแรกจะนำเสนอวิธีการกระจายความเชื่อมั่นสองทิศทางสำหรับอัลกอริทึมกระจายความเชื่อมั่น (belief propagation algorithm) ของรหัสแอลดีพีซี นอกจากนี้ จะแสดงวิธีการวิเคราะห์สมรรถนะด้วยวิธีการเอ็กซิตชาร์ท (extrinsic information transfer charts, EXIT charts) หัวข้อถัดไป นำเสนออัลกอริทึมการถอดรหัสสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก โดยวิธีการถอดรหัสที่ได้นำเสนอทั้ง 2 หัวข้อ สามารถประยุกต์ใช้กับรหัสนอนไบนารีแอลดีพีซีที่ได้รับความนิยมในปัจจุบัน และในหัวข้อสุดท้าย อธิบายการถอดรหัสแอลดีพีซีแบบสองมิติสำหรับระบบบันทึกข้อมูลเชิงแม่เหล็กและระบบบันทึกข้อมูลแบบแฟลช (flash memory) รวมถึงแสดงการวิเคราะห์สมรรถนะของการถอดรหัสที่ได้นำเสนอ

6.1 การถอดรหัสกระจายความเชื่อมั่นสองทิศทาง

ในหัวข้อที่ 4.3 (บทที่ 4) อธิบายการกระจายข่าวสารเรียงลำดับแบบเลเยอร์และชัฟเฟิล โดยจะเห็นว่าวิธีการกระจายข่าวสารแบบเลเยอร์และชัฟเฟิล ให้สมรรถนะที่ดีกว่าอัลกอริทึมการถอดรหัสแอลดีพีซีแบบทั่วไป ในงานวิจัย [13] ได้นำเสนอการกระจายความเชื่อมั่นสองทิศทางสำหรับการกระจายข่าวสารเรียงลำดับแบบชัฟเฟิล โดยประยุกต์ใช้ข่าวสารที่ได้จากการถอดรหัสที่มีลำดับของการคำนวณข่าวสารแตกต่างกัน ทำให้ สมรรถนะของการถอดรหัสแอลดีพีซีเพิ่มสูงขึ้น อย่างไรก็ตาม การออกแบบวงจรถอดรหัสที่ใช้อัลกอริทึมแบบชัฟเฟิลจะมีความซับซ้อนมากกว่าอัลกอริทึมแบบเลเยอร์ [15] ทำให้ ในงานวิจัยนี้ สนใจการประยุกต์ใช้ข่าวสารที่ได้จากกระจายความเชื่อมั่นสองทิศทางสำหรับอัลกอริทึมแบบเลเยอร์

พิจารณาอัลกอริทึมกระจายความเชื่อมั่นแบบอัตราส่วนความน่าจะเป็นแบบล็อกในหัวข้อที่ 4.2 (บทที่ 4) เพื่อความสะดวกในการอธิบาย ในบทนี้จะกำหนดให้ $V_{ij}^{(l)}$ แทนความเชื่อมั่น $L(q_{ij})$ ที่ออกจากโนดตัวแปรในการถอดรหัสวนซ้ำลำดับที่ l และ $C_{ji}^{(l)}$ แทนความเชื่อมั่น $L(r_{ij})$ ที่ออกจากโนดตรวจสอบในการถอดรหัสวนซ้ำลำดับที่ l ดังนั้น ความเชื่อมั่นในรูปอัตราส่วนความน่าจะเป็นแบบล็อกที่ออกจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j เขียนใหม่ได้เป็น

$$V_{ij}^{(l)} = Y_i + \sum_{j' \in C_i \setminus j} C_{j'i}^{(l-1)} \tag{6.1}$$

เมื่อ Y_i คือความเชื่อมั่นที่ได้รับจากช่องสัญญาณ และความเชื่อมั่นที่ออกจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i แสดงได้ดังนี้

$$C_{ji}^{(l)} = 2\tanh^{-1}\left(\prod_{i' \in V_j \setminus i} \tanh\left(\frac{V_{i'j}^{(l)}}{2}\right)\right) \tag{6.2}$$

จากสมการที่ 6.1 จะสังเกตได้ว่า ความเชื่อมั่นที่ออกจากโนดตัวแปรในการถอดรหัสวนซ้ำลำดับที่ l คำนวณได้จากความเชื่อมั่นที่ได้รับจากช่องสัญญาณ และความเชื่อมั่นที่ได้รับจากโนดตรวจสอบของการถอดรหัสวนซ้ำลำดับที่ $l-1$

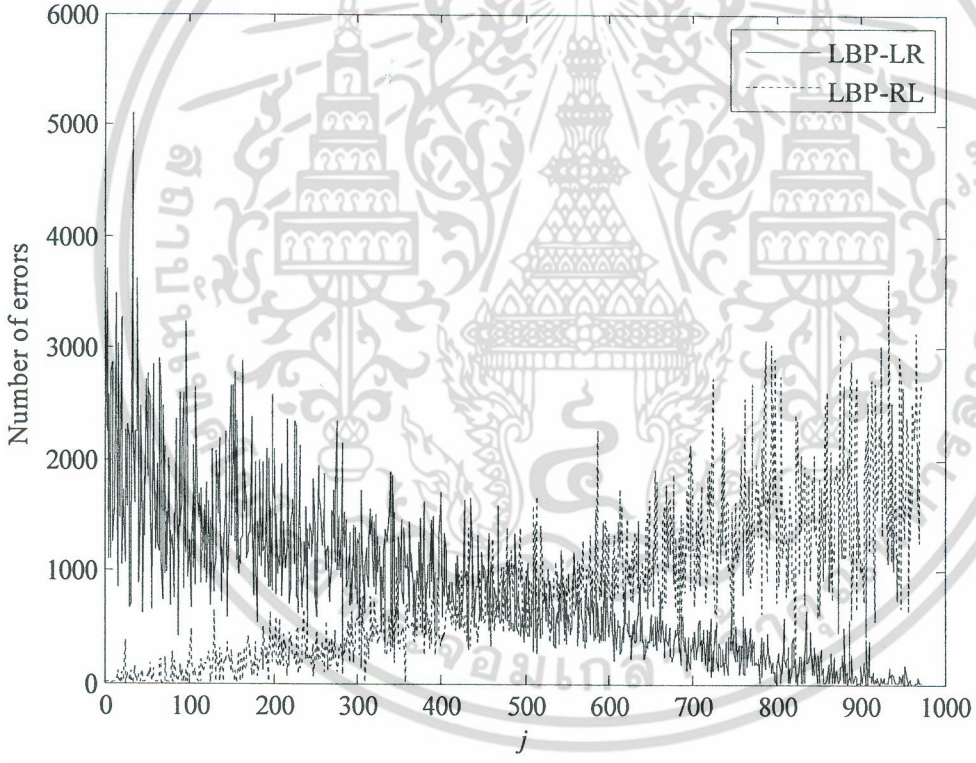
ในหัวข้อที่ 4.3 (บทที่ 4) อธิบายลำดับการกระจายความเชื่อมั่นของการถอดรหัสแอลดีพีซี โดยลำดับแบบเลเยอร์ หรือ อัลกอริทึมแอลบีพี (layered belief propagation, LBP) การคำนวณความเชื่อมั่นที่ออกจากโนดตัวแปรในการถอดรหัสวนซ้ำลำดับที่ l จะเกี่ยวข้องกับความเชื่อมั่นของโนดตรวจสอบของการถอดรหัสวนซ้ำลำดับที่ $l-1$ และ l (สังเกตได้จากรูปที่ 4.5) ดังนั้น ความเชื่อมั่นที่ออกจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j ของอัลกอริทึมแอลบีพี สามารถเขียนอยู่ในรูปสมการได้ ดังนี้

$$V_{ij}^{(l)} = Y_i + \sum_{\substack{j' \in C_i \setminus j \\ j' > j}} C_{j'i}^{(l-1)} + \sum_{\substack{j' \in C_i \setminus j \\ j' < j}} C_{j'i}^{(l)} \tag{6.3}$$

ทำให้ ข่าวสารในกราฟแทนเนอร์ของอัลกอริทึมแอลบีพีแตกต่างจากอัลกอริทึมการถอดรหัสแอลดีพีซีแบบทั่วไปหรืออัลกอริทึมบีพี (belief propagation, BP) โดยอัตราบิตผิดพลาดที่ได้จากการถอดรหัสด้วยอัลกอริทึมแอลบีพีจะต่ำกว่าอัลกอริทึมบีพีดังรูปที่ 4.7 (บทที่ 4) นอกจากนี้ วงจรถอดรหัสของอัลกอริทึมแอลบีพีจะมีความซับซ้อนใกล้เคียงกับวงจรการถอดรหัสบีพี [40]

ในการกระจายข่าวสารเรียงลำดับแบบเลเยอร์หรืออัลกอริทึมแอลบีพี ข่าวสารในกราฟแทนเนอร์จะถูกคำนวณโดยเริ่มจากโนดตรวจสอบลำดับที่หนึ่งไป ยังโนดตรวจสอบลำดับสุดท้าย ในทางกลับกัน สามารถคำนวณโดยเริ่มจากโนดตรวจสอบลำดับสุดท้ายไปยังโนดตรวจสอบลำดับที่หนึ่งก็ได้ รูปที่ 6.1 แสดงจำนวนครั้งที่เกิดความผิดพลาดของโนดตรวจสอบลำดับที่ j (ความผิดพลาดของโนดตรวจสอบ นิยามด้วยสมการ $\mathbf{c}.\mathbf{H}^T \neq \mathbf{0}$ หรือซินโดรม (syndrome) ของการถอดรหัส) ในการส่งคำรหัสจำนวน 1,000,000 ชุด ผ่านช่องสัญญาณรบกวนเกาส์สีขาวบวกไบนารีอินพุตซึ่งมีค่าเอสเอ็นอาร์เท่ากับ 4 dB โดยกำหนดให้รหัสแอลดีพีซีมีความยาวคำรหัสเท่ากับ 1944 บิต และอัตรารหัสเท่ากับ 1/2 ตามมาตรฐานการสื่อสารไร้สาย IEEE 802.11n [45] และมีดีกรีของโนดตัวแปรเท่ากับ 3 จำนวนการถอดรหัสวนซ้ำเท่ากับ 2 รอบ จากรูปจะสังเกตว่าอัลกอริทึมแอลบีพี-แอลอาร์ (LBP-LR) ซึ่งเริ่มคำนวณข่าวสารจากโนดตรวจสอบลำดับที่หนึ่งไปยังโนดตรวจสอบลำดับสุดท้าย

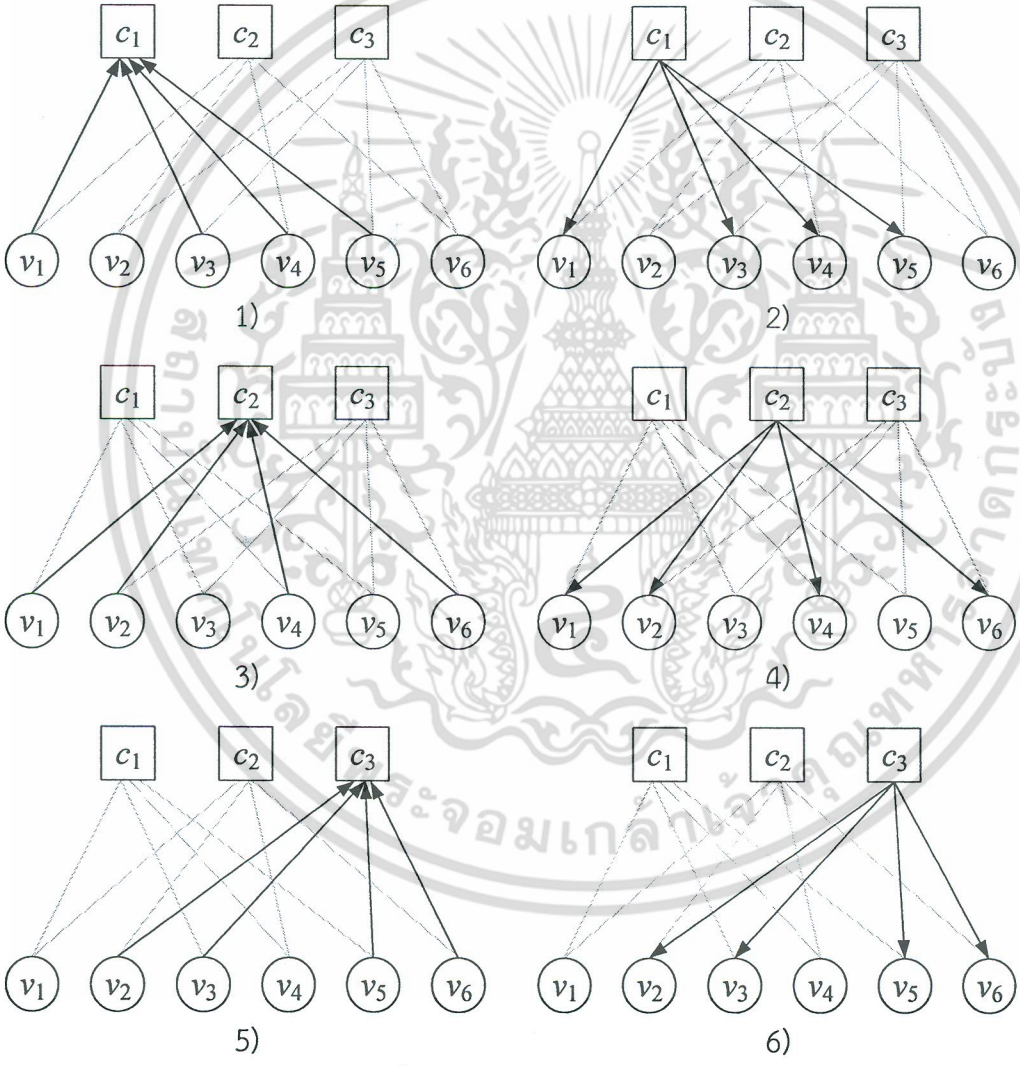
(จากโนดตรวจสอบด้านซ้ายไปยังโนดตรวจสอบด้านขวาในกราฟแทนเนอร์) จำนวนความผิดพลาดของโนดตรวจสอบจะลดลงตามลำดับ เช่นเดียวกับ อัลกอริทึมแอลบีพี-อาร์แอล (LBP-RL) ซึ่งเริ่มคำนวณข่าวสารจากโนดตรวจสอบลำดับสุดท้ายไปยังโนดตรวจสอบลำดับที่หนึ่ง (จากโนดตรวจสอบด้านขวาไปยังโนดตรวจสอบด้านซ้ายในกราฟแทนเนอร์) ทำให้ ในงานวิจัยนี้นำเสนอการประยุกต์ใช้ข่าวสารที่ได้จากการกระจายความเชื่อมั่นสองทิศทาง (จากโนดตรวจสอบด้านซ้ายไปยังโนดตรวจสอบด้านขวา และ จากโนดตรวจสอบด้านขวาไปยังโนดตรวจสอบด้านซ้าย) สำหรับการถอดรหัสด้วยอัลกอริทึมแอลบีพี โดยการถอดรหัสแอลดีพีซีที่นำเสนอนี้ เรียกว่า อัลกอริทึมเอ็มบีพี (mixed scheduling for belief-propagation: MBP) ซึ่งแบ่งเป็นกรณีที่ไม่มีการซิงโครไนซ์ (synchro nization) และกรณีที่มีการซิงโครไนซ์ของวงจรถอดรหัสแอลดีพีซี



รูปที่ 6.1 จำนวนความผิดพลาดของโนดตรวจสอบในการถอดรหัสข้อมูล 1,000,000 ชุด

6.1.1 อัลกอริทึมเอ็มบีพี

พิจารณาการถอดรหัสแอลบีพีทิศทางจากซ้ายไปขวาในรูปที่ 6.2 ขั้นตอนการถอดรหัสจะเริ่มต้นจากการคำนวณข่าวสารจากโนดตัวแปร v_1, v_3, v_4, v_5 ไปยังโนดตรวจสอบ c_1 จากนั้นคำนวณข่าวสารจากโนดตรวจสอบ c_1 กลับไปยังโนดตัวแปร ขั้นตอนต่อไปเป็นการคำนวณข่าวสารจากโนดตัวแปร v_1, v_2, v_4, v_6 ไปยังโนดตรวจสอบ c_2 ในที่นี้ จะสังเกตได้ว่า โนดตัวแปร v_1, v_6 ได้รับข่าวสารจากโนดตรวจสอบ c_1 ในการคำนวณขั้นตอนแรก ทำให้ โนดตรวจสอบ c_2 ได้รับข่าวสารจากโนดตรวจสอบ c_1 สำหรับการคำนวณข่าวสารจากโนดตรวจสอบ c_3 จะใช้ข่าวสารจากโนดตรวจสอบ c_2 ผ่านทางโนดตัวแปร v_2, v_6 และโนดตรวจสอบ c_1 ผ่านทางโนดตัวแปร v_3, v_5



