การออกแบบรหัสโพลาร์แบบแบ่งส่วนโดยใช้เทคนิคการตัดเส้นทางและการเลือกซีอาร์ซี

DESIGN OF PARTITIONED POLAR CODING WITH PATH ELIMINATION AND CRC SELECTION TECHNIQUES

อนุสรณ์ วงค์ษา

ANUSORN WONGSA

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2567

KMITL-2024-EN-M-017-254

DESIGN OF PARTITIONED POLAR CODING WITH PATH ELIMINATION AND CRC SELECTION TECHNIQUES

ANUSORN WONGSA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN TELECOMUNICATION ENGINEERING

SCHOOL OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2024

KMITL-2024-EN-M-017-254

หัวข้อวิทยานิพนธ์	การออกแบบรหัสโพลาร์แบบแบ่งส่วนโดยใช้เทคนิคการตัดเส้นทางและการเลือกซีอาร์ซี
นักศึกษา	นายอนุสรณ์ วงค์ษา
รหัสประจ าตัว	62601094
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2567
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร.เวธิต ภาคย์พิสุทธิ์

บทคัดย่อ

รหัสโพลาร์ที่มีรหัส CRC ที่ถูกอินเทอร์ลีฟ ซึ่งถูกใช้งานในมาตรฐานการสื่อสารไร้สายยุคที่ 5 ให้สมมรถนะการแก้ไขความผิดพลาดที่ดีเยี่ยมภายใต้ตัวถอดรหัสหักล้างต่อเนื่องแบบลิส แต่ต้องแลกกับความซับซ้อนที่สูงเมื่อถูกใช้งานจริง หนึ่งในเทคนิคการลดความซับซ้อนนั้นคือการแบ่งส่วนตัวถอดรหัสที่สามารถลดขนาดพื้นที่หน่วยความจาได้อย่างมาก แต่ต้องแลกกับสมรรถนะการแก้ไขความผิดพลาดที่สูญเสียเมื่อเทียบกับการถอดรหัสแบบดั้งเดิม วิทยานิพนธ์ฉบับนี้จึงน าเทคนิคการถอดรหัสที่ถูกแบ่งส่วนมาใช้งานร่วมกับรหัสโพลาร์ตามมาตรฐาน 5G จากนั้นได้นาเสนอเทคนิคการถอดรหัสเพิ่มเติมทั้งวิธีการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทางที่สามารถปรับปรุงสมรรถนะการแก้ไขความผิดพลาดให้แก่รหัสโพลาร์ที่มีรหัส CRC ที่ถูกอินเทอร์ลีฟภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิส ซึ่งยังสามารถใช้งานเพื่อชดเชยสมรรถนะที่สูญเสียไปภายใต้ตัวถอดรหัสที่ถูกแบ่งส่วนได้เช่นกัน เทคนิคการถอดรหัสที่นาเสนอทางานร่วมกับรหัส CRC ภายในรหัสโพลาร์ โดยช่วยให้ตัวถอดรหัสเลือกบิตรหัสที่ถูกต้องได้ดีขึ้น วิทยานิพนธ์ยังได้นาเสนอเกณฑ์การเลือกรหัส CRC ที่เหมาะสมกับการถอดรหัสที่ถูกแบ่งส่วนร่วมกับวิธีการปรับค่าความน่าเชื่อถือเส้นทาง โดยเลือกพหุนาม CRC จากค่าน้ำหนักแถวแรกจากเมทริกซ์พาริตีตรวจสอบของรหัส CRC ผลการจาลองแสดงให้เห็นว่า หากเลือกตัวถอดรหัสที่ถูกแบ่งส่วนที่เหมาะสมใช้งานร่วมกับรหัสโพลาร์ตามมาตรฐาน 5G จะสามารถลดขนาดพื้นที่หน่วยความจาได้ถึงร้อยละ 46.31 ขณะที่สูญเสียสมรรถนะอัตราเฟรมผิดพลาดเพียง 0.02 dB และถ้าหากใช้งานวิธีการปรับค่าความน่าเชื่อถือเส้นทางร่วมจะสามารถชดเชยสมรรถนะอัตราเฟรมผิดพลาดมากถึง 0.2 dB และเกณฑ์การเลือกรหัส CRC ที่นาเสนอแสดงให้เห็นว่ารหัส CRC ที่มีค่าน้าหนักแถวแรกที่น้อยลงจะให้สมรรถนะการแก้ไขความผิดพลาดที่ดีกว่ารหัส CRC ที่มีค่าน้ าหนักแถวแรกมากกว่า

Thesis	Design of partitioned polar coding with path elimination and CRC selection techniques
Student	Mr. Anusorn Wongsa
Student ID.	62601094
Degree	Master of Engineering
Program	Telecommunications Engineering
Year	2024
Thesis Advisor	Assoc. Prof. Watid Phakpisut Ph.D.

ABSTRACT

Polar code with interleaved CRC code, which is implemented in the fifth-generation wireless communication standard, provides excellent error-correcting performance under successive cancellation list decoder. However, this comes with high complexity in its practical implementation. One such complexity reduction technique is decoder partitioning, which can greatly reduce the size of the memory area, but at the trade-off of losing error-correcting performance compared with a conventional decoder. This thesis includes a partition decoding technique using with the polar code in 5G. The thesis then proposes additional decoding techniques such as path elimination and path metric adjustment, which can improve error-correcting performance for a polar code with interleaved CRC under a successive cancellation list. This is also able to compensate for the performance loss under a partition decoder. The proposed decoding technique works with an inner CRC code of a polar code that allows the decoder to better select the correct decoding bits. This thesis also proposes the CRC selection criteria that suit for a partition decoding along with a path metric adjustment technique which is select the CRC polynomial based on first-row weight of its parity-check matrix of the CRC code. The simulations show that if the partitioned decoder is optimally selected for the polar code in 5G, the partitioned decoder is able to lower the memory area up to 46.31% with a 0.02 dB loss of frame error rate performance. Furthermore, by incorporating the path metric adjustment method, it can compensate for the performance loss up to 0.2 dB. The proposed CRC selection criteria results reveal that CRCs with lower first-row weight will provide superior error-correcting performance than CRCs with higher first-row weight

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้จะส าเร็จลุล่วงไปมิได้ หากมิได้รับความแนะน าค าสั่งสอนและความกรุณาจากท่านอาจารย์ที่ปรึกษาของผู้เขียน รองศาสตราจารย์ ดร.เวธิต ภาคย์พิสุทธิ์ โดยผู้เขียนได้รับการสั่งสอนความรู้พื้นฐานตั้งแต่ที่ก้าวเข้ามาในหลักสูตร อีกทั้งตลอดระยะเวลาการทาวิจัยที่ผู้เขียนได้รับแนวทางคาแนะนา คาสั่งสอน และประสบการณ์ที่ช่วยผู้เขียนในการเรียนและการทาวิจัย จนกระทั่งผลักดันให้ผู้เขียนสามารถตีพิมพ์บทความทางวิชาการได้ นอกจากนี้ยังสร้างทรรศนะคติที่ดีในการทางาน ทาวิจัย รวมถึงการใช้ชีวิตให้เหมาะสมแก่การเป็นนักศึกษาปริญญาโทที่ทางานวิจัย ผู้เขียนรู้สึกทราบซึ้งและขอบคุณต่อความเมตตากรุณาจากอาจารย์ที่ปรึกษา รวมบุคลากรฝ่ายสนับสนุน และอาจารย์ท่านอื่นภายในภาควิชา ที่ช่วยดูแลและให้ข้อมูล ข้อคิด และความรู้พื้นฐานที่ส าคัญต่อการด าเนินการวิจัย

ทั้งนี้สาหรับคุณทรัพย์ที่ผู้เขียนได้รับความช่วยเหลือตลอดการศึกษาในหลักสูตรดังกล่าว ผู้เขียนได้รับความสนับสนุนค่าธรรมเนียมการศึกษาจากสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง จากนั้นอาจารย์ที่ปรึกษาของผู้เขียน รองศาสตราจารย์ ดร.เวธิต ภาคย์พิสุทธิ์ ยังได้ให้เงินสนับสนุนในการใช้ในชีวิตประจาวันผ่านการจ้างเป็นผู้ช่วยนักวิจัยจากโครงการ จากหน่วยงานภายนอก และครอบครัวสาหรับการสนับสนุนด้านอื่น ซึ่งต้องขอขอบพระคุณทุกภาคส่วนที่ให้ผู้เขียนสามารถเลี้ยงชีพในการศึกษาระดับปริญญาโทตลอดมา

อนุสรณ์ วงค์ษา

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

บทน จะเกริ่นน การพัฒนาของเทคโนโลยีการเข้ารหัสช่องสัญญาณ (channel coding) ที่มาของรหัสโพลาร์ (polar codes) การพัฒนารหัสโพลาร์ก่อนที่จะถูกนามาประยุกต์ใช้ในมาตรฐานการสื่อสารไร้สายยุคที่ 5 โดยเฉพาะอย่างยิ่ง การนารหัสตรวจสอบด้วยส่วนซ้าซ้อนแบบวน (cyclic redundancy check) หรือ CRC เข้ามาช่วยเพิ่มสมรรถภาพของการถอดรหัสของรหัสโพลาร์ จากนั้นจะอธิบายปัญหาความซับซ้อนของการถอดรหัสโพลาร์ซึ่งเป็นจุดประสงค์ของงานวิจัยของวิทยานิพนธ์ฉบับนี้

1.1 ความสำคัญและความเป็นมาของปัญหา

การเข้ารหัสช่องสัญญาณ (channel coding) เป็นวิธีการเข้ารหัสข้อมูลดิจิทัลเพื่อแก้ไขความผิดพลาดของข้อมูลในระบบสื่อสาร การพัฒนารหัสช่องสัญญาณมีจุดเริ่มมาจากงานวิจัยของ คลอดด์ แชนนอน ในปี พ.ศ. 2491 [1] ในงานวิจัยได้พิสูจน์ว่าการสื่อสารดิจิทัลจะปราศจากความผิดพลาดของข้อมูลก็ต่อเมื่อการส่งข้อมูลมีปริมาณข่าวสารไม่เกินค่าความจุช่องสัญญาณหรือเรียกได้ว่า ความจุช่องสัญญาณ (channel capacity) การค้นพบดังกล่าวก่อให้เกิดการศึกษาและวิจัยการเข้ารหัสช่องสัญญาณ และการประยุกต์ใช้ทฤษฎีข่าวสาร (information theory) ในการสื่อสารดิจิทัล รหัสช่องสัญญาณถูกคิดค้นเป็นจานวนมาก แต่ยังไม่มีรหัสใดที่มีสมรรถนะเข้าใกล้ความจุช่องสัญญาณจนกระทั่งการค้นพบรหัสเทอร์โบ (turbo code) ในปี พ.ศ. 2536 [2] ที่แสดงให้เห็นว่าสามารถสร้างรหัสช่องสัญญาณที่มีสมรรถนะใกล้เข้าใกล้ความจุช่องสัญญาณได้จริง นาไปสู่การค้นพบรหัสแอลดีพีซี (low-density parity-check: LDPC) ใหม่ ที่เคยถูกน เสนอไปก่อนหน้าเมื่อปี พ.ศ. 2514 [3] ซึ่งรหัสแอลดีพีซีสามารถให้สมรรถนะเข้าใกล้ความจุช่องสัญญาณเช่นเดียวกับรหัสเทอร์โบ ทั้งนี้ การพิสูจน์สมรรถนะของรหัสเทอร์โบและรหัสแอลดีพีซีจะเป็นการพิสูจน์ประสิทธิภาพของวงจรถอดรหัสว่าสามารถเข้าใกล้ความจุช่องสัญญาณ จนกระทั่งปี พ.ศ. 2552 ได้มีการค้นพบรหัสโพลาร์ โดยเออร์ดัล อริคัน [4] ซึ่งสามารถพิสูจน์ได้ว่าวงจรเข้ารหัสโพลาร์มีสมรรถนะเข้าใกล้ความจุช่องสัญญาณ รหัสโพลาร์จึงได้รับความสนใจอย่างมาก อย่างไรก็ตาม ในทางปฏิบัติยังพบปัญหาการถอดรหัสโพลาร์ที่ยังไม่สามารถให้สมรรถนะที่ดีใกล้เคียงกับรหัสเทอร์โบและรหัสแอลดีพีซี จนกระทั่งมีการค้นพบวิธีการถอดรหัสหักล้างต่อเนื่องแบบลิส (successive cancellation list) ที่ทางานร่วมกับรหัสตรวจสอบด้วยส่วนซ้าซ้อนแบบวน (cyclic redundancy check) หรือ CRC [5], [6] ทาให้รหัสโพลาร์มีสมรรถนะใกล้เคียงกับรหัสช่องสัญญาณชนิดอื่น ๆ ปัจจุบันรหัสโพลาร์ถูกเลือกใช้งานในมาตรฐานการสื่อสารไร้สายยุคที่ 5 หรือมาตรฐาน 5G อย่างไรก็ตาม รหัสโพลาร์ยังคงประสบปัญหาเรื่องสมรรถนะการแก้ไขความผิดพลาดข้อมูลดิจิทัลที่มีความยาวคา

รหัสปานกลางถึงยาว อีกทั้งปัญหาความซับซ้อนของวงจรถอดรหัสที่ใช้วิธีการถอดรหัสหักล้างต่อเนื่องแบบลิส ซึ่งการประยุกต์ใช้งานจริงมีความซับซ้อนและใช้หน่วยความจ ำ นวนมาก วิทยานิพนธ์ฉบับนี้จึงมุ่งเน้นแก้ไขความซับซ้อนของวงจรถอดรหัส โดยเฉพาะอย่างยิ่งวงจรถอดรหัสโพลาร์ที่ใช้ในมาตรฐาน 5G นอกจากนี้ ยังนาเสนอวิธีการออกแบบรหัส CRC ที่มีความเหมาะสมกับวงจรถอดรหัสโพลาร์ที่ใช้หน่วยความจ าขนาดเล็ก

1.2 จุดประสงค์ของวิทยานิพนธ์

1) ใช้งานตัวถอดรหัสที่ลดหน่วยความจา เช่น ตัวถอดรหัสแบบแบ่งส่วน ร่วมกับรหัสโพลาร์ตามมาตรฐาน 5G อย่างเหมาะสม เพื่อการความซับซ้อนการถอดรหัส ขณะที่สูญเสียสมรรถนะการถอดรหัสเพียงเล็กน้อย

2) น าเสนอการใช้รหัส CRC ที่ถูกอินเทอร์ลีฟภายในมาตรฐาน 5G เพื่อเพิ่มสมรรถนะของตัวถอดรหัสแบบแบ่งส่วนด้วยเทคนิคการเลือกเส้นทางการถอดรหัส

3) นาเสนอการออกแบบรหัส CRC ที่ถูกอินเทอร์ลีฟ ที่สามารถกระจายในตัวถอดรหัสแบบแบ่งส่วนได้ดี โดยพิจารณาสมรรถนะของตัวถอดรหัสแบบแบ่งส่วน ที่มีอิทธิผลจากน้ำหนักแถวแรกของเมทริกซ์พาริตีตรวจสอบของรหัส CRC ที่ถูกอินเทอร์ลีฟ

1.3 สรุปผลการวิจัย

1) วิทยานิพนธ์ได้นาวิธีการลดความซับซ้อนและขนาดหน่วยความจาของวงจรถอดรหัสโพลาร์โดยการประยุกต์ใช้วิธีการแบ่งส่วนตัวถอดรหัส ผลการทดลองแสดงให้เห็นว่าการแบ่งส่วนตัวถอดรหัสสามารถลดขนาดของหน่วยความจาของวงจรถอดรหัสโพลาร์มาตรฐาน 5G ได้มากกว่า 46.31% ขณะที่สูญเสียสมรรถนะอัตราเฟรมผิดพลาดเพียง 0.02 dB

2) วิทยานิพนธ์ได้นาเสนอวิธีการคานวณค่าความน่าเชื่อถือในวงจรถอดรหัสโพลาร์ที่มีการประยุกต์ใช้วิธีการแบ่งส่วนตัวถอดรหัส ผลการทดลองแสดงให้เห็นว่าการปรับค่าความน่าเชื่อถือของเส้นทางโดยใช้บิต CRC สามารถเพิ่มสมรรถนะอัตราเฟรมผิดพลาดได้ 0.2 dB

3) วิทยานิพนธ์ได้นาเสนอวิธีการออกแบบรหัส CRC แบบอินเทอร์ลีฟร่วมที่เหมาะสมกับวงจรถอดรหัสโพลาร์ที่มีการประยุกต์ใช้วิธีการแบ่งส่วนตัวถอดรหัส โดยได้ค้นพบว่าหากทาการกระจายบิต CRC ไปยังตาแหน่งด้านหน้าของคารหัสได้มากจะสามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดได้ ซึ่งการกระจายของบิต CRC สามารถใช้ค่าน้ำหนักแถวแรกเป็นเกณฑ์ได้ โดยรหัส CRC ที่ถูกอินเทอร์ลีฟที่มีค่าน้าหนักแถวแรกน้อย เท่ากับ 25 สามารถให้สมรรถนะอัตราเฟรมผิดพลาดที่ดีกว่ารหัส CRC ที่ถูกอินเทอร์ลีฟที่มีค่าน้ำหนักแถวแรกน้อย เท่ากับ 154 กว่า 0.08 dB

1.4 งานวิจัยที่เกี่ยวข้องและทิศทางการวิจัย

รหัสโพลาร์ได้รับความสนใจอย่างมาก จากการถอดรหัสหักล้างต่อเนื่องแบบลิส ที่ทางานร่วมกับรหัส CRC ที่สามารถให้สมรรถนะการแก้ไขความผิดพลาดที่ดีใกล้เคียงกับรหัสช่องสัญญาณอื่น แต่ยังประสบปัญหาอื่น เช่น ปัญหาความซับซ้อนของวงจรถอดรหัส โดยเฉพาะการใช้งานหน่วยความจาที่มากของวงจรถอดรหัสหักล้างต่อเนื่องแบบลิส จึงมีงานวิจัยจานวนมากที่นาเสนอเทคนิคการลดความซับซ้อนของวงจรถอดรหัส หนึ่งในวิธีการลดความซับซ้อนคือ การเปลี่ยนโหนดทดแทน ถูกนาเสนอครั้งแรกใน [7] ที่ได้น าเสนอการค นวณโหนดรูปแบบใหม่ทดแทนโครงสร้างการถอดรหัสหักล้างต่อเนื่องแบบลิส โดยได้ทดแทนโหนดที่อยู่บนตาแหน่งบิตแช่แข็งทั้งหมดและบิตข้อมูลทั้งหมด โดยสาหรับโหนดบิตแช่แข็งทั้งหมดให้ทาการถอดรหัสโดยตัดสินใจบิตเป็นศูนย์ทั้งหมด และสาหรับโหนดบิตข้อมูลให้เปลี่ยนมาถอดรหัสด้วยอัลกอริทึมการตัดสินใจแบบฮาร์ดจากค่าความน่าเชื่อถือบนโหนดดังกล่าว ซึ่งการทดแทนโหนดดังกล่าวทาให้ลดประมาณการคานวณการถอดรหัสภายใต้โหนดที่ถูกแทนที่ ส่งผลให้สามารถลดความหน่วงในการคานวณ รวมถึงลดการใช้งานหน่วยความจาภายใต้โหนดที่ถูกทดแทน เทคนิคการเปลี่ยนโหนดทดแทนยังได้ถูกนาเสนอต่ออย่างมากมาย สาหรับโหนดทดแทนประเภทอื่น ซึ่งทิศทางการนาเสนอจะเป็นการทาให้โหนดเป็นนัยทั่วไป (generalization) หรือเป็นการนาเสนอโหนดประเภทใหม่ที่ท าให้โหนดหลายประเภทถูกทดแทนได้ [8] นอกจากนี้ เทคนิคการตัดเส้นทางการถอดรหัส ยังเป็นอีกหนึ่งวิธีที่นามาลดความซับซ้อนการถอดรหัส [9], [10] โดยวิธีดังกล่าวจะมุ่งเน้นไปที่การตัดเส้นทางการถอดรหัสให้น้อยลงกว่าขนาดลิสของตัวถอดรหัสหักล้างต่อเนื่องแบบลิส ซึ่งหลักการเกณฑ์ที่ใช้ในการตัดเส้นทางการถอดรหัสออกคือการพิจารณาค่าความน่าเชื่อถือเส้นทางการถอดรหัส ซึ่งอาจพิจารณาว่าเมื่อเส้นทางใดเส้นทางหนึ่งมีความน่าเชื่อถือที่ต่าเกินกว่าที่จะถูกเลือกเป็นเส้นทางการถอดรหัสสุดท้าย จะทาการตัดออกระหว่างกระบวนการถอดรหัส หรืออาจตั้งขีดแบ่งการตัดสินใจ (decision threshold) สาหรับการตัดเส้นทางการถอดรหัสภายใต้ตัวถอดรหัสหักล้างต่อเนื่องแบบลิส อีกหนึ่งวิธีการลดความซับซ้อนวงจรถอดรหัสโพลาร์ที่วิทยานิพนธ์นาใช้งานและนาเสนอเทคนิคการปรุงปรุงควบคู่คือ การแบ่งส่วนตัวถอดรหัส [11], [12] เทคนิคดังกล่าวเริ่มต้นจากให้โครงสร้างต้นไม้ของตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ซ้ าซ้อนใช้งานหน่วยความจาที่ตาแหน่งเดียวกัน จากนั้นในแต่ละชั้นการถอดรหัสของตัวถอดรหัสหักล้างต่อเนื่อง ตัวถอดรหัสแบบแบ่งส่วนสามารถลดทอนจานวนเส้นทางการถอดรหัสในชั้นการถอดรหัสชั้นบนได้ วิธีการดังกล่างสามารถลดความซับซ้อนของตัวถอดรหัสหักล้างต่อเนื่องแบบลิสได้ โดยลดการใช้งานหน่วยความจาในการเก็บข้อความภายในโครงสร้างการถอดรหัสได้ แต่ต้องแลกกับการสูญเสียสมรรถนะการแก้ไขความผิดพลาดของตัวถอดรหัสแบบแบ่งส่วน เมื่อเทียบกับตัวถอดรหัสหักล้างต่อเนื่องแบบลิส

วิทยานิพนธ์นี้จึงน าตัวถอดรหัสแบบแบ่งส่วนเข้ามาใช้ร่วมกับรหัสโพลาร์ตามมาตรฐาน 5G ซึ่งสามารถลดขนาดของหน่วยความจาของวงจรถอดรหัสโพลาร์มาตรฐาน 5G ได้มากกว่า 46.31% ขณะที่

สูญเสียสมรรถนะอัตราเฟรมผิดพลาดเพียง 0.02 dB จากนั้นวิทยานิพนธ์ยังน าเสนอการใช้รหัส CRC ที่ถูกอินเทอร์ลีฟภายในมาตรฐาน 5G เพื่อเพิ่มสมรรถนะตัวถอดรหัสแบบแบ่งส่วนด้วยเทคนิคการเลือกเส้นทางการถอดรหัส ทั้งวิธีการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทางการถอดรหัส วิธีการปรับค่าความน่าเชื่อถือเส้นทางการถอดรหัสสามารถเพิ่มสมรรถนะอัตราเฟรมผิดพลาดได้ 0.2 dB และสุดท้ายวิทยานิพนธ์ยังได้น าเสนอหลักเกณฑ์การออกแบบรหัส CRC ที่ถูกอินเทอร์ลีฟที่ส่งผลต่อสมรรถนะการแก้ไขความผิดพลาดภายใต้ตัวถอดรหัสแบบแบ่งส่วน โดยค้นพบว่าหากบิต CRC ที่ถูกอินเทอร์ลีฟสามารถกระจายไปในแต่ละส่วนการถอดรหัสได้ จะสามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดของตัวถอดรหัสแบบแบ่งส่วนได้

1.5 ขอบเขตการวิจัย

วิทยานิพนธ์ฉบับนี้จะศึกษาและจาลองสมรรถนะการแก้ไขความผิดพลาดของวงจรถอดรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิสที่ทางานร่วมกับรหัส CRC โดยการจาลองสมรรถนะจะถูกจาลองภายใต้ช่องสัญญาณรบกวนแบบเกาส์เซียนขาวบวก (additive white Gaussian noise) หรือ AWGN ที่ไม่มีการลดทอน (fading) และการสร้างรหัสโพลาร์ใช้หลักการประมาณเกาส์เซียน (Gaussian approximation) ส าหรับการสร้างรหัสโพลาร์มาตรฐาน 5G โดยจะอ้างอิงเอกสารของ 3GPP

1.6 ส่วนประกอบของวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้ประกอบด้วย 6 บท บทแรก จะอธิบายถึงความสาคัญ ความเป็นมา และจุดประสงค์ของวิทยานิพนธ์ รวมทั้งสรุปผลโดยย่อของการดาเนินการวิจัยในวิทยานิพนธ์ฉบับนี้ บทที่ 2 อธิบายทฤษฎีพื้นฐานของรหัสโพลาร์ทั้งการเข้ารหัส ถอดรหัส และการสร้างรหัส นอกจากนี้ยังได้อธิบายรหัสย่อยที่ใช้งานร่วมกับรหัสโพลาร์ เช่น รหัส CRC และเทคนิคการลดความซับซ้อนของการถอดรหัสโพลาร์ที่มีการนาเสนอในงานวิจัยต่างๆ ซึ่งจะเป็นส่วนประกอบสาคัญวิทยานิพนธ์ฉบับนี้ เช่น ตัวถอดรหัสแบบแบ่งส่วน บทที่ 3 มีเนื้อหาของรหัสโพลาร์ในมาตรฐาน 5G บทที่ 4 จะอธิบายการประยุกต์ใช้งานตัวถอดรหัสแบบแบ่งส่วนในวงจรถอดรหัสโพลาร์มาตรฐาน 5G จากนั้นจะนาเสนอวิธีการคานวณค่าความน่าเชื่อถือในวงจรถอดรหัสโพลาร์ที่มีการประยุกต์ใช้ในวิธีการแบ่งส่วนตัวถอดรหัส สุดท้ายจะอธิบายรายละเอียดการออกแบบรหัส CRC ที่เหมาะสมกับการถอดรหัสหักล้างต่อเนื่องแบบลิสที่มีการแบ่งส่วนตัวถอดรหัส สาหรับการทดลองสมรรถนะการแก้ไขความผิดพลาด และผลการออกแบบจะอธิบายในบทที่ 5 และสุดท้ายจะสรุปผลการด าเนินการวิจัยและข้อเสนอแนะในบทที่ 6

บทที่ 2
ทฤษฎีพื้นฐานของรหัสโพลาร์

บทที่ 2 ทฤษฎีพื้นฐานของรหัสโพลาร์ จะเริ่มต้นจากการอธิบายสัญกรณ์และอักษรย่อที่ใช้ในวิทยานิพนธ์ฉบับนี้ จากนั้นจะกล่าวถึงพื้นฐานของรหัสโพลาร์ เช่น แนวคิดของรหัสโพลาร์ การเข้ารหัส การสร้างรหัส และการถอดรหัสแบบหักล้างต่อเนื่อง รวมถึงรหัสย่อยที่ใช้งานร่วมกับรหัสโพลาร์ เช่น รหัสตรวจสอบด้วยส่วนซ้ำซ้อนแบบวน (cyclic redundancy check) หรือรหัส CRC และรหัสพาริตีตรวจสอบ (parity check) และเทคนิคการลดความซับซ้อนของการถอดรหัสโพลาร์ที่มีการนาเสนอในงานวิจัยต่าง ๆ โดยเนื้อหาดังกล่าวจะเป็นส่วนส าคัญซึ่งเกี่ยวข้องกับการวิจัยในวิทยานิพนธ์นี้

2.1 สัญกรณ์และอักษรย่อ

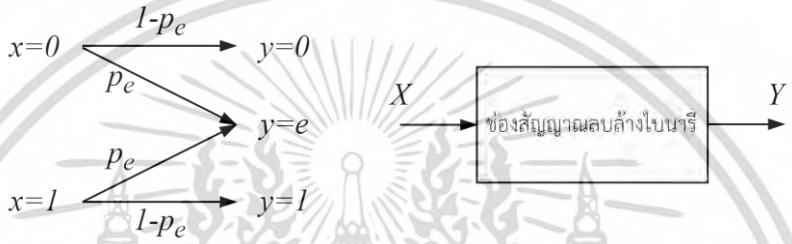
สาหรับตัวแปรสุ่ม (random variable) แทนด้วยอักษรพิมพ์ใหญ่ เช่น X หรือ Y และค่าที่สุ่มจากตัวแปรสุ่ม แทนด้วยอักษรพิมพ์เล็ก เช่น x หรือ y ค่าคงที่และตัวแปรอื่น ๆ สามารถใช้ได้ทั้งอักษรพิมพ์ใหญ่และเล็ก ทั้งนี้ เพื่อไม่ให้สับสนกับตัวแปรสุ่ม ความหมายของอักษรจะขึ้นอยู่กับบริบทของประโยค ตัวแปรที่เป็นค่าสเกลาร์จะแทนด้วยอักษรตัวบาง สาหรับตัวแปรที่เป็นเวกเตอร์ (vector) และเมทริกซ์ (matrix) แทนด้วยแปรที่มีตัวห้อยและตัวยก เช่น x_m^n หรือ y_0^{n-1} โดยที่ตัวห้อยจะหมายถึงตาแหน่งแรกของสมาชิกและตัวยกหมายถึงตาแหน่งสุดท้ายของสมาชิก และสมาชิกของเวกเตอร์สามารถแสดงด้วยตัวแปรที่มีตัวห้อย ตัวอย่างเช่น สมาชิกลาดับที่ $|\mathbf{x}|$ ของเวกเตอร์ y_0^{n-1} แสดงด้วยตัวแปร y_i และสมาชิกลาดับที่ m ถึง n ของเวกเตอร์ x_m^n แสดงด้วยเวกเตอร์ที่ $x_m^n \triangleq \{x_m, x_{m+1}, \ldots, x_n\}$ โดยที่ $m \geq 1$ $n \leq |x|$ และ $m < n$ นอกจากนี้ สามารถใช้เวกเตอร์ใด ๆ บ่งชี้สมาชิกลาดับต่าง ๆ ของเวกเตอร์ x ตัวอย่างเช่น เช่น $x_y \triangleq \{x_i | i \in y\}$ โดยประโยคจะก าหนดให้ x และ y เป็นเวกเตอร์ ตัวแปรจะเป็นเวกเตอร์หรือเมทริกซ์จะขึ้นอยู่กับบริบทของประโยค และหากเป็นเมทริกซ์ สมาชิกย่อยจะเป็นเวกเตอร์ จานวนสมาชิกของเวกเตอร์จะใช้สัญลักษณ์ $|x_m^n|$ ซึ่งมีค่าเท่ากับ $n-m-1$ เพื่อไม่ให้สับสนกับค่านอร์ม (norm) ของเวกเตอร์ ที่ใช้สัญลักษณ์ $\|x\|$ และค่าสัมบูรณ์ (absolute) ที่ใช้สัญลักษณ์ $|x|$

2.2 ช่องสัญญาณรบกวนและการโพลาไรซ์ช่องสัญญาณ

2.2.1 ช่องสัญญาณรบกวน

ช่องสัญญาณรบกวน (noisy channel) เป็นส่วนประกอบหลักในระบบสื่อสารดิจิทัล ในทางทฤษฎี ช่องสัญญาณรบกวนในระบบสื่อสารสามารถจาลองด้วยแบบจาลอง (model) ที่มีคุณสมบัติ

สอดคล้องกับระบบสื่อสาร หนึ่งในแบบจาลองช่องสัญญาณที่เรียบง่ายก็คือช่องสัญญาณลบล้างไบนารี (binary erasure channel) หรือ BEC โดยสัญญาณไบนารี $Xd(\mathbf{v},\mathbf{w}) = w(\mathbf{v}+\mathbf{w})$ ที่ใช้ถูกส่งผ่านช่องสัญญาณ ณ เวลาใด ๆ ประกอบด้วยสัญญาณที่มีแอมพลิจูดเท่ากับ $x=0$ และ $x=1$ แทนบิตข้อมูลดิจิทัลคือ บิต 0 และ บิต 1 ตามลาดับ และมีสัญญาณ Y ที่ได้รับจากช่องสัญญาณมีแอมพลิจูดอยู่ 3 รูปแบบ ได้แก่ คือ $y=0$ $y=1$ และ $y=e$ แทนกรณีที่ได้รับข้อมูลดิจิทัลคือบิต 0 บิต 1 และกรณีไม่ทราบว่าข้อมูลดิจิทัลที่ได้รับคืออะไร แสดงดังภาพที่ 2.1

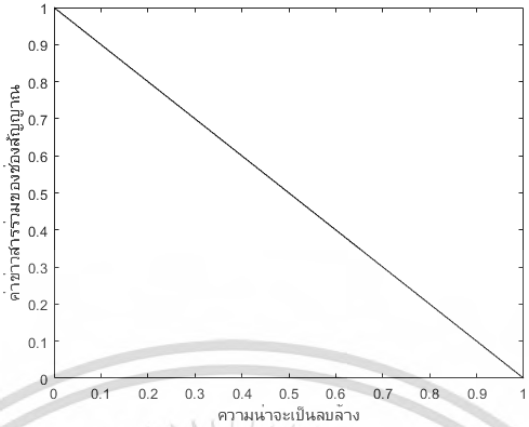


ภาพที่ 2.1 ช่องสัญญาณ BEC

โดยสัญญาณส่งจะถูกปรับเปลี่ยนเป็นสัญญาณจานวน 3 รูปแบบ โดยมีความน่าจะเป็นในการปรับเปลี่ยนสัญญาณที่แตกต่างกันเรียกว่าความน่าจะเป็นการเปลี่ยนผ่าน (transition probability) สาหรับช่องสัญญาณ BEC จะกาหนดความน่าจะเป็นการเปลี่ยนผ่านให้มีค่าเท่ากับความน่าจะเป็นลบล้าง (erasure probability) p_e ขณะที่ความน่าจะเป็นการเปลี่ยนผ่านสาหรับการรับบิต 0 และ 1 จะมีค่าเท่ากับ $1-p_e$

ข่าวสารร่วม (mutual information) ระหว่างสัญญาณส่ง X และสัญญาณรับ Y ถือเป็นตัวชี้วัดความสามารถในการส่งข้อมูลผ่านช่องสัญญาณใด ๆ หากช่องสัญญาณมีค่าข่าวสารร่วมสูง จะสื่อถึงความสามารถในการส่งข้อมูลที่มีปริมาณมากได้อย่างถูกต้อง ข่าวสารร่วม (mutual information) ระหว่างสัญญาณส่ง X และสัญญาณรับ Y ของช่องสัญญาณ BEC จะมีความสัมพันธ์กับค่าความน่าจะเป็นลบล้าง ดังสมการที่ 2.1 และแสดงดังภาพที่ 2.2

$$I(X;Y) = 1-p_e \tag{2.1}$$



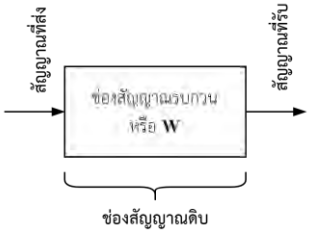
ภาพที่ 2.2 ความสัมพันธ์ระหว่างความจุช่องสัญญาณกับความน่าจะเป็นลบล้างของช่องสัญญาณ BEC

พิจารณาค่าข่าวสารร่วมเมื่อกำหนดให้ความน่าจะเป็นลบล้างมีค่าใด ๆ ดังภาพที่ 2.2 หากพิจารณาช่องสัญญาณ BEC ที่มีความน่าจะเป็นลบล้าง เท่ากับ $p_e = 0$ ช่องสัญญาณจะมีค่าข่าวสารร่วมเท่ากับ 1 หมายถึงการส่งข้อมูลผ่านช่องสัญญาณจะถูกต้องทั้งหมด หาก $p_e = 0.5$ ช่องสัญญาณจะมีค่าข่าวสารร่วมเท่ากับ 0.5 หมายความว่าการส่งข้อมูลผ่านช่องสัญญาณจะถูกต้องเพียงครึ่งหนึ่ง และหาก $p_e = 1$ ช่องสัญญาณจะมีค่าข่าวสารร่วมเท่ากับ 0 หมายความว่าการส่งข้อมูลผ่านช่องสัญญาณจะผิดทั้งหมด

2.2.2 การโพลาไรซ์ช่องสัญญาณ

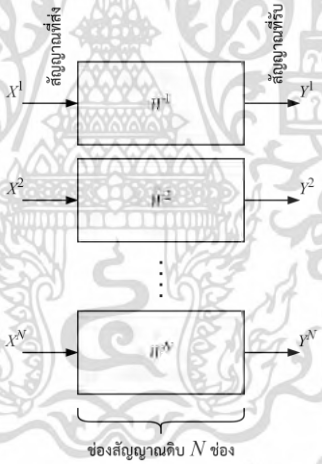
การโพลาไรซ์ช่องสัญญาณ (channel polarization) เป็นการทาให้ช่องสัญญาณรบกวนใด ๆ สามารถพิจารณาได้เป็นช่องสัญญาณรบกวนที่ประกอบไปด้วยช่องสัญญาณย่อยจานวนมาก โดยช่องสัญญาณย่อยจะมีคุณสมบัติที่แตกต่างกัน ช่องสัญญาณย่อยบางช่องสัญญาณจะมีสัญญาณรบกวนต่า (noiseless subchannel) หรือมีค่าข่าวสารร่วมสูง และช่องสัญญาณย่อยบางช่องสัญญาณจะมีสัญญาณรบกวนสูง (noisy subchannel) หรือมีค่าข่าวสารร่วมต่ำ[4]

กาหนดให้ช่องสัญญาณรบกวนแทนด้วยสัญลักษณ์ $W : X \to Y$ ในที่นี้จะเรียกช่องสัญญาณดังกล่าวว่า ช่องสัญญาณดิบ (raw channel) ดังภาพที่ 2.3 โดยสัญญาณ x ที่ถูกส่งผ่านช่องสัญญาณดิบแทนด้วยตัวแปรสุ่ม X และสัญญาณ y ที่ได้รับแทนด้วยตัวแปรสุ่ม Y กาหนดให้ความน่าจะเป็นการเปลี่ยนผ่าน (transition probability) ของช่องสัญญาณ W เขียนแทนด้วยสัญลักษณ์ $W\left(y|x\right)$



ภาพที่ 2.3 บิตข้อมูลส่งผ่านช่องสัญญาณดิบ

สาหรับช่องสัญญาณดิบที่มีช่องสัญญาณจานวน N ช่อง แสดงดังภาพที่ 2.4 ทั้งนี้ สามารถเขียนช่องสัญญาณจ นวน N ช่อง ด้วยสัญลักษณ์ $W^N : X^N \to Y^N$ โดยสัญญาณ x_1^N จ านวน N ชุด ที่ถูกส่งผ่านช่องสัญญาณดิบ N ช่อง แทนด้วยตัวแปรสุ่ม X^N และสัญญาณ $\mathbf{y}_1^N$ จานวน N ชุด ที่ได้รับแทนด้วยตัวแปรสุ่ม Y^N กาหนดให้ความน่าจะเป็นการเปลี่ยนผ่านของช่องสัญญาณ W^N เขียนแทนด้วยสัญลักษณ์ $W^N\left(y_1^N \middle| x_1^N\right)$



ภาพที่ 2.4 ช่องสัญญาณดิบจ านวน N ช่อง

2.2.2.1 การรวมช่องสัญญาณ (channel combining)

การรวมช่องสัญญาณดิบ W จ านวน N ช่องสัญญาณ สามารถด าเนินการในรูปแบบรีคลูซีฟ (recursive) โดยที่ N ต้องมีค่าเท่ากับสองยกก าลังด้วยจ านวนเต็มบวกใด ๆ โดยผลการรวมช่องสัญญาณจะสร้างช่องสัญญาณที่ถูกสังเคราะห์มาดังสมการที่ 2.2

$$W_N : X^N \to Y^N \tag{2.2}$$

โดยที่ W_N คือ ช่องสัญญาณที่เกิดจากการรวมช่องสัญญาดิบจ านวน N ช่อง

X^N คือ ตัวแปรสุ่มของสัญญาณที่ถูกส่งผ่านช่องสัญญาณ W_N

Y^N คือ ตัวแปรสุ่มของสัญญาณที่ได้รับจากช่องสัญญาณ W_N

โดยสามารถเขียนความน่าจะเป็นการเปลี่ยนผ่านของช่องสัญญาณดิบ N ช่อง ได้โดย

$$\begin{aligned} W_N\left(y_1^N \middle| u_1^N\right) &= W^N\left(y_1^N \middle| x_1^N\right) \\ &= W^N\left(y_1^N \middle| u_1^N G_N\right) \end{aligned} \tag{2.3}$$

โดยที่ $W_N(y_1^N \middle| u_1^N)$ คือ ความน่าจะเป็นการเปลี่ยนผ่านของช่องสัญญาณ W_N

y_1^N คือ สัญญาณที่ได้รับจากช่องสัญญาณ W_N

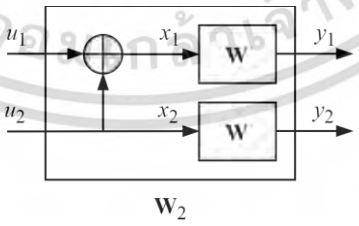
x_1^N คือ สัญญาณที่เกิดจากการด าเนินการระหว่าง u_1^N และ G_N

u_1^N คือ สัญญาณที่ถูกส่งผ่านช่องสัญญาณ W_N

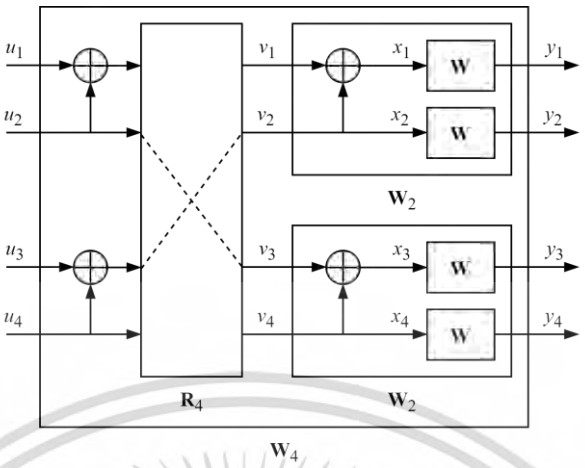
G_N คือ เมทริกซ์ก าเนิด(Generator matrix)

จะสังเกตได้ว่าช่องสัญญาณ W_N ที่ได้จากการรวมช่องสัญญาณ W^N จะมีการนาสัญญาณ u_1^N มาดาเนินการกับเมทริกซ์ G_N ตัวอย่างเช่น การส่งข้อมูล u_1^N ผ่านช่องสัญญาณรบกวนในภาพที่ 2.5 ซึ่งเป็นการรวมช่องสัญญาณ W ที่เป็นอิสระกัน 2 ช่องเข้าด้วยกันเป็นช่องสัญญาณ W_2 กรณีนาช่องสัญญาณ W_2 จานวน 2 ช่องสัญญาณรวมกันเพื่อสร้างช่องสัญญาณที่มีจานวนอินพุตเท่ากับ 4 หรือ $N=4$ จะได้ช่องสัญญาณ W_4 ดังภาพที่ 2.6 ทั้งนี้ จะต้องมีกระบวนการเรียงสับเปลี่ยน R_4 เพื่อรวมช่องสัญญาณ W_2 จ านวนช่องสัญญาณ

จากตัวอย่างการสร้างช่องสัญญาณ W_2 และ W_4 จะสังเกตได้ว่าโครงสร้างช่องสัญญาณ W_N ที่มีจานวน $N>2$ ขึ้นไป สามารถสร้างได้จากการรวมช่องสัญญาณ $W_{N/2}$ จานวน 2 ช่องสัญญาณ โดยการแปลง u_N เป็น x_N สามารถแสดงด้วยเมทริกซ์ กนิด G_N ร่วมกับเมทริกซ์การเรียงสับเปลี่ยน R_N



ภาพที่ 2.5 การรวมช่องสัญญาณ W เพื่อสร้างช่องสัญญาณ W_2



ภาพที่ 2.6 การรวมช่องสัญญาณ W_2 เพื่อสร้างช่องสัญญาณ W_4

2.2.2.2 การแยกช่องสัญญาณ (channel splitting)

การแยกช่องสัญญาณจะเป็นการพิจารณา ช่องสัญญาณ W_N ออกเป็นช่องสัญญาณย่อย $W_N^{(i)}$ จ านวน N ช่องสัญญาณ โดยช่องสัญญาณย่อย $W_N^{(i)}$ นิยามได้ดังนี้

$$W_N^{(i)} : X \to Y^N \times X^{i-1} \tag{2.4}$$

โดยที่ $W_N^{(i)}$ คือ ช่องสัญญาณล าดับที่ i

X คือ ตัวแปรสุ่มสัญญาณที่ส่งไปยังช่องสัญญาณรบกวน

Y^N คือ ตัวแปรสุ่มสัญญาณที่รับจากช่องสัญญาณรบกวนจ านวน N ช่องสัญญาณ

X^{i-1} คือ ตัวแปรสุ่มสัญญาณที่ส่งก่อนหน้าจ านวน $i-1$ ช่องสัญญาณ

ทั้งนี้ สามารถเขียนความน่าจะเป็นการเปลี่ยนผ่านของช่องสัญญาณย่อยล าดับที่ i ได้ดังนี้

$$W_N^{(i)}\left(y_1^N, u_1^{i-1} \middle| u_i\right) \triangleq \sum_{u_{i+1}^N \in X^{N-i}} \frac{1}{2^{N-1}} W_N\left(y_1^N \middle| u_1^N\right) \tag{2.5}$$

โดยที่ $W_N^{(i)}$ คือ ความน่าจะเป็นการเปลี่ยนผ่านของช่องสัญญาณย่อยล าดับที่ i

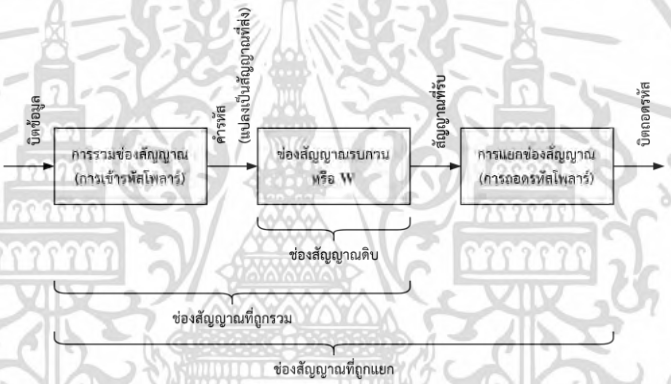
y_1^N คือ สัญญาณที่ได้รับจากช่องสัญญาณ W_N

u_1^N คือ สัญญาณที่ถูกส่งผ่านช่องสัญญาณ W_N

ช่องสัญญาณ $W_N^{(i)}$ สามารถพิจารณาได้เป็นช่องสัญญาณใหม่ของบิตล าดับที่ i โดยการตัดสินใจบิตล าดับที่ i จะน าสัญญาณที่ได้รับจากช่องสัญญาณทั้งหมดและบิตข้อมูล u_1^{i-1} หรือบิตข้อมูลล าดับก่อนหน้าของบิตข้อมูลล าดับที่ i ทั้งหมด

2.3 รหัสโพลาร์

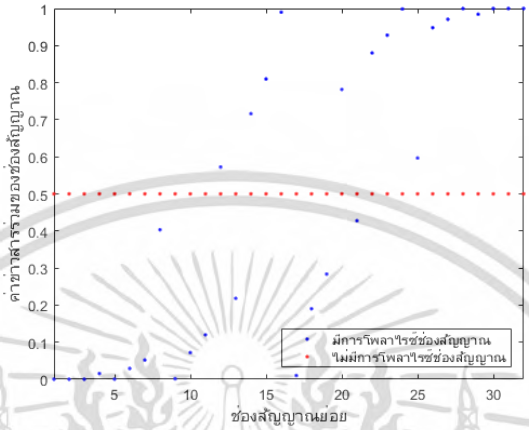
รหัสโพลาร์ถูกนาเสนอครั้งแรกในปี พ.ศ. 2552 [4] ซึ่งรหัสโพลาร์จัดเป็นรหัสช่องสัญญาณ (channel codes) ที่สามารถพิสูจน์ได้ว่าการส่งข้อมูลสามารถเข้าใกล้ความจุช่องสัญญาณ ปัจจุบัน รหัสโพลาร์ถูกน ามประยุกต์ใช้งานในระบบสื่อสารไร้สายยุคที่ 5 กรณีการสื่อสารในช่องสัญญาณควบคุม [13] รหัสโพลาร์ประยุกต์ใช้ทฤษฎีการโพลาไรซ์ช่องสัญญาณ โดยจะท าการสังเคราะห์ช่องสัญญาณ ซึ่งประกอบไปด้วยกระบวนการรวมช่องสัญญาณ (channel combining) ที่เกิดขึ้นเมื่อท ากระบวนการเข้ารหัสโพลาร์ และการแยกช่องสัญญาณ (channel splitting) ที่จะเกิดขึ้นเมื่อด าเนินการถอดรหัสเสร็จสิ้น ความสัมพันธ์ของกระบวนการเข้ารหัสและถอดรหัสโพลาร์กับทฤษฎีการโพลาไรซ์ช่องสัญญาณสามารถแสดงได้ดังภาพที่ 2.7



ภาพที่ 2.7 ช่องสัญญาณที่เกิดจากกระบวนการเข้ารหัสและถอดรหัสโพลาร์

ในฝั่งส่งบิตข้อมูลที่ต้องการส่งผ่านช่องสัญญาณดิบ จะถูกคั่นด้วยการเข้ารหัสโพลาร์ดังภาพที่ 2.7 เพื่อท าการสังเคราะห์ช่องสัญญาณดิบเป็นช่องสัญญาณที่ถูกสังเคราะห์ขึ้นมาใหม่ จากนั้น ในฝั่งรับจะมีการถอดรหัสโพลาร์ ซึ่งช่องสัญญาณที่ถูกสังเคราะห์ขึ้นด้วยวงจรเข้ารหัสโพลาร์จะถูกแยกเป็นช่องสัญญาณย่อยหรือช่องสัญญาณที่ถูกโพลาไรซ์ คุณสมบัติของช่องสัญญาณที่ถูกโพลาไรซ์คือบางช่องสัญญาณย่อยจะมีสัญญาณรบกวนต่ าหรือมีค่าข่าวสารร่วมสูง ซึ่งเหมาะสมกับการส่งข้อมูลผ่านช่องสัญญาณดังกล่าว และบางช่องสัญญาณย่อยจะมีสัญญาณรบกวนสูงหรือมีค่าข่าวสารร่วมต่ า ซึ่งช่องสัญญาณดังกล่าวจะไม่เหมาะสมกับการส่งข้อมูล โดยการเข้ารหัสโพลาร์จะก าหนดให้บิตข้อมูลที่ผ่านช่องสัญญาณย่อยนี้เป็นบิต 0 หรือเรียกว่าบิตแช่แข็ง ภาพที่ 2.8 แสดงค่าข่าวสารร่วมของช่องสัญญาณดิบกับช่องสัญญาณที่ถูกโพลาไรซ์ เมื่อช่องสัญญาณรบกวนคือช่องสัญญาณ BEC ที่มีค่าความน่าจะเป็นลบล้างเท่ากับ 0.5 จานวน 32 ช่องสัญญาณ และใช้กระบวนการรวมช่องสัญญาณตามที่อธิบายในข้างต้น