รูปที่ 6.2 อัลกอริทึมแอลบีพี

1) LBP-LR 2) LBP-RL

รูปที่ 6.3 การส่งผ่านข่าวสารของอัลกอริทึมแอลบีพี

ดังนั้น สามารถเขียนความสัมพันธ์ของโนดตรวจสอบในกระบวนการถอดรหัสแอลบีพีทิศทางจากซ้ายไปขวาดังรูปที่ 6.3 (1) ในทางกลับกัน การถอดรหัสแอลบีพีทิศทางจากขวาไปซ้าย ข่าวสารจากโนดตรวจสอบ c_3 จะถูกส่งไปยังโนดตรวจสอบ c_1, c_2 ดังรูปที่ 6.2 (2) จากตรงนี้ จะสังเกตได้ว่าการส่งผ่านข่าวสารจากซ้ายไปขวาทำให้โนดตรวจสอบ c_2 ได้รับข่าวสารจากโนดตรวจสอบ c_1 ต่างจากการส่งผ่านข่าวสารจากขวาไปซ้ายซึ่งทำให้โนดตรวจสอบ c_2 ได้รับข่าวสารจากโนดตรวจสอบ c_3 ทั้งนี้ อาจกล่าวได้ว่า ในกระบวนการถอดรหัสแอลบีพีทิศทางจากซ้ายไปขวาจะทำให้โนดตรวจสอบที่อยู่ด้านขวาได้รับข่าวสารจากโนดตรวจสอบที่อยู่ด้านซ้ายในปริมาณที่มาก ต่างจากการถอดรหัสแอลบีพีทิศทางจากขวาไปซ้าย โนดตรวจสอบที่อยู่ด้านขวาจะได้รับข่าวสารจากโนดตรวจสอบที่อยู่ด้านซ้ายในปริมาณที่น้อย ทำให้การถอดรหัสทั้งสองมีความผิดพลาดของโนดตรวจสอบแตกต่างกันดังรูปที่ 6.1

ความผิดพลาดของโนดตรวจสอบที่แตกต่างกันของการถอดรหัสด้วยอัลกอริทึมแอลบีพี ทำให้คำรหัสที่ได้จากการถอดรหัสแอลบีพี-แอลอาร์ และแอลบีพี-อาร์แอล มีตำแหน่งของบิตผิดพลาดแตกต่างกัน ดังนั้น ในงานวิจัยนี้ จึงนำเสนอการประยุกต์ใช้ข่าวสารที่ได้จากการถอดรหัสแอลบีพีทั้งสองทิศทาง โดยการถอดรหัสแอลดีพีซีที่นำเสนอนี้ เรียกว่า อัลกอริทึมเอ็มบีพี (mixed scheduling for belief-propagation: MBP) ซึ่งแบ่งเป็นกรณีที่ไม่มีการซิงโครไนซ์ (synchronization) และกรณีที่มีการซิงโครไนซ์ระหว่างกระบวนการถอดรหัส กำหนดให้ $\vec{V}_{ij}^{(l)}$ และ $\overleftarrow{V}_{ij}^{(l)}$ แทนความเชื่อมั่นที่ออกจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j ของการถอดรหัสแอลบีพีจากทางด้านซ้ายไปขวาและขวาไปซ้าย ตามลำดับ และ $\vec{C}_{ji}^{(l)}$ และ $\overleftarrow{C}_{ji}^{(l)}$ แทนความเชื่อมั่นที่ออกจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i ของการถอดรหัสแอลบีพีจากทางด้านซ้ายไปขวา และขวาไปซ้าย โดย $1 \le i \le N$ และ $1 \le j \le N-K$ เมื่อ N คือจำนวนบิตคำรหัส และ K คือจำนวนบิตข้อมูล ขั้นตอนการถอดรหัสด้วยอัลกอริทึมเอ็มบีพีกรณีไม่มีการซิงโครไนซ์ แสดงได้ดังนี้

1) การคำนวณข่าวสารที่ได้รับจากช่องสัญญาณ

กำหนดให้ลำดับการวนซ้ำเท่ากับ $l=1$ และจำนวนการวนซ้ำสูงสุดเท่ากับ $I_{\max}$ โดยข่าวสาร Y_i คำนวณได้จากอัตราส่วนความน่าจะเป็นแบบล็อกของสัญญาณที่ได้รับ y_i จากช่องสัญญาณในบทที่ 2

2) การคำนวณข่าวสารของโนดตัวแปรและโนดตรวจสอบ

ข่าวสารจะถูกแพร่กระจายตามลำดับของโนดตรวจสอบ ตัวอย่างเช่น การแพร่กระจายทิศทางจากซ้ายไปขวาในรูปที่ 4.5 (บทที่ 4) โดยการวนซ้ำลำดับที่ l ข่าวสาร $\vec{V}_{ij}^{(l)}$ และ $\vec{V}_{ij}^{(l)}$ ที่ออกจากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบลำดับที่ j คำนวณได้จากข่าวสารที่ได้รับจากช่องสัญญาณและโนดตรวจสอบในการวนซ้ำลำดับที่ l และ $l-1$ ตามสมการดังต่อไปนี้

$$\vec{V}_{ij}^{(l)} = Y_i + \sum_{\substack{j' \in C_i \setminus j \\ j' > j}} \vec{C}_{j'i}^{(l-1)} + \sum_{\substack{j' \in C_i \setminus j \\ j' < j}} \vec{C}_{j'i}^{(l)} \tag{6.4}$$

$$\vec{V}_{ij}^{(l)} = Y_i + \sum_{\substack{j' \in C_i \setminus j \\ j' > j}} \vec{C}_{j'i}^{(l-1)} + \sum_{\substack{j' \in C_i \setminus j \\ j' < j}} \vec{C}_{j'i}^{(l)} \tag{6.5}$$

เมื่อ $C_i \setminus j$ คือเซตของโนดตรวจสอบที่มีเส้นเชื่อมไปยังโนดตัวแปรลำดับที่ i ยกเว้นโนดตรวจสอบลำดับที่ j โดยที่การวนซ้ำลำดับที่ $l=1$ กำหนดให้ข่าวสาร $\vec{C}_{j'i}^{(l-1)} = \vec{C}_{j'i}^{(l-1)} = 0$ เสมอ

สำหรับข่าวสาร $\vec{C}_{ji}^{(l)}$ และ $\vec{C}_{ji}^{(l)}$ ที่ออกจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i คำนวณได้จากข่าวสารที่ได้รับจากโนดตัวแปรในการวนซ้ำลำดับที่ l ตามสมการดังต่อไปนี้

$$\vec{C}_{ji}^{(l)} = 2\tanh^{-1}\left(\prod_{i' \in V_j \setminus i} \tanh\left(\frac{\vec{V}_{i'j}^{(l)}}{2} \right) \right) \tag{6.6}$$

$$\vec{C}_{ji}^{(l)} = 2\tanh^{-1}\left(\prod_{i' \in V_j \setminus i} \tanh\left(\frac{\vec{V}_{i'j}^{(l)}}{2} \right) \right) \tag{6.7}$$

เมื่อ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบลำดับที่ j ยกเว้นโนดตัวแปรลำดับที่ i

3) การตัดสินใจคำรหัส

สำหรับข่าวสารในรูปอัตราส่วนความน่าจะเป็นแบบล็อกของคำรหัสลำดับที่ i คำนวณได้จากข่าวสารที่ได้รับจากช่องสัญญาณและโนดตรวจสอบตามสมการต่อไปนี้

$$W_i^{(l)} = 2Y_i + \sum_{j' \in C_i \setminus j} \vec{C}_{j'i}^{(l)} + \sum_{j' \in C_i \setminus j} \vec{C}_{j'i}^{(l)} \tag{6.8}$$

และทำการตัดสินใจคำรหัสที่ได้จากการถอดรหัสวนซ้ำลำดับที่ l จากสมการต่อไปนี้

$$\hat{v}_i = \begin{cases} 1\ , & W_i < 0 \\ 0\ , & W_i > 0 \end{cases} \tag{6.9}$$

4) การทำซ้ำ

เมื่อ $\hat{\mathbf{v}}.\mathbf{H}^{\mathrm{T}} = \mathbf{0}$ หรือ $l = l_{\max}$ ให้จบขั้นตอนการถอดรหัส ไม่เช่นนั้น กำหนดให้ $l = l + 1$ และทำซ้ำขั้นตอนที่ 2-3

การถอดรหัสด้วยอัลกอริทึมเอ็มบีพีกรณีไม่มีการซิงโครไนซ์ตามที่ได้อธิบายในข้างต้น จะเป็นการถอดรหัสที่กระจายความเชื่อมั่นสองทิศทางโดยใช้วงจรถอดรหัสจำนวน 2 ตัว โดยวงจรถอดรหัสตัวแรกทำการถอดรหัสแบบกระจายความเชื่อมั่นจากซ้ายไปขวา และวงจรถอดรหัสตัวที่สองแบบขวาไปซ้าย จากนั้นทำการรวมความเชื่อมั่นที่ได้จากวงจรถอดรหัสทั้งสองตามสมการที่ 6.8 ทั้งนี้ การบวกความเชื่อมั่นที่ได้จากการถอดรหัสทั้งสอง เปรียบเสมือนการตัดสินใจเลือกคำรหัสที่มีความเชื่อมั่นสูงสุด ตัวอย่างเช่น วงจรถอดรหัสตัวแรกให้ความเชื่อมั่นของคำรหัสบิตที่ i เท่ากับ -10 (ตัดสินใจเลือกคำรหัส $\hat{v}_i = 1$) และวงจรถอดรหัสตัวที่สองให้ความเชื่อมั่นของคำรหัสบิตที่ i เท่ากับ 60 (ตัดสินใจเลือกคำรหัส $\hat{v}_i = 0$) เมื่อทำการรวมความเชื่อมั่นที่ได้จากการถอดรหัสทั้งสองตัว จะได้ความเชื่อมั่นของคำรหัสบิตที่ i เท่ากับ 50 (ตัดสินใจเลือกคำรหัส $\hat{v}_i = 0$) เปรียบเสมือนการตัดสินใจเลือกคำรหัสจากวงจรถอดรหัสตัวที่สอง เนื่องจากคำรหัสจากวงจรถอดรหัสตัวที่สองมีความเชื่อมั่นสูงกว่าวงจรถอดรหัสตัวที่หนึ่ง

สำหรับอัลกอริทึมเอ็มบีพีกรณีที่มีการซิงโครไนซ์ จะเป็นการแลกเปลี่ยนข่าวสารระหว่างวงจรถอดรหัสสองตัวในระหว่างกระบวนการถอดรหัส กล่าวคือ เมื่อวงจรถอดรหัสตัวแรกซึ่งกระจายความเชื่อมั่นจากซ้ายไปขวา คำนวณข่าวสาร $\vec{C}_{ji}^{(l)}$ ที่ออกจากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปรลำดับที่ i เสร็จสิ้น จะทำการส่งข่าวสาร $\vec{C}_{ji}^{(l)}$ ไปยังวงจรถอดรหัสตัวที่สองซึ่งกระจายความเชื่อมั่นจากขวาไปซ้าย ทำให้ข่าวสาร $\overleftarrow{C}_{ji}^{(l)}$ ถูกแทนที่ด้วยข่าวสาร $\vec{C}_{ji}^{(l)}$ ในทางกลับกัน วงจรถอดรหัสวงจรถอดรหัสตัวที่สองซึ่งกระจายความเชื่อมั่นจากขวาไปซ้าย ข่าวสาร $\overleftarrow{C}_{ji}^{(l)}$ จะถูกแทนที่ด้วยข่าวสาร $\overleftarrow{C}_{ji}^{(l)}$ ที่ส่งมาจากวงจรถอดรหัสตัวแรกซึ่งกระจายความเชื่อมั่นจากซ้ายไปขวา

อัลกอริทึมเอ็มบีพีกรณีที่ไม่มีการซิงโครไนซ์และมีการซิงโครไนซ์ จำเป็นต้องใช้วงจรถอดรหัสแอลบีพีจำนวนสองตัวซึ่งทำการกระจายความเชื่อมั่นในทิศทางที่แตกต่างกัน ทำให้ความซับซ้อน (จำนวนวงจรบวกและคูณ) ของการถอดรหัสเพิ่มขึ้น 1 เท่า เมื่อเทียบกับวงจรถอดรหัสแอลบีพี สำหรับหน่วยความจำที่ใช้เก็บข่าวสารของ วงจรถอดรหัสเอ็มบีพีกรณีไม่มีการซิงโครไนซ์ จะต้องใช้หน่วยความจำเพิ่มขึ้น 1 เท่า เพื่อเก็บข่าวสารของวงจรถอดรหัสสองตัว สำหรับการถอดรหัสเอ็มบีพี

กรณีมีการซิงโครไนซ์ จะใช้หน่วยความจำจำนวนเท่าเดิม เนื่องจากการแลกเปลี่ยนข่าวสารระหว่างวงจรถอดรหัสทั้งสองในระหว่างการถอดรหัส จะทำให้สามารถใช้หน่วยความจำร่วมกันได้

6.1.2 การวิเคราะห์สมรรถนะของอัลกอริทึมเอ็มบีพี

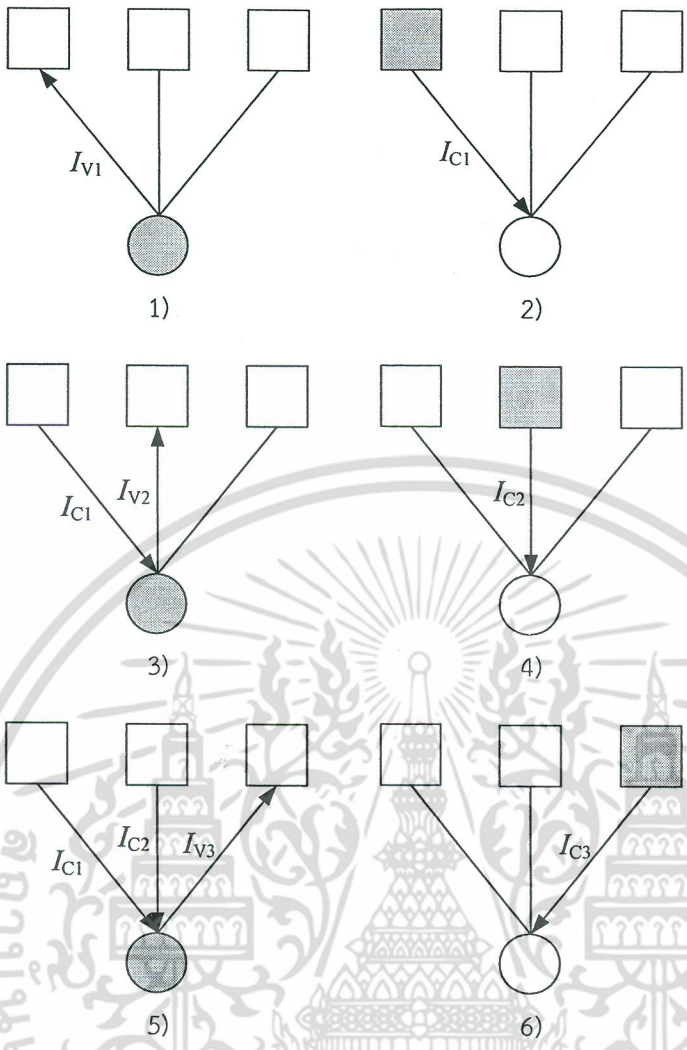
ในหัวข้อที่ 4.2.1 (บทที่ 4) อธิบายการวิเคราะห์รหัสแอลดีพีซีด้วยวิธีการเอ็กซิทชาร์ท อย่างไรก็ตาม วิธีการดังกล่าว จำกัดเฉพาะการถอดรหัสแอลดีพีซีแบบปรกติหรืออัลกอริทึมบีพี ดังนั้น ในหัวข้อนี้ จะแสดงการวิเคราะห์รหัสแอลดีพีซีเมื่อทำการถอดรหัสด้วยอัลกอริทึมแอลบีพี และเอ็มบีพี ที่ได้นำเสนอในงานวิจัย พิจารณาเมทริกซ์พาริตี้เช็คของรหัสแอลดีพีซีแบบควอไซไซคลิกในสมการที่ 5.1 (บทที่ 5) ซึ่งมีจำนวนเลขหนึ่งในแต่ละแถวและหลักเท่ากับ d_c และ d_v ตามลำดับ จากรูปที่ 5.1 (บทที่ 5) จะพบว่า โนดตัวแปรและโนดตรวจสอบของรหัสแอลดีพีซีแบบควอไซไซคลิกถูกแบ่งออกเป็นกลุ่ม โดยโนดตัวแปรภายในกลุ่มจะมีเส้นเชื่อมไปยังโนดตรวจสอบแตกต่างกันเสมอ ดังนั้น อาจกล่าวได้ว่า ในการถอดรหัสวนซ้ำ 1 รอบ โนดตัวแปรที่อยู่ในกลุ่มเดียวกันจะเป็นอิสระต่อกัน ทำให้ สามารถพิจารณาโนดตัวแปรแยกจากกันได้ พิจารณาการแลกเปลี่ยนข่าวสารร่วมของโนดตรวจสอบและโนดตัวแปรของการถอดรหัสด้วยอัลกอริทึมแอลบีพีจำนวน 1 รอบ ในรูปที่ 6.4 เมื่อกำหนดให้ โนดตัวแปรมีเส้นเชื่อมไปยังโนดตรวจสอบจำนวน 3 เส้น