จากภาพจะพบว่าช่องสัญญาณที่ถูกโพลาไรซ์จะประกอบด้วยช่องสัญญาณที่มีค่าข่าวสารร่วมสูง และช่องสัญญาณที่มีค่าข่าวสารร่วมต่ำ



ภาพที่ 2.8 การเปรียบเทียบค่าข่าวสารร่วมของช่องสัญญาณดิบกับช่องสัญญาณที่ถูกโพลาไรซ์

2.4 การเข้ารหัสโพลาร์

การเข้ารหัสโพลาร์จะเข้ารหัสชุดบิตขนาด $N = 2^n$ บิต โดยที่ n เป็นจำนวนเต็มบวกใด ๆ โดยชุดบิตดังกล่าวประกอบไปด้วยบิตข้อมูล (information bits) ขนาด K บิต และบิตที่เหลือเป็นบิตที่ระบบการสื่อสารทั้งฝั่งส่งและฝั่งรับทราบ ซึ่งเรียกว่าบิตแช่แข็ง (frozen bits) ขนาด $N-K$ บิต อัตรารหัส (code rate) หรืออัตราส่วนระหว่างขนาดบิตข้อมูลต่อขนาดคารหัสจึงมีค่าเท่ากับ K/N ในที่นี้จะกำหนดให้ตำแหน่งของบิตข้อมูลแทนด้วยเซต $\mathcal{A}^I$ และตำแหน่งของบิตแช่แข็งแทนด้วยเซต $\mathcal{A}^F$

การเข้ารหัสโพลาร์เปรียบเสมือนการรวมช่องสัญญาณจำนวน N ช่องสัญญาณ ซึ่งการร่วมช่องสัญญาณจะทำการแปลงบิตข้อมูล u_1^N ไปเป็นบิตคารหัส x_1^N เพื่อส่งผ่านช่องสัญญาณรบกวน [4] ทั้งนี้ สามารถแสดงการแปลงโดยใช้เมทริกซ์กำเนิด G_N ดังนี้

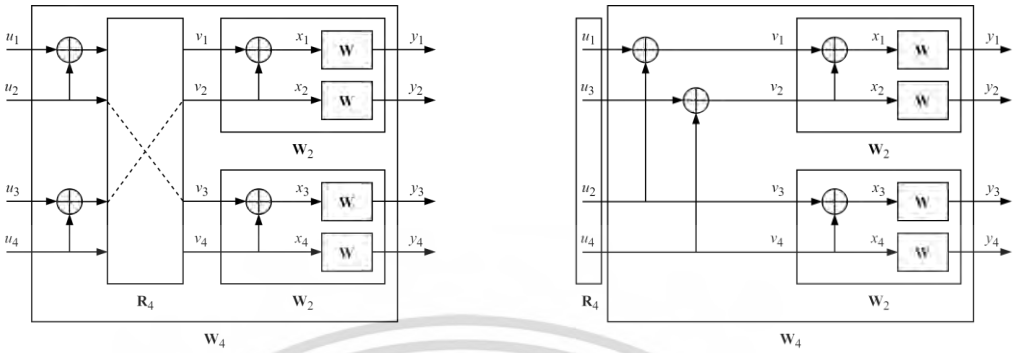
$$x_1^N = u_1^N G_N \tag{2.6}$$

โดยที่ x_1^N คือ คำรหัสขนาด N บิต

u_1^N คือ บิตข้อมูลที่ต้องการเข้ารหัสขนาด N บิต

G_N คือ เมทริกซ์กำเนิดของรหัสโพลาร์

จากภาพที่ 2.6 จะสังเกตว่าโครงสร้างการเข้ารหัสมีกระบวนการเรียงสับเปลี่ยน $\mathbf{R}_N$ แทรกอยู่ ซึ่งหากทำการสับเปลี่ยนลำดับของบิตข้อมูลจะทำให้ได้ภาพที่ 2.9



ก) โครงสร้างก่อนการสับเปลี่ยน ข) โครงสร้างหลังการสับเปลี่ยน

ภาพที่ 2.9 โครงสร้างการเข้ารหัสโพลาร์ที่สับเปลี่ยนของบิตข้อมูล

เมื่อพิจารณาจากภาพที่ 2.9 ดังนั้น-เมทริกซ์ก าเนิด G_N สามารถสร้างจากได้จาก

$$G_N = B_N F^{\otimes N} \tag{2.7}$$

โดยที่ B_N คือ เมทริกซ์เรียงสับเปลี่ยน

$F^{\otimes N}$ คือ เมทริกซ์การรวมช่องสัญญาณ เมื่อ $\otimes$ คือตัวคูณแบบโครเนคเคอร์โดยที่

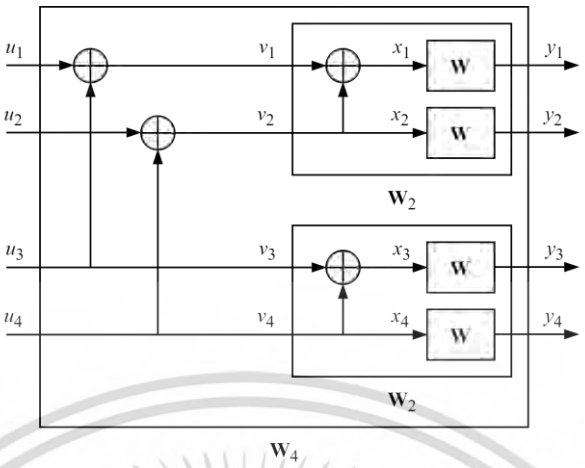
$F^{\otimes 2} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ ดังนั้น $F^{\otimes 4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

นอกจากนี้ จากภาพที่ 2.9 โครงสร้างทั้งสองสามารถเขียนเป็นรูปสมการได้ดังสมการที่ 2.8 และ 2.9 ตามล าดับ

$$x_1^N = u_1^N \left(B_N F_N \right) \tag{2.8}$$

$$x_1^N = \left(u_1^N B_N \right) F_N \tag{2.9}$$

เนื่องจากในการถอดรหัสโพลาร์ จะต้องมีกระบวนเรียงสับเปลี่ยนบิตเช่นเดียวกับการเข้ารหัส ดังนั้นในวิทยานิพนธ์ฉบับนี้ จะไม่พิจารณาเมทริกซ์ B_N และกาหนดให้ $G_N = F_N$ ซึ่งการเรียงสับเปลี่ยนออกถูกตัดออกจากฝั่งส่งและฝั่งรับ ท าให้ได้โครงสร้างการเข้ารหัสดังภาพที่ 2.10



ภาพที่ 2.10 โครงสร้างการเข้ารหัสโพลาร์ส าหรับช่องสัญญาณ $N = 4$

2.5 การถอดรหัสโพลาร์

หลังจากบิตข้อมูล u_1^N ถูกเข้ารหัส ค ารหัส x_1^N จะถูกท าการมอดูเลตและส่งผ่านช่องสัญญาณรบกวน ตัวถอดรหัสจะได้รับสัญญาณ y_1^N และท าการประมาณบิตถอดรหัส $\hat{u}_1^N$ การถอดรหัสโพลาร์นี้จะเป็นการถอดรหัสด้วยหลักการหักกล้างต่อเนื่อง ซึ่งเป็นขั้นตอนในการแยกช่องสัญญาณที่ถูกสังเคราะห์ให้กลายเป็นช่องสัญญาณที่ถูกโพลาไรซ์ ซึ่งจะท าให้ช่องสัญญาณย่อยบางช่องสัญญาณมีความน่าเชื่อถือมากขึ้นหรือมีความน่าจะเป็นความผิดพลาดต่ าและบางช่องสัญญาณมีความน่าเชื่อถือต่ าหรือมีความน่าจะเป็นความผิดพลาดสูง [4]

ระหว่างการถอดรหัส ตัวถอดรหัสจะไม่น าสัญญาณที่ได้รับ y_1^N จากช่องสัญญาณรบกวนมาคานวณโดยตรง แต่จะแปลงเป็นค่าความน่าจะเป็นหรือค่าอัตราส่วนความน่าจะเป็นลอการิทึม (log-likelihood ratio) หรือค่า LLR กาหนดให้ช่องสัญญาณรบกวนคือช่องสัญญาณรบกวนแบบเกาส์เซียนขาวบวกที่มีค่าเฉลี่ย μ เท่ากับ -1 สาหรับบิต 0 และเท่ากับ 1 สาหรับบิต 1 และมีค่าความแปรปวนเท่ากับ σ ดังนั้นค่า LLR สามารถค านวณได้จาก y_1^N ดังนี้

$$
\begin{aligned}
L_i &= \ln \frac{p\left(y_i \middle| x_i = -1\right)}{p\left(y_i \middle| x_i = 1\right)} \\
&= \ln \frac{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{y-(-1)}{\sigma}\right)^2}}{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{y-1}{\sigma}\right)^2}} \\
&= \ln e^{\frac{-(y+1)^2 - -(y-1)^2}{2\sigma^2}} \\
&= \frac{-2y}{\sigma^2}
\end{aligned}
\tag{2.10}
$$

และตัดสินใจบิตถอดรหัสจากค่า LLR ดังนี้

$$
\hat{u}_i = \begin{cases} 0 & \text{หาก } L_i \geq 0 \\ 1 & \text{อื่น ๆ} \end{cases} \tag{2.11}
$$

โดยที่ $\hat{u}_i$ คือ บิตถอดรหัสที่ i

2.5.1 การถอดรหัสโพลาร์ด้วยการหักล้างต่อเนื่อง

การถอดรหัสหักล้างต่อเนื่องสาหรับรหัสโพลาร์จะนาสัญญาณ y_1^N แปลงเป็นค่าความน่าจะเป็นของช่องสัญญาณที่ถูกสังเคราะห์ $W_N\left(y_1^N \middle| u_1^N\right)$ จากนั้นในระหว่างการถอดรหัส ตัวถอดรหัสจะคานวณค่า LLR ได้ดังนี้

$$
L_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right) \triangleq \ln \frac{W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 0\right)}{W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 1\right)} \tag{2.12}
$$

โดยที่ $L_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right)$ คือ ค่า LLR ของช่องสัญญาณที่ถูกแยก N ช่อง

$W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 0\right)$ คือ ค่าความน่าจะเป็นเงื่อนไขเมื่อ $u_i = 0$ ของช่องสัญญาณที่ถูกโพลาไรซ์ที่ i จาก N ช่อง

$W_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1} \middle| 1\right)$ คือ ค่าความน่าจะเป็นเงื่อนไขเมื่อ $u_i = 1$ ของช่องสัญญาณที่ถูกโพลาไรซ์ที่ i จาก N ช่อง

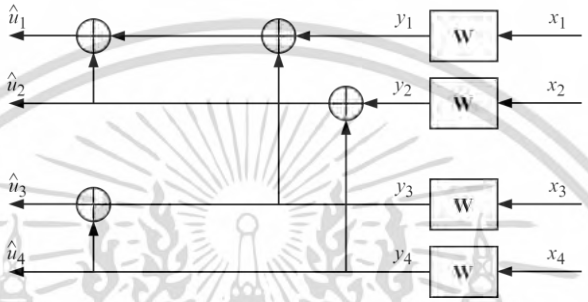
และทางการตัดสินใจบิตถอดรหัสจากค่า log-likelihood ดังนี้

$$
\hat{u}_i = \begin{cases} 0 & \text{หาก } L_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right) \geq 0 \\ 1 & \text{อื่น ๆ} \end{cases} \tag{2.13}
$$

โดยที่ $\hat{u}_i$ คือ บิตถอดรหัสที่ i

สังเกตได้ว่าในการค นวณค่า LLR ของช่องสัญญาณที่ถูกโพลาไรซ์ที่ i ดังสมการที่ 2.12 หรือการตัดสินใจบิตถอดรหัสที่ i ดังสมการที่ *2.13* จะใช้ค่าของช่องสัญญาณก่อนหน้าตาแหน่งที่ i หรือ ต าแหน่งที่ $\{1,2,...,i-1\}$ ร่วมในการค านวณ[14]

โครงสร้างการถอดรหัสหักล้างต่อเนื่องมีโครงสร้างที่เหมือนกันโครงสร้างการเข้ารหัส ในกรณีนี้สามารถพิจารณาโครงสร้างการถอดรหัสคือโครงสร้างการเข้ารหัสแบบกลับด้าน แสดงดังภาพที่ 2.11



ภาพที่ 2.11 โครงสร้างการถอดรหัสหักล้างต่อเนื่องขนาด $N=4$

โครงสร้างการถอดรหัสหักล้างต่อเนื่องจะประกอบไปด้วยตัวดาเนินการ 2 ชนิด คือ โหนดตรวจสอบ (check node) และโหนดตัวแปร (variable node) แสดงดังภาพที่ 2.12 โดยตัวดาเนินการทั้งสองจะทาการคานวณค่าที่ตัวถอดรหัสได้รับมาจากช่องสัญญาณรบกวน เพื่อทาการถอดรหัสและตัดสินใจค่าบิตถอดรหัส $\hat{\mathbf{u}}_1^N$ ในขั้นตอนสุดท้าย

ก) โหนดตรวจสอบ ข) โหนดตัวแปร

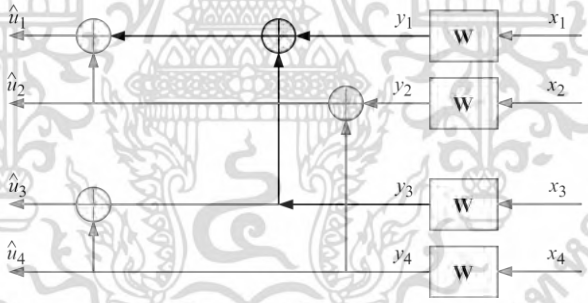
ภาพที่ 2.12 ตัวด าเนินการโหนดตรวจสอบและโหนดตัวแปรในโครงสร้างการถอดรหัสหักล้างต่อเนื่อง

กระบวนการถอดรหัสหักล้างต่อเนื่องสามารถแบ่งได้เป็น 4 กระบวนการ ซึ่งมีลักษณะการทางานในรูปแบบเรียกซ้า (recursive) โดยที่ตัวดาเนินการจะที่มี 2 อินพุตและ 1 เอาต์พุต โดยที่จะแทนอินพุตทั้ง 2 ด้วยตัวแปร a และ b และตัวแปร y สาหรับเอาต์พุตของตัวดาเนินการ แสดงดังภาพที่ 2.13

ภาพที่ 2.13 การแทนตัวแปรส าหรับตัวด าเนินการโหนดตรวจสอบและโหนดตัวแปร

1) ตัวดาเนินการโหนดตรวจสอบ หากดาเนินการกับเลขฐานสองจะเป็นตัวดาเนินการที่เทียบเท่ากับตัวด าเนินการเอ็กซ์คลูซีฟออร์ (exclusive-or) หรือ XOR หากด าเนินการกับเลขฐานสิบ เช่น ค่าความน่าจะเป็นหรือค่า LLR แสดงได้ดังภาพที่ 2.14 จะค านวณได้ดังนี้

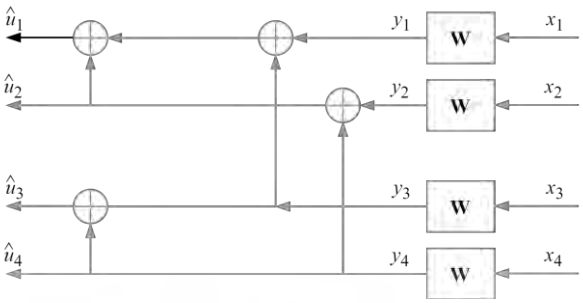
$$\begin{aligned} L\left(y|x\right) &= \ln\left(\frac{p\left(y|x=-1\right)}{p\left(y|x=1\right)}\right) \\ &= \ln\left(\frac{p\left(y|a=1\right)p\left(y|b=1\right)+p\left(y|a=-1\right)p\left(y|b=-1\right)}{p\left(y|a=1\right)p\left(y|b=-1\right)+p\left(y|a=-1\right)p\left(y|b=1\right)}\right) \\ &= \ln\left(\frac{1+e^{L(y|a)+L(y|b)}}{e^{L(y|a)}+e^{L(y|b)}}\right) \end{aligned} \tag{2.14}$$



ภาพที่ 2.14 ขั้นตอนการคานวณโหนดตรวจสอบในโครงสร้างตัวถอดรหัสหักล้างต่อเนื่อง

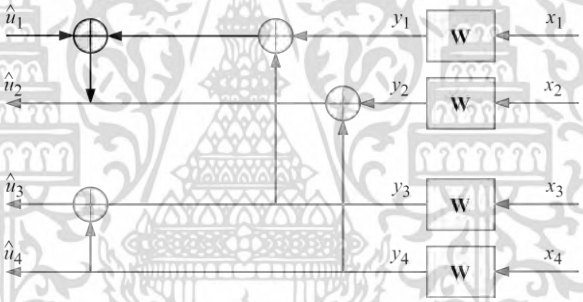
2) การตัดสินใจแบบฮาร์ด จะตัดสินใจบิตถอดรหัสจากค่าความน่าจะเป็นหรือค่า LLR ณ ระดับสุดท้ายของตัวถอดรหัส แสดงได้ดังภาพที่ 2.15 และสามารถค านวณได้ดังนี้

$$\hat{u}_i = \begin{cases} 0 & \text{หาก } L\left(y|x\right) \geq 0 \text{ หรือเป็นบิตแช่แข็ง} \\ 1 & \text{อื่น ๆ} \end{cases} \tag{2.15}$$



ภาพที่ 2.15 ขั้นตอนการตัดสินใจแบบฮาร์ดในโครงสร้างตัวถอดรหัสหักล้างต่อเนื่อง

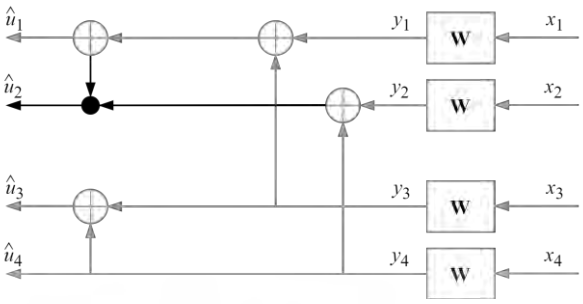
3) กระบวนการป้อนไปข้างหน้า ซึ่งจะประกอบไปด้วยตัวดาเนินการโหนดตรวจสอบ และตัวดาเนินการโหนดตัวแปร สาหรับโหนดตรวจสอบ เนื่องจากกระบวนการป้อนกลับจะป้อนค่าจากการตัดสินใจแบบฮาร์ดหรือบิตไบนารี ตัวด าเนินการโหนดสอบจะท างานแบบ XOR ดังภาพที่ 2.16



ภาพที่ 2.16 ขั้นตอนการคานวณโหนดตรวจสอบของกระบวนการป้อนไปข้างหน้าในโครงสร้างตัวถอดรหัสหักล้างต่อเนื่อง

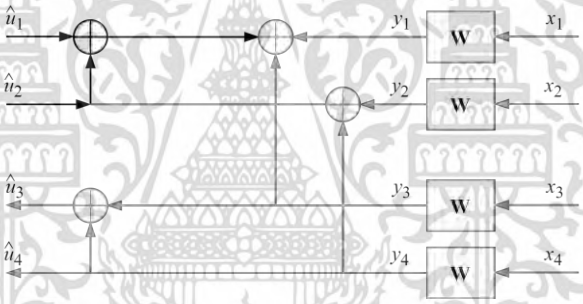
สาหรับโหนดตัวแปร หากดาเนินการกับเลขฐานสองหรือบิตไบนารีจะทาการเลือกเอาต์พุตจากอินพุตที่มีจานวนมากที่สุด หากอินพุตทั้งบิต 0 และ 1 มีจานวนเท่ากันจะทาการสุ่ม หากดาเนินการกับเลขฐานสิบเช่นค่าความน่าจะเป็นหรือค่า LLR กระบวนการนี้ค่าบิตไบนารีที่ได้จากโหนดตรวจสอบจะถูกค านวณร่วมกับค่า LLR แสดงได้ดังภาพที่ 2.17 และค านวณโดย

$$L\left(y|x\right)=\left(1-2\hat{u}\right)L\left(y|a\right)+L\left(y|b\right) \tag{2.16}$$



ภาพที่ 2.17 ขั้นตอนการค านวณโหนดตัวแปรของกระบวนการป้อนไปข้างหน้าในโครงสร้างตัวถอดรหัสหักล้างต่อเนื่อง

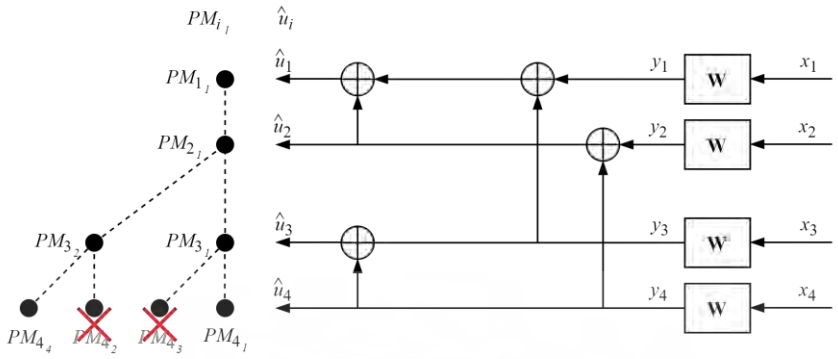
4) กระบวนการป้อนกลับ จะใช้ตัวด าเนินการโหนดตรวจสอบที่ป้อนค่าจากการตัดสินใจแบบฮาร์ดหรือบิตไบนารี ตัวด าเนินการโหนดสอบจะท างานแบบXOR ดังภาพที่ 2.18



ภาพที่ 2.18 ขั้นตอนการคานวณโหนดตรวจสอบของกระบวนการป้อนกลับในโครงสร้างตัวถอดรหัสหักล้างต่อเนื่อง

2.5.2 การถอดรหัสโพลาร์ด้วยการหักล้างต่อเนื่องแบบลิส

การถอดรหัสหักล้างต่อเนื่องต่อเนื่องแบบลิสจะแตกต่างจากการถอดรหัสหักล้างต่อเนื่องที่ขั้นตอนการตัดสินใจแบบฮาร์ด ในการถอดรหัสหักล้างต่อเนื่องจะท าการตัดสินใจบิตทันที แต่การถอดรหัสหักล้างต่อเนื่องแบบลิสนั้นจะยังไม่ตัดสินใจบิตทันที แต่จะทาการเก็บค่า LLR ของบิตถอดรหัส เพื่อจะได้เก็บความเป็นไปได้ของบิตข้อมูลทุกต าแหน่ง [6], [14] ทั้งนี้ การเก็บค่า LLR ของบิตถอดรหัสสามารถมองได้เส้นทางการถอดรหัสดังภาพที่ 2.19



ภาพที่ 2.19 ตัวถอดรหัสหักล้างต่อเนื่องแบบลิส

เมื่อทาการถอดรหัสมาถึงตาแหน่งบิตข้อมูล เส้นทางการถอดรหัสจะถูกแยกออกเป็น 2 เส้นทาง ทั้งนี้ จ านวนเส้นทางจะถูกจากัดไว้เพียงจานวน L ลิส ภาพที่ 2.19 แสดงตัวอย่างการถอดรหัสหักล้างต่อเนื่องแบบลิส เมื่อ $L=2$ และ $\mathcal{A}^F \in \{1,2\}$ สังเกตว่าที่ต าแหน่ง $i=4$ เส้นทางการถอดรหัสควรมีจานวน 4 ลิส แต่เนื่องจากจานวนเส้นทางการถอดรหัสถูกจากัดไว้ที่ค่า L ทาให้มีเส้นทางการถอดรหัสถูกกาจัดเหลือเพียง 2 เส้นทาง การเลือกเส้นทางการถอดรหัสจะเลือกจากค่าความน่าเชื่อถือเส้นทาง โดยจะเลือกกาจัดเส้นทางการถอดรหัสกับเส้นทางที่มีค่าความน่าเชื่อถือเส้นทางที่ต่าออก โดยค่าความน่าเชื่อถือเส้นทางสามารถค านวณได้ดังนี้

$$PM_{i_l} = PM_{i-1_l} + \ln\left(1+e^{-(1-2\hat{u}_{i_l})y_{i_l}}\right) \tag{2.17}$$

โดยที่ PM_{i_l} คือ ค่าความน่าเชื่อถือเส้นทาง ณ ต าแหน่งบิตที่ i และเส้นทางการถอดรหัสที่ l

$\hat{u}_{i_l}$ คือ บิตถอดรหัส ณ ต าแหน่งบิตที่ i และเส้นทางการถอดรหัสที่ l

y_{i_l} คือ ค่า LLR ระดับสุดท้ายของโครงสร้างถอดรหัส ณ ตาแหน่งบิตที่ i และเส้นทางการถอดรหัสที่ l

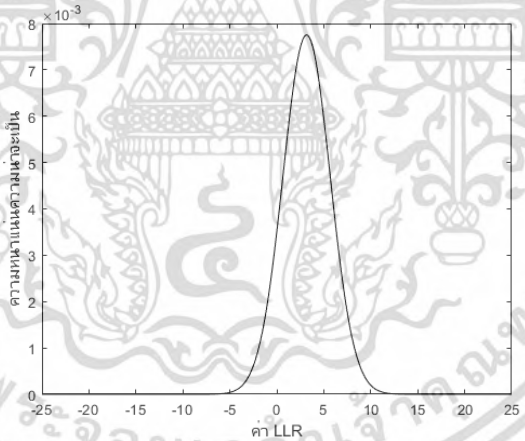
2.6 การสร้างรหัสโพลาร์

การสร้างรหัสโพลาร์มีเป้าหมายเพื่อหาต าแหน่งของบิตแช่แข็ง และบิตข้อมูล โดยใช้คุณสมบัติของการโพลาไรซ์ช่องสัญญาณ การสร้างรหัสโพลาร์สามารถทาได้หลายวิธี โดยแต่ละวิธีอาจใช้ตัวชี้วัดในการสร้างที่แตกต่างกัน เช่น ค่าข่าวสารร่วม (mutual information) ค่าความน่าจะเป็นความผิดพลาด (error probability) เป็นต้น การสร้างรหัสโพลาร์ที่ดีจะช่วยให้รหัสโพลาร์สามารถแก้ไขความผิดพลาดในการสื่อสาร ส่งผลให้มีสมรรถนะการแก้ไขความผิดพลาดสูงขึ้น

2.6.1 การสร้างรหัสโพลาร์ด้วยหลักการวิวัฒนาการความหนาแน่น

หลักการวิวัฒนาการความหนาแน่น (density evolution) เป็นอัลกอริทึมการวิเคราะห์ฟังก์ชันความหนาแน่นความน่าจะเป็น (probability density function) หรือ pdf ของข้อมูลที่ส่งผ่าน (message passing) ภายในโครงสร้างตัวถอดรหัส โดยหาความน่าจะเป็นบิตผิดจาก pdf ของแต่ละช่องสัญญาณย่อยที่ใช้ส่งบิตข้อมูล โดยเลือกช่องสัญญาณย่อยที่มีความน่าจะเป็นบิตผิดต่ำที่สุดเป็นตาแหน่งสาหรับส่งบิตข้อมูล $\mathcal{A}^I$ และเลือกช่องสัญญาณย่อยที่มีความน่าจะเป็นบิตผิดสูงที่สุดเป็นต าแหน่งสาหรับส่งบิตแช่แข็ง $\mathcal{A}^F$ [15]

หลักการวิวัฒนาการความหนาแน่นจะอยู่บนฐานของโครงสร้างตัวถอดรหัส ตัวดาเนินการจะประกอบไปด้วยโหนดตรวจสอบและโหนดตัวแปร โครงสร้างตัวถอดรหัสจะดาเนินการส่งผ่านค่าความน่าจะเป็นหรือค่า LLR ในรูปฟังก์ชัน pdf แสดงดังภาพที่ 2.20 ของแต่ละช่องสัญญาณย่อยไปตามโครงสร้างตัวถอดรหัส ฟังก์ชัน pdf จะถูกตัวด าเนินการค านวณทให้ฟังก์ชัน pdf เปลี่ยนรูปร่างไปตามตัวดาเนินการในโครงสร้างตัวถอดรหัส สุดท้ายของขั้นตอนการถอดรหัส จะได้ผลลัพธ์ของฟังก์ชัน pdf ของแต่ละช่องสัญญาณย่อยซึ่งสามารถน ามาใช้เลือกส่งบิตข้อมูลหรือบิตแช่แข็งต่อไป



ภาพที่ 2.20 ฟังก์ชัน pdf ของค่า LLR

ฟังก์ชัน pdf ของค่า LLR ก่อนที่จะส่งผ่านโครงสร้างตัวถอดรหัส จะถูกคานวณขึ้นมาโดยสมมุติฐานบิตที่ทาการส่งเป็นบิต 0 ทั้งหมดหรือ $x=-1$ โดยค่า LLR มีการกระจายแบบเกาส์เซียน (Gaussian distribution) และมีฟังก์ชัน pdf ดังสมการนี้

$$p(L)=\frac{1}{\sqrt{2\pi\sigma_L^2}}e^{-\frac{1}{2\sigma_L^2}(L-\mu_L)^2} \tag{2.18}$$

โดยที่ μ_L คือ ค่าเฉลี่ยของค่า LLR

σ_L^2 คือ ค่าความแปรปรวนของค่า LLR

ค่าเฉลี่ย μ_x และค่าคาดหวัง (expected value) แทนด้วยสัญลักษณ์ $E(x)$ โดยค่าเฉลี่ยของ LLR แสดงได้ดังสมการนี้

$$\begin{aligned}\mu_L &= E(L)\\ &= E\left(\frac{-2y}{\sigma_{\text{ch}}^2}\right)\\ &= \frac{2}{\sigma_{\text{ch}}^2}\end{aligned} \tag{2.19}$$

โดยที่ σ_{ch}^2 คือ ค่าความแปรปรวนของช่องสัญญาณรบกวน สามารถแสดงได้ดังสมการนี้

$$\begin{aligned}\sigma_L^2 &= E\left(L^2\right) - E^2\left(L\right)\\ &= E\left(\left(\frac{-2y}{\sigma_{\text{ch}}^2}\right)^2\right) - E^2\left(\frac{-2y}{\sigma_{\text{ch}}^2}\right)\\ &= \frac{4}{\sigma_{\text{ch}}^2}E\left(y^2\right) - \frac{4}{\sigma_{\text{ch}}^2}\\ &= \frac{4}{\sigma_{\text{ch}}^2}\\ &= 2\mu_L\end{aligned} \tag{2.20}$$

การกระจายแบบเกาส์เซียน $\mathcal{N}\left(\mu, \sigma_L^2\right)$ ที่มีค่าเฉลี่ยและค่าความแปรปรวนดังสมการที่ 2.19 และ 2.20 เขียนแทนได้โดย $\mathcal{N}\left(\frac{2}{\sigma_{ch}^2}, \frac{4}{\sigma_{ch}^2}\right)$ เมื่อนาค่าเฉลี่ยและค่าความแปรปรวนแทนในสมการที่ 2.18 จะได้ฟังก์ชัน pdf ของค่า LLR ดังสมการนี้

$$p(L) = \frac{1}{\sqrt{\frac{8\pi}{\sigma_{ch}^2}}} e^{-\frac{1}{\frac{8}{\sigma_{ch}^2}}\left(L-\frac{2}{\sigma_{ch}^2}\right)^2} \tag{2.21}$$

จะสังเกตได้ว่าในสมการจะประกอบไปด้วยค่าแปรปรวนของช่องสัญญาณรบกวน ซึ่งจะเปลี่ยนแปลงตามคุณภาพของช่องสัญญาณ ค่าแปรปรวนของช่องสัญญาณรบกวนสามารถคานวณได้ดังนี้

$$
\begin{aligned}
SNR &= 10\log_{10}\left(\frac{E_c}{N_0}\right) \\
&= 10\log_{10}\left(\frac{E_b}{RN_0}\right) \\
&= 10\log_{10}\left(\frac{1}{2R\sigma_{ch}^2}\right)
\end{aligned}
\tag{2.22}
$$

$$
\sigma_{ch}^2 = \frac{1}{2R\left(10^{\frac{SNR}{10}}\right)}
$$

โดยที่ SNR คือ อัตราส่วนสัญญาณที่ต้องการต่อสัญญาณรบกวน

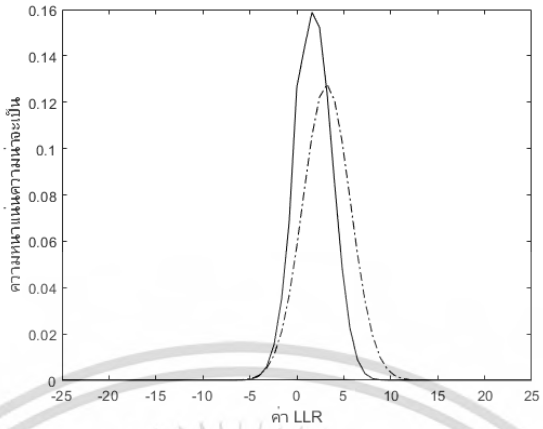
$\frac{E_c}{N_0}$ คือ อัตราส่วนพลังงานของค ซหัสต่อพลังงานของสัญญาณรบกวน

$\frac{E_b}{N_0}$ คือ อัตราส่วนพลังงานของบิตข้อมูลต่อพลังงานของสัญญาณรบกวน

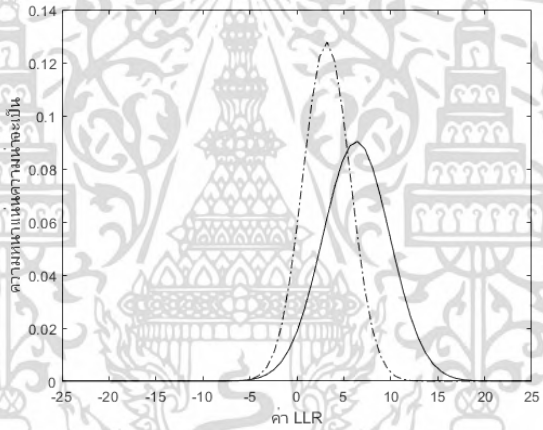
ตัวดาเนินการโหนดตรวจสอบและโหนดตัวแปรจะคานวณเหมือนกับการถอดรหัส โดยจะคานวณทุกความเป็นไปได้ของค่า LLR เช่น อินพุตของโหนดตรวจสอบ 2 ตัว มีค่า pdf เป็น $p_A\left(L\left(y|a\right)=-2.6\right)=0.025$ และ $p_B\left(L\left(y|b\right)=1.2\right)=0.07$ ผลลัพธ์จากโหนดตรวจสอบของทั้ง 2 อินพุตนี้จะได้ค่าของฟังก์ชัน pdf ที่ $p_X\left(L\left(y|x\right)=-1\right)=0.00175$ แสดงดังสมการที่ 2.23 และหากเป็นอินพุตของโหนดตัวแปร 2 ตัว มีค่า pdf เป็น $p_A\left(L\left(y|a\right)=-2.6\right)=0.025$ และ $p_B\left(L\left(y|b\right)=1.2\right)=0.07$ ผลลัพธ์จากโหนดตัวแปรของทั้ง 2 อินพุตนี้จะได้ค่าของฟังก์ชัน pdf ที่ $p_X\left(L\left(y|x\right)=-1.4\right)=0.00175$ แสดงดังสมการที่ 2.24 โดยแนวโน้มของฟังก์ชัน pdf ของค่า LLR ที่ผ่านโหนดตรวจสอบ จะมีแนวโน้มที่กราฟแคบลง เนื่องจากเกิดการคูณกันดังภาพที่ 2.21 และที่ผ่านโหนดตัวแปร จะมีแนวโน้มที่กราฟเลื่อนไปทางขวาเนื่องจากเกิดการบวกกันดังภาพที่ 2.22

$$
p_X\left(\ln\left(\frac{1+e^{L(y|a)+L(y|b)}}{e^{L(y|a)}+e^{L(y|b)}}\right)\right) = p_A\left(L\left(y|a\right)\right)p_B\left(L\left(y|b\right)\right) \tag{2.23}
$$

$$
p_X\left(L\left(y|a\right)+L\left(y|b\right)\right) = p_A\left(L\left(y|a\right)\right)p_B\left(L\left(y|b\right)\right) \tag{2.24}
$$



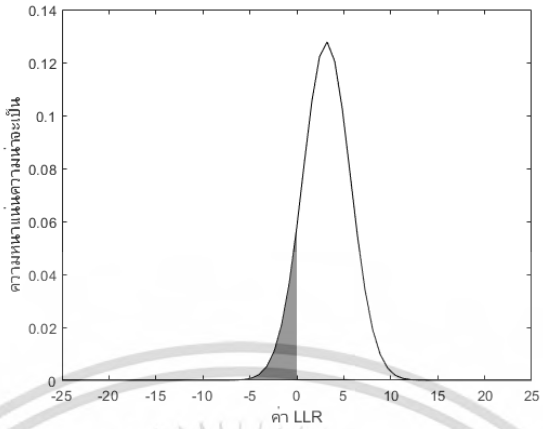
ภาพที่ 2.21 แนวโน้มของฟังก์ชัน pdf ของค่า LLR ที่ผ่านตัวด าเนินการโหนดตรวจสอบ



ภาพที่ 2.22 แนวโน้มของฟังก์ชัน pdf ของค่า LLR ที่ผ่านตัวด าเนินการโหนดตัวแปร

ฟังก์ชัน pdf ของค่า LLR จะถูกนามาใช้วิเคราะห์ความน่าเชื่อถือของช่องสัญญาณย่อย โดยพิจารณาจากผลรวมของความน่าจะเป็นที่วงจรถอดรหัสตัดสินใจบิต 1 กรณีนี้จะหมายถึงบิตผิด หรือผลรวมของความน่าจะเป็นที่ค่า LLR เป็นลบ แสดงดังภาพที่ 2.23 ในส่วนที่แรเงาสีเทา และสามารถใช้ฟังก์ชัน cdf $F_L(0)$ หรือเทียบเท่ากับความน่าจะเป็นผิดพลาด P_e ในการตัดสินใจบิต ดังสมการที่ 2.25

$$P_e = P[L \le 0] \tag{2.25}$$



ภาพที่ 2.23 พื้นที่แรเงาแสดงความน่าจะเป็นบิตผิดที่ได้จากการวิเคราะห์ความน่าเชื่อถือของช่องสัญญาณย่อย

2.6.2 การสร้างรหัสโพลาร์ด้วยหลักการประมาณเกาส์เซียน

การคำนวณด้วยหลักการวิวัฒนาการความหนาแน่นจำเป็นต้องคำนวณทุกความเป็นไปได้ของค่า LLR ซึ่งต้องใช้การคำนวณด้วยการคอนโวลูชัน (convolution) จำนวนมาก หลักการประมาณเกาส์เซียน (Gaussian approximation) สามารถลดความซับซ้อนในการคำนวณได้โดยการลดการคำนวณฟังก์ชัน pdf ทั้งนี้ เนื่องจากค่า LLR ที่ตำแหน่งต่างๆ ในโครงสร้างตัวถอดรหัสจะมีรูปร่างใกล้เคียงกับการกระจายแบบเกาส์เซียน หลักการประมาณเกาส์เซียนจะกำหนดให้ฟังก์ชัน pdf ของ LLR ในโครงสร้างตัวถอดรหัสมีลักษณะเหมือนกับกระจายแบบเกาส์เซียนเท่านั้น ทำให้ สามารถใช้เพียงค่าเฉลี่ย (ค่าความแปรปรวน สามารถแปลงเป็นค่าเฉลี่ยจากสมการที่ 2.20) [16] ในการคำนวณค่าเฉลี่ยของค่า LLR ของแต่ละช่องสัญญาณย่อย สามารถคำนวณได้ดังนี้

$$\mu_{L_n^{(2i-1)}} = \phi^{-1}\left(1-\left(1-\phi\left(u_{L_{n/2}^{(i)}}\right)\right)^2\right) \tag{2.26}$$

$$\mu_{L_n^{(2i)}} = 2\mu_{L_{n/2}^{(i)}} \tag{2.27}$$

โดยที่ $\mu_{L_{ll}}$ คือ ค่าเฉลี่ยของค่า LLR ที่ระดับชั้น ll ของโครงสร้างตัวถอดรหัส

$\mu_{L_{ll-1}}$ คือ ค่าเฉลี่ยของค่า LLR ที่ระดับชั้นก่อนหน้าชั้น ll ของโครงสร้างตัวถอดรหัส

และ $$\phi(x) = \begin{cases} 1-\dfrac{1}{\sqrt{4\pi x}}\displaystyle\int_{-\infty}^{\infty}\tanh\frac{\mu_x}{2}e^{-\frac{(\mu_x-x)^2}{4x}}dx, & x>0 \\ 1, & x=0 \end{cases} \tag{2.28}$$

โดยกาหนดให้ค่าเฉลี่ยของค่า LLR ที่ระดับชั้นแรกมีค่าเท่ากับ $\mu_{L_{ll=1}} = \frac{2}{\sigma^2}$ จากนั้นจึงสามารถคานวณความน่าจะเป็นความผิดพลาดของช่องสัญญาณย่อยได้ดังนี้

$$P_e\left(W_N^{(i)}\right) \approx Q\left(\sqrt{\mu_{L_n^{(i)}}/2}\right) \tag{2.29}$$

โดยที่ $P_e\left(W_N^{(i)}\right)$ คือ ค่าความน่าจะเป็นความผิดพลาดของช่องสัญญาณย่อย $W_N^{(i)}$

2.6.3 การสร้างรหัสโพลาร์ด้วยหลักการขยายเบต้า

การสร้างรหัสโพลาร์ในหัวข้อที่ผ่านมา ผลลัพธ์จะแตกต่างกันไปตามคุณภาพช่องสัญญาณ เช่น ค่า SNR ค่าความน่าจะเป็นลบล้าง เป็นต้น ทาให้ต้องสร้างรหัสโพลาร์ใหม่เมื่อคุณภาพช่องสัญญาณเปลี่ยนไป กล่าวได้ว่าความน่าเชื่อถือของช่องสัญญาณย่อยจะขึ้นอยู่กับช่องสัญญาณรบกวน (channel dependent) หลักการขยายเบต้าใช้หลักการคานวณความน่าเชื่อถือของช่องสัญญาณที่ไม่ขึ้นอยู่กับช่องสัญญาณรบกวน (channel independent) ทาให้สามารถเตรียมการคานวณลาดับความน่าเชื่อถือของช่องสัญญาณย่อยไว้ก่อนการสื่อสารจริงได้ [17] การคานวณจะใช้ค่าน้าหนักโพลาไรซ์ (polarization weight) ของช่องสัญญาณย่อย $W_N^{(i)}$ แทนด้วยสัญลักษณ์ $PW\left(W_N^{(i)}\right)$ ตาแหน่งช่องสัญญาณย่อยแทนด้วยสัญลักษณ์ i และการขยายไบนารีของ i แทนด้วยสัญลักษณ์ $b = \{b_{n-1}, \ldots, b_1, b_0\}$ เช่น ตาแหน่งช่องสัญญาณย่อยที่ $i = 12$ จากช่องสัญญาณย่อยทั้งหมด $N = 2^n = 16$ จะสามารถขยายไบนารีได้เป็น $b = \{1,1,0,0\}$ ค่าน้าหนักโพลาร์สามารถคานวณได้ดังนี้

$$PW\left(W_N^{(i)}\right) = \sum_{j=0}^{n-1} b_j \beta^j \tag{2.30}$$

สาหรับช่องสัญญาณรบกวน AWGN จะกาหนดให้ค่า $\beta = 2^{1/4}$ จากการสังเกต โดยที่ช่องสัญญาณย่อยที่มีค่าน้าหนักโพลาไรซ์มากจะมีความน่าเชื่อถือมาก

2.7 รหัสย่อยของรหัสโพลาร์

รหัสโพลาร์ทั่วไปถือเป็นรหัสที่สามารถพิสูจน์ได้ว่าการส่งข้อมูลสามารถเข้าใกล้ความจุช่องสัญญาณ อย่างไรก็ตาม ในทางปฏิบัติรหัสโพลาร์ให้สมรรถนะการแก้ไขความผิดพลาดที่ไม่ดีตามที่คาดหวัง สาหรับรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิสสามารถเพิ่มสมรรถนะขึ้นมาได้ โดยการถอดรหัสแบบลิสนั้นสามารถเพิ่มสมรรถนะให้เข้าใกล้การถอดรหัสความน่าจะเป็นภายหลังสูงสุด (maximum a posteriori) หรือ MAP แต่สมรรถนะก็ยังไม่สามารถทัดเทียมกับรหัสอื่น ๆ ที่มีสมมรถนะสูง รหัสอื่น ๆ จึงถูกนามาใช้งานร่วมกับรหัสโพลาร์เพื่อเพิ่มสมรรถนะการแก้ไขความผิดพลาด โดยนารหัสอื่นมาเข้ารหัสหรือถอดรหัสต่อกับรหัสโพลาร์ (concatenated) ซึ่งจะเรียกรหัสที่นามาต่อว่ารหัสย่อย การ

ใช้งานรหัสย่อยร่วมกับรหัสโพลาร์สามารถเพิ่มสมรรถนะของรหัสโพลาร์ให้ทัดเทียมหรือดีกว่ารหัสที่มีสมรรถนะการแก้ไขความผิดพลาดที่ดีได้ เช่น รหัสแอลดีพีซี (low-density parity-check: LDPC)

2.7.1 รหัสโพลาร์ร่วมกับ CRC

รหัสโพลาร์ร่วมกับ CRC ถูกนาเสนอเพื่อเพิ่มสมรรถนะการแก้ไขความผิดพลาดของรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิส การตรวจสอบด้วยส่วนซ้าซ้อนแบบวน (cyclic redundancy check) หรือ CRC สามารถใช้งานร่วมกับรหัสโพลาร์ได้โดยบิตข้อมูลจะถูกเข้ารหัส CRC ได้บิต CRC และนามาต่อท้ายกับบิตข้อมูลได้คารหัส CRC ในรูปแบบอนุกรม หรือ systematic จากนั้นจะถูกเข้ารหัสโพลาร์ ในส่วนการถอดรหัส จะดาเนินการถอดรหัสหักล้างต่อเนื่องแบบลิสตามปกติ กระบวนการเข้ารหัสโพลาร์ร่วมกับ CRC แสดงได้ดังภาพที่ 2.24

ภาพที่ 2.24 กระบวนการเข้ารหัสโพลาร์ร่วมกับ CRC

2.7.1.1 รหัส CRC

รหัส CRC เป็นอัลกอริทึมในการตรวจสอบความผิดพลาด ถูกใช้งานในการสื่อสารดิจิทัลเพื่อตรวจสอบความผิดพลาดที่อาจเกิดขึ้นของข้อมูล [18] รหัส CRC มีคุณสมบัติเป็นรหัสวนหรือ cyclic ที่ดาเนินการบน $GF(2)$ กาหนดให้พหุนามใด ๆ $a(x)=a_b x^b+a_{b-1}x^{b-1}+\ldots+a_1x^1+a_0$ โดยที่ b เท่ากับดีกรีสูงสุด การเข้ารหัส CRC จะทาการเข้ารหัสบิตข้อมูลในรูปพหุนาม $m(x)$ มีดีกรีสูงสุดเท่ากับ $k-1$ มีดีกรีสูงสุดเท่ากับ $c(x)$ คารหัสในรูปพหุนาม $c(x)$ ที่มีดีกรีสูงสุดเท่ากับ $n-1$ สามารถแสดงสมการได้ดังนี้

$$c(x)=m(x)g(x) \tag{2.31}$$

โดยที่ n คือ ความยาวค ารหัส

k คือ ความยาวบิตข้อมูล

พหุนามกาเนิด $g(x)=x^{n-k}+g_{n-k-1}x^{n-k-1}+g_{n-k-2}x^{n-k-2}+\ldots+g_1x+1$ สามารถสร้างเมทริกซ์ก าเนิดโดยการน าสัมประสิทธิ์ของพหุนามก าเนิดมาท าการเลื่อนวนในแต่ละแถวต่าง ๆ ของเมทริกซ์กาเนิดดังนี้

$$G=\begin{bmatrix} 1 & g_{n-k-1} & g_{n-k-2} & \cdots & g_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & g_{n-k-1} & \cdots & g_2 & g_1 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & g_{n-k-1} & g_{n-k-2} & g_{n-k-3} & \cdots & g_1 & 1 \end{bmatrix} \tag{2.32}$$

สาหรับการเข้ารหัส CRC รูปแบบ systematic ทาได้โดยการเติมบิต CRC ต่อจากบิตข้อมูล $m(x)$ โดยบิต CRC $r(x)$ มีดีกรีสูงสุดเท่ากับ $n-k-1$ ดังนี้

$$m(x)x^{n-k}=a(x)g(x)+r(x) \tag{2.33}$$

ย้ายพจน์ $r(x)$ ไปทางซ้ายจะได้ค ารหัสดังนี้

$$c(x)=m(x)x^{n-k}+r(x) \tag{2.34}$$

โดยที่ $r(x)$ คือ เศษจากการหาร $m(x)x^{n-k}$ ด้วย $g(x)$

การสร้างเมทริกซ์กาเนิดในรูปแบบ systematic ทาได้โดย กาหนดให้บิตข้อมูลในรูปพนุนาม $m_i(x)=X^i$ เป็นบิตข้อมูลที่มีบิต 1 เพียงต าแหน่งที่ i จากนั้น จะจัดรูปของสมการที่ 2.33 ใหม่ได้ดังนี้

$$\begin{aligned} x^{n-k+i} &= m_i(x)x^{n-k} \\ &= a_i(x)g(x)+r_i(x) \end{aligned} \tag{2.35}$$

โดยที่จะได้เศษ $r_i(x)$ จากการหาร $m_i(x)x^{n-k}$ ดังนี้

$$r_i(x)=r_{i,n-k-1}x^{n-k-1}+r_{i,n-k-2}x^{n-k-2}+\ldots+r_{i,1}x+r_{i,0} \tag{2.36}$$

และเนื่องจาก $r_i(x)+x^{n-k-i}$ หารด้วย $g(x)$ ลงตัว จึงสามารถสร้างเมทริกซ์กาเนิดในรูปแบบ systematic ได้โดยการน าเศษ $r_i(x)$ จากการหาร $m_i(x)x^{n-k}$ ของตาแหน่ง $0\le i<k$ มาเรียงในแถวทั้งหมด k แถวของเมทริกซ์ก าเนิดขนาด $k\times n$ ดังนี้

$$G=\begin{bmatrix} 1 & 0 & \cdots & 0 & r_{k-1,n-k-1} & r_{k-1,n-k-2} & \cdots & r_{k-1,1} & r_{k-1,0} \\ 0 & 1 & \cdots & 0 & r_{k-2,n-k-1} & r_{k-2,n-k-2} & \cdots & r_{k-2,1} & r_{k-2,0} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & r_{0,n-k-1} & r_{0,n-k-2} & \cdots & r_{0,1} & r_{0,0} \end{bmatrix} \tag{2.37}$$