การแลกเปลี่ยนข่าวสารร่วมของอัลกอริทึมแอลบีพีจะเริ่มจาก การคำนวณข่าวสารร่วม I_{V1} จากโนดตัวแปรไปยังโนดตรวจสอบดังรูปที่ 6.4 โดยทั่วไป ข่าวสารร่วมที่ออกจากโนดตัวแปรคำนวณได้จากข่าวสารร่วมที่ได้รับจากโนดตรวจสอบและช่องสัญญาณ อย่างไรก็ตาม กรณีการถอดรหัสรอบแรกจะยังปราศจากข่าวสารร่วมจากโนดตรวจสอบ ทำให้ จากสมการที่ 4.74 ข่าวสารร่วม I_{V1} จะมีค่าเท่ากับ

$$I_{\mathrm{V1}} = J\left(\sqrt{\sigma_{\mathrm{CH}}^2}\right) \tag{6.10}$$

จากนั้น คำนวณข่าวสารร่วม I_{C1} จากโนดตรวจสอบไปยังโนดตัวแปรโดยใช้สมการที่ 4.78 (บทที่ 4) ซึ่งเขียนใหม่ได้เป็น

$$I_{\mathrm{C1}} = 1 - J\left(\sqrt{(d_c - 1)[J^{-1}(1 - I_{\mathrm{V1}})]^2}\right) \tag{6.11}$$



รูปที่ 6.4 การคำนวณข่าวสารร่วมของอัลกอริทึมแอลบีพี

ลำดับต่อไป เป็นการคำนวณข่าวสารร่วม I_{V2} จากโนดตัวแปรไปยังโนดตรวจสอบ ซึ่งเกี่ยวข้องกับข่าวสารร่วม I_{C1} ที่ได้รับจากโนดตรวจสอบและช่องสัญญาณ ดังนี้

$$I_{V2} = J\left(\sqrt{[J^{-1}(I_{C1})]^2 + \sigma_{CH}^2}\right) \tag{6.12}$$

ข่าวสารร่วม I_{C2} และ I_{C3} จะมีสมการคล้ายกับการคำนวณข่าวสารร่วม I_{C1} สำหรับข่าวสารร่วม I_{V3} สามารถคำนวณได้จาก

$$I_{V3} = J\left(\sqrt{[J^{-1}(I_{C1})]^2 + [J^{-1}(I_{C2})]^2 + \sigma_{CH}^2}\right) \tag{6.13}$$

การวิเคราะห์สมรรถนะของการถอดรหัสด้วยอัลกอริทึมแอลบีพี จะเริ่มจาก การกำหนดค่าเอสเอ็นอาร์ของช่องสัญญาณรบกวนเกาส์สีขาวบวก จากนั้นคำนวณข่าวสารร่วมตามขั้นตอนดังรูปที่ 6.4 โดยทำซ้ำจนกระทั่งข่าวสารร่วมมีค่าคงที่ (การทำซ้ำขั้นตอนในรูปที่ 6.4 เปรียบเสมือนการถอดรหัสวนซ้ำของรหัสแอลดีพีซี) ค่าเทรสโฮลด์ของรหัสแอลดีพีซีจะมีค่าเท่ากับค่าเอสเอ็นอาร์ต่ำสุดที่ทำให้ข่าวสารร่วมที่ออกจากโนดตัวแปรและโนดตรวจสอบมีค่าเท่ากับ 1 สำหรับการถอดรหัสด้วยอัลกอริทึมเอ็มบีพีกรณีมีการซิงโครไนซ์ที่นำเสนอในงานวิจัย สามารถใช้ขั้นตอนการคำนวณข่าวสารร่วมตามที่อธิบายในข้างต้น โดยแบ่งเป็นการถอดรหัสที่คำนวณข่าวสารร่วมจากโนดตรวจสอบด้านซ้ายไปยังโนดตรวจสอบด้านขวา และการถอดรหัสที่คำนวณข่าวสารร่วมจากโนดตรวจสอบด้านขวาไปยังโนดตรวจสอบด้านซ้าย โดยมีการแลกเปลี่ยนข่าวสารร่วมที่ออกจากโนดตรวจสอบในระหว่างขั้นตอนการถอดรหัส

ตารางที่ 6.1 และ 6.2 แสดงค่าเทรสโฮลด์และจำนวนการวนซ้ำเมื่อใช้อัลกอริทึมถอดรหัสแบบบีพี แอลบีพี และเอ็มบีพี สำหรับรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 1/2 และ 8/9 ตามลำดับ จากตารางจะสังเกตได้ว่าการใช้อัลกอริทึมถอดรหัสแบบต่างๆ จะไม่ส่งผลต่อค่าเทรสโฮลด์แต่จะมีผลต่อจำนวนการถอดรหัสวนซ้ำ โดยการถอดรหัสแอลบีพีจะใช้จำนวนการถอดรหัสน้อยกว่าการถอดรหัสบีพี ดังนั้น เมื่อกำหนดให้การถอดรหัสมีจำนวนการวนซ้ำเท่ากัน อัลกอริทึมแอลบีพีจะมีสมรรถนะที่ดีกว่าการถอดรหัสบีพี สำหรับการถอดรหัสเอ็มบีพีกรณีมีการซิงโครไนซ์ จะใช้จำนวนการถอดรหัสวนซ้ำน้อยกว่าการถอดรหัสอื่นๆ ยกเว้นกรณีรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 1/2 และ $d_v = 2$

ตารางที่ 6.1 ค่าเทรสโฮลด์และจำนวนการวนซ้ำของรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 1/2

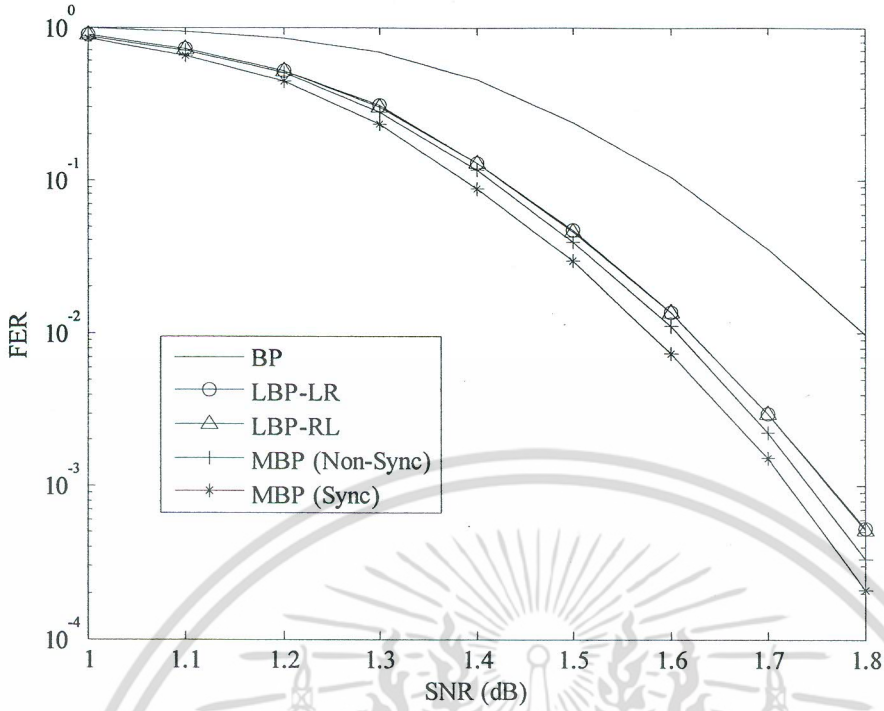
(d_v, d_c)	อัลกอริทึม	เทรสโฮลด์ (dB)	จำนวนการถอดรหัสวนซ้ำ (รอบ)
(2, 4)	BP	3.037	1,720
	LBP	3.037	860
	MBP	3.037	860
(3, 6)	BP	1.102	617
	LBP	1.102	309
	MBP	1.102	257
(4, 8)	BP	1.534	950
	LBP	1.534	475
	MBP	1.534	369

ตารางที่ 6.2 ค่าเทรสโฮลด์และจำนวนการวนซ้ำของรหัสแอลดีพีซีเมื่ออัตรารหัสเท่ากับ 8/9

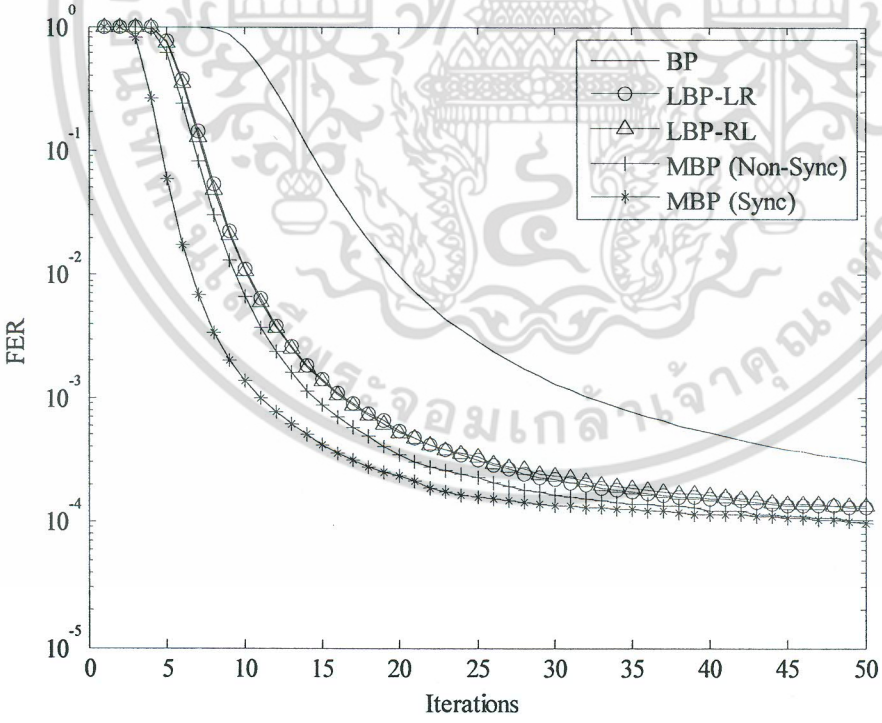
(d_v, d_c)	อัลกอริทึม	เทรสโฮลด์ (dB)	จำนวนการถอดรหัสวนซ้ำ (รอบ)
(2 , 18)	BP	4.723	665
	LBP	4.723	333
	MBP	4.723	332
(3 , 27)	BP	3.502	277
	LBP	3.502	138
	MBP	3.502	115
(4 , 36)	BP	3.517	237
	LBP	3.517	119
	MBP	3.517	92

6.1.3 ผลการจำลองสมรรถนะของอัลกอริทึมเอ็มบีพี

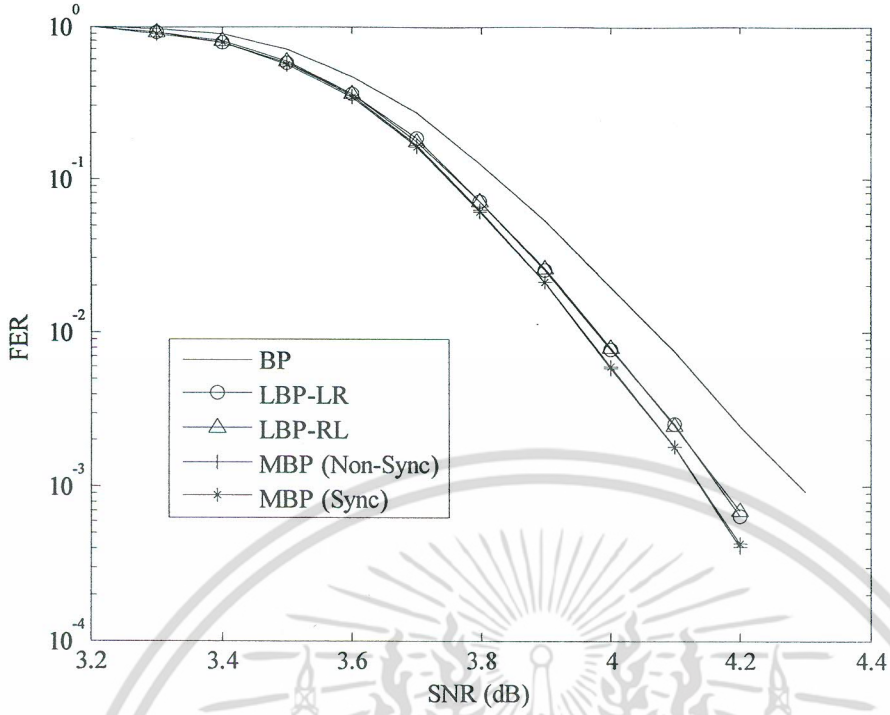
รูปที่ 6.5 แสดงอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2 เมื่อกำหนดให้ดีกรีของโนดตัวแปรเท่ากับ $d_v = 3$ และจำนวนการถอดรหัสวนซ้ำเท่ากับ 20 รอบ จากรูป สังเกตได้ว่า อัลกอริทึมแอลบีพี-แอลอาร์ และอัลกอริทึมแอลบีพี-อาร์แอล มีอัตราเฟรมผิดพลาดที่เท่ากัน สำหรับอัลกอริทึมเอ็มบีพีกรณีไม่มีการซิงโครไนซ์จะให้ผลที่ดีกว่าอัลกอริทึมแอลบีพี ทั้งนี้ สามารถอธิบายได้จากตำแหน่งบิตผิดพลาดที่แตกต่างกันของการถอดรหัสกระจายข่าวสารสองทิศทาง ทำให้วิธีการรวมความเชื่อมั่นที่ได้จากการถอดรหัสในอัลกอริทึมเอ็มบีพี จะเปรียบเสมือนการเลือกคำรหัสที่มีความเชื่อมั่นมากที่สุดหรือมีความน่าจะเป็นของบิตผิดพลาดต่ำสุด สำหรับอัลกอริทึมเอ็มบีพีกรณีมีการซิงโครไนซ์ จะให้ผลที่ดีกว่าอัลกอริทึมแอลบีพีและบีพี ซึ่งอธิบายได้จากตารางที่ 6.1 รูปที่ 6.6 แสดงอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2 เมื่อจำนวนการถอดรหัสวนซ้ำเริ่มจาก 1 ถึง 50 รอบ จากรูปจะเห็นว่า อัลกอริทึมเอ็มบีพีที่ได้นำเสนอให้อัตราเฟรมผิดพลาดที่ต่ำกว่าอัลกอริทึมอื่นทุกจำนวนรอบของการถอดรหัสวนซ้ำ นอกจากนี้ เมื่อจำนวนการถอดรหัสวนซ้ำเท่ากับ 4 ถึง 35 รอบ อัลกอริทึมเอ็มบีพีกรณีมีการซิงโครไนซ์จะให้อัตราเฟรมผิดพลาดต่ำกว่ากรณีไม่มีการซิงโครไนซ์ สำหรับสมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 8/9 เมื่อจำนวนการถอดรหัสวนซ้ำเท่ากับ 20 รอบ แสดงได้ดังรูปที่ 6.7 ในที่นี้ อัลกอริทึมเอ็มบีพีกรณีไม่มีการซิงโครไนซ์และกรณีมีการซิงโครไนซ์จะให้สมรรถนะที่เท่ากัน โดยที่อัตราเฟรมผิดพลาดเท่ากับ 7×10^{-4} อัลกอริทึมเอ็มบีพีใช้ค่าเอสเอ็นอาร์ลดลง 0.04 dB เมื่อเทียบกับอัลกอริทึมแอลบีพี รูปที่ 6.8 แสดงอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 8/9 ที่จำนวนการถอดรหัสวนซ้ำแตกต่างกัน โดยจะพบว่า เมื่อจำนวนการถอดรหัสวนซ้ำมากกว่า 25 รอบ อัลกอริทึมเอ็มบีพีกรณีไม่มีการซิงโครไนซ์จะให้สมรรถนะที่ดีกว่ากรณีมีการซิงโครไนซ์