และเขียนเมทริกซ์พาริตีตรวจสอบในรูปแบบ systematic ได้ดังสมการนี้

$$H=\begin{bmatrix} r_{k-1,n-k-1} & r_{k-2,n-k-1} & \cdots & r_{1,n-k-1} & r_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ r_{k-1,n-k-2} & r_{k-2,n-k-2} & \cdots & r_{1,n-k-2} & r_{0,n-k-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{k-1,0} & r_{k-2,0} & \cdots & r_{1,0} & r_{0,0} & 0 & 0 & \cdots & 1 \end{bmatrix} \tag{2.38}$$

การเข้ารหัส CRC ในทางปฏิบัติจะมีกระบวนการโดยการนา $m(x)x^{n-k}$ หารด้วย $g(x)$ จากนั้นน าเศษ $r(x)$ จากการหารต่อท้าย $m(x)x^{n-k}$ ได้ค ารหัส $c(x)$ ดังสมการที่ 2.34

การถอดรหัส CRC มีกระบวนการที่คล้ายคลึงกับการเข้ารหัส โดยสามารถนาบิตที่ได้รับ $\hat{c}(x)$ หารด้วย $g(x)$ หากหารลงตัวหรือเกิดเศษเป็น 0 จะถือว่าบิตที่ได้รับเหมือนกับค ชรหัส $c(x)$ ซึ่งถือว่าไม่เกิดความผิดพลาดใด ๆ

2.7.1.2 ความสัมพันธ์ของพหุนามกำเนิดและพหุนามพาริตีตรวจสอบ

รหัสบล็อกเชิงเส้นทั่วไป บิตข้อมูล m จะสามารถเข้ารหัสได้โดยการคูณกับเมทริกซ์กาเนิด G อย่างไรก็ตาม สาหรับรหัส cyclic จะสามารถเข้ารหัสบิตข้อมูลได้โดยพหุนามกาเนิด โดยพหุนามกาเนิดจะสามารถนาไปสร้างรีจิสเตอร์แบบเลื่อน (shift register) เพื่อใช้ในการเข้ารหัส รหัส CRC จึงมักใช้งานพหุนามกาเนิดมากกว่าเขียนเป็นรูปเมทริกซ์ รหัสบล็อกเชิงเส้นทั่วไปจะใช้งานเมทริกซ์พาริตีตรวจสอบในการถอดรหัส สาหรับรหัส CRC ก็สามารถใช้งานเมทริกซ์พาริตีตรวจสอบได้เช่นกัน โดยเมทริกซ์ตรวจสอบสามารถสร้างได้จากพหุนามพาริตีตรวจสอบ

ก าหนดให้พหุนามก าเนิด $g(x)$ เขียนได้ดังสมการนี้

$$x^n + 1 = g(x)\,f(x) \tag{2.39}$$

โดยที่ $f(x)$ มีดีกรีสูงสุดเท่ากับ k จากนั้นพหุนามพาริตีตรวจสอบ $h(x)$ จะเป็นพหุนามส่วนกลับ (reciprocal polynomial) ของ $f(x)$ พหุนามพาริตีตรวจสอบแสดงได้ดังสมการนี้

$$\begin{aligned} h(x) &= x^k f\left(x^{-1}\right) \\ &= 1 + f_{k-1}x + \ldots + f_1 x^{k-1} + x^k \\ &= 1 + h_1 x + \ldots + h_{k-1}x^{k-1} + x^k \end{aligned} \tag{2.40}$$

และสามารถสร้างเมทริกซ์พาริตีตรวจสอบได้โดย

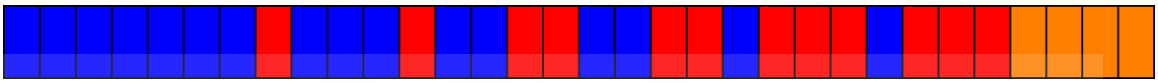
$$H = \begin{bmatrix} 1 & h_1 & h_2 & \cdots & h_{k-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & h_1 & \cdots & h_{k-2} & h_{k-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & h_1 & h_2 & h_3 & \cdots & h_{k-1} & 1 \end{bmatrix} \tag{2.41}$$

โดยที่ H มีขนาด $(n-k)\times n$ และแถวสุดท้ายของเมทริกซ์จะมีการเลื่อนวนไปซ้ายจานวน $n-k-1$ ครั้ง

2.7.1.3 รหัสโพลาร์ที่มี CRC ช่วย

รหัสโพลาร์ที่มี CRC ช่วย (CRC-aided polar code) จะทาการเข้ารหัส CRC ร่วมกับรหัสโพลาร์ได้ดังสมการที่ 2.34 โดยบิต CRC จะถูกต่อท้ายกับบิตข้อมูล แสดงดังภาพที่ 2.25 และสามารถแสดง

ความสัมพันธ์ระหว่างบิต CRC กับบิตข้อมูลของค ชรัส CRC ได้ดังสมการที่ 4.1 [5], [6] การเข้ารหัส CRC ร่วมกับรหัสโพลาร์ถูกพิสูจน์ให้เห็นว่าเป็นการเพิ่มการกระจายของน้ำหนักแฮมมิง (Hamming weight) ของค ชรัสให้สูงขึ้น ส่งผลให้มีสมรรถนะการแก้ไขความผิดพลาดเพิ่มขึ้น [19]



ภาพที่ 2.25 ต าแหน่งของบิต CRC (สีส้ม) บิตข้อมูล (สีแดง) และบิตแช่แข็ง (สีน ้าเงิน)

การถอดรหัสจะดาเนินการถอดรหัสหักล้างต่อเนื่องแบบลิสปกติ แต่ในขั้นตอนการถอดรหัสหลังจากบิตสุดท้าย เส้นทางการถอดรหัสทุก L เส้นทาง จะผ่านการถอดรหัส CRC เพื่อตรวจสอบความผิดพลาด เส้นทางการถอดรหัสที่ผิดพลาดจะถูกคัดออกและเส้นทางการถอดรหัสที่ถูกต้องถูกคัดเลือกต่อไป หากเหลือเพียงเส้นทางเดียว จะเลือกเส้นทางดังกล่าวเป็นบิตถอดรหัส หากเหลือมากกว่าหนึ่งเส้นทาง จะถูกเลือกด้วยค่าความน่าเชื่อเส้นทางเส้นทางที่น่าเชื่อถือที่สุด และหากไม่มีเส้นทางใดผ่านการถอดรหัส CRC เส้นทางทั้งหมดจะถูกคัดเลือกโดยค่าความน่าเชื่อเส้นทางตามปกติ

2.7.2 รหัสโพลาร์พาริตีตรวจสอบ

รหัสโพลาร์พาริตีตรวจสอบ (parity-check polar code) ถูกนาเสนอเพื่อเพิ่มสมรรถนะการแก้ไขความผิดพลาดของรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิสเช่นเดียวกับรหัสโพลาร์ร่วมกับ CRC [19], [20] เนื่องจากรหัส CRC ที่ใช้งานร่วมกับรหัสโพลาร์สามารถพิจารณาความสัมพันธ์ระหว่างบิต CRC และบิตข้อมูลได้ โดยความสัมพันธ์ในเมทริกซ์พาริตีตรวจสอบจะขึ้นอยู่กับพหุนามกาเนิดเป็นตัวกาหนดตาแหน่งของบิต CRC รวมถึงความสัมพันธ์ของบิต CRC กับบิตข้อมูล ซึ่งไม่ยืดหยุ่นในการออกแบบ โดยบิต CRC สามารถเรียกแทนได้ว่าบิตพาริตี สาหรับรหัสโพลาร์พาริตีตรวจสอบสามารถวางบิตพาริตีไว้ที่ต าแหน่งใดก็ได้และบิตพาริตีสามารถเลือกความสัมพันธ์กับบิตข้อมูลบิตใดก็ได้ แสดงดัง**ภาพที่ 2.26**

ภาพที่ 2.26 ตาแหน่งของบิตพาริตี (สีส้ม) บิตข้อมูล (สีแดง) และบิตแช่แข็ง (สีน้าเงิน) สาหรับการเข้ารหัสโพลาร์

การเข้ารหัสพาริตีตรวจสอบสามารถแบ่งเป็นขั้นตอนย่อยได้ดังนี้

1) เลือกต าแหน่งบิตพาริตีโดยต าแหน่งบิตพาริตีจะมีความยืดหยุ่น สามารถแทรกอยู่ระหว่างบิตข้อมูลหรือต่อท้ายบิตข้อมูลก็ได้

2) ก าหนดความสัมพันธ์ของบิตพาริตีกับบิตข้อมูล โดยบิตข้อมูลที่มีความสัมพันธ์กับบิตพาริตีจะต้องอยู่ตาแหน่งก่อนหน้าบิตพาริตีทุกบิต จากนั้นจะสามารถแสดงตาแหน่งของชุดบิตพาริตี $p=\{p_0,p_1,\ldots p_{r-1}\}$ มีความยาว r บิต และชุดบิตข้อมูล $m=\{m_0,m_1,\ldots,m_{k-1}\}$ มีความยาว k บิต ดังนี้

$$u_{\mathcal{A}^I,\mathcal{A}^P}=\{m_0,m_1,\ldots,p_0,m_2,m_3,\ldots,p_1,m_{k-2},\ldots,p_{r-2},m_{k-1},\ldots,p_{r-1}\} \quad (2.42)$$

3) นาบิตพาริตี บิตข้อมูล และบิตแช่แข็งเรียงตามตาแหน่งจากการสร้างรหัสและเข้ารหัสโพลาร์

การถอดรหัสพาริตีตรวจสอบจะถอดรหัสภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิส โดยร่วมถอดรหัสบิตพาริตีระหว่างการถอดรหัสหักล้างต่อเนื่องแบบลิสมีขั้นตอนดังนี้

1) ถอดรหัสหักล้างต่อเนื่องแบบลิสปกติ

2) เมื่อถึงต าแหน่งบิตพาริตี บิตพาริตีจะถูกตัดสินใจจากความสัมพันธ์กับบิตข้อมูลในต าแหน่งก่อนหน้า โดยทุกบิตในความสัมพันธ์จะต้องรวมกันภายใต้ $GF(2)$ ได้เท่ากับ 0 แทนการตัดสินใจจากค่า LLR ของตัวถอดรหัสชั้นสุดท้าย แสดงความสัมพันธ์ในรูปแถวของเมทริกซ์พาริตีตรวจสอบได้ดังสมการที่ 4.1

3) ด าเนินการถอดรหัสหักล้างต่อเนื่องแบบลิสจนสิ้นสุดปกติ

2.7.3 รหัสย่อยอื่น ๆ

รหัสโพลาร์ยังถูกนาเสนอให้มีการใช้งานร่วมกับรหัสย่อยอื่น ๆ เพื่อเพิ่มสมรรถนะการแก้ไขความผิดพลาดของรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิส เช่น รหัส Bose-Chaudhuri-Hocquenghem หรือ BCH โดยมีการกาหนดบิตพิเศษเพิ่มเติมคือบิตแช่แข็งพลวัต (dynamic frozen bit) ซึ่งจะมีคุณสมบัติคล้ายบิตพาริตีซึ่งมีความสัมพันธ์กับบิตข้อมูล และมีการถอดรหัสร่วมกับการถอดรหัสรหัสหักล้างต่อเนื่องแบบลิสของรหัสโพลาร์ [21] นอกจากนี้ยังมีการนารหัสอื่น ๆ มาเข้ารหัสและถอดรหัสต่อกับรหัสโพลาร์ เช่น รหัสแอลดีพีซีและรหัส Reed-Solomon หรือ RS โดยสามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดได้เมื่อเทียบกับรหัสโพลาร์แบบปกติ

2.8 การแบ่งส่วนตัวถอดรหัส

การถอดรหัสหักล้างต่อเนื่องแบบลิสเป็นการถอดรหัสโพลาร์ที่ให้สมรรถนะดี แต่เป็นการถอดรหัสที่ต้องใช้งานหน่วยความจาขนาดใหญ่สาหรับการเก็บค่าในการคานวณการถอดรหัส โดยเฉพาะ

ยิ่งขนาดลิสเพิ่มมากขึ้น นั้นหมายถึงความว่าการใช้งานบนอุปกรณ์จริงจะต้องการพื้นที่หน่วยความจาจานวนมาก ซึ่งในงานวิจัยได้มีการสังเกตว่าตัวถอดรหัสหักล้างต่อเนื่องมีการใช้งานหน่วยความจากว่า 45% ของพื้นที่วงจรถอดรหัสทั้งหมด วิธีการแบ่งส่วนตัวตัวถอดรหัสจึงถูกน าเสนอใน [11] เพื่อการลดการใช้งานหน่วยความจ าจานวนมาก

2.8.1 ความซับซ้อนการถอดรหัสโพลาร์

ความซับซ้อนของรหัสโพลาร์สามารถเกิดขึ้นได้ทุกส่วนของระบบ ทั้งการเข้ารหัส การสร้างรหัส และการถอดรหัส หากความซับซ้อนของระบบลดต่าลง ระบบจะสามารถรองรับปริมาณข้อมูลต่อพื้นที่หรือเวลามากขึ้นได้ โดยส่วนแรกของวิทยานิพนธ์ฉบับนี้จะมุ่งเน้นการลดความซับซ้อนการถอดรหัสโพลาร์ การถอดรหัสหักล้างต่อเนื่องแบบลิสให้สมรรถนะในการแก้ไขความผิดพลาดที่ยอดเยี่ยม แต่กลับมีข้อเสียเมื่อเทียบกับการถอดรหัสแบบลิสทั่วไป นั้นคือการใช้งานหน่วยความจาขนาดใหญ่ ส่งผลให้พื้นที่ของวงจรถอดรหัสมีขนาดใหญ่และยังเพิ่มความหน่วงเวลาในการคานวณได้เช่นกัน พื้นที่หน่วยความจาของตัวถอดรหัสหักล้างต่อเนื่องสามารถค านวณได้ดังสมการนี้

$$M_{SCL} = \left(N + \left(N-1\right)L\right)Q_{\alpha} + LQ_{PM} + \left(2N-1\right)L \tag{2.43}$$

โดยที่ M_{SCL} คือ พื้นที่หน่วยความจ าของตัวถอดรหัสหักล้างต่อเนื่อง

Q_{α} คือ ระดับการควอนไทซ์ของค่า LLR

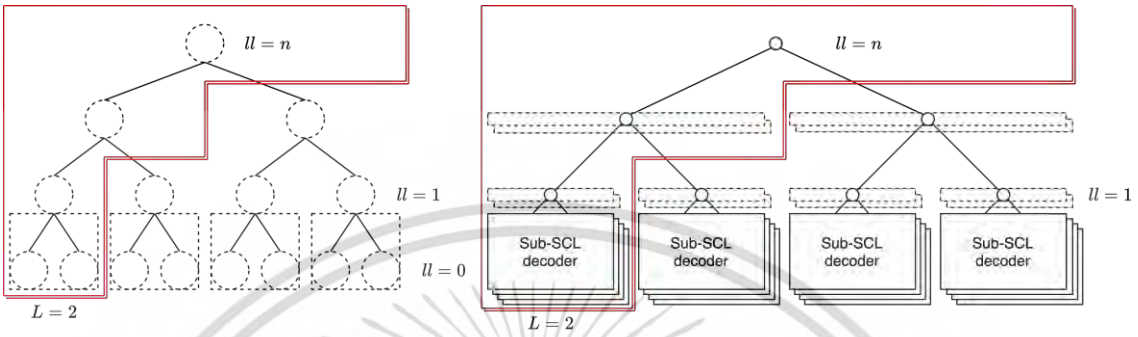
Q_{PM} คือ ระดับการควอนไทซ์ของค่าความน่าเชื่อถือเส้นทาง

ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนถูกนาเสนออยู่ 3 ชนิด ประกอบด้วย ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วน (partitioned successive cancellation list) หรือ PSCL ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนทั่วไป (generalized PSCL) หรือ GPSCL และตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนและแบ่งระดับ (layered PSCL) หรือ LPSCL [12] โดยหลักการแบ่งส่วนตัวถอดรหัสพื้นฐานจะมี 2 ขั้นตอนหลัก ประกอบด้วย การแตกโครงสร้างต้นไม้ตัวถอดรหัสเป็นส่วน ๆ (partitions) แทนด้วย P และการลดจานวนลิสการถอดรหัสในระดับชั้นส่วนบนของโครงสร้างตัวถอดรหัส

1) การแบ่งส่วนตัวถอดรหัสหักล้างต่อเนื่องแบบลิส

โครงสร้างต้นไม้ตัวถอดรหัสหักล้างต่อเนื่องสามารถแบ่งเป็นโครงสร้างย่อยได้ดังภาพที่ 2.27 โดยโครงสร้างย่อยส่วนล่างสามารถกาหนดให้เป็นตัวถอดรหัสหักล้างต่อเนื่องความยาวเท่ากับ N/P บิต จานวน P ส่วน และจะถอดรหัสหักล้างต่อเนื่องแบบลิสปกติ สาหรับการใช้งานหน่วยความจา โหนดใน

แต่ละระดับชั้นในโครงสร้างสามารถใช้งานหน่วยความจ ร่วมกันได้ เนื่องจากค่าการค านวณในโหนดจะถูกใช้งานเพียงครั้งเดียว

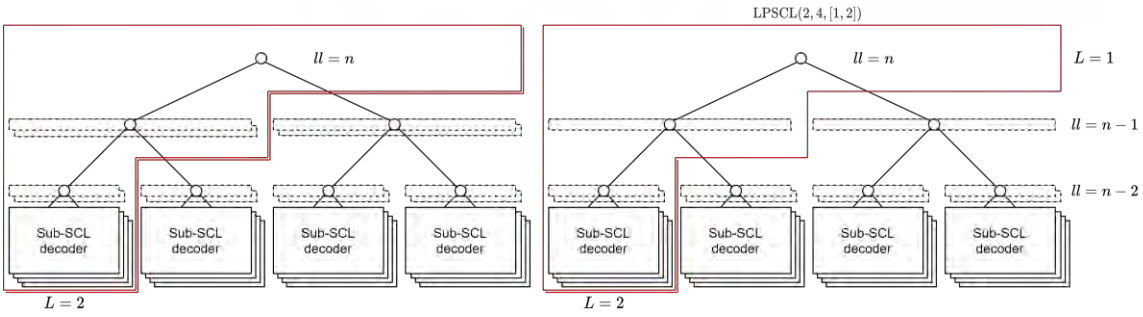


ภาพที่ 2.27 การแบ่งส่วนตัวถอดรหัสหักล้างต่อเนื่องแบบลิส

จากภาพที่ 2.27 กรอบสีแดงแสดงถึงขนาดพื้นที่หน่วยความจาที่ลดลง โดยค่าการคานวณการถอดรหัสของโครงสร้างด้านขวาสามารถเก็บไว้ในตาแหน่งเดียวกับโครงสร้างในทางซ้ายของแต่ละระดับชั้นการถอดรหัสได้ เนื่องจากค่าการถอดรหัสในโครงสร้างทางซ้ายจะไม่ได้ถูกใช้งานเมื่อทาการค านวณค่าการถอดรหัสในโครงสร้างฝั่งขวา การแบ่งส่วนตัวถอดรหัสขั้นตอนนี้จะยังคงสมรรถนะการแก้ไขความผิดพลาดไว้คงเดิม

2) การลดเส้นทางการถอดรหัสในโครงสร้างตัวถอดรหัสส่วนบน

สาหรับโครงสร้างส่วนบนจะถอดรหัสด้วยตัวหักล้างต่อเนื่อง ดังนั้นจึงมีการตัดเส้นทางการถอดรหัสจากโครงสร้างย่อยส่วนล่างที่มีขนาดลิสเท่ากับ L ลิส เพื่อให้สามารถถอดรหัสในโครงสร้างส่วนบนที่มีขนาดลิส $L=1$ ได้ต่อเนื่อง โดยการตัดเส้นทางสามารถตัดได้โดยใช้ค่าความน่าเชื่อถือเส้นทางดังสมการที่ 2.17 หรือใช้รหัส CRC ในการช่วยตัดเส้นทาง สาหรับการใช้งานหน่วยความจ โหนด การลดจานวนเส้นทางถอดรหัสที่โครงสร้างส่วนบน จะสามารถลดจานวนหน่วยความจาสาหรับการเก็บค่าการค านวณในโหนดที่โครงสร้างส่วนบน ดังภาพที่ 2.28



ภาพที่ 2.28 การลดเส้นทางการถอดรหัสในโครงสร้างตัวถอดรหัสส่วนบน

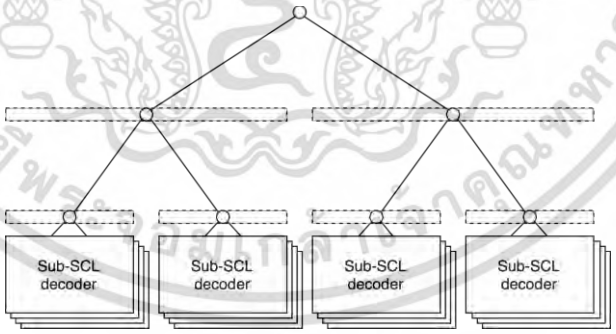
จากภาพที่ 2.28 จานวนกรอบสีแดงที่ลดลงในตัวถอดรหัสระดับบนหมายถึงจานวนเส้นทางการถอดรหัสที่ถูกตัดออก ดังภาพ ตัวถอดรหัสระดับชั้นที่ $ll = n-2$ จะมีเส้นทางการถอดรหัสจานวน $L = 2$ และถูกตัดเส้นทางการถอดรหัสออกที่ระดับชั้น $ll = n-1$ เหลือเส้นทางการถอดรหัสเพียง $L = 1$ ซึ่งในกรณีนี้ ต าแหน่งขสบิตถอดรหัส $\hat{u}_i$ ที่จะท าการตัดเส้นทางการถอดรหัสออกจะเป็นตาแหน่งที่ $i = N/2^{n-ll}$ ซึ่งจะเท่ากับ $i = N/2$

ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนที่เคยนาเสนอชนิดต่าง ๆ จะมีเงื่อนไขการลดเส้นทางการถอดรหัสในโครงสร้างตัวถอดรหัสส่วนบนแตกต่างไปดังนี้

2.8.2 PSCL

หลักการแบ่งส่วนตัวถอดรหัสของตัวถอดรหัส PSCL แทนด้วย $\mathrm{PSCL}(L,P)$ โครงสร้างย่อยส่วนล่างจะถอดรหัสด้วยการถอดรหัสหักล้างต่อเนื่องแบบลิสที่มีขนาดลิสเท่ากับ L ลิส แบ่งออกเป็น P ส่วน แต่ละส่วนมีความยาวเท่ากับ N/P บิต และโครงสร้างส่วนบนสามารถส่งผ่านคารหัสได้เพียง 1 เส้นทาง แสดงดังภาพที่ 2.29 ตัวถอดรหัส PSCL สามารถค านวณการใช้พื้นที่หน่วยความจาได้ดังสมการนี้

$$M_{PSCL} = \left(\sum_{k=0}^{\log_2 P} \frac{N}{2^k} + \left(\frac{N}{P} - 1 \right) L \right) Q_\alpha + LQ_{PM} + \sum_{k=1}^{\log_2 P} \frac{N}{2^k} + \left(\frac{2N}{P} - 1 \right) L \qquad (2.44)$$



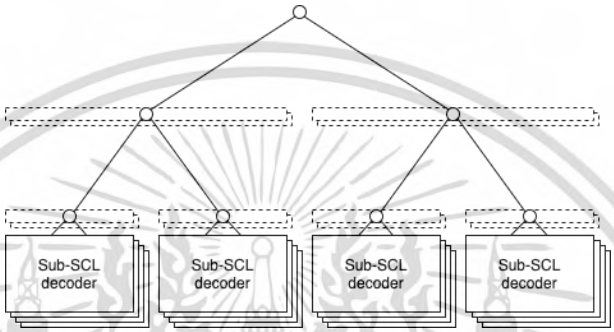
ภาพที่ 2.29 ตัวถอดรหัส $\mathrm{PSCL}(4,4)$

2.8.3 GPSCL

หลักการแบ่งส่วนตัวถอดรหัสของตัวถอดรหัส GPSCL แทนด้วย $\mathrm{GPSCL}(L,P,S)$ โครงสร้างย่อยส่วนล่างจะถอดรหัสด้วยการถอดรหัสหักล้างต่อเนื่องแบบลิสที่มีขนาดลิสเท่ากับ L ลิส แบ่งออกเป็น P ส่วน แต่ละส่วนมีความยาวเท่ากับ N/P บิต และโครงสร้างส่วนบนสามารถส่งผ่านคา

รหัสได้เพียง S เส้นทาง โดยที่ $S \le L$ แสดงดังภาพที่ 2.30 โดยที่ตัวถอดรหัส $\mathrm{GPSCL}(L,P,1)$ จะเทียบเท่ากับตัวถอดรหัส $\mathrm{PSCL}(L,P)$ ตัวถอดรหัส GPSCL สามารถคานวณการใช้พื้นที่หน่วยความจาได้ดังสมการนี้

$$M_{GPSCL} = \left(N + S\sum_{k=0}^{\log_2 P} \frac{N}{2^k} + \left(\frac{N}{P} - 1\right)L \right) Q_\alpha + LQ_{PM} + S\sum_{k=1}^{\log_2 P} \frac{N}{2^k} + \left(\frac{2N}{P} - 1\right)L \quad (2.45)$$