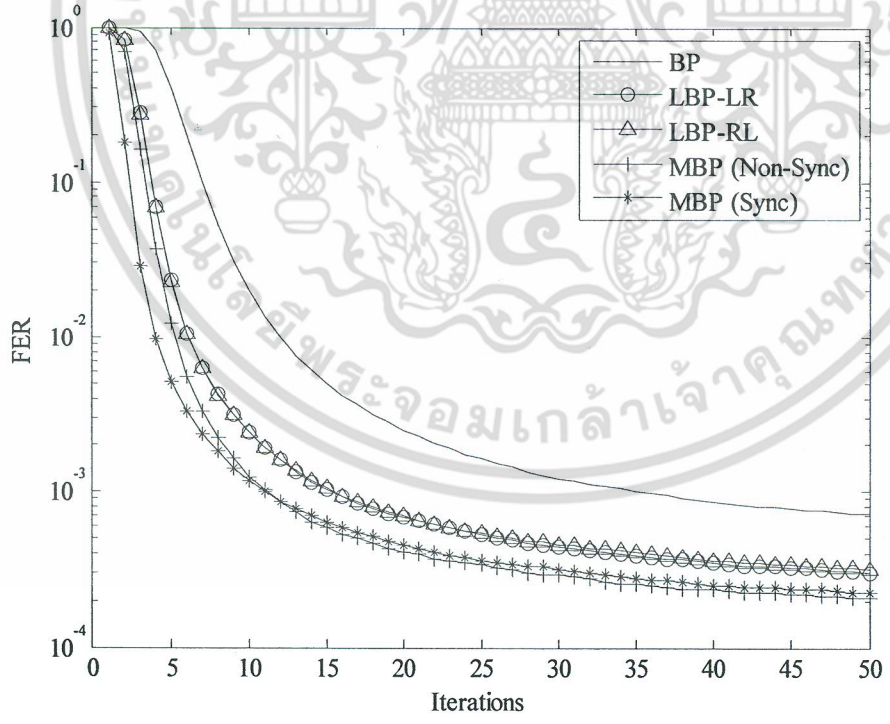
รูปที่ 6.5 อัตราเฟรมผิดพลาดที่ค่าเอสเอ็นอาร์ใดๆ ของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2



รูปที่ 6.6 อัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2 เมื่อใช้การถอดรหัสวนซ้ำจำนวนรอบใดๆ



รูปที่ 6.7 อัตราเฟรมผิดพลาดที่ค่าเอสเอ็นอาร์ใดๆ ของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 8/9



รูปที่ 6.8 อัตราเฟรมผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 8/9 เมื่อใช้การถอดรหัสวนซ้ำจำนวนรอบใดๆ

6.2 การถอดรหัสสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

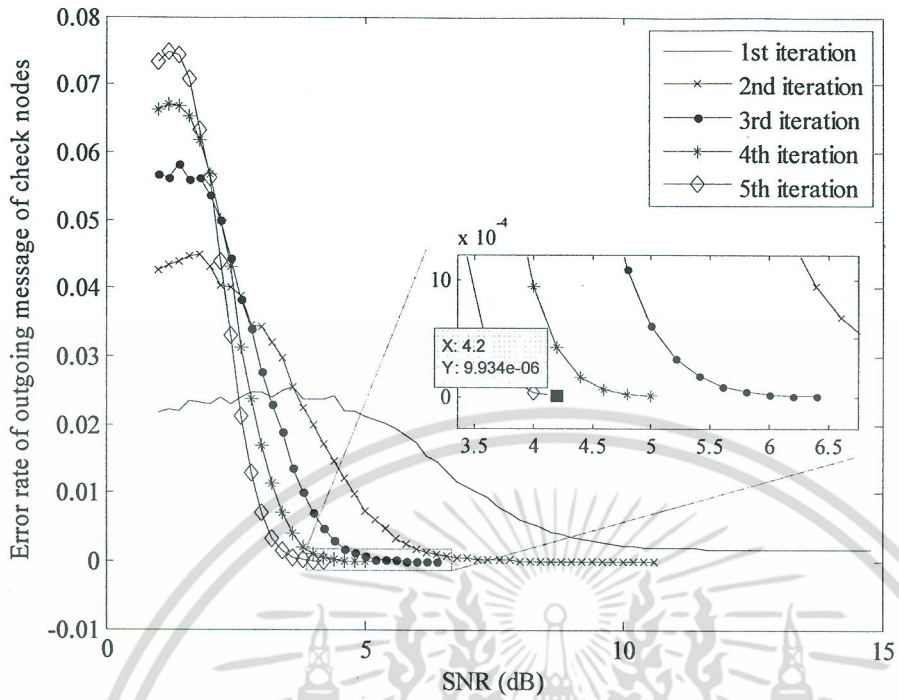
ระบบบันทึกข้อมูลเชิงแม่เหล็กแบบบิตแพทเทิร์น (bit patterned media recording) [16] เป็นเทคโนโลยีทางเลือกสำหรับการบันทึกข้อมูลที่มีความหนาแน่นสูง โดยสื่อบันทึกที่ใช้เก็บข้อมูลจะมีลักษณะเป็นไอแลนด์เชิงแม่เหล็ก (magnetic island) เรียงตัวกันบนแผ่นรองรับที่ทำจากวัสดุที่ไม่เป็นแม่เหล็ก ทำให้ สามารถจัดการปัญหาเรื่องขีดจำกัดซูเปอร์พาราแม็กเนติก (super-paramagnetic limit) ของสื่อบันทึกข้อมูล อย่างไรก็ตาม ในกระบวนการบันทึกอาจเกิดปัญหาที่เรียกว่า การเขียนผิดพลาด (written-in error) [17] ซึ่งเกิดจากตำแหน่งของหัวเขียนไม่ตรงกับตำแหน่งของไอแลนด์เชิงแม่เหล็ก ส่งผลให้ เกิดความผิดพลาดในการบันทึกข้อมูล ทั้งนี้ สามารถจำลองเหตุการณ์เขียนและอ่านข้อมูลในสื่อบันทึก ด้วยแบบจำลองช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวกในหัวข้อที่ 2.1.3 (บทที่ 2) โดยทั่วไป รหัสแอลดีพีซีที่ประยุกต์ใช้งานในระบบบันทึกข้อมูลเชิงแม่เหล็กถูกออกแบบสำหรับการทำงานภายใต้สัญญาณรบกวนเกาส์เซียนขาวบวก ดังนั้น เมื่อการบันทึกข้อมูลเกิดปัญหาการเขียนผิดพลาด (จำลองโดยใช้ช่องสัญญาณสมมาตรไบนารี) จะส่งผลให้สมรรถนะการแก้ไขบิตผิดพลาดของรหัสแอลดีพีซีลดลง [50] ในงานวิจัย [18] ได้ศึกษาฟังก์ชันความหนาแน่นความน่าจะเป็นของสัญญาณที่ได้รับจากช่องสัญญาณ โดยนำเสนอการคำนวณอัตราส่วนความน่าจะเป็นแบบล็อกของการถอดรหัสแอลดีพีซี รายละเอียดอธิบายในหัวข้อที่ 2.1.3 (บทที่ 2) อย่างไรก็ตาม งานวิจัยที่กล่าวมา เป็นการปรับปรุงสัญญาณอินพุทของวงจรถอดรหัสแอลดีพีซีให้สอดคล้องกับช่องสัญญาณ ปราศจากการปรับปรุงกระบวนการถอดรหัส ดังนั้น ในงานวิจัยนี้จึงนำเสนอการปรับปรุงกระบวนการถอดรหัสแอลดีพีซี ซึ่งทำงานในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก โดยให้สมรรถนะการแก้ไขความผิดพลาดสูงขึ้นกว่าการปรับปรุงสัญญาณอินพุทของวงจรถอดรหัสในงานวิจัยก่อนหน้า นอกจากนี้ ในงานวิจัยจะแสดงวิธีการคำนวณความจุช่องสัญญาณและขอบเขตความผิดพลาดของช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

6.2.1 ความจุช่องสัญญาณและขอบเขตความผิดพลาด

เพื่อความต่อเนื่องของเนื้อหาในวิทยานิพนธ์ วิธีการคำนวณความจุช่องสัญญาณและขอบเขตความผิดพลาด จะแสดงในหัวข้อที่ 2.2.2 และ 2.2.3 (บทที่ 2)

6.2.2 อัลกอริทึมการถอดรหัสแอลดีพีซี

ขั้นตอนการถอดรหัสแอลดีพีซีจะเกี่ยวข้องกับการคำนวณข่าวสารระหว่างโนดตัวแปรและโนดตรวจสอบ ซึ่งข่าวสารที่ออกจากโนดตัวแปรจะเกี่ยวข้องกับข่าวสารที่ได้รับจากโนดตรวจสอบและช่องสัญญาณ โดยช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก ข่าวสารที่ได้รับจากช่องสัญญาณจะอยู่ในรูปอัตราส่วนความน่าจะเป็นแบบล็อกซึ่งคำนวณได้จากสมการที่ 2.14 (บทที่ 2)



รูปที่ 6.9 อัตราผิดพลาดของข่าวสารที่ออกจากโนดตรวจสอบอันเนื่องมาจากความน่าจะเป็นตัดข้าม $p_{\mathrm{BSC}} = 5\times10^{-3}$ ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

พิจารณาข่าวสารที่ออกจากโนดตรวจสอบของรหัสแอลดีพีซี ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวกซึ่งความน่าจะเป็นตัดข้ามเท่ากับ $p_{\mathrm{BSC}} = 5\times10^{-3}$ ดังรูปที่ 6.9 เมื่อกำหนดให้ อัตรารหัสเท่ากับ 1/2 ดีกรีของโนดตัวแปรและโนดตรวจสอบเท่ากับ 3 และ 6 ตามลำดับ ในที่นี้ แกนตั้งจะแสดงอัตราผิดพลาดของข่าวสารที่ออกจากโนดตรวจสอบเมื่อเทียบกับ กรณีที่ความน่าจะเป็นตัดข้ามเท่ากับ $p_{\mathrm{BSC}} = 0$ กล่าวคือ แสดงความผิดพลาดของข่าวสารที่ออกจากโนดตรวจสอบซึ่งเป็นผลมาจากความน่าจะเป็นตัดข้ามที่เกิดขึ้นในช่องสัญญาณ จากรูป จะสังเกตได้ว่าเมื่อค่าเอสเอ็นอาร์เพิ่มขึ้นอัตราผิดพลาดของข่าวสารที่ออกจากโนดตรวจสอบมีแนวโน้มเป็นค่าคงที่ ดังนั้น อัตราผิดพลาดที่เกิดขึ้นสามารถนำไปปรับปรุงข่าวสารที่ออกจากโนดตรวจสอบ

พิจารณาการคำนวณข่าวสารที่ออกจากโนดตรวจสอบ กรณีจำนวนเส้นเชื่อมของโนดตรวจสอบเป็นเลขคู่ ดังสมการที่ 4.4 และ 4.9 (บทที่ 4) เพื่อความสะดวก เขียนใหม่อีกครั้งได้เป็น

$$r_{ji}(1) = \frac{1}{2} + \frac{1}{2}\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right) \tag{6.14}$$

$$r_{ji}(0) = 1 - r_{ji}(1) \tag{6.15}$$

เนื่องจากข่าวสารที่ออกจากโนดตรวจสอบมีความผิดพลาดเกิดขึ้น ในที่นี้ กำหนดให้ p_{LDPC} คืออัตราผิดพลาดที่เกิดขึ้นของข่าวสารที่ออกจากโนดตรวจสอบ ดังนั้น ความน่าจะเป็นของโนดตัวแปรลำดับที่ i มีค่าเท่ากับ 1 คำนวณใหม่ได้ ดังนี้

$$\begin{aligned} r_{ji}^{\mathrm{new}}(1) &= (1-p_{\mathrm{LDPC}})r_{ji}(1) + p_{\mathrm{LDPC}}r_{ji}(0) \\ &= (1-p_{\mathrm{LDPC}})\left(\frac{1}{2}+\frac{1}{2}\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right)\right) + p_{\mathrm{LDPC}}\left(\frac{1}{2}-\frac{1}{2}\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right)\right) \end{aligned} \tag{6.16}$$

จาก $r_{ji}^{\mathrm{new}}(1) = 1 - r_{ji}^{\mathrm{new}}(0)$ ดังนั้น

$$1-r_{ji}^{\mathrm{new}}(0) = (1-p_{\mathrm{LDPC}})\left(\frac{1}{2}+\frac{1}{2}\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right)\right) + p_{\mathrm{LDPC}}\left(\frac{1}{2}-\frac{1}{2}\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right)\right) \tag{6.17}$$

จัดรูปใหม่จะได้

$$1-2r_{ji}^{\mathrm{new}}(0) = (1-2p_{\mathrm{LDPC}})\prod_{i'\in V_j\setminus i}\left(1-2q_{i'j}(0)\right) \tag{6.18}$$

จากความสัมพันธ์ $1-2P(x=0) = -\tanh\left(\frac{1}{2}\log\left(\frac{P(x=0)}{P(x=1)}\right)\right)$ ทำให้

$$-\tanh\left(\frac{1}{2}\log\left(\frac{r_{ji}^{\mathrm{new}}(0)}{r_{ji}^{\mathrm{new}}(1)}\right)\right) = (1-2p_{\mathrm{LDPC}})\prod_{i'\in V_j\setminus i}\left(-\tanh\left(\frac{1}{2}\log\left(\frac{q_{i'j}(0)}{q_{i'j}(1)}\right)\right)\right) \tag{6.19}$$

ดังนั้น ข่าวสารที่ออกจากโนดตรวจสอบในรูปอัตราส่วนความน่าจะเป็นแบบล็อก กรณีเส้นเชื่อมของโนดตรวจสอบเป็นเลขคู่ คำนวณได้จาก

$$L(r_{ji}^{\mathrm{new}}) = 2\tanh^{-1}\left((1-2p_{\mathrm{LDPC}})\prod_{i'\in V_j\setminus i}\tanh\left(\frac{1}{2}L(q_{i'j})\right)\right) \tag{6.20}$$

เมื่อ $V_j \setminus i$ คือเซตของโนดตัวแปรที่มีเส้นเชื่อมไปยังโนดตรวจสอบลำดับที่ j ยกเว้นโนดตัวแปรลำดับที่ i สำหรับการคำนวณกรณีเส้นเชื่อมของโนดตรวจสอบเป็นเลขคี่ จะมีผลลัพธ์เท่ากับสมการที่ 6.20

ขั้นตอนการถอดรหัสแอลดีพีซีในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก แสดงในตารางต่อไปนี้

ตารางที่ 6.3 อัลกอริทึมถอดรหัสแอลดีพีซีในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

---

for $i=1$ **to** N
  คำนวณความเชื่อมั่น $L(R_i)$ ของโนดตัวแปรลำดับที่ i ที่ได้รับจากช่องสัญญาณ
  โดยใช้สมการที่ 2.14 (บทที่ 2)
end
กำหนดให้ความเชื่อมั่น $L(r_{ji})=0$ เมื่อ $1\le i\le N$ และ $1\le j\le M$
for $l=1$ **to** l_{MAX}
  for $i=1$ **to** N
    for all $j\in C_i$
      คำนวณความเชื่อมั่น $L(q_{ij})$ จากโนดตัวแปรลำดับที่ i ไปยังโนดตรวจสอบ
      ลำดับที่ j โดยใช้สมการที่ 4.44 (บทที่ 4)
    end
  end
  for $j=1$ **to** M
    for all $i\in V_j$
      คำนวณความเชื่อมั่น $L(r_{ji})$ จากโนดตรวจสอบลำดับที่ j ไปยังโนดตัวแปร
      ลำดับที่ i โดยใช้สมการที่ 6.20
    end
  end
end
for $i=1$ **to** N
  คำนวณความเชื่อมั่น $L(Q_i)$ ของโนดตัวแปรลำดับที่ i โดยใช้สมการที่ 4.45
  หลังจากนั้นทำการตัดสินใจคำรหัสที่ถูกส่งผ่านช่องสัญญาณโดยใช้สมการที่ 4.46
end