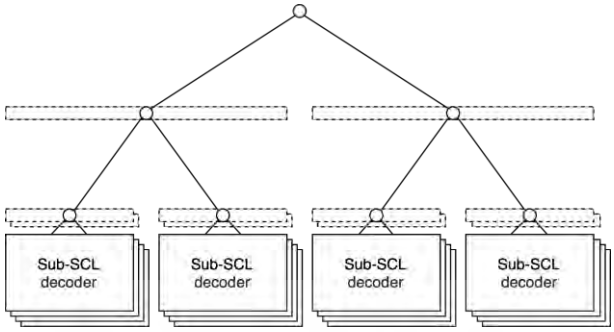


ภาพที่ 2.30 ตัวถอดรหัส $\mathrm{GPSCL}(4,4,2)$

2.8.4 LPSCL

หลักการแบ่งส่วนตัวถอดรหัสของตัวถอดรหัส LPSCL แทนด้วย $\mathrm{LPSCL}(L,P,s)$ โครงสร้างย่อยส่วนล่างจะถอดรหัสด้วยการถอดรหัสหักล้างต่อเนื่องแบบลิสที่มีขนาดลิสเท่ากับ L ลิส แบ่งออกเป็น P ส่วน แต่ละส่วนมีความยาวเท่ากับ N/P บิต และโครงสร้างส่วนบนสามารถส่งผ่านคารหัสได้เพียง s เส้นทาง โดยที่ $s \in \{n-\log_2 P, n-\log_2 P+1, \ldots, n-1\}$ และ $|s| = \log_2 P$ โดยที่ตัวถอดรหัส $\mathrm{LPSCL}(L,P,\{2,2,\ldots 2\})$ จะเทียบเท่ากับตัวถอดรหัส $\mathrm{GPSCL}(L,P,2)$ และตัวถอดรหัส $\mathrm{LPSCL}(L,P,\{1,1,\ldots 1\})$ จะเทียบเท่ากับตัวถอดรหัส $\mathrm{GPSCL}(L,P,1)$ และ $\mathrm{PSCL}(L,P)$ แสดงดังภาพที่ 2.31 ตัวถอดรหัส LPSCL สามารถค านวณการใช้พื้นที่หน่วยความจ าได้ดังสมการนี้

$$M_{LPSCL} = \left(N + \sum_{k=0}^{\log_2 P} s_k \frac{N}{2^k} + \left(\frac{N}{P} - 1\right)L \right) Q_\alpha + LQ_{PM} + \sum_{k=1}^{\log_2 P} s_k \frac{N}{2^k} + \left(\frac{2N}{P} - 1\right)L \quad (2.46)$$



ภาพที่ 2.31 ตัวถอดรหัส $\mathrm{LPSCL}\left(4,4,\{1,2\}\right)$

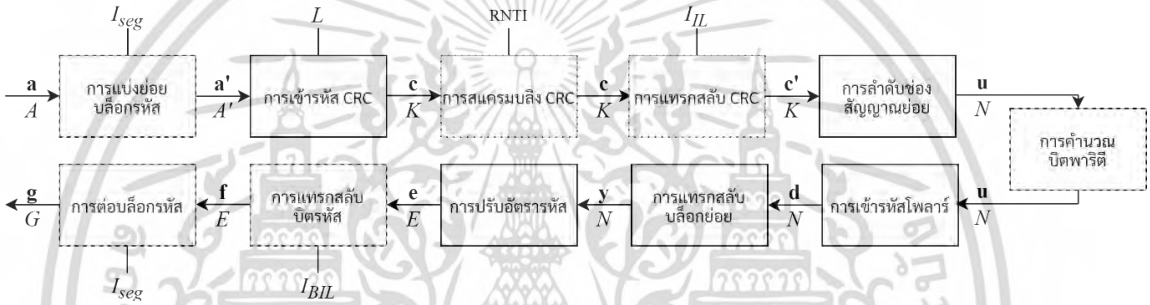
บทที่ 3
รหัสโพลาร์ในมาตรฐาน 5G

บทที่ 3 รหัสโพลาร์ในมาตรฐาน 5G จะกล่าวถึงรายละเอียดของรหัสโพลาร์ที่ถูกน ไปใช้งานในมาตรฐาน 5G ที่ถูกกาหนดโดยองค์กรความร่วมมือรุ่นที่ 3 (3rd generation partnership project) หรือ 3GPP ซึ่งมาตรฐานดังกล่าวได้ถูกนามาใช้งานในโครงข่ายการสื่อสารไร้สายในปัจจุบัน โดยรายละเอียดของรหัสโพลาร์ในมาตรฐาน 5G สามารถจาแนกเป็น 11 กระบวนการย่อย โดยวิทยานิพนธ์ฉบับนี้จะมีการใช้งานรหัสโพลาร์ตามมาตรฐาน 5G ร่วมกับสิ่งที่น าเสนอในวิทยานิพนธ์

3.1 รหัสโพลาร์ตามมาตรฐาน 5G

รหัสโพลาร์เป็นรหัสช่องสัญญาณที่สามารถพิสูจน์ได้ว่ามีสมรรถนะเข้าใกล้ขีดจากัดแชนนอน รวมถึงมีโครงสร้างการเข้ารหัสและถอดรหัสที่เรียบง่าย จึงเป็นรหัสช่องสัญญาณที่น่าสนใจและถูกเลือกใช้งานในมาตรฐาน 5G สาหรับการสื่อสารในช่องสัญญาณควบคุม สาหรับมาตรฐาน 5G เป็นเทคโนโลยีการสื่อสารไร้สายยุคที่ 5 ที่มีขีดความสามารถสูง สหภาพโทรคมนาคมระหว่างประเทศ (international telecommunication union) หรือ ITU ได้กาหนดรูปแบบการใช้งานของเทคโนโลยีมาตรฐาน 5G เป็น 3 รูปแบบ ได้แก่ enhanced mobile broadband หรือ eMBB สาหรับการใช้งานที่เน้นประมาณข้อมูลสูงและความเร็วสูง ultra-reliable and low latency communications หรือ URLLC สาหรับการใช้งานที่มีความน่าเชื่อถือสูง ความหน่วงต่า และเวลาสูญเสีย (downtime) ต าและ massive machine type communications หรือ mMTC สา หรับการใช้งานที่เน้นการเชื่อมต่ออุปกรณ์จ านวนมากในบริเวณพื้นที่จากัด ซึ่ง ITU ยังได้ตั้งเป้าหมายขีดความสามารถในการสื่อสารตามมาตรฐาน 5G เช่น ความเร็วสูงสุดที่ 20 Gbps ความหน่วงสูงสุดที่ 1 us หรือจานวนอุปกรณ์ต่อขนาดพื้นที่ โดยหากมาตรฐานการสื่อสารไร้สายสามารถบรรลุเป้าหมายการสื่อสารไร้สายได้ จะถือว่าเป็นมาตรฐาน 5G จากนั้นจึงมีโครงการความร่วมมือรุ่นที่ 3 (3rd generation partnership project) หรือ 3GPP เป็นหน่วยงานความร่วมมือในการกาหนดรายละเอียดมาตรฐานทางเทคนิค ได้จัดตั้งการประชุมเพื่อออกรายละเอียดมาตรฐาน ให้สอดคล้องกับเป้าหมายขีดความสามารถที่ ITU กาหนดไว้ ซึ่งได้มาตรฐานที่ชื่อว่า 5G new radio หรือมาตรฐาน 5G แบบย่อ และหนึ่งในรายละเอียดของมาตรฐาน 5G คือการเข้ารหัสช่องสัญญาณสาหรับมาตรฐาน 5G โดยผลลัพธ์จากการประชุมทั้งสิ้น 14 ครั้ง ได้บทสรุปว่ามีการน ารหัสช่องสัญญาณมาใช้งาน 2 ชนิดหลัก คือ รหัสแอลดีพีซี สาหรับช่องสัญญาณข้อมูล (data channel) เนื่องจากสามารถส่งข้อมูลปริมาณมากต่อพื้นที่วงจรถอดรหัส (throughput) ที่สูง อีกทั้งมีความซับซ้อนของวงจรถอดรหัสต่าในกรณีความยาวคารหัสยาว เนื่องจากสามารถประมวลผลแบบขนานได้ และรหัสโพลาร์ สาหรับช่องสัญญาณ

ควบคุม (control channel) เนื่องจากให้สมรรถนะการแก้ไขความผิดพลาดที่ดีในกรณีความยาวคารหัสสั้น ซึ่งเป็นลักษณะของข้อมูลในช่องสัญญาณควบคุมที่มีขนาดเล็ก นอกจากนี้ยังมีการนารหัสบล็อกเชิงเส้นอื่น ๆ มาใช้งานในกรณีเฉพาะ [13] รายละเอียดของรหัสช่องสัญญาณในมาตรฐานจะกาหนดไว้เพียงการเข้ารหัสเท่านั้น ซึ่งจะเพิ่มความยืดหยุ่นในการเลือกใช้งานตัวถอดรหัส เพื่อให้สอดคล้องกับการใช้งานรูปแบบต่าง ๆ เช่น สาหรับรหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิส สามารถเลือกใช้ตัวถอดรหัสที่มีขนาดลิส L ต่าเพื่อลดความซับซ้อนและความหน่วงในการถอดรหัส สาหรับการใช้งานรูปแบบ URLLC ได้ โดยในหัวข้อถัดไปจะให้รายละเอียดของการเข้ารหัสโพลาร์ที่ใช้งานในมาตรฐาน 5G ส าหรับช่องสัญญาณควบคุม



ภาพที่ 3.1 รหัสโพลาร์ตามมาตรฐาน 5G สามารถแบ่งเป็นกระบวนการทั้งหมด 11 ขั้นตอนย่อย ช่องสัญญาณ UCI ใช้งานเฉพาะกระบวนการในกล่องเส้นประขีดจะถูกใช้งานเฉพาะ และกล่องเส้นประจุดสาหรับช่องสัญญาณ BCH และ DCI และกระบวนการในกล่องเส้นหนาจะถูกใช้งานในทุกช่องสัญญาณ ตัวอักษรหนาคือเวกเตอร์ของข้อมูลระหว่างกระบวนการและตัวอักษรเอียงคือความยาวของเวกเตอร์

กระบวนการเข้ารหัสสาหรับช่องสัญญาณอัปลิงก์ (uplink) มีกระบวนการเข้ารหัสที่เพิ่มเติมมากกว่าการเข้ารหัสสาหรับช่องสัญญาณดาวน์ลิงก์ (downlink) จะประกอบด้วย การแบ่งย่อยบล็อกรหัส การคานวณพาริตี การอินเทอร์ลีฟบิตรหัส และการต่อบล็อกรหัส ขณะที่ช่องสัญญาณดาวน์ลิงก์จะมีกระบวนการเข้ารหัสการสแครมบลิง CRC และการอินเทอร์ลีฟ CRC ที่เพิ่มเติมมากกว่าการเข้ารหัสสาหรับช่องสัญญาณอัปลิงก์ กระบวนการเข้ารหัสแสดงได้ดังภาพที่ 3.1 ประเภทช่องสัญญาณที่ใช้งานรหัสโพลาร์ตามมาตรฐาน 5G สามารถสรุปได้โดยละเอียดดังตารางที่ 3.1 และค่าพารามิเตอร์ต่าง ๆ จะเป็นตัวกาหนดรูปแบบการทางานของการเข้ารหัสโพลาร์ พารามิเตอร์สาหรับการเข้ารหัสโพลาร์ถูกแสดงดังตารางที่ 3.2 โดยมีรายละเอียดดังต่อไปนี้

1) ความยาวเพย์โหลดแทนด้วย A มีความยาวบิตข้อมูลสูงสุดคือ $A \leq 1706$

2) ความยาวบิต CRC แทนด้วย $|r|$ ได้ก าหนดพหุนาม CRC ส าหรับการเข้ารหัสไว้ดังนี้

$$g_{24A}(x) = x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$$

$$g_{24B}(x) = x^{24} + x^{23} + x^6 + x^5 + x + 1$$

$$g_{24C}(x) = x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + x^{15} + x^{13} + x^{12} + x^8 + x^4 + x^2 + x + 1$$

$$g_{16}(x) = x^{16} + x^{12} + x^5 + 1$$

$$g_{11}(x) = x^{11} + x^{10} + x^9 + x^5 + 1$$

$$g_6(x) = x^6 + x^5 + 1$$

โดยพหุนาม g_6 ความยาว $|r| = 6$ บิตและพหุนาม g_{11} ความยาว $|r| = 11$ บิตจะถูกใช้สาหรับช่องสัญญาณ UCI บิตและส าหรับช่องสัญญาณ DCI จะใช้งานพหุนาม g_{24C} ที่มีความยาว $|r| = 24$ บิต

3) ความยาวบิตข้อมูลส าหรับการเข้ารหัสโพลาร์มีความยาวเท่ากับ K บิต โดยจะรวมถึงเพย์โหลดขาเข้า บิต CRC และบิตพาริตี โดยเงื่อนไขที่ $K < N$ บิต

4) ความยาวค ารหัสแม่แทนด้วย $N = 2^n$ บิต โดย n สามารถค านวณโดยสมการที่ x

$$n = \max(\min(n_1, n_2, n_{\max}), n_{\min}) \tag{3.1}$$

โดยที่ $n_{\min}$ และ $n_{\max}$ สามารถสื่อได้ว่าเป็นขอบเขตสาหรับการกาหนดความยาวต่าสุดและสูงสุดตามลาดับ โดยที่ช่องสัญญาณ DCI และ BCH มีค่า $n_{\min} = 5$ และ $n_{\max} = 9$ ขณะที่ช่องสัญญาณ UCI จะมีค่า $n_{\min} = 5$ และ $n_{\max} = 10$ ส าหรับ n_1 และ n_2 ค านวณได้ดังสมการที่ x และ x

$$n_1 = \begin{cases} \lfloor \log_2 E \rfloor & \text{หาก } E \le (9/8)\cdot 2^{(\lfloor \log_2 E \rfloor)} \text{ และ } K/E < 9/16 \\ \lceil \log_2 E \rceil & \text{อื่น ๆ} \end{cases} \tag{3.2}$$

$$n_2 = \lceil \log_2 (K/R_{\min}) \rceil \qquad \text{โดยที่ } R_{\min} = 1/8 \tag{3.3}$$

5) ค ารหัสหลังด าเนินการปรับอัตรารหัสมีความยาวเท่ากับ E บิต เพื่อให้สามารถเลือกความยาว E ที่ต้องการ โดยมีความยาวสูงสุด $E \le 8192$ บิต หากความยาวคารหัสมีค่าเท่ากับ $E < N$ บิต หรือไม่เกินความยาวคารหัสแม่ คารหัสแม่จะด าเนินการช็อตเทน (shortening) หรือดาเนินการพังก์เชอร์ (puncturing) ซึ่งจะร่วมพิจารณากับเงื่อนไขอื่น แต่หากความยาวคารหัสมีค่าเท่ากับ $E > N$ จะทาให้คารหัสแม่บางบิตจะถูกส่งซ้ า

6) อัตรารหัสแทนด้วย $R = A/E$ คืออัตราส่วนระหว่างความยาวเพย์โหลดขาเข้าต่อความยาวค ารหัส

7) ความยาว U คือความยาวของบิตที่ถูกออกจากกระบวนการปรับอัตรารหัสในกรณีการช็อตเทนและการพังก์เชอร์

8) ความยาว T เป็นความยาวที่ใช้ในการกาหนดบิตแซ่แข็งก่อนการปรับอัตรารหัสในรูปแบบการพังก์เชอร์ โดยจะกาหนดตาแหน่งบิตแรกถึงตาแหน่งที่ U เป็นบิตแซ่แข็ง ซึ่งสุดท้ายการพังก์เชอร์จะตัดบิตออกเป็นความยาว $|Q_I|$ บิต ตามที่กล่าวข้างต้น

9) ความยาวบิตข้อมูลแทนด้วย $|Q_F|$ ความยาวบิตแซ่แข็งแทนด้วย n_{PC} และบิตพาริตีมีความยาวเท่ากับ n_{PC} บิต

ตารางที่ 3.1 การเข้ารหัสช่องสัญญาณของแต่ละประเภทช่องสัญญาณ

ช่องสัญญาณข้อมูล (data channel)	**การเข้ารหัสช่องสัญญาณ**
uplink shared channel (UL-SCH)	low-density parity-check (LDPC) code
downlink shared channels (DL-SCH)	
paging channel (PCH)	
broadcast channel (BCH)	polar code
ช่องสัญญาณควบคุม (control channel)	**การเข้ารหัสช่องสัญญาณ**
downlink control information (DCI)	polar code
uplink control information (UCI)	
	block code

ตารางที่ 3.2 พารามิเตอร์และขอบเขตของรหัสโพลาร์ในแต่ละช่องสัญญาณตามมาตรฐาน 5G

		UCI				DCI	BCH
		$A \geq 20$		$12 \leq A \leq 19$			
		$(A \geq 1013) \vee (A \geq 360 \wedge G \geq 1088)$	$(A < 360) \vee (A < 1013 \wedge G < 1088)$	$E - A \leq 175$	$E - A > 175$		
เลขชี้กำลังสูงสุดความยาวรหัสแม่	$n_{\max}$	10				9	
ตัวบ่งชี้การอินเทอร์ลีฟ CRC	I_{IL}	0				1	
ตัวบ่งชี้การอินเทอร์ลีฟบิตรหัส	I_{BIL}	1				0	
ตัวบ่งชี้การแบ่งย่อยบล็อกรหัส	I_{seg}	1	0			0	
ความยาวเพย์โหลดขาเข้าสูงสุด	$A_{\max}$	1706				140	32
ความยาวเพย์โหลดขาเข้าต่ำสุด	$A_{\min}$	12				1	32

ความยาวบิต CRC	$\|r\|$	11	6		24
ความยาวบิตพาริตีตรวจสอบ	n_{PC}	0	3		0
ความยาวบิตพาริตีตรวจสอบเลือกจากน้ำหนักแถวที่ต่ำสุด	n_{PC}^{wm}	0	0	1	0

3.1.1 การแบ่งย่อยบล็อกรหัส

การแบ่งย่อยบล็อกรหัสเป็นการแบ่งย่อยข้อมูลเพย์โหลด a ออกเป็น 2 ส่วนและทาการเข้ารหัสแยกกัน ใช้งานในเฉพาะช่องสัญญาณ UCI เพื่อไม่ให้มีความซับซ้อนมากเกินไปในการเข้ารหัส (เกิดจากความยาวข้อมูล) ในช่องสัญญาณ UCI จะมีการส่งข้อมูลขนาดใหญ่ เช่น คุณภาพช่องสัญญาณไปยัง radio access network หรือ RAN จากอุปกรณ์ผู้ใช้งาน (user equipment: UE)

กรณีช่องสัญญาณ UCI และมีเงื่อนไขว่า $(A \geq 360 \wedge E \geq 1088) \vee A \geq 1013$ กระบวนการนี้จะดำเนินการและตัวบ่งชี้การแบ่งย่อยบล็อกรหัสจะถูกตั้งค่าให้ $I_{seg} = 1$ เวกเตอร์ a ความยาว A จะถูกแบ่งย่อยเป็น 2 เวกเตอร์ a' ความยาว $A' = A/2$ หากความยาว A เป็นจานวนคี่ a' ส่วนแรกจะแบ่ง $\lfloor A/2 \rfloor$ บิตแรกจาก a และเติมบิต 0 ไว้ด้านหน้า

สาหรับช่องสัญญาณ BCH และ DCI กระบวนการนี้จะไม่ดาเนินการและตั้งค่าให้ $I_{seg} = 0$ เวกเตอร์ a จะผ่านไปยังกระบวนการเข้ารหัส CRC ถัดไป

3.1.2 การต่อท้าย CRC

ภาพที่ 3.2 โครงสร้างการเข้ารหัส CRC

การเข้ารหัส CRC จะทาการเข้ารหัสรูปแบบ systematic ภายใต้ $GF(2)$ โดยที่บิต CRC ความยาว $|r|$ บิต จะถูกต่อท้ายจากเวกเตอร์ a ความยาว A จากอินพุต (หรือ a' ความยาว A' ในกรณีที่ $I_{seg} = 1$) ดังภาพที่ 3.2 โดยจะได้เวกเตอร์ c ที่มีความยาว $K = A + |r|$ (หรือ c' ความยาว $K = A' + |r|$ ในกรณีที่ $I_{seg} = 1$)

กรณีช่องสัญญาณ UCI ในเงื่อนไขที่เวกเตอร์ a มีความยาว $12 \le A \le 19$ จะใช้งานพหุนาม g_6 ในการเข้ารหัส CRC ความยาว $|r| = 6$ และจะเข้ารหัส CRC โดยใช้พหุนาม g_{11} ในการคานวณบิต CRC ความยาว $|r| = 11$ หากมีเงื่อนไข $A \ge 20$ จะได้เวกเตอร์ c เป็นผลลัพธ์

กรณีช่องสัญญาณ BCH การเข้ารหัสจะใช้งานพหุนาม g_{24C} ในการคานวณบิต CRC ความยาว $|r| = 24$ จากนั้นกระบวนการจะทาการสแครมบลิงเวกเตอร์ a ความยาว $A = A_{\min} = A_{\max} = 32$ (ความยาวเดียวตามมาตรฐาน) ด้วยเวกเตอร์ขนาดเท่ากันก่อนหน้ากระบวนการเข้ารหัสช่องสัญญาณ โดยการท าอ็อกซ์คลูซีฟออร์ จากนั้นจะด าเนินการเข้ารหัส CRC ได้ผลลัพธ์เป็นเวกเตอร์ c ความยาว $K = 56$ บิต

กรณีช่องสัญญาณ DCI พหุนาม g_{24C} จะถูกในการเข้ารหัส CRC โดยได้ผลลัพธ์บิต CRC ความยาว $|r| = 24$ การเข้ารหัส CRC สาหรับช่องสัญญาณ DCI จะแตกต่างจากการเข้ารหัส CRC ทั่วไป โดยตัวตั้งในการคานวณ CRC จะนาเวกเตอร์ 1 ขนาดเท่ากับความยาวบิต CRC ไว้ด้านหน้าและตามด้วยเวกเตอร์ a ความยาว A (ซึ่งต่างจากวิธีทั่วไปที่จะนาเวกเตอร์ a ไว้ด้านหน้าและตามหลังด้วยเวกเตอร์ 0 ขนาดเท่ากับความยาวบิต CRC ไว้ด้านหลัง) สุดท้ายจะน าบิตCRC ที่ได้จากการค านวณต่อท้ายเวกเตอร์ a ตามปกติ เวกเตอร์ a สามารถมีความยาวได้ $A_{\min} = 1$ ถึง $A_{\max} = 140$ จะได้ผลลัพธ์เป็นเวกเตอร์ c

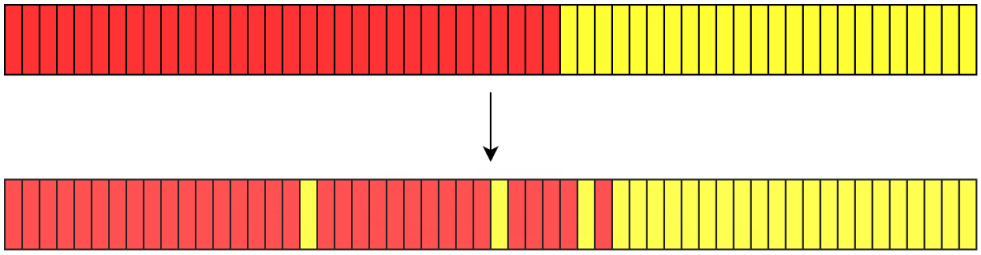
3.1.3 การสแครมบลิง CRC

เวกเตอร์ c จะถูกสแครมบลิง เพื่อใช้ในการทา (blind detection หรือ blind decoding) ของการส่งข้อมูลระหว่าง RAN และอุปกรณ์ผู้ใช้งานในการสื่อสารผ่านช่องสัญญาณ DCI ในขณะการสื่อสารอุปกรณ์ การระบุตัวตนของอุปกรณ์ผู้ใช้งานจากฝั่ง RAN จะไม่มีการใส่ข้อมูลส่วนหัว (header) แต่จะทาการสแครมบลิงรหัสเฉพาะตัวของอุปกรณ์ผู้ใช้งานที่ต้องการสื่อสาร จากนั้นอุปกรณ์ RAN จะส่งข้อมูลในลักษณะออกอากาศ (broadcast) ให้อุปกรณ์ผู้ใช้งานโดยรอบ จากนั้นอุปกรณ์ผู้ใช้งานจะทาการถอดรหัสของข้อมูล blind detection การสแครมบลิงจะทาให้อุปกรณ์ผู้ใช้งานมีโอกาสถอดรหัสผิดสูงต่อข้อมูลที่ฝังรหัสเฉพาะตัวไม่ตรงกัน และข้อมูลที่ฝังรหัสตรงกับอุปกรณ์ผู้ใช้งานสามารถถอดรหัสได้ถูกต้องและสามารถรับข้อมูลได้ ซึ่งรหัสเฉพาะดังกล่าวจะถูกกาหนดโดย radio network temporary identifier (RNTI)

กรณีช่องสัญญาณ DCI ที่มีการเข้ารหัส CRC ความยาว $|r| = 24$ บิต ชุดบิต c_{A+8}^{A+L-1} (บิต CRC 16 บิตท้ายสุด) จะถูกสแครมบลิงกับบิต RNTI ที่ความยาว 16 บิตเท่ากัน บิต RNTI จะถูกเลือกตามเงื่อนไขช่องสัญญาณและหน้าที่ของข้อมูลตามมาตรฐาน 5G

สาหรับช่องสัญญาณ BCH และ UCI กระบวนการนี้จะไม่ทางานเวกเตอร์ c จะผ่านไปยังกระบวนการอินเทอร์ลีฟ CRC ถัดไป

3.1.4 การอินเทอร์ลีฟ CRC



ภาพที่ 3.3 ตัวอย่างลาดับการอินเทอร์ลีฟ CRC สาหรับช่องสัญญาณ BCH ที่ $A=32$ $|r|=24$ และ $K=56$ โดยสีแดงและสีเหลืองคือบิตข้อมูลและบิต CRC ตามล าดับ

เวกเตอร์ c จากกระบวนก่อนหน้าจะถูกอินเทอร์ลีฟตามลำดับดังตารางที่ 3.3 ลาดับการอินเทอร์ลีฟ $\Pi_{IL}^{\max}(i)$ สาหรับการอินเทอร์ลีฟ CRC (เรียงค่า i จากซ้ายไปขวา บนลงล่าง) เพื่อให้สามารถดำเนินการเทคนิคการเลิกก่อน ในการถอดรหัส เพื่อลดความซับซ้อนในการถอดรหัสจากการถอดรหัสผิดพลาด โดยจะหยุดการถอดรหัสระหว่างการถอดรหัสหากพบความผิดพลาด การอินเทอร์ลีฟ CRC สำหรับช่องสัญญาณ BCH ได้แสดงดังภาพที่ 3.3

กรณีช่องสัญญาณ BCH และ DCI จะทำการอินเทอร์ลีฟ CRC และตั้งค่าตัวบ่งชี้ $I_{IL}=1$ เนื่องจากเวกเตอร์ a สามารถมีหลายความยาวได้ ดังนั้นเวกเตอร์ c ไม่จำเป็นต้องมีความยาวเท่ากับลำดับบิตอินเทอร์ลีฟสูงสุด $K_{IL}^{\max}=164$ บิต วิธีการอินเทอร์ลีฟสามารถนำเวกเตอร์ c ต่อท้ายด้วยบิตว่าง (null) จนมีความยาวเท่ากับ $K_{IL}^{\max}$ จากนั้นทำการอินเทอร์ลีฟตามลำดับการอินเทอร์ลีฟดังตารางที่ 3.3 และนำบิตว่างออกจากเวกเตอร์หลังจากการอินเทอร์ลีฟ จะได้ผลลัพธ์เป็นเวกเตอร์ c'

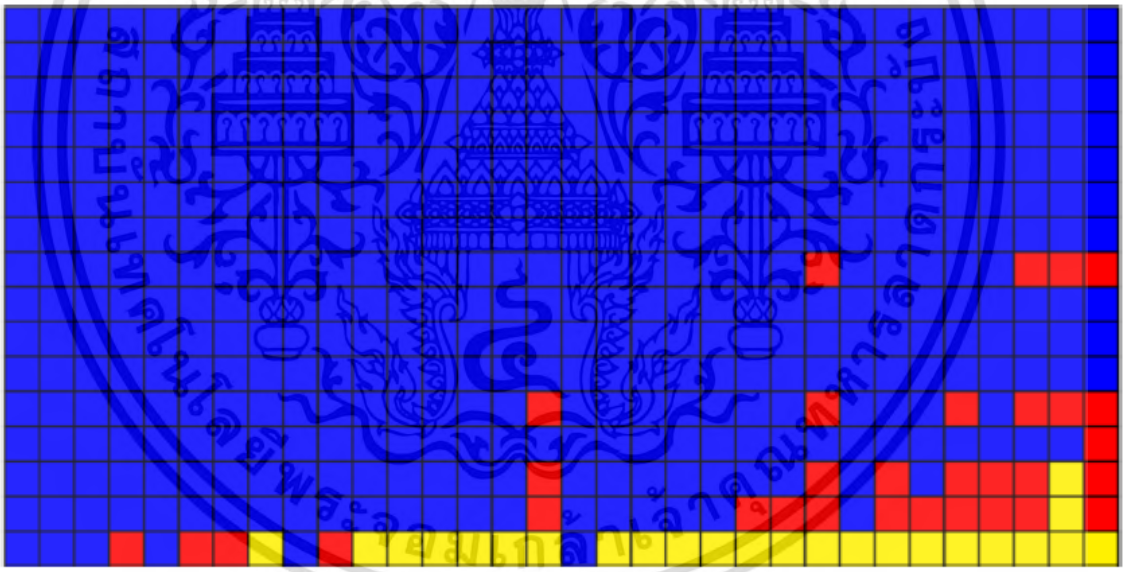
สำหรับช่องสัญญาณ UCI จะไม่มีการอินเทอร์ลีฟ CRC และตั้งค่าตัวบ่งชี้ $I_{IL}=0$ เวกเตอร์ c จะผ่านไปยังกระบวนการล าดับช่องสัญญาณย่อยถัดไป

ตารางที่ 3.3 ลาดับการอินเทอร์ลีฟ $\Pi_{IL}^{\max}(i)$ สาหรับการอินเทอร์ลีฟ CRC (เรียงค่า i จากซ้ายไปขวา บนลงล่าง)

0	2	4	7	9	14	19	20	24	25	26	28	31
34	42	45	49	50	51	53	54	56	58	59	61	62
65	66	67	69	70	71	72	76	77	81	82	83	87
88	89	91	93	95	98	101	104	106	108	110	111	113

115	118	119	120	122	123	126	127	129	132	134	138	139
140	1	3	5	8	10	15	21	27	29	32	35	43
46	52	55	57	60	63	68	73	78	84	90	92	94
96	99	102	105	107	109	112	114	116	121	124	128	130
133	135	141	6	11	16	22	30	33	36	44	47	64
74	79	85	97	100	103	117	125	131	136	142	12	17
23	37	48	75	80	86	137	143	13	18	38	144	39
145	40	146	41	147	148	149	150	151	152	153	154	155
156	157	158	159	160	161	162	163					

3.1.5 การลำดับช่องสัญญาณย่อย



ภาพที่ 3.4 ตัวอย่างการลาดับช่องสัญญาณย่อยสาหรับช่องสัญญาณ BCH ที่เวกเตอร์ c' ความยาว $K = 56$ บิต และเวกเตอร์ u ความยาว $N = 2^n = 512$ บิต หรือ $n = n_{\max} = 9$ สีน้าเงินสีแดงและสีเหลืองคือบิตแซ่แข็ง บิตข้อมูลและบิต CRC ตามล าดับ

กระบวนการนี้จะทำการสร้างรหัสโพลาร์ เพื่อเรียงบิตข้อมูล บิต CRC และบิตแซ่แข็งตามลำดับความน่าเชื่อถือช่องสัญญาณย่อยตาม [ดังตารางที่ 5.3.1.2-1] ได้ผลลัพธ์เป็นเวกเตอร์ u ความ

ยาว N โดยกำหนดตำแหน่งของบิตแซ่แข็งด้วย $\mathcal{A}^F$ และบิตข้อมูลด้วย $\mathcal{A}^I$ บิตข้อมูลหรือเวกเตอร์ c (หรือ c') จากกระบวนการก่อนจะถูกวางไว้สำหรับตำแหน่งบิตข้อมูล ส่วนตำแหน่งบิตแซ่แข็งจะถูกกำหนดค่าบิตเท่ากับ 0 การเลือกความยาว N จะมีเกณฑ์การเลือกตามสมการที่ 3.*1* 3.*2* และ 3.*3* โดยความยาว $N = 2^n$ สุดท้ายจะได้จากการเลือกค่า n สุดท้าย การเลือกตำแหน่งของบิตแซ่แข็งจะสอดคล้องกับเงื่อนการปรับอัตรารหัส โดยการปรับอัตรารหัสเป็นการปรับขนาดคำรหัสก่อนส่งผ่านช่องสัญญาณให้มีความยาวเท่ากับ E บิต ภาพที่ 3.4 คือตัวอย่างการลำดับช้องสัญญาณย่อยของช่องสัญญาณ BCH

1) การเลือกตำแหน่งบิตแซ่แข็งส าหรับทุกช่องสัญญาณ สรุปขั้นตอนได้ 2 ขั้นตอนดังนี้

1.1) เลือกตาแหน่งบิตแซ่แข็งสาหรับการปรับอัตรารหัส หาก $K/E \le 7/16$ จะปรับอัตรารหัสด้วยการพังก์เจอร์ ซึ่งจะก าหนดบิตแซ่แข็งที่ T ต าแหน่งแรกในกรณีอื่นจะปรับอัตรารหัสด้วยการช็อตเทน ซึ่งจะก าหนดบิตแซ่แข็งที่ $U = N - E$ ต าแหน่งสุดท้าย T ค านวณได้ดังสมการที่ *3.4*

$$T = \begin{cases} \left\lceil \frac{3}{4}N - \frac{E}{2} \right\rceil - 1 & \text{หาก } E \ge \frac{3}{4}N \\ \left\lceil \frac{9}{16}N - \frac{E}{4} \right\rceil - 1 & \text{อื่น ๆ} \end{cases} \tag{3.4}$$

สาเหตุที่ใช้ความยาว T เพิ่มเติมจาก U เพื่อป้องกันไม่ให้บิตข้อมูลถูกพังก์เจอร์ไปในการปรับอัตรารหัส

1.2) หากจำนวนบิตแซ่แข็งสำหรับการปรับอัตรารหัสยังมีขนาดไม่เกินจำนวนบิตแซ่แข็งที่มีได้ จะทำการกำหนดตำแหน่งบิตแซ่แข็งเพิ่มเติมตามจำนวนที่เหลือและกำหนดตามลำดับความน่าเชื่อถือช่องสัญญาณตาม [ดังตารางที่ 5.3.1.2-1] ซึ่งสามารถสรุปขั้นตอนการเลือกตำแหน่งบิตแซ่แข็งตามลำดับความน่าเชื่อถือช่องสัญญาณได้ 2 ขั้นตอนดังนี้

1.2.1) เลือกลำดับช่องสัญญาณ $\mathcal{A}$ เรียงจากลำดับน้อยไปลำดับมากตามความยาวคำรหัสแม่ N ซึ่งจะได้ลำดับความน่าเชื่อถือ $W(\mathcal{A})$ ที่คู่กับลำดับช่องสัญญาณ $\mathcal{A}$

1.2.2) ตำแหน่งของบิตแซ่แข็งจะอยู่ในตำแหน่งของลำดับช่องสัญญาณที่คู่กับลำดับความน่าเชื่อถือที่ต่ำที่สุดตามจำนวนบิตแซ่แข็ง $\left|\mathcal{A}^F\right|$ ที่ออกแบบไว้

ตัวอย่างเช่น กรณี $N = 8$ ประกอบด้วยบิตแซ่แข็งและบิตข้อมูลเท่ากัน จะเลือกลำดับช่องสัญญาณมา 8 ลำดับที่ 0 1 2 4 3 5 6 7 (ตามคอลัมน์ลำดับช่องสัญญาณ) ซึ่งจะได้ลำดับความน่าเชื่อถือเป็น 0 1 2 3 7 8 11 24 (ตามคอลัมน์ลำดับความน่าเชื่อถือ) มาตามลำดับคู่กัน จะได้ตำแหน่งบิตแซ่แข็งที่ 0 1 2 4 เนื่องจากที่ลำดับช่องสัญญาณ 0 1 2 4 คู่กับลำดับความน่าเชื่อถือที่ต่ำที่สุด (0 1 2 3) และได้ตำแหน่งบิตข้อมูลที่ 3 5 6 7

กรณีที่ $N=16$ ประกอบด้วยบิตแซ่แข็งและบิตข้อมูลเท่ากัน จะเลือกลำดับช่องสัญญาณมา 16 ลำดับที่ 0 1 2 4 8 3 5 9 6 10 12 7 11 13 14 15 (ตามคอลัมน์ลำดับช่องสัญญาณ) ซึ่งจะได้ลำดับความน่าเชื่อถือเป็น 0 1 2 3 4 7 8 10 11 13 16 24 28 33 35 76 (ตามคอลัมน์ลำดับความน่าเชื่อถือ) มาตามลำดับคู่กัน จะได้ตำแหน่งบิตแซ่แข็งที่ 0 1 2 4 8 3 5 9 เนื่องจากที่ลำดับช่องสัญญาณ 0 1 2 4 8 3 5 9 คู่กับลำดับความน่าเชื่อถือที่ต่ำที่สุด (0 1 2 3 4 7 8 10) และได้ตำแหน่งบิตข้อมูลที่ 6 10 12 7 11 13 14 15

2) การเลือกจำนวนช่องสัญญาณย่อย

กรณีช่องสัญญาณ UCI ที่มีเงื่อนไข $12\le A\le 19$ จะมีการใช้งานบิตพาริตี ซึ่งต าแหน่งของบิตพาริตี $\mathcal{A}^{PC}$ จะถูกแทรกไปตาแหน่งจานวน $n_{PC}=3$ บิต หากการเข้ารหัสมีเงื่อนไข $E-A\le 175$ ตาแหน่งบิตพาริตีจะถูกเลือกจากตาแหน่งที่มีความน่าเชื่อถือต่าที่สุดทั้ง 3 บิต แต่หากรหัสมีเงื่อนไข $E-A>175$ ตาแหน่งบิตพาริตีจะถูกเลือกจากต ขแหน่งที่มีความน่าเชื่อถือต่าที่สุดเพียง 2 บิต โดยบิตที่เหลือจะถูกเลือกตาแหน่งที่มีน้าหนักแถวของเมทริกซ์ G_N ต่าที่สุด ซึ่งหากมีตาแหน่งดังกล่าวมากกว่าหนึ่งตาแหน่ง จะเลือกตาแหน่งดังกล่าวที่ความน่าเชื่อถือสูงที่สุดเท่านั้น ทาให้จานวนของบิตแซ่แข็งจะลดลงเหลือ $\left|\mathcal{A}^{F}\right|=N-\left(K+3\right)$

สาหรับช่องสัญญาณ UCI ที่เงื่อนไข $A\ge 20$ ช่องสัญญาณ BCH และ DCI จะไม่มีการใช้งานบิตพาริตี ซึ่งจะเลือกบิตแซ่แข็งตามจ านวน $\left|\mathcal{A}^{F}\right|=N-K$

3.1.6 การคำนวณบิตพาริตีตรวจสอบ

กรณีช่องสัญญาณ UCI มีการใช้งานบิตพาริตีและถูกเลือกตาแหน่งของบิตพาริตีแล้ว จะสามารถค านวณบิตพาริตีโดยรีจิสเตอร์วนซ้ า(shift register) ขนาด 5 บิต โดยตั้งค่าบิตเริ่มต้นเป็น 0 บิตพาริตีจะถูกคานวณโดยการเอ็กซ์คลูซีฟออร์กับบิตตาแหน่งก่อนหน้าเว้นระยะครั้งละ 5 บิต โดยจะเอ็กซ์คลูซีฟออร์เฉพาะบิตข้อมูล ซึ่งจะไม่รวมบิตพาริตี บิต CRC และบิตแซ่แข็งตาแหน่งก่อนหน้า การค านวณบิตพาริตี u_i แสดงดังสมการที่ 3.5

$$u_i=\bigoplus_{j=\lfloor i_{PC}/5\rfloor}^{q-1}u_{5j+p} \tag{3.5}$$

โดยที่ $q=\lfloor i/5\rfloor$ $p=\mathrm{mod}(i,5)$ และ $i_{PC}\in Q_{PC}$ คือค่าตาแหน่งบิตพาริตีสูงสุดที่น้อยกว่า i ที่ $\mathrm{mod}(i_{PC},5)=p$ หากไม่มีค่าตาแหน่งพาริตีนั้นจะกาหนดให้ $i_{PC}=0$ ผลลัพธ์เวกเตอร์ u หลังการค านวณบิตพาริตีจะถูกส่งไปกระบวนการถัดไปเพื่อการเข้ารหัสโพลาร์

สาหรับช่องสัญญาณ BCH และ DCI จะไม่มีการใช้งานบิตพาริตี เวกเตอร์ u จากกระบวนการก่อนหน้าจะถูกส่งไปกระบวนการถัดไปเพื่อการเข้ารหัสโพลาร์

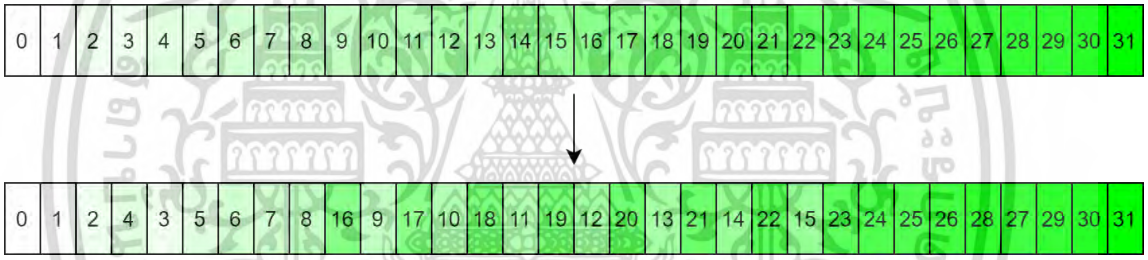
3.1.7 การเข้ารหัสโพลาร์

การเข้ารหัสโพลาร์ส าหรับช่องสัญญาณทุกกรณี สามารถเขียนในรูปสมการทางคณิตศาสตร์ได้ดังสมการที่ 3.6

$$d = uG_N \tag{3.6}$$

โดยที่ $G_N = G_2^{\otimes n}$ $G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ และ u คือชุดบิตที่จะท การเข้ารหัสความยาว N บิต ประกอบด้วย บิตข้อมูล บิต CRC และบิตแช่แข็ง รวมถึงบิตพาริตี หากมีการใช้งาน ผลลัพธ์การเข้ารหัสจะได้ค ารหัสแม่ d ความยาว N บิต ในทางปฏิบัติการเข้ารหัสจะทาได้โดยตัวดาเนินการเอ็กซ์คลูซีฟออร์ตามโครงสร้างดังภาพที่ 2.10 โครงสร้างการเข้ารหัสสามารถขยายขนาดคารหัสได้ในลักษณะการเรียกซ้า ซึ่งจะมีขนาดเพิ่มเป็นจ านวนสองเท่า จึงเป็นสาเหตุที่ความยาวค ารหัสแม่มีขนาด $N = 2^n$ บิต

3.1.8 การอินเทอร์ลีฟบล็อกย่อย



ภาพที่ 3.5 ล าดับการอินเทอร์ลีฟบล็อกย่อย

เวกเตอร์ d ความยาว N จากกระบวนการก่อนหน้าสาหรับทุกช่องสัญญาณจะถูกแบ่งเป็น 32 บล็อกย่อย ความยาวบล็อกละ $N/32$ แทนลาดับบิตในการอินเทอร์ลีฟโดย $J(j)$ ผลลัพธ์จะได้เวกเตอร์ y ความยาว N โดยที่ $y_j = d_{J(j)}$ และ $j = 0,1,...,N-1$ สามารถคานวณลาดับบิตในการอินเทอร์ลีฟดังสมการที่ 3.7

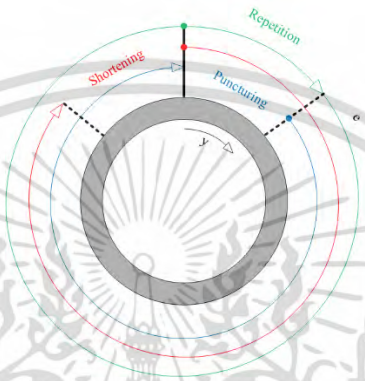
$$J(j) = \left(P\left(\left\lfloor 32\frac{j}{N} \right\rfloor \right) \cdot \frac{N}{32} \right) + \mathrm{mod}\left(j, \frac{N}{32} \right) \tag{3.7}$$

โดยตารางที่ 3.4 จะแสดงถึงล าดับการอินเทอร์ลีฟ $P(i)$ และแสดงได้ดังภาพที่ 3.5

ตารางที่ 3.4 ล าดับการอินเทอร์ลีฟ $P(i)$ ส าหรับการอินเทอร์ลีฟบล็อกย่อย (เรียงค่า i จากซ้ายไปขวาบนลงล่าง)

0	1	2	4	3	5	6	7	8	16	9	17	10	18	11	19
12	20	13	21	14	22	15	23	24	25	26	28	27	29	30	31

3.1.9 การปรับอัตรารหัส



ภาพที่ 3.6 บัฟเฟอร์วงกลมส าหรับการปรับอัตรารหัส โดยให้วงกลมสีเทาเป็นความยาวของเวกเตอร์ y และลูกศรสีต่าง ๆ เป็นเวกเตอร์ e ที่จะเลือกบิตในเวกเตอร์ y ส่งไปยังกระบวนการถัดไป

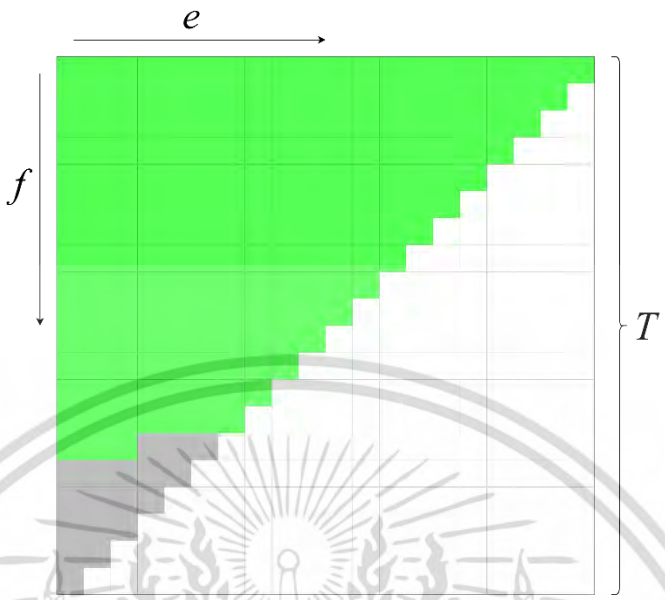
การปรับอัตรารหัสจะท าการปรับความยาวคารหัส ซึ่งถูกก าหนดความยาวไว้โดยคารหัส e ความยาว E บิต กระบวนการนี้เวกเตอร์ y จะถูกตัดบิตออกได้ผลลัพธ์เป็นเวกเตอร์ e การปรับอัตรารหัสทั้ง 3 รูปแบบสามารถสรุปได้ดังภาพที่ 3.6 และมีรายละเอียดดังนี้

1) การพังก์เจอร์ (puncturing) จะด าเนินการหากมีเงื่อนไข $E < N$ และ $K/E \le 7/16$ โดยจะบิตจานวน $U = N - E$ บิตแรก จะได้ผลลัพธ์เวกเตอร์ e ที่ความยาว E โดยที่ $e_i = y_{i+U}$ และ $i = 0,1,...,E-1$

2) การช็อตเทน (shortening) จะด าเนินการหากมีเงื่อนไข $E < N$ และ $K/E > 7/16$ โดยจะตัดบิตจานวน $U = N - E$ บิตสุดท้าย จะได้ผลลัพธ์เวกเตอร์ e ที่ความยาว E โดยที่ $e_i = y_i$ และ $i = 0,1,...,E-1$

3) การส่งซ้ า (repetition) จะด าเนินการหากมีเงื่อนไข $E > N$ โดยจะส่งบิตจานวน $U = N - E$ บิตแรกซ้ า ผลลัพธ์จะได้เวกเตอร์ e ที่ความยาว E โดยที่ $e_i = y_{\mathrm{mod}(i,N)}$ และ $i = 0,1,...,E-1$

3.1.10 การอินเทอร์ลีฟบิตรหัส



ภาพที่ 3.7 รูปแบบการอินเทอร์ลีฟแบบสามเหลี่ยมขั้นบันได

ก่อนที่คารหัสจะถูกปรับอัตรารหัสจะถูกส่งไปยังการสื่อสารระบบถัดไปเพื่อการมอดูเลชันเวกเตอร์ e จะถูกอินเทอร์ลีฟอีกครั้งโดยอินเทอร์ลีฟรูปแบบสามเหลี่ยมขั้นบันได การอินเทอร์ลีฟนี้จะช่วยให้สมรรถนะการแก้ไขความผิดพลาดดีขึ้น ส าหรับการสื่อสารที่ใช้การมอดูเลชันล าดับสูง

กรณีช่องสัญญาณ UCI จะดาเนินการอินเทอร์ลีฟบิตรหัสและให้ $I_{BIL}=1$ รูปแบบการอินเทอร์ลีฟจะดาเนินการตามโครงสร้างสามเหลี่ยมขั้นบันไดที่มีขนาด $T\times T$ ดังภาพที่ 3.7 T จะมีความยาวเท่ากับจานวนเต็มค่าน้อยสุดที่ $T(T+1)/2\geq E$ บิตในเวกเตอร์ e จะถูกใส่ไว้ในโครงสร้างสามเหลี่ยม v จากทิศซ้ายไปขวาตามด้วยบนลงล่างเป็นลาดับดังภาพที่ 3.7 ในส่วนที่แรเงาเป็นสีเขียว จากนั้นจะสร้างผลลัพธ์ โดยการนาค่าออกจากโครงสร้างสามเหลี่ยม v จากทิศบนลงล่างตามด้วยซ้ายไปขวา เก็บไว้ในเวกเตอร์ f ซึ่งเป็นเวกเตอร์ที่ผ่านการอินเทอร์ลีฟบิตรหัส โดยสามารถมองได้ว่าตาแหน่งสีขาวในโครงสร้างสามเหลี่ยมเทียบได้กับการแทนค่าบิตว่างในเมทริกซ์ v สามารถแสดงได้ดังสมการที่ 3.8

$$v_{i,j}=\begin{cases}\text{null} & \text{หาก } i+j\geq T \text{ หรือ } j+iT-i\left((i+1)/2\right)\geq E \\ e_{j+iT-i((i+1)/2)} & \text{อื่น ๆ}\end{cases} \tag{3.8}$$

โดยที่ $i=0,1,...,T$ และ $j=0,1,...,T$

สาหรับช่องสัญญาณ BCH และ DCI จะไม่ดาเนินการอินเทอร์ลีฟบิตรหัสและตั้งค่าตัวบ่งชี้ $I_{BIL}=0$ เวกเตอร์ e จากกระบวนการปรับอัตรารหัสจะถูกส่งไปยังการสื่อสารชั้นถัดไป