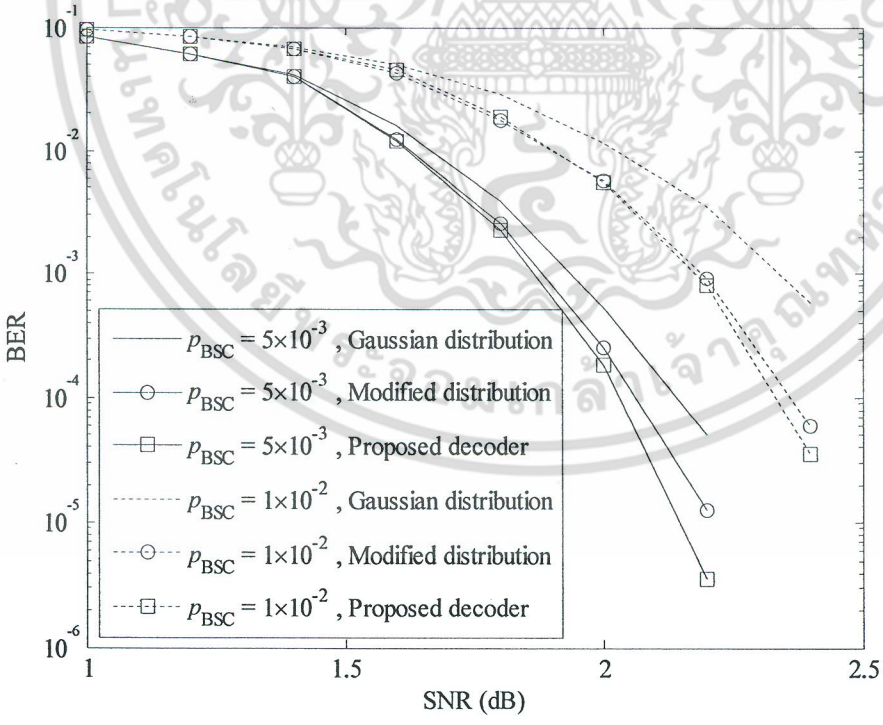
6.2.3 ผลการจำลองสมรรถนะของอัลกอริทึมการถอดรหัสแอลดีพีซี

กำหนดให้ รหัสแอลดีพีซีมีความยาวคำรหัสเท่ากับ 4,096 บิต ดีกรีของโนดตัวแปรเท่ากับ 3 และจำนวนการถอดรหัสวนซ้ำเท่ากับ 30 รอบ รูปที่ 6.10 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2 ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก ในที่นี้ เพื่อความสะดวก จะกำหนดให้อัตราผิดพลาดของข่าวสารที่ออกจากโนดตรวจสอบ p_{LDPC} เท่ากับ ความน่าจะเป็นตัดข้ามของช่องสัญญาณสมมาตรไบนารี p_{BSC} จากรูป จะสังเกตได้ว่า วิธีการปรับปรุงอินพุทของวงจรถอดรหัสแอลดีพีซีที่ถูกนำเสนอในงานวิจัย [18] (แทนด้วยสัญลักษณ์วงกลม) ให้สมรรถนะที่ดีกว่าวงจรถอดรหัสแอลดีพีซีแบบทั่วไป (แทนด้วยเส้นตรง) สำหรับวิธีการถอดรหัสที่ได้นำเสนอใน

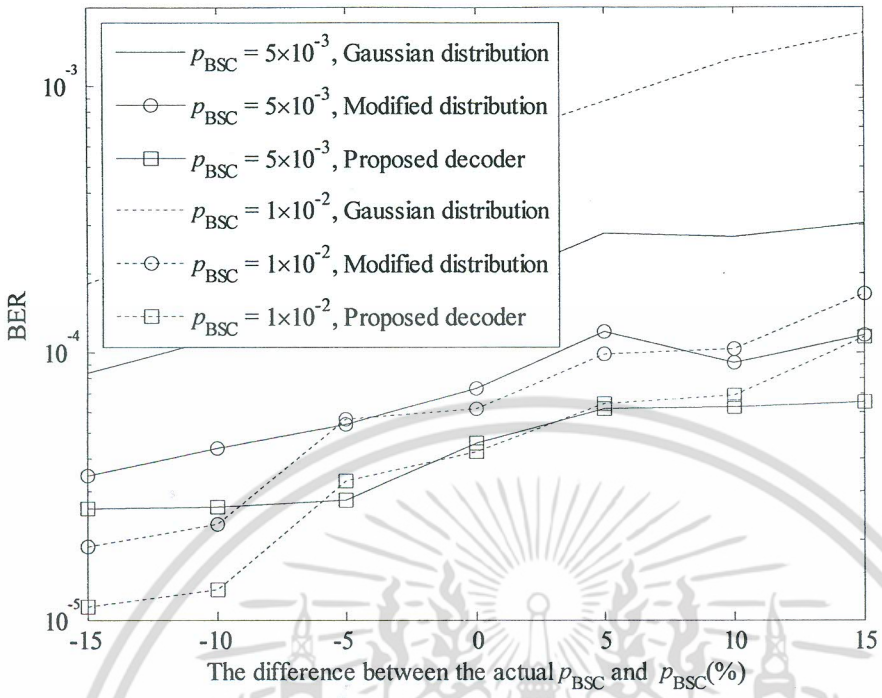
งานวิจัยนี้ (แทนด้วยสัญลักษณ์สี่เหลี่ยม) จะให้อัตราบิตผิดพลาดต่ำกว่าการถอดรหัสอื่นๆ โดยเมื่ออัตราบิตผิดพลาดเท่ากับ 6×10^{-5} วิธีการถอดรหัสที่นำเสนอจะใช้ค่าเอสเอ็นอาร์ต่ำกว่าวิธีการปรับปรุงอินพุทของวงจรถอดรหัส ประมาณ 0.05 dB และ 0.04 dB ที่ค่าตัดข้ามของช่องสัญญาณสมมาตรไบนารีเท่ากับ 5×10^{-3} และ 1×10^{-2} ตามลำดับ

รูปที่ 6.11 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีเมื่อค่าตัดข้าม p_{BSC} ที่กำหนดให้กับวงจรถอดรหัสแตกต่างจากค่าตัดข้าม p_{BSC} ที่เกิดขึ้นจริงในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก จากรูป เมื่อค่าตัดข้าม p_{BSC} ที่เกิดขึ้นจริงมีค่าน้อยกว่าค่าตัดข้าม p_{BSC} ที่กำหนดให้กับวงจรถอดรหัส จะส่งผลให้อัตราบิตผิดพลาดต่ำลง ในทางกลับกัน เมื่อค่าตัดข้ามที่เกิดขึ้นจริงมากกว่าค่าตัดข้ามที่กำหนดให้กับวงจรถอดรหัส จะส่งผลให้อัตราบิตผิดพลาดสูงขึ้น ทั้งนี้ สังเกตได้ว่าความแตกต่างของค่าตัดข้ามที่เกิดขึ้น ส่งผลต่อสมรรถนะของการถอดรหัสแอลดีพีซี อย่างไรก็ตาม วิธีการถอดรหัสแอลดีพีซีที่ได้นำเสนอยังคงให้สมรรถนะที่ดีกว่า การปรับปรุงอินพุทของวงจรถอดรหัส

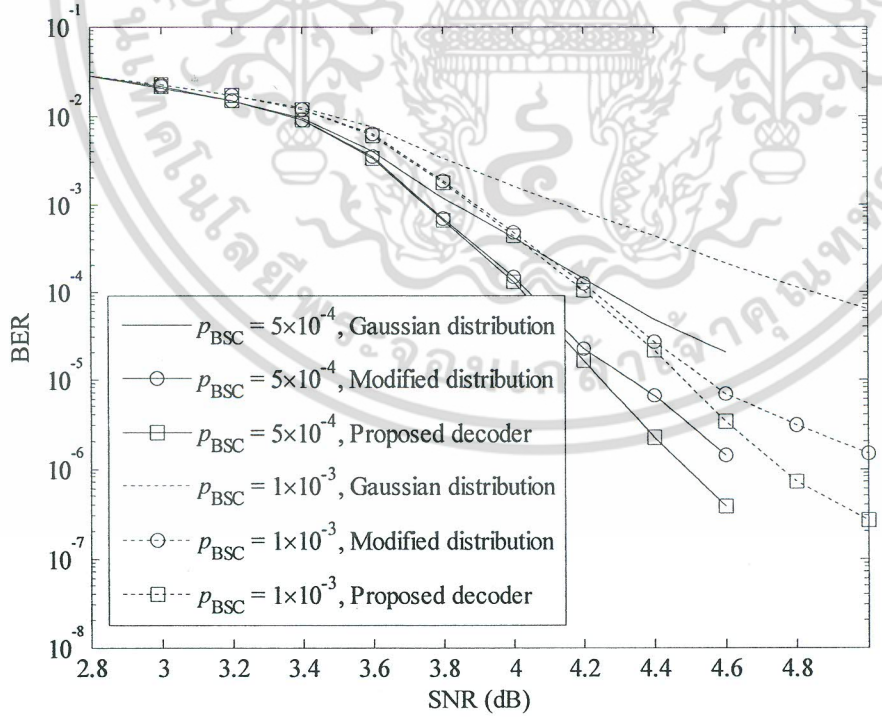
รูปที่ 6.12 แสดงอัตราบิตผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 7/8 ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก เมื่ออัตราบิตผิดพลาดเท่ากับ 2×10^{-5} วิธีการถอดรหัสที่นำเสนอจะใช้ค่าเอสเอ็นอาร์ต่ำกว่าวิธีการปรับปรุงอินพุทของวงจรถอดรหัส ประมาณ 0.15 dB และ 0.3 dB ที่ค่าตัดข้ามของช่องสัญญาณสมมาตรไบนารีเท่ากับ 5×10^{-4} และ 1×10^{-3} ตามลำดับ



รูปที่ 6.10 อัตราบิตผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 1/2 ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก



รูปที่ 6.11 อัตราบิตผิดพลาดของรหัสแอลดีพีซีเมื่อค่าตัดข้าม p_{BSC} ที่กำหนดให้วงจรถอดรหัสแตกต่างจากจากค่าตัดข้าม p_{BSC} ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก



รูปที่ 6.12 อัตราบิตผิดพลาดของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 7/8 ในช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก

6.3 การถอดรหัสสองมิติ

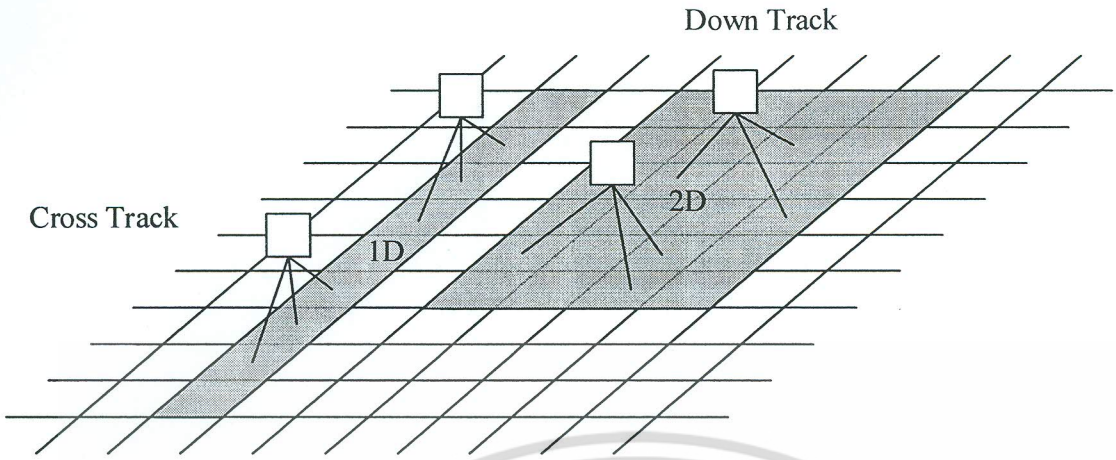
ในระบบบันทึกข้อมูลเชิงแม่เหล็ก ข้อมูลจะถูกบันทึกลงในสื่อบันทึกตามแนวเส้นรอบวงซึ่งเรียกว่าแทร็ก (track) ดังรูปที่ 1.1 โดยแต่ละแทร็กจะถูกแบ่งออกเป็นเซกเตอร์ (sector) และแต่ละเซกเตอร์จะเก็บข้อมูล 512 ไบต์ หรือ 4,096 บิต (ในอนาคต เซกเตอร์จะเก็บข้อมูล 4,096 ไบต์ หรือ 32,768 บิต ทำให้ สมรรถนะของรหัสแอลดีพีซีเพิ่มสูงขึ้น ดังรูปที่ 3.4 (บทที่ 3)) โดยทั่วไป คำรหัสที่ได้จากการเข้ารหัสแอลดีพีซี จะถูกบันทึกลงในแทร็กเดียวกันหรือเซกเตอร์เดียวกัน ในที่นี้ จะเรียกว่ารหัสแอลดีพีซีแบบหนึ่งมิติ อย่างไรก็ตาม แทร็กที่อยู่ติดกันจะมีค่าเอสเอ็นอาร์ที่แตกต่างกันอันเนื่องมาจาก ขนาดของแทร็ก การใช้หัวอ่านจำนวนหลายหัว เป็นต้น นอกจากนี้ เซกเตอร์ที่อยู่ติดกันอาจมีค่าเอสเอ็นอาร์ที่แตกต่างกันได้เช่นกันเนื่องจากพื้นผิวของสื่อบันทึกมีแตกต่างกัน ดังนั้น ในงานวิจัยนี้ จึงนำเสนอรหัสแอลดีพีซีแบบสองมิติ ซึ่งคำรหัสถูกแบ่งและบันทึกลงในแทร็กที่แตกต่างกัน ดังรูปที่ 6.13 เป็นผลให้ ในกระบวนการถอดรหัส บิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์สูงสามารถช่วยบิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์ต่ำ นอกจากนี้ ในงานวิจัย จะแสดงการวิเคราะห์สมรรถนะของรหัสแอลดีพีซีเมื่อทำการถอดรหัสแบบสองมิติ วิธีการที่นำเสนอนี้ สามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีแบบสองมิติซึ่งให้สมรรถนะการแก้ไขบิตผิดพลาดสูง

6.3.1 การวิเคราะห์สมรรถนะของการถอดรหัสสองมิติ

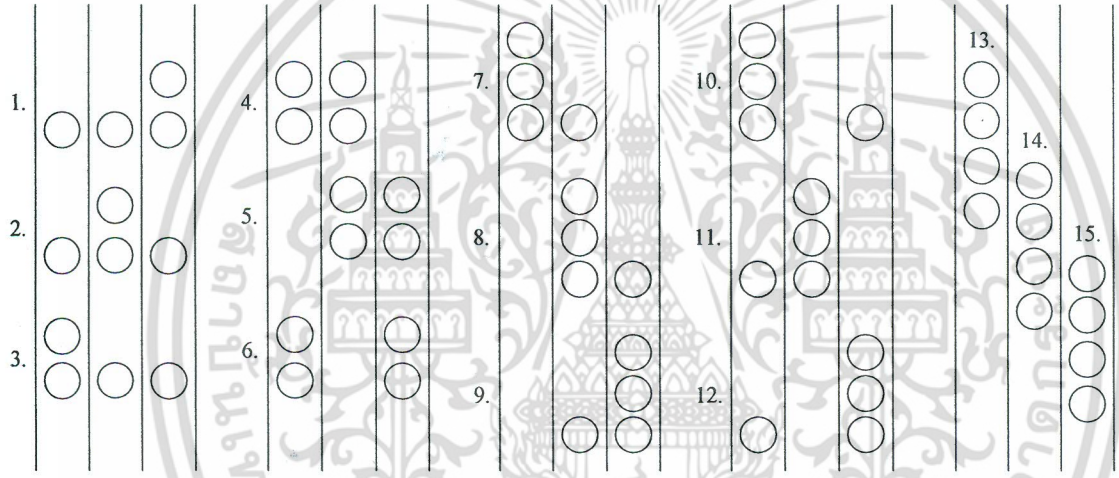
สมมุติให้ รหัสแอลดีพีซีสองมิติ มีจำนวนโนดตัวแปรที่เชื่อมไปยังโนดตรวจสอบเท่ากับ 4 โนด และจำนวนแทร็กที่ใช้ในการบันทึกข้อมูลเท่ากับ 3 แทร็ก ดังนั้น รูปแบบการกระจายตัวของโนดตัวแปรจะมีจำนวนเท่ากับ 15 รูปแบบ ดังรูปที่ 6.14 กำหนดให้ $\gamma_{n,l}$ คืออัตราส่วนของจำนวนโนดตัวแปรในแทร็กลำดับที่ l ต่อจำนวนโนดตัวแปรทั้งหมดของรูปแบบการกระจายตัวลำดับที่ n โดยที่ $\sum_l \gamma_{n,l} = 1$ เสมอ ตัวอย่างเช่น รูปแบบการกระจายตัวลำดับที่ 1 ในรูปที่ 6.14 จะมีอัตราส่วนเท่ากับ $\gamma_{1,1} = 1/4$, $\gamma_{1,2} = 1/4$, $\gamma_{1,3} = 2/4$ และรูปแบบการกระจายตัวลำดับที่ 2 จะมีอัตราส่วนเท่ากับ $\gamma_{2,1} = 1/4$, $\gamma_{2,2} = 2/4$, $\gamma_{2,3} = 1/4$ จากสมการที่ 4.75 (บทที่ 4) การคำนวณข่าวสารร่วมที่ออกจากโนดตัวแปรสามารถเขียนอยู่ในรูปฟังก์ชัน $I_{\mathrm{E,V}}(I_{\mathrm{A,V}}, d_v, \sigma^2_{\mathrm{CH}})$ ดังนั้น ข่าวสารร่วมที่ออกจากโนดตัวแปรของการถอดรหัสแอลดีพีซีสองมิติคำนวณได้จาก

$$I^{\mathrm{2D}}_{\mathrm{E,V}} = \frac{1}{N}\sum_{n=1}^{N}\sum_{l=1}^{L}\gamma_{n,l} I_{\mathrm{E,V}}(I^{2D}_{\mathrm{A,V}}, d_v, \sigma^2_{\mathrm{CH}_l}) \tag{6.21}$$

เมื่อ N คือจำนวนรูปแบบการกระจายตัวของโนดตัวแปร และ L คือจำนวนแทร็กที่ใช้ในการบันทึกข้อมูล



รูปที่ 6.13 รหัสแอลดีพีซีแบบสองมิติ



รูปที่ 6.14 รูปแบบการกระจายตัวของโนดตัวแปรจำนวน 4 โนด

เนื่องจากการวิเคราะห์สมรรถนะภาพของรหัสแอลดีพีซีด้วยวิธีการเอ็กซิตชาร์ทจะสมมุติให้คำรหัสมีความยาวเป็นอนันต์ ดังนั้น รูปแบบการกระจายตัวของโนดตัวแปรจะมีความน่าจะเป็นในการเกิดเท่ากัน ทำให้ สมการที่ 6.21 มีค่าเท่ากับ

$$I_{\mathrm{E,V}}^{\mathrm{2D}} = \frac{1}{L}\sum_{l=1}^{L} I_{\mathrm{E,V}}(I_{\mathrm{A,V}}^{2D}, d_v, \sigma_{\mathrm{CH}_l}^2) \tag{6.22}$$

จากสมการที่ 4.78 (บทที่ 4) การคำนวณข่าวสารร่วมที่ออกจากโนดตรวจสอบสามารถเขียนอยู่ในรูปฟังก์ชัน $I_{\mathrm{E,C}}(I_{\mathrm{A,C}}, d_c)$ ดังนั้น ข่าวสารร่วมที่ออกจากโนดตรวจสอบของการถอดรหัสแอลดีพีซีสองมิติคำนวณได้จาก

$$I_{\mathrm{E,C}}^{\mathrm{2D}} = I_{\mathrm{E,C}}(I_{\mathrm{A,C}}^{2D}, d_c) \tag{6.23}$$

การวิเคราะห์สมรรถนะของรหัสแอลดีพีซีแบบสองมิติ จะเริ่มจากการกำหนดค่าเอสเอ็นอาร์ของแทร็กที่ใช้ในการบันทึกข้อมูล จากนั้นคำนวณข่าวสารร่วมโดยใช้สมการที่ 6.22 และ 6.23 จนกระทั่งข่าวสารร่วมมีค่าคงที่ ค่าเทรสโฮลด์ของรหัสแอลดีพีซีสองมิติจะมีค่าเท่ากับเอสเอ็นอาร์ต่ำสุดของแทร็กต่างๆ ซึ่งทำให้ข่าวสารร่วมที่ออกจากโนดตรวจสอบและโนดตัวแปรมีค่าเท่ากับ 1

6.3.2 แบบจำลองช่องสัญญาณสองมิติ

กำหนดให้ แทร็กที่ใช้ในการบันทึกข้อมูลมีจำนวนเท่ากับ L แทร็ก โดยแต่ละแทร็กจะมีค่าเอสเอ็นอาร์เท่ากับ SNR_l เดซิเบล เมื่อ l คือลำดับที่ของแทร็ก และค่าเอสเอ็นอาร์ของแต่ละแทร็กจะเป็น $\mathrm{SNR}_1 < \mathrm{SNR}_2 < \ldots < \mathrm{SNR}_L$ เสมอ ดังนั้น ค่าเฉลี่ยเอสเอ็นอาร์ของช่องสัญญาณสองมิติจะมีค่าเท่ากับ

$$\mathrm{SNR}_{\mathrm{avg}} = \frac{1}{L}\sum_{l=1}^{L}\mathrm{SNR}_l \tag{6.24}$$

ความแตกต่างของเอสเอ็นอาร์ระหว่างแทร็กลำดับที่ i กับแทร็กลำดับที่ $i+1$ เมื่อ $1 \le i \le L-1$ จะมีค่าเท่ากับ

$$\Delta_i = \mathrm{SNR}_{i+1} - \mathrm{SNR}_i \tag{6.25}$$

ในงานวิจัยนี้ กำหนดให้ ความแตกต่างของเอสเอ็นอาร์ระหว่างแทร็กใดๆ มีค่าเท่ากับ $\Delta = \Delta_1 = \Delta_2 = \ldots = \Delta_L$ ดังนั้น ค่าเฉลี่ยเอสเอ็นอาร์ของช่องสัญญาณจะมีค่าเท่ากับ

$$\mathrm{SNR}_{\mathrm{avg}} = \mathrm{SNR}_{\lceil L/2 \rceil} \tag{6.26}$$

เมื่อ $\lceil . \rceil$ คือตัวดำเนินการปัดเศษขึ้น

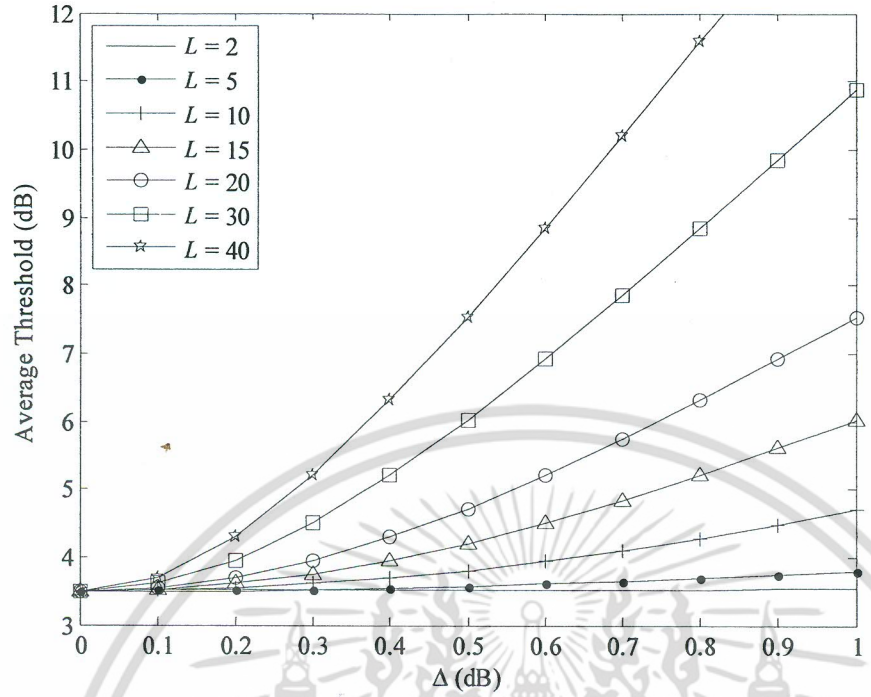
6.3.3 ผลการจำลองสมรรถนะของการถอดรหัสสองมิติ

รูปที่ 6.15 แสดงค่าเฉลี่ยเทรสโฮลด์ (ค่าเฉลี่ยเอสเอ็นอาร์ต่ำสุดที่ทำให้การถอดรหัสปราศจากความผิดพลาด) ของรหัสแอลดีพีซีแบบสองมิติเมื่ออัตรารหัสเท่ากับ 8/9 และดีกรีของโนดตัวแปรเท่ากับ 3 จากรูป จะเห็นว่า เมื่อความแตกต่างของเอสเอ็นอาร์ Δ หรือจำนวนแทร็กที่ใช้ในการบันทึกข้อมูล L เพิ่มขึ้น จะทำให้ค่าเฉลี่ยเทรสโฮลด์เพิ่มขึ้น โดยค่าเฉลี่ยเทรสโฮลด์ที่เกิดขึ้น จะมีค่ามากกว่าค่าเฉลี่ยเทรสโฮลด์กรณีความแตกต่างของเอสเอ็นอาร์เท่ากับ $\Delta = 0$ หรือกรณีรหัสแอลดีพีซีแบบหนึ่งมิติ รูปที่ 6.16 แสดงค่าเฉลี่ยเทรสโฮลด์ของรหัสแอลดีพีซีแบบสองมิติเมื่ออัตรารหัสเท่ากับ 1/2 และดีกรีของโนดตัวแปรเท่ากับ 3 โดยจะสังเกตได้ว่า เมื่อความแตกต่างของเอสเอ็นอาร์ Δ หรือจำนวน

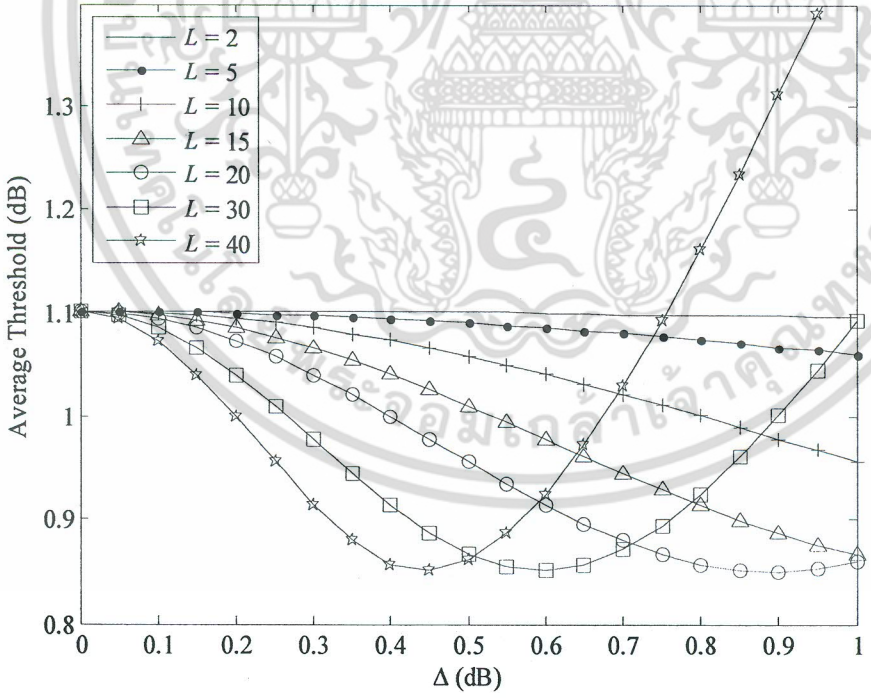
แทร็กที่ใช้ในการบันทึกข้อมูล L เพิ่มขึ้น จะทำให้ค่าเฉลี่ยเทรสโฮลด์ลดลง โดยค่าเฉลี่ยเทรสโฮลด์จะมีค่าน้อยกว่าค่าเฉลี่ยเทรสโฮลด์กรณีความแตกต่างของเอสเอ็นอาร์เท่ากับ $\Delta = 0$ หรือกรณีรหัสแอลดีพีซีแบบหนึ่งมิติ ในที่นี้ เมื่อความแตกต่างของเอสเอ็นอาร์เท่ากับ $\Delta = 0.45$ และจำนวนแทร็กเท่ากับ $L = 40$ จะทำให้รหัสแอลดีพีซีแบบสองมิติใช้ค่าเฉลี่ยเทรสโฮลด์ลดลง 0.251 dB เมื่อเทียบกับรหัสแอลดีพีซีแบบหนึ่งมิติ ดังนั้น จากผลลัพธ์ที่แสดงในรูปที่ 6.15 และ 6.16 อาจกล่าวได้ว่า สำหรับรหัสแอลดีพีซีแบบสองมิติที่อัตรารหัสสูง ความแตกต่างของเอสเอ็นอาร์ Δ จะทำให้สมรรถนะของการถอดรหัสลดลง อย่างไรก็ตาม สำหรับรหัสแอลดีพีซีแบบสองมิติที่อัตรารหัสปานกลาง ความแตกต่างของเอสเอ็นอาร์ Δ จะทำให้สมรรถนะของการถอดรหัส ดีขึ้น ในทางปฏิบัติสามารถทำได้โดยการเขียนข้อมูลให้ขนาดของแทร็กแตกต่างกันมากขึ้น เพื่อทำให้ความแตกต่างของเอสเอ็นอาร์ Δ เพิ่มขึ้น

รูปที่ 6.17 แสดงค่าเทรสโฮลด์ของแทร็กที่ 1 และแทร็กที่ L ของค่าเฉลี่ยเทรสโฮลด์ที่แสดงในรูปที่ 6.15 เมื่อค่าเทรสโฮลด์ของแทร็กที่ 1 ลดลง จะทำให้ค่าเทรสโฮลด์ของแทร็กที่ L เพิ่มขึ้น (จากแบบจำลองช่องสัญญาณ ค่าเอสเอ็นอาร์ของแทร็กที่ L จะมากกว่าหรือเท่ากับแทร็กที่ 1 เสมอ) ซึ่งกรณีจำนวนแทร็กเท่ากับ $L = 2$ ค่าเทรสโฮลด์ต่ำสุดที่เป็นไปได้ของแทร็กที่ 1 มีแนวโน้มคงที่เท่ากับ 1.8 dB โดยประมาณ กล่าวคือ การบันทึกข้อมูลโดยใช้รหัสแอลดีพีซีสองมิติที่มีจำนวนแทร็กเท่ากับ $L = 2$ ค่าเอสเอ็นอาร์ของแทร็กต่างๆ จะต้องมากกว่า 1.8 dB เสมอ รูปที่ 6.18 แสดงค่าเทรสโฮลด์ของแทร็กที่ 1 และแทร็กที่ L สำหรับการบันทึกข้อมูลโดยใช้อัตรารหัสเท่ากับ 1/2 จากรูปจะเห็นได้ว่า กรณีจำนวนแทร็กเท่ากับ $L = 2$ ค่าเทรสโฮลด์ต่ำสุดของแทร็กที่ 1 ยังคงมีแนวโน้มคงที่ ดังนั้น อาจกล่าวได้ว่า การบันทึกข้อมูลโดยใช้รหัสแอลดีพีซีสองมิติ จำนวนแทร็กควรมีค่าที่มากกว่า 2 เพื่อทำให้การบันทึกข้อมูลลงในแทร็กที่มีค่าเอสเอ็นอาร์ต่ำสามารถกระทำได้

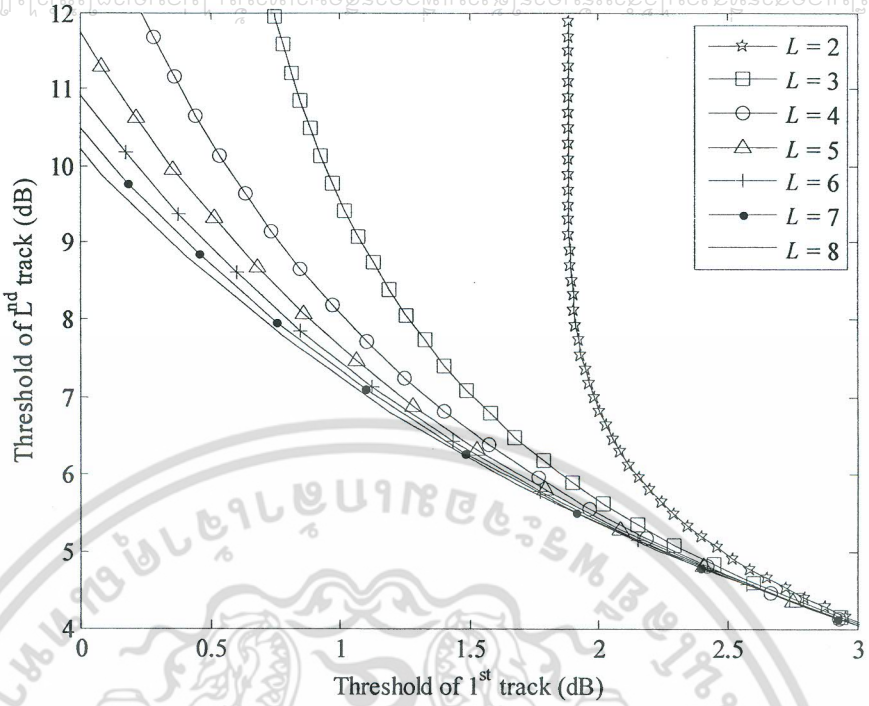
กำหนดให้ รหัสแอลดีพีซีสองมิติมีความยาวคำรหัสเท่ากับ 10,000 บิต ดีกรีของโนดตัวแปรเท่ากับ 3 จำนวนแทร็กที่ใช้บันทึกข้อมูลเท่ากับ 40 แทร็ก และจำนวนการถอดรหัสวนซ้ำเท่ากับ 50 รอบ รูปที่ 6.19 แสดงอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีสองมิติกรณีอัตรารหัสเท่ากับ 8/9 จากรูปจะเห็นว่า เมื่อความแตกต่างของเอสเอ็นอาร์ Δ เพิ่มขึ้น สมรรถนะของรหัสแอลดีพีซีสองมิติที่อัตรารหัส 8/9 จะลดลง สอดคล้องกับผลการวิเคราะห์ค่าเทรสโฮลด์ในรูปที่ 6.15 ซึ่งความแตกต่างของเอสเอ็นอาร์ Δ ที่เพิ่มขึ้น ทำให้ค่าเทรสโฮลด์ของการถอดรหัสเพิ่มขึ้น สำหรับอัตราเฟรมผิดพลาดของรหัสแอลดีพีซีสองมิติกรณีอัตรารหัสเท่ากับ 1/2 แสดงในรูปที่ 6.20 เมื่อความแตกต่างของเอสเอ็นอาร์ Δ เพิ่มขึ้น สมรรถนะของรหัสแอลดีพีซีสองมิติจะเพิ่มขึ้น โดยที่อัตราเฟรมผิดพลาดเท่ากับ 2×10^{-5} รหัสแอลดีพีซีสองมิติที่มี $\Delta = 0.45$ จะให้ค่าเฉลี่ยเอสเอ็นอาร์ลดลง 0.16 dB เมื่อเทียบกับรหัสแอลดีพีซีสองมิติที่มี $\Delta = 0$ ใกล้เคียงกับผลการวิเคราะห์ค่าเทรสโฮลด์ในรูปที่ 6.16