3.1.11 การต่อบล็อกรหัส

กรณีช่องสัญญาณ UCI หากมีการดาเนินการแบ่งบล็อกรหัสหรือมีเงื่อนไขว่า $(A \geq 360 \wedge E \geq 1088) \vee A \geq 1013$ และมีตัวบ่งชี้ $I_{seg} = 1$ เวกเตอร์ f ทั้งสองจะนามาต่อกันตามล าดับเดิม

ส าหรับช่องสัญญาณ BCH และ DCI จะไม่การแบ่งบล็อกรหัสและมีตัวบ่งชี้ $I_{BIL} = 0$ อยู่แล้ว ท างานกระบวนการต่อบล็อกรหัสไม่ท างาน เวกเตอร์ e จากกระบวนการปรับอัตรารหัสจะถูกส่งไปยังการสื่อสารชั้นถัดไป

บทที่ 4
เทคนิคการถอดรหัสและการออกแบบรหัส CRC สำหรับการถอดรหัสโพลาร์แบบแบ่งส่วน

บทที่ 2 กล่าวถึงทฤษฎีในรหัสโพลาร์ โดยเฉพาะตัวถอดรหัสหักล้างต่อเนื่องแบบลิส ซึ่งเป็นการถอดรหัสที่ให้สมรรถนะการแก้ไขความผิดพลาดที่สูง แต่ก็เป็นการถอดรหัสที่มีความซับซ้อนสูงเช่นเดียวกัน จึงได้มีงานวิจัยที่ศึกษาวิธีการลดความซับซ้อนของตัวถอดรหัสหักล้างต่อเนื่องด้วยวิธีการแบ่งส่วนตัวถอดรหัส ในบทที่ 4 จะนาเสนอการใช้ตัวถอดรหัสแบบแบ่งส่วนสาหรับการถอดรหัสโพลาร์ตามมาตรฐาน 5G โดยเลือกตัวถอดรหัสแบบแบ่งส่วนที่ใช้งานหน่วยความจาให้น้อย ขณะที่ไม่สูญเสียสมรรถนะการถอดรหัสมากเกินไป นอกจากนี้ยังนาเสนอเทคนิคการถอดรหัสด้วยการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทาง เทคนิคการถอดรหัสดังกล่าวจะประยุกต์ใช้ใช้บิต CRC แบบอินเทอร์ลีฟ โดยเฉพาะตัวถอดรหัสแบบแบ่งส่วนที่มีการตัดเส้นทางการถอดรหัส ณ ตาแหน่งท้ายส่วนตัวถอดรหัส ค่าความน่าเชื่อถือเส้นทางจะช่วยให้เส้นทางการถอดรหัสที่ถูกต้องไม่ถูกกาจัดออก สุดท้ายได้นาเสนอการออกแบบรหัส CRC แบบอินเทอร์ลีฟที่เหมาะสมกับตัวถอดรหัสแบบแบ่งส่วน เมื่อใช้ร่วมกับการถอดรหัสด้วยการปรับค่าความน่าเชื่อถือเส้นทาง จะให้สมรรถนะการแก้ไขความผิดพลาดที่ดี

4.1 การลดความซับซ้อนการถอดรหัสโพลาร์มาตรฐาน 5G โดยใช้ตัวถอดรหัสแบบแบ่งส่วน

ตัวถอดรหัสหักล้างต่อเนื่องแบบลิส เป็นการถอดรหัสที่มีความซับซ้อนสูง โดยเฉพาะอย่างยิ่งการใช้งานหน่วยความจ าซึ่งจะส่งผลให้ขนาดวงจรถอดรหัสมีขนาดใหญ่ และเนื่องด้วยมาตรฐาน 5G ไม่ได้กาหนดเงื่อนไขการถอดรหัสโพลาร์ ในทางปฏิบัติจึงสามารถเลือกใช้ตัวถอดรหัสที่เหมาะสมกับเป้าหมายของการใช้งาน เช่น หากต้องการใช้ในงานที่มีความน่าเชื่อมั่นสูง ควรใช้ตัวถอดรหัสที่ให้สมรรถนะที่ดี เช่น ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่มี CRC ช่วย หากเน้นการใช้งานภายในวงจรขนาดเล็กและราคาถูกควรเลือกตัวถอดรหัสที่มีความซับซ้อนต่ าเช่น ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วน เป็นต้น

ในวิทยานิพนธ์นี้ ได้แสดงถึงผลการจาลองตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนที่เหมาะสมกับรหัสโพลาร์ตามมาตรฐาน 5G ทั้งช่องสัญญาณดาวน์ลิงก์และอัปลิงก์ โดยจะค้นหารูปแบบตัวถอดรหัสที่สามารถลดขนาดหน่วยความจ าได้มากที่สุด ขณะที่สูญเสียสมรรถนะการแก้ไขความผิดพลาดต่าที่สุด ภายใต้รูปแบบตัวถอดรหัสหักล้างต่อเนื่องแบบลิสที่ถูกแบ่งส่วนทั้ง 3 รูปแบบ ในหัวข้อที่ 5.1 ตัว

ถอดรหัสแต่ละประเภทสามารถปรับลดพารามิเตอร์ที่สามารถส่งผลต่อการลดขนาดหน่วยความจาได้ ทั้ง จ านวนส่วนแบ่ง และจ านวนเส้นทางการถอดรหัสที่ผ่านไปยังส่วนแบ่งถัดไปส าหรับGPSCL และ LPSCL

4.2 เทคนิคการถอดรหัสสำหรับการถอดรหัสโพลาร์แบบแบ่งส่วน

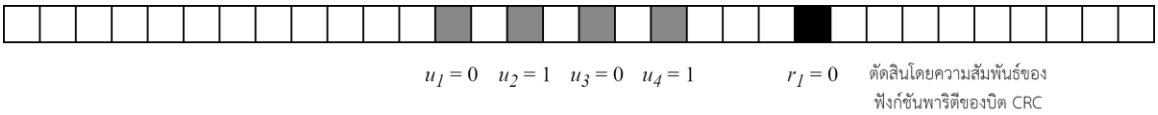
การเข้ารหัสโพลาร์ร่วมกับ CRC และรหัสโพลาร์พาริตีตรวจสอบ ได้ถูกพิสูจน์ว่าสามารถช่วยเพิ่มสมรรถนะการถอดรหัสได้ โดยมีการพิสูจน์ว่าบิตพาริตีของรหัส CRC และรหัสพาริตีตรวจสอบสามารถช่วยลดจ านวนค ารหัสที่มีน้ าหนักแฮมมิงต่าได้ นอกจากการที่บิตพาริตีเหล่านี้ช่วยเพิ่มสมรรถนะการแก้ไขความผิดพลาดแล้ว บิตพาริตียังสามารถน าไปใช้ในเทคนิคการเลิกก่อน เพื่อไม่ให้เสียเวลาในการถอดรหัสข้อมูลที่ผิดพลาดอยู่แล้ว โดยใช้ร่วมกับเทคนิคการอินเทอร์ลีฟเพื่อให้บิตพาริติจากรหัส CRC กระจายไปยังต าแหน่งต้นของชุดบิตข้อมูล แต่การอินเทอร์ลีฟมีข้อเสียด้านสมรรถนะการแก้ไขความผิดพลาด โดยที่การอินเทอร์ลีฟทาให้การลดจานวนคารหัสที่มีน้าหนักแฮมมิงต่าทาได้แย่กว่ารหัส CRC ทั่วไป ส่งผลให้มีสมรรถนะการแก้ไขความผิดพลาดที่แย่กว่า อย่างไรก็ตามวิทยานิพนธ์ได้นาเสนอวิธีการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทางที่ใช้ความสัมพันธ์ของบิตข้อมูลกับบิต CRC ที่ถูกอินเทอร์ลีฟ ในการตัดสินใจบิต CRC ระหว่างการถอดรหัส การตัดสินบิต CRC ด้วยวิธีการปรับค่าความน่าเชื่อถือเส้นทางส่งผลให้ค่าความน่าเชื่อถือเส้นทางแตกต่างไปจากการถอดรหัสหักล้างต่อเนื่องแบบลิสปกติ ณ ตาแหน่งบิตถอดรหัสต่าง ๆ ค่าความน่าเชื่อถือเส้นทางที่แตกต่างกันนี้ ส่งผลให้กลไกการตัดเส้นทางการถอดรหัสของการถอดรหัสหักล้างต่อเนื่องแบบลิสทางานแตกต่างกัน ซึ่งจะท าให้เส้นทางการถอดรหัสที่ถูกต้องมีค่าความน่าเชื่อถือเส้นทางมากขึ้น ส่งผลให้เส้นทางการถอดรหัสดังกล่าวมีโอกาสอยู่ในตัวถอดรหัสหักล้างต่อเนื่องแบบลิสจนขั้นตอนสุดท้ายและถูกเลือกออกมาเป็นบิตถอดรหัสสุดท้าย ซึ่งจะเพิ่มสมรรถนะการแก้ไขความผิดพลาดได้

4.2.1 การอินเทอร์ลีฟของรหัส CRC และการประยุกต์ใช้งาน

หากพิจารณาเมทริกซ์พาริตีตรวจสอบในรูปแบบ systematic ดังสมการที่ 2.38 แถวของเมทริกซ์จะสื่อถึงความสัมพันธ์ของบิต CRC กับบิตข้อมูล โดยแถวจานวน $n-k$ แถวแสดงถึงความสัมพันธ์ของบิต CRC จ านวน $n-k$ บิต โดยความสัมพันธ์ดังนี้

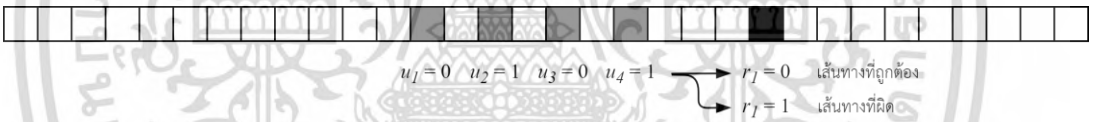
$$0 = \sum \left(h_i \right)^T \tag{4.1}$$

ความสัมพันธ์ดังกล่าวสามารถใช้ตรวจสอบความผิดพลาด (error detecting) ของคารหัสได้ โดยหากทุกบิตในความสัมพันธ์บวกรวมกันได้ไม่เท่ากับ 0 จะถือว่าบางบิตเกิดความผิดพลาด นอกจากนี้ยังสามารถใช้งานในรูปแบบการแก้ไขความผิดพลาด (error correcting) ที่ตัดสินใจบิตตามความสัมพันธ์ได้ดังภาพที่ 4.1



ภาพที่ 4.1 การถอดรหัสบิต CRC รูปแบบการแก้ไขความผิดพลาด โดยตัดสินใจบิต CRC ตามความสัมพันธ์ดังสมการที่ 4.1

รหัส CRC แบบอินเทอร์ลีฟจะเป็นการแทรกสลับบิต CRC ให้กระจายไปอยู่ระหว่างบิตข้อมูล ทั้งนี้ ส าหรับการถอดรหัสที่มีลักษณะเป็นลาดับ จะท าให้การถอดรหัสมีโอกาสเจอบิต CRC ก่อนบิตข้อมูลอื่น ๆ ทาให้ตัวถอดรหัสสามารถตัดสินใจบิต CRC ด้วยรูปแบบการแก้ไขความผิดพลาด ซึ่งสามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดแก่ตัวถอดรหัสแบบลิส ดังภาพที่ 4.1 หรือท าให้ตัวถอดรหัสตรวจสอบความผิดพลาดในระหว่างการถอดรหัสได้ โดยเมื่อตัวถอดรหัสด าเนินการถอดรหัสที่ตาแหน่งบิต CRC ตัวถอดรหัสสามารถตรวจสอบความผิดพลาดได้ตามความสัมพันธ์ดังสมการที่ 4.1 หากเกิดความผิดพลาด ตัวถอดรหัสามารถหยุดท างานได้ทันทีหรือการเลิกก่อน (early termination) ดังภาพที่ 4.2



ภาพที่ 4.2 การเลิกก่อน หากความสัมพันธ์ของบิต CRC ไม่ตรงตามเงื่อนไขสมการที่ 4.1

การอินเทอร์ลีฟ CRC ในขั้นตอนการเข้ารหัส สามารถดาเนินการได้โดยการเข้ารหัส CRC แบบปกติดังสมการที่ *2.33* ได้ผลลัพธ์เป็นคารหัส CRC รูปแบบ systematic จากนั้นท าการสลับตาแหน่งค ารหัสCRC ตามล าดับการอินเทอร์ลีฟ ล าดับอินเทอร์ลีฟสามารถถูกก าหนดได้ตามมาตรฐาน เช่น ลาดับการอินเทอร์ลีฟบิต CRC สาหรับรหัสโพลาร์ตามมาตรฐาน 5G ดังตารางที่ 3.3 หรือกาหนดได้ตามโครงสร้างเมทริกซ์พาริตีตรวจสอบของรหัส CRC หลังจากสลับตาแหน่งคารหัส CRC เมทริกซ์พาริตีตรวจสอบต้องถูกสลับหลักเพื่อให้ตาแหน่งสอดคล้องกับคารหัส CRC จากนั้นจึงสามารถถอดรหัส CRC อินเทอร์ลีฟได้จากเมทริกซ์พาริตีตรวจสอบ

4.2.2 การสร้างเมทริกซ์พาริตีตรวจสอบจากพหุนามสร้างของรหัส CRC แบบอินเทอร์ลีฟ

กาหนดให้ H คือเมทริกซ์พาริตีตรวจสอบที่สร้างมาจากพหุนามกาเนิด CRC $g(x)$ การอินเทอร์ลีฟ CRC จะทาการแทรกสลับหลักของเมทริกซ์ H ให้สมาชิกเลข 1 ของแต่ละแถวติดกัน โดย

กาหนดให้ $h(x)$ เป็นพนุนามฟังก์ชันพาริตีตรวจสอบของเมทริกซ์แต่ละแถวและ h คือเวกเตอร์สัมประสิทธิ์ของพหุนามก่อนหน้า ขั้นตอนการสร้างเมทริกซ์ H สาหรับรหัส CRC ที่มีการอินเทอร์ลีฟ มีดังนี้

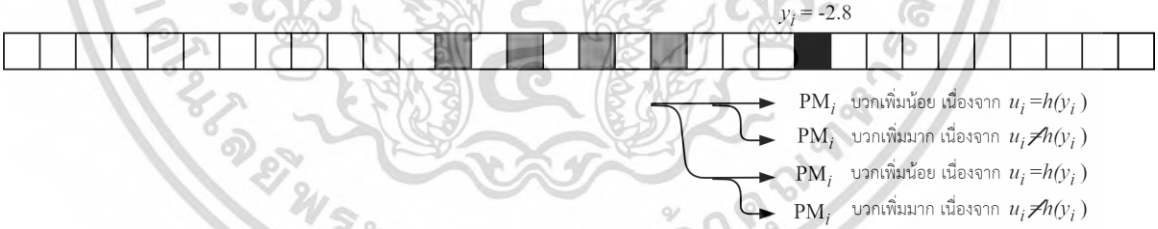
1) ค้นหาพหุนามฟังก์ชันพาริตีตรวจสอบ $h(x)$ โดยการค้นหาค่าพีเรียด (period) M ของพหุนามกาเนิด $g(x)$ จากจานวนเต็มบวกที่ต่าที่สุดที่ $x^{M-1}/g(x)$ หารลงตัว จากนั้นจะสามารถ ค านวณพหุนามฟังก์ชันพาริตีตรวจสอบ โดยที่ $h(x)=x^M+1/g(x)$

2) สร้างเมทริกซ์พาริตีตรวจสอบ H โดยการใช้ค่าสัมประสิทธิ์ของพหุนาม $h(x)$ วางไว้ที่แถวสุดท้ายของเมทริกซ์ H ความยาว $k+|r|$ บิต ส าหรับแถวด้านบนของแต่ละแถว จะท าการเลื่อนบิตไปทางซ้ายของค่าสัมประสิทธิ์ของแถวด้านล่าง

3) สุดท้าย ขั้นตอนการอินเทอร์ลีฟ จะท าการสลับแถวของเมทริกซ์ H โดยเริ่มพิจารณาจากแถวแรก โดยให้สมาชิกเลขหนึ่งย้ายไปอยู่ทางซ้ายทั้งหมด เมื่อสมาชิกของแถวแรกอยู่ทางซ้ายหมดแล้ว ให้พิจารณาสมาชิกของแถวถัดไปจนแถวสุดท้าย

4.2.3 การถอดรหัสด้วยวิธีการตัดเส้นทาง

การถอดรหัสหักล้างต่อเนื่องแบบลิสแบบปกติ ขั้นตอนการถอดรหัสบิตที่ต าแหน่งบิต CRC จะตัดสินบิตด้วยค่า LLR ของตัวถอดรหัส โดยไม่สนใจความสัมพันธ์ของบิตข้อมูลกับบิต CRC สามารถแสดงได้ดังภาพที่ 4.3

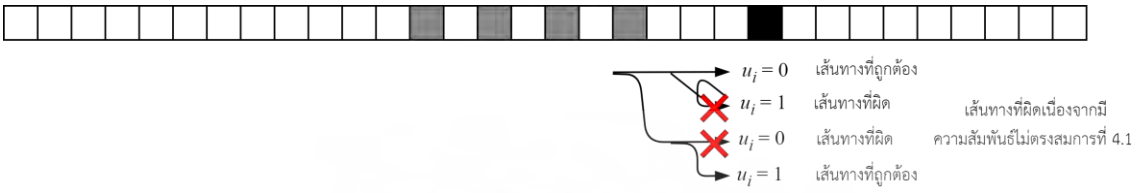


ภาพที่ 4.3 การถอดรหัสหักล้างต่อเนื่องแบบลิสแบบปกติที่ต าแหน่งบิตCRC

โดยการใช้งานรหัส CRC ในการถอดรหัสจะอยู่ในขั้นตอนสุดท้าย ซึ่งคือการเลือกเส้นทางถอดรหัสสุดท้าย จากที่ใช้เพียงค่าความน่าเชื่อถือเส้นทางเพียงอย่างเดียว รหัส CRC จะถูกนามาใช้ในการเลือกเส้นทางการถอดรหัสสุดท้ายด้วย ซึ่งท าให้มีโอกาสเลือกเส้นทางที่ถูกต้องมากขึ้น

ขณะที่การถอดรหัสหักล้างต่อเนื่องแบบลิสด้วยการตัดเส้นทางด้วยวิธีการตรวจสอบเส้นทางจะใช้ความสัมพันธ์ของบิต CRC กับบิตข้อมูลในการตัดเส้นทางการถอดรหัส ตามสมการที่ 4.*1* แสดงดัง

ภาพที่ 4.4 โดยในระหว่างกระบวนการถอดรหัส เส้นทางการถอดรหัสจะถูกเพิ่มขึ้นเป็นสองเท่าจากการตัดสินใจบิต $\hat{u}_{i_l} \in \{0,1\}$ จากนั้น หากเส้นทางการถอดรหัสมีจ านวนที่เกินขนาดลิส L



ภาพที่ 4.4 การถอดรหัสหักล้างต่อเนื่องแบบลิสด้วยการตรวจสอบเส้นทางที่ต าแหน่งบิต CRC

4.2.4 การถอดรหัสด้วยวิธีการปรับค่าความน่าเชื่อถือเส้นทาง

การถอดรหัสหักล้างต่อเนื่องแบบลิสแบบปกติ ขั้นตอนการถอดรหัสบิตที่ต าแหน่งบิต CRC จะตัดสินบิตด้วยค่า LLR ของตัวถอดรหัส โดยไม่สนใจความสัมพันธ์ของบิตข้อมูลกับบิต CRC สามารถแสดงได้ดังภาพที่ 4.3

ขณะที่การถอดรหัสหักล้างต่อเนื่องแบบลิสด้วยการปรับค่าความน่าเชื่อถือเส้นทาง ขั้นตอนการรหัสบิตที่ตาแหน่งบิต CRC จะนาความสัมพันธ์ของบิตข้อมูลกับบิต CRC มาใช้ในการตัดสินใจบิต CRC แสดงดังภาพที่ 4.5 กาหนดให้ความยาวบิตข้อมูลเท่ากับ k ความยาวบิต CRC เท่ากับ $|r|$ จะมีความยาวคารหัส CRC คือ $k+|r|$ ตาแหน่งของบิต CRC ในคารหัส CRC แทนด้วย p โดยที่ $p_0^{r-1} = \{p_0, p_1, \ldots, p_{r-1}\}$ และ $p \subset \{0,1,\ldots,k+r-1\}$ และกาหนดให้ q_r ตาแหน่งของฟังก์ชันความสัมพันธ์บิต CRC ที่ $|r|$ โดยที่ $q_r \subset \{0,1,\ldots,p_{r-1}\}$ และ p_{r-1} เป็นสมาชิกที่มีค่ามากที่สุดใน q_r การตัดสินใจบิต CRC จะใช้ฟังก์ชันความสัมพันธ์ดังนี้

$$\hat{u}_{p_{r-1}} = \bigoplus_{i \in q_{r-1} \setminus p_{r-1}} \hat{u}_i \tag{4.2}$$

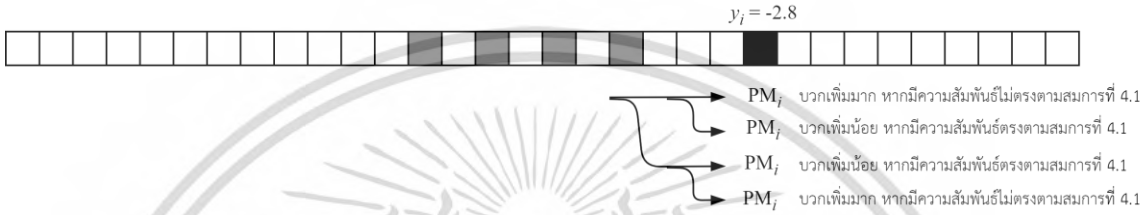
และค านวณค่าความน่าเชื่อถือเส้นทางที่ต าแหน่งบิต CRC ดังนี้

$$PM_{p_{r-1}} = PM_{p_{r-1}-1} + \ln\left(1 + e^{-(1-2\hat{u}_{p_{r-1}})y_{p_{r-1}}}\right) \tag{4.3}$$

โดยจะได้ผลลัพธ์เป็นสองเงื่อนไข หากบิต CRC ที่ตัดสินใจจากฟังก์ชันความสัมพันธ์ มีค่าเท่ากับบิต CRC ที่ตัดสินใจ ค่าความน่าเชื่อถือเส้นทางจะเพิ่มขึ้นเล็กน้อยจากพจน์เลขชี้กาลังลบ หากบิต CRC ที่ตัดสินใจจากฟังก์ชันความสัมพันธ์บิต CRC มีค่าไม่เท่ากับบิต CRC ที่ตัดสินใจ ค่าความน่าเชื่อถือเส้นทางจะเพิ่มขึ้นมากจากพจน์เลขชี้ก าลังบวก วิธีการดังกล่าวเปรียบเสมือนว่าบิต CRC ที่ตัดสินใจจากฟังก์ชันความสัมพันธ์เป็นบิตที่ถูกต้อง แล้วเมื่อค่า LLR ณ ตาแหน่งบิตถอดรหัสที่เส้นทางการถอดรหัสนั้นไม่ตรงกับฟังก์ชันความสัมพันธ์ การถอดรหัสจะถือว่าเส้นทางการถอดรหัสนั้นผิดพลาด โดยการเพิ่มค่าความน่าเชื่อถือ

เส้นทาง ณ เส้นทางนั้น นอกจากนั้นวิธีการปรับค่าความน่าเชื่อถือเส้นทางจะไม่มีการแยกเส้นทางการถอดรหัสดังภาพที่ 4.5

$$PM_{p_{r-1}} = \begin{cases} PM_{p_{r-1}-1} + \ln\left(1+e^{-|y_{p_{r-1}}|}\right) & , \hat{u}_{p_{r-1}} = \hat{u}_i \\ PM_{p_{r-1}-1} + \ln\left(1+e^{|y_{p_{r-1}}|}\right) & \text{อื่น ๆ} \end{cases} \tag{4.4}$$



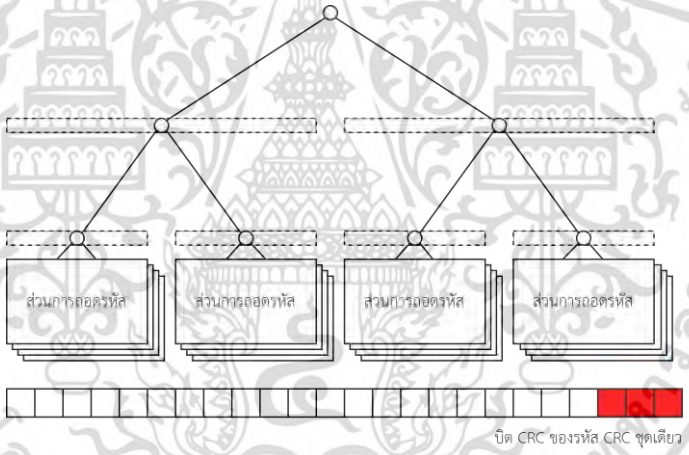
ภาพที่ 4.5 การถอดรหัสหักล้างต่อเนื่องแบบลิสด้วยการปรับค่าความน่าเชื่อถือเส้นทางที่ตาแหน่งบิต CRC

4.3 การออกแบบรหัส CRC แบบอินเทอร์ลีฟสำหรับการถอดรหัสโพลาร์ที่มีการแบ่งส่วนและใช้วิธีการปรับค่าความน่าเชื่อถือเส้นทาง