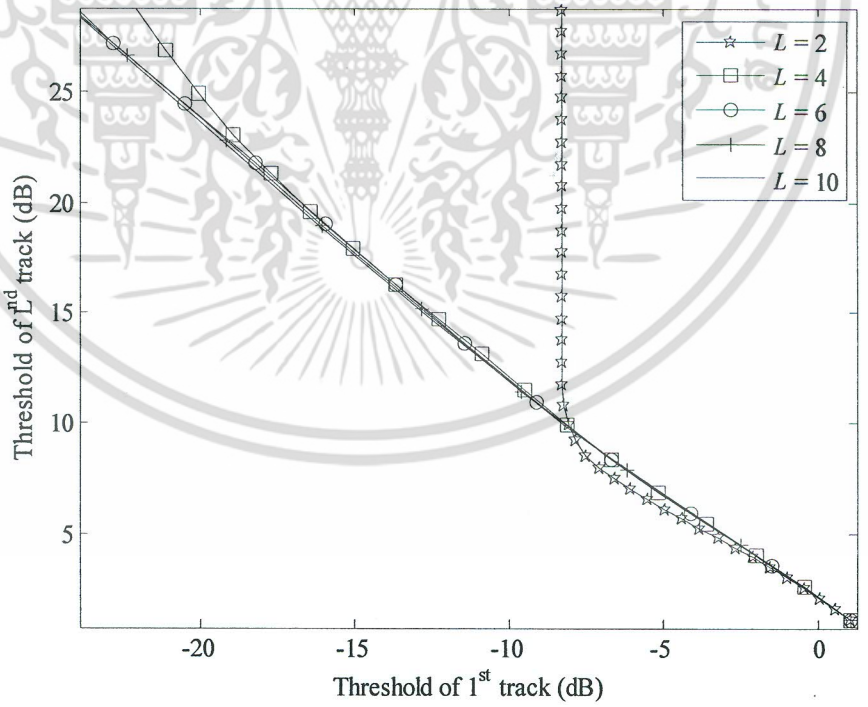
รูปที่ 6.15 ค่าเทรสโฮลด์เฉลี่ยของรหัสแอลดีพีซีสองมิติเมื่ออัตรารหัสเท่ากับ 8/9



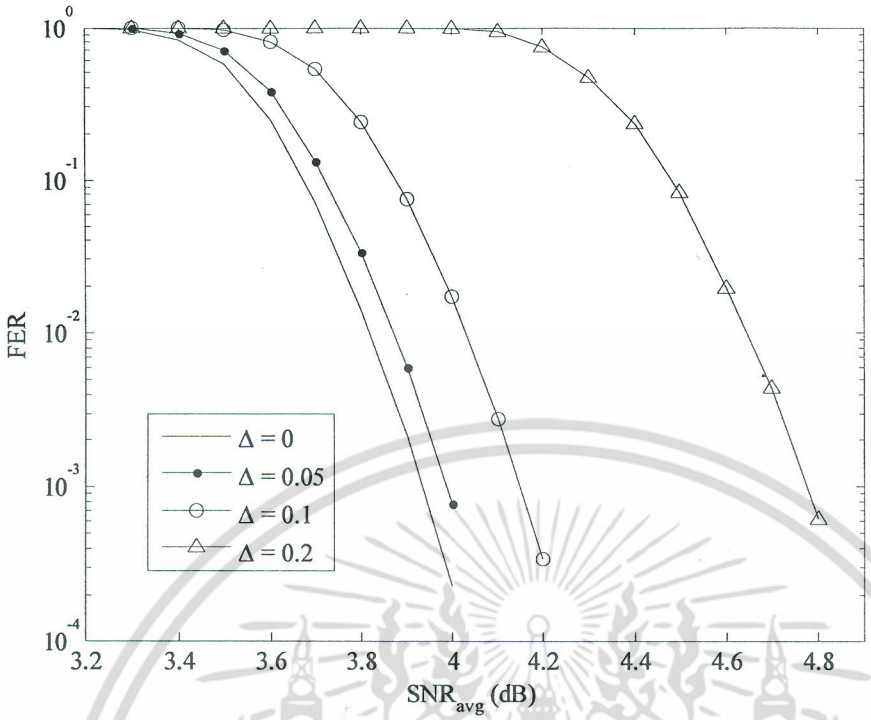
รูปที่ 6.16 ค่าเทรสโฮลด์เฉลี่ยของรหัสแอลดีพีซีสองมิติเมื่ออัตรารหัสเท่ากับ 1/2



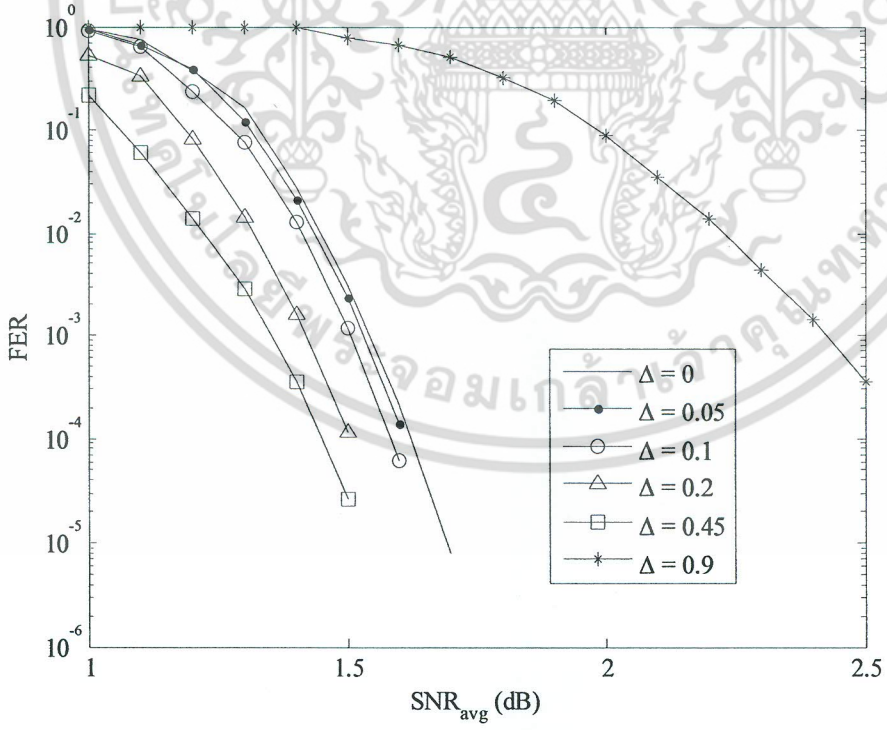
รูปที่ 6.17 ค่าเทรสโฮลด์ของแทร็กที่ 1 และแทร็กที่ L ของรหัสแอลดีพีซีสองมิติ เมื่ออัตรารหัสเท่ากับ 8/9



รูปที่ 6.18 ค่าเทรสโฮลด์ของแทร็กที่ 1 และแทร็กที่ L ของรหัสแอลดีพีซีสองมิติ เมื่ออัตรารหัสเท่ากับ 1/2



รูปที่ 6.19 อัตราเฟรมผิดพลาดของรหัสแอลดีพีซีสองมิติเมื่ออัตรารหัสเท่ากับ 8/9



รูปที่ 6.20 อัตราเฟรมผิดพลาดของรหัสแอลดีพีซีสองมิติเมื่ออัตรารหัสเท่ากับ 1/2

บทที่ 7
สรุปผลการวิจัย

งานวิจัยของวิทยานิพนธ์ฉบับนี้ แบ่งออกเป็น 2 ส่วนหลัก ได้แก่ การปรับปรุงสมรรถนะของการออกแบบรหัสแอลดีพีซี (บทที่ 5) และการปรับปรุงสมรรถนะของการถอดรหัสแอลดีพีซี (บทที่ 6)

สรุปผลการวิจัยที่เกี่ยวข้องกับการปรับปรุงสมรรถนะของการออกแบบรหัสแอลดีพีซี ดังนี้

1. รหัสควอไซไซคลิกวัฏจักรสูง (หัวข้อ 5.1)

โครงสร้างรหัสแอลดีพีซีแบบควอไซไซคลิกถูกนำมาประยุกต์ใช้งานในปัจจุบัน เนื่องจากการเข้ารหัสมีความซับซ้อนต่ำ ดังนั้น งานวิจัยนี้จึงมุ่งเน้นการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก โดยงานวิจัย ได้นำเสนออัลกอริทึมพีอีจีที่มีการดัดแปลงเพื่อแก้ปัญหาสถานการณ์ตัวเลือกมากหรืออัลกอริทึมพีอีจีคิวซีแม็กสำหรับการออกแบบรหัสแอลดีพีซีแบบควอไซไซคลิก วิธีการออกแบบรหัสแอลดีพีซีที่ได้นำเสนอนี้ ทำให้รหัสแอลดีพีซีมีวัฏจักรขนาดสูง ผลการทดลอง แสดงให้เห็นว่าที่อัตรารหัส 5/6 การออกแบบด้วยอัลกอริทึมพีอีจีคิวซีแม็ก ทำให้ กราฟแทนเนอร์มีวัฏจักรขนาด 8 จำนวน 10.50% ซึ่งการออกแบบด้วยอัลกอริทึมพีอีจีและอัลกอริทึมพีอีจีคิวซีที่นำเสนอในงานวิจัยก่อนหน้ามีวัฏจักรขนาด 8 จำนวน 3.55% และ 3.74% ตามลำดับ ส่งผลให้ รหัสแอลดีพีซีที่ออกแบบด้วยอัลกอริทึมพีอีจีคิวซีแม็กให้สมรรถนะของการแก้ไขบิตผิดพลาดสูงกว่ารหัสแอลดีพีซีที่ได้รับการออกแบบด้วยอัลกอริทึมพีอีจีและอัลกอริทึมพีอีจีคิวซี โดยที่อัตราบิตผิดพลาดเท่ากับ 4×10^{-8} รหัสแอลดีพีซีที่นำเสนอใช้ค่าเอสเอ็นอาร์ลดลง 0.12 dB

2. รหัสอินเทอร์ลิฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน (หัวข้อ 5.2)

สำหรับช่องสัญญาณผลตอบสนองบางส่วน นิยมใช้ วงจรถอดรหัสเทอร์โบอีควอไลเซชันซึ่งประกอบไปด้วยวงจรหาวีเทอร์บิและวงจรถอดรหัสแอลดีพีซี อย่างไรก็ตาม การประยุกต์ใช้งานรหัสแอลดีพีซีแบบควอไซไซคลิกและแบบอาร์เรย์ในวงจรถอดรหัสเทอร์โบอีควอไลเซชัน จะก่อให้เกิดวัฏจักรเทียมที่ส่งผลต่อสมรรถนะของการถอดรหัส ดังนั้น ในงานวิจัยนี้ จึงนำเสนอรหัสไอแม็กซึ่งลดจำนวนวัฏจักรเทียมของวงจรถอดรหัสเทอร์โบอีควอไลเซชัน ผลการทดลอง แสดงให้เห็นว่า ที่อัตรารหัส 0.91 รหัสไอแม็กมีจำนวนวัฏจักรเทียมน้อยกว่ารหัสที่ได้รับการนำเสนอในงานวิจัยก่อนหน้า อีกทั้ง รหัสไอแม็กปราศจากวัฏจักรขนาด 4 ทำให้ อัตราบิตผิดพลาดของรหัสไอแม็กต่ำกว่ารหัสอื่นโดยที่อัตราบิตผิดพลาดเท่ากับ 4×10^{-7} รหัสแอลดีพีซีที่นำเสนอใช้ค่าเอสเอ็นอาร์ลดลง 0.5 dB ภายใต้ช่องสัญญาณผลตอบสนองบางส่วน EPR2

3. รหัสโปรโตกราฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน (หัวข้อ 5.3)

ปัจจุบันรหัสโปรโตกราฟได้ความสนใจอย่างมาก เนื่องจาก การวิเคราะห์สมรรถนะของรหัสโปรโตกราฟสามารถประยุกต์ใช้วิธีการเอ็กซิตชาร์ทเพื่อคำนวณค่าเทรสโฮลด์ หรือค่าเอสเอ็นอาร์ต่ำสุดที่ทำให้ข้อมูลปราศจากบิตผิดพลาดในทางทฤษฎี ทำให้สามารถออกแบบรหัสโปรโตราฟที่มีสมรรถนะเข้าใกล้ขีดจำกัดของแชนนอนได้ อย่างไรก็ตาม ในงานวิจัยก่อนหน้าการวิเคราะห์สมรรถนะของรหัสโปรโตกราฟสำหรับช่องสัญญาณผลตอบสนองบางส่วน จำกัดเฉพาะกรณีฟิลด์จำกัด GF(2) ซึ่งปัจจุบันรหัสแอลดีพีซีบนฟิลด์จำกัด GF(q) เมื่อ $q>2$ ได้รับความนิยมในการประยุกต์ใช้งาน ทำให้ งานวิจัยนี้นำเสนอวิธีการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสโปรโตกราฟบนฟิลด์จำกัด GF(q) สำหรับช่องสัญญาณผลตอบสนองบางส่วน ผลการวิเคราะห์แสดงให้เห็นว่า ในช่องสัญญาณแบบ PR1 และ PR2 รหัสอาร์เอให้สมรรถนะที่ดีเมื่อฟิลด์จำกัดมีค่าน้อย และรหัสสม่ำเสมอ $d_v=2$ จะมีสมรรถนะที่ดีสุดเมื่อฟิลด์จำกัดมีค่าสูง

สรุปผลการวิจัยที่เกี่ยวข้องกับการปรับปรุงสมรรถนะของการถอดรหัสแอลดีพีซี ดังนี้

1. การถอดรหัสกระจายความเชื่อมั่นสองทิศทาง (หัวข้อ 6.1)

การออกแบบวงจรถอดรหัสแอลดีพีซีในปัจจุบัน อัลกอริทึมแอลบีพีได้รับความนิยมในการประยุกต์ใช้งาน เนื่องจาก การถอดรหัสให้อัตราบิตผิดพลาดต่ำและการออกแบบวงจรมีความซับซ้อนที่มีความเหมาะสม ดังนั้น ในงานวิจัยนี้ จึงนำเสนอการปรับปรุงอัลกอริทึมแอลบีพีด้วยวิธีการกระจายความเชื่อมั่นสองทิศทาง ผลการจำลองแสดงให้เห็นว่า วิธีการที่นำเสนอนี้ ให้อัตราบิตผิดพลาดต่ำลงเมื่อใช้จำนวนการถอดรหัสวนซ้ำที่เท่ากัน โดยเมื่ออัตรารหัสเท่ากับ 8/9 อัตราเฟรมผิดพลาดเท่ากับ 7×10^{-4} การถอดรหัสที่ได้นำเสนอใช้ค่าเอสเอ็นอาร์ลดลง 0.04 dB นอกจากนี้ ในงานวิจัย แสดงการวิเคราะห์สมรรถนะของการถอดรหัสด้วยวิธีการเอ็กซิตชาร์ท โดยพบว่าวิธีการถอดรหัสที่ได้นำเสนอให้ค่าเทรสโฮลด์เท่ากับวิธีการถอดรหัสในงานวิจัยก่อนหน้า แต่ใช้จำนวนรอบของการถอดรหัสวนซ้ำที่ลดลง

2. การถอดรหัสสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก (หัวข้อ 6.2)

ในระบบบันทึกข้อมูลเชิงแม่เหล็กแบบบิตแพทเทิร์น กระบวนการบันทึกอาจเกิดปัญหาที่เรียกว่าการเขียนผิดพลาด ส่งผลให้ เกิดความผิดพลาดในการบันทึกข้อมูล ทั้งนี้ สามารถจำลองการเขียนและอ่านข้อมูลด้วยแบบจำลองช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก ในงานวิจัยก่อนหน้าได้นำเสนอการปรับปรุงสัญญาณอินพุทของวงจรถอดรหัสแอลดีพีซี อย่างไรก็ตาม วิธีการดังกล่าวปราศจากการปรับปรุงกระบวนการถอดรหัส ดังนั้น ในงานวิจัยนี้จึงนำเสนอการปรับปรุงกระบวนการถอดรหัสแอลดีพีซีสำหรับช่องสัญญาณเรียงต่อสมมาตรไบนารีและเกาส์สีขาวบวก ผลการจำลองแสดงให้เห็นว่า สำหรับรหัสแอลดีพีซีอัตรารหัสเท่ากับ 7/8 อัตราบิตผิดพลาดเท่ากับ 2×10^{-5} วิธีการถอดรหัสที่นำเสนอ จะใช้ค่าเอสเอ็นอาร์ต่ำกว่าวิธีการปรับปรุงสัญญาณอินพุทของวงจรถอดรหัส

ประมาณ 0.15 และ 0.3 dB เมื่อความน่าจะเป็นตัดข้ามของช่องสัญญาณสมมาตรไบนารีเท่ากับ 5×10^{-4} และ 1×10^{-3} ตามลำดับ

3. การถอดรหัสสองมิติ (หัวข้อ 6.3)

ในระบบบันทึกข้อมูลเชิงแม่เหล็ก โดยทั่วไป คำรหัสที่ได้จากการเข้ารหัสแอลดีพีซีจะถูกบันทึกลงในแทร็กเดียวกัน อย่างไรก็ตาม แทร็กต่างๆ ในสื่อบันทึกข้อมูลจะมีค่าเอสเอ็นอาร์ที่แตกต่างกันเสมอ ทำให้ งานวิจัยนี้ นำเสนอรหัสแอลดีพีซีแบบสองมิติ ซึ่งคำรหัสจะถูกแบ่งและบันทึกลงในแทร็กที่แตกต่างกัน เป็นผลให้ ในกระบวนการถอดรหัส บิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์สูงสามารถช่วยบิตคำรหัสที่อยู่ในแทร็กซึ่งมีค่าเอสเอ็นอาร์ต่ำ โดยงานวิจัยนำเสนอวิธีการวิเคราะห์สมรรถนะทางทฤษฎีของรหัสแอลดีพีซีเมื่อทำการถอดรหัสแบบสองมิติ ผลการวิเคราะห์แสดงให้เห็นว่าที่อัตรารหัสสูง ความแตกต่างของค่าเอสเอ็นอาร์ระหว่างแทร็กจะทำให้สมรรถนะของการถอดรหัสลดลง อย่างไรก็ตาม สำหรับรหัสแอลดีพีซีแบบสองมิติที่อัตรารหัสปานกลาง ความแตกต่างของค่าเอสเอ็นอาร์จะทำให้สมรรถนะของการถอดรหัสดีขึ้น ในทางปฏิบัติ ความแตกต่างของค่าเอสเอ็นอาร์แต่ละแทร็กสามารถทำได้โดยการเขียนแทร็กให้มีขนาดที่แตกต่างกัน นอกจากนี้ การบันทึกข้อมูลโดยใช้รหัสแอลดีพีซีแบบสองมิติ จำนวนแทร็กที่ใช้ในการบันทึกควรมากกว่า 2 แทร็ก เพื่อทำให้การบันทึกข้อมูลลงในแทร็กที่มีค่าเอสเอ็นอาร์ต่ำสามารถกระทำได้

บรรณานุกรม

[1] R. Gallager, "Low-density parity-check codes," **IRE Transactions on Information Theory,** vol. 8, pp. 21-28, 1962.

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

[3] R. M. Tanner, "A recursive approach to low complexity codes," **IEEE Transactions on Information Theory**, vol. 27, pp. 533–547, 1981.

[4] Z. Li and B.V.K.V. Kumar, "A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph," **in Proc. Asilomar Conference on Signals, Systems and Computers**, pp. 1990-1994, Nov. 2004.

[5] X.Y. Hu, E. Eleftheriou and D.M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," **IEEE Transactions on Information Theory,** vol. 51, pp. 386-398, Jan. 2005.

[6] C. Douillard, M. Jezequel, and C. Berrou, "Iterative correction of intersymbol interference: Turbo equalization," **European Transactions on Telecommunications**, vol. 6, no. 5, pp. 507–511, Sep.–Oct. 1995.

[7] J. Hagenauer and P. Hoeher, "A Viterbi algorithm with soft-decision outputs and its applications," **in Proc. IEEE Global Communications Conference**, pp. 47.11-47.17, Nov. 1989.

[8] T. Kanaoka and T. Morita, "Structured LDPC Codes with Reversed MTR/ECC for Magnetic Recording Channels," **IEEE Transactions on Magnetics,** vol. 42, no. 10, pp. 2561-2563, Oct. 2006.

[9] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," **JPL IPN Progress Report**, Aug. 2003.

[10]T.V. Nguyen, "Protograph-based LDPC codes for partial response channels," in *Proc. IEEE ICC* 2012, pp. 2166-2170, Jun. 2012.

[11]Y. Fang, P. Chen, L. Wang and F.C.M. Lau, "Design of protograph LDPC codes for partial response channels," **IEEE Transactions on Communications,** vol. 60, no. 10, pp. 2809-2819, Oct. 2012.

[12]M. Davey and D. J. C. MacKay, "Low density parity check codes over GF(q)," **IEEE Communication Letters**, vol. 2, no. 6, pp. 165–167, Jun. 1998.

[13]J. Zhang, Y. Wang, M. P. C. Fossorier and J. S. Yedidia, "Iterative Decoding With Replicas," **IEEE Transactions on Information Theory**, vol. 53, pp. 1644-1663, 2007.

[14]Z. Juntan and M. Fossorier, "Shuffled belief propagation decoding," **in Proc. Asilomar Conference on Signals, System and Computer**, pp. 8-15, 2002

[15]D.E. Hocevar, "A reduced complexity decoder architecture via layered decoding of LDPC codes," **in Proc. IEEE Workshop on Signal Processing Systems**, pp. 107-12, 2004.

[16]H.J. Richter, *et al.*, "Recording on bit-patterned media at densities of 1 Tb/in^2 and beyond," **IEEE Transactions on Magnetics**, vol. 42, no. 10, pp. 2255–2260, Oct. 2006.

[17]H. Muraoka and S.J. Greaves, "Statistical modeling of write error rates in bit patterned media for 10 Tb/in^2 recording," **IEEE Transactions on Magnetics**, vol. 47, no. 1, pp. 26-34, Jan. 2011.

[18]A.R. Iyengar, P.H. Siegel, and J.K. Wolf, "LDPC codes for the cascaded BSC-BAWGN channel," **in Proc. 47th Annual Allerton Conference on Communication, Control and Computing**, pp. 620-627, Sept. 2009.

[19]A. Lender, "Correlative level coding for binary-data transmission," **IEEE Spectrum**, vol. 3, no. 2, pp. 104-115, Feb. 1966.

[20]E. R. Kretzmer, "Generalization of a technique for binary data transmission," **IEEE Transactions on Communication Technology**, vol. 14, no. 1, pp. 67-68, Feb. 1967.

[21]R. Karabed and P.H. Siegel, "Even-mark-modulation for optical recording," **in Proc. IEEE International Conference on Communications**, vol. 3, pp. 1628-1632, Jun. 1989.

[22]H. Thapar and A. Patel, "A class of partial response systems for increasing storage density in magnetic recording," **IEEE Transactions on Magnetics**, vol. 23, no. 5, pp. 3666-3668, Sept. 1987.

[23]D. Arnold and H.-A. Loeliger, "On the information rate of binary-input channels with memory," **in Proc. IEEE International Conference on Communications**, vol. 7, pp. 2692–2695, Jun. 2001.

[24]L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," **IEEE Transactions on Information Theory**, vol. 20, no. 3, pp. 284–287, Mar. 1974.

[25]T. Cover and J. Thomas, **Elements of Information Theory**, 2nd edn., New York, Wiley, 2006.

[26]A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," **IEEE Transactions on Information Theory**, vol. 13, no. 4, pp. 260–269, Apr. 1967.

[27]G. D. Forney, Jr., "The Viterbi algorithm," **Proceedings of the IEEE**, vol. 61, no. 3, pp. 268–278, Mar. 1973.

[28]T. J. Richardson, and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," **IEEE Transactions on Information Theory**, vol. 47, pp. 599-618, 2001

[29]W. E. Ryan and S. Lin, **Channel Codes**, Cambridge university press, 2009.

[30]T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," **IEEE Transactions on Information Theory**, vol. 47, no. 2, pp. 638-656, 2001

[31]S. Lin and D. J. Costello, Jr., **Error Control Coding: Fundamentals and Applications**, 2nd ed., Prentice-Hall, 2004.

[32]T. J. Richardson and M. A. Shokrollahi, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," **IEEE Transactions on Information Theory**, vol. 47, no. 2, pp. 619-637, 2001

[33]T. Tian, C. Jones, J. Villasenor, and R. Wesel, "Construction of irregular LDPC codes with low error floors," **in Proc. IEEE International Conference on Communications**, pp. 3125–3129, May 2003.

[34]C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes.," **in Proc. IEEE International Conference on Communications**, vol.2, pp. 1064-1070, 1993.

[35]D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," **IEEE Transactions on Information Theory**, vol. 45, pp. 399-431, Mar. 1999.

[36]M. Blaum, R. Roth, "New array codes for multiple phased burst correction," **IEEE Transactions on Information Theory**, vol. 39, no. 1, pp. 66-77, Jan 1933.

[37]I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," **Journal of the Society for Industrial and Applied Mathematics**, vol. 8, pp. 300-304, 1960.

[38]J. L. Fan, "Array codes as low-density parity check codes," **in Proc. International Symposium on Turbo Codes & Related Topics**, pp. 543-546, 2000.

[39]E. Eleftheriou and S. Olcer, "Low-density parity-check codes for digital subscriber lines," **in Proc. IEEE International Conference on Communications**, pp. 1752-1757 vol.3, 2002.

[40]M. M. Mansour and N. R. Shanbhag, "High-throughput LDPC decoders," **IEEE Transactions on Very Large Scale Integration Systems**, pp. 976-96, 2003.

[41]Y. M. Chang, A. I. V. Casado, M. C. F. Chang, and R. D. Wesel, "Lower-Complexity Layered Belief-Propagation Decoding of LDPC Codes," **in Proc. IEEE International Conference on Communications**, pp. 1155-1160, 2008.

[42]S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," **IEEE Transactions on Communications**, vol. 52, pp. 670-678, Apr. 2004.

[43]G. Liva and M. Chiani, "Protograph LDPC codes design based on EXIT analysis," **in Proc. IEEE Global Communications Conference**, pp. 3250-3254. Nov. 2007.

[44]A. Abbasfar, D. Divsalar and K. Yao, "Accumulate-repeat-accumulate codes," **IEEE Transactions on Communications**, vol. 55, no. 4, pp. 692–702, Apr. 2007.

[45]"IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," **IEEE Std 802.11n-2009**, pp. c1-502, 2009.

[46]P. Supnithi, W. Phakphisut and W. Singhaudom, "Structured LDPC codes to reduce pseudo cycles for turbo equalization in perpendicular magnetic recording," **IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences**, vol. E94-A, no. 6, pp. 1441-1448, Jun. 2011.

[47]R. Koetter, A.C. Singer and M. Tuchler, "Turbo equalization," **IEEE Signal Processing Magazine**, pp. 67-80, Jan. 2004.

[48]A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," **IEEE Transactions on Information Theory**, vol. 52, no. 2, pp. 549-583, Feb. 2006.

[49]B.Y. Chang, L. Dolecek and D. Divsalar, "EXIT chart analysis and design of nonbinary protograph-based LDPC codes," **in Proc. IEEE Military Communications Conference**, pp. 566-571, Nov. 2011.

[50]Y. Nakamura, Y. Okamoto, H. Osawa, H. Aoi and H. Muraoka, "A study of LDPC coding and iterative decoding system in magnetic recording system using bit-patterned medium with write error," **IEEE Transactions on Magnetics**, vol. 45, no. 10, pp. 3753-3756, Oct. 2009.

ผลงานวิจัยที่ได้รับการตีพิมพ์

ผลงานวิจัยที่ได้รับการตีพิมพ์ในวารสารวิชาการ

1. W. Phakphisut, P. Supnithi and N. Puttarak, "EXIT Chart Analysis of Nonbinary Protograph LDPC Codes for Partial Response Channels," **IEEE Transaction on Magnetics**, vol. 50, no. 11, Nov. 2014.
2. W. Phakphisut, P. Prompakdee and P. Supnithi, "Design of Quasi-Cyclic LDPC codes with Maximized Girth Property," **IEICE Transactions on Fundamentals**, vol. E96-A, no. 11, pp. 2128-2133, Nov. 2013.
3. P. Supnithi, W. Wiriya, W. Phakphisut and N. Puttarak, "LDPC Decoder using Pattern-Dependent Modified LLR for the Bit Patterned Media Storage with Written-in Errors," **IEEE Transaction on Magnetics**, vol. 48, no. 11, pp.4606-4609, Nov. 2012
4. W. Phakphisut, P.Supnithi, T.Sopon and L.M.M. Myint, "Serial belief propagation for the high-rate LDPC decoders and performances in the bit patterned media systems with media noise," **IEEE Transaction on Magnetics**, vol. 47, no. 10, pp. 3562 - 3565, Oct. 2011.
5. P. Supnithi, W. Phakphisut and W. Singhaudom, "Structured LDPC Codes to Reduce Pseudo Cycles for Turbo Equalization in Perpendicular Magnetic Recording," **IEICE Transactions on Fundamentals**, vol. E94-A, no. 6, pp. 1441-1448, Apr. 2011.

ผลงานวิจัยที่ได้รับการนำเสนอในงานประชุมวิชาการระดับนานาชาติ

1. W. Phakphisut, P. Supnithi, "Decoding Algorithm of LDPC codes for Cascaded BSC-AWGN channels," **Asia-Pacific Signal and Information Processing Association Annual Summit and Conference**, Siem Reap, Cambodia, December 9-12, 2014.
2. W. Phakphisut, P. Supnithi and N. Puttarak, "EXIT Chart Analysis of Nonbinary Protograph LDPC Codes for Partial Response Channels," **IEEE International Magnetics Conference**, Dresden, Germany, May 4-8, 2014.

3. W. Phakphisut, P. Prompakdee, P. L. Phong and P. Supnithi, "Design of Quasi-cyclic LDPC codes with maximized girth property," **International Workshop on Smart Info-Media Systems in Asia, Bangkok**, Thailand, Sep. 6–Sep. 8, 2012
4. W.Phakphisut and P.Supnithi, "Mixed-Scheduling Belief Propagation for LDPC Decoders in the Magnetic Recording Systems" **International Symposium on Information Theory and its Applications**, Hawaii, USA, Oct. 28-31, 2012.
5. P. Supnithi, W. Wiriya, W. Phakphisut and N. Puttarak, "LDPC Decoder using Pattern-Dependent Modified LLR for the Bit Patterned Media Storage with Written-in Errors," **IEEE International Magnetics Conference**, Vancouver, Canada, May 9-11, 2012.
6. W. Phakphisut, P. Supnithi and N. Puttarak, "Mixed-Scheduling Belief Propagation for LDPC Decoders in the Bit Patterned Media Storage," **IEEE International Magnetics Conference**, Vancouver, Canada, May 9-11, 2012.
7. W. Wiriya, W. Phakphisut and P. Supnithi, "LDPC Decoder with Modified LLR for Bit Patterned Media with Write Errors," **IEEE Intelligent Signal Processing and Communication Systems**, Chiangmai, Thailand, December 7-9, 2011.
8. P. Prompakdee, W. Phakphisut and P. Supnithi, "Quasi-cyclic LDPC codes based on PEG algorithm with maximized girth property," **IEEE Intelligent Signal Processing and Communication Systems**, Chiangmai, Thailand, December 7-9, 2011.
9. W. Phakphisut, T. Sopon, P. Supnithi, L.M.M. Myint and A. Siritaratiwat, "Serial belief propagation for the high-rate LDPC decoders and performances in the bit patterned media systems with media noise," **IEEE International Magnetics Conference**, Taipei, Taiwan, April 25-29, 2011.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายเวธิต ภาคย์พิสุทธิ์
วัน เดือน ปีเกิด	9 พฤษภาคม 2530
ที่อยู่	42 ถ.เทศบาล 7 ต.ตลาดหลวง อ.เมือง จ.อ่างทอง 14000
ประวัติการศึกษา	2552 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
	2554 วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีการบันทึกข้อมูล สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง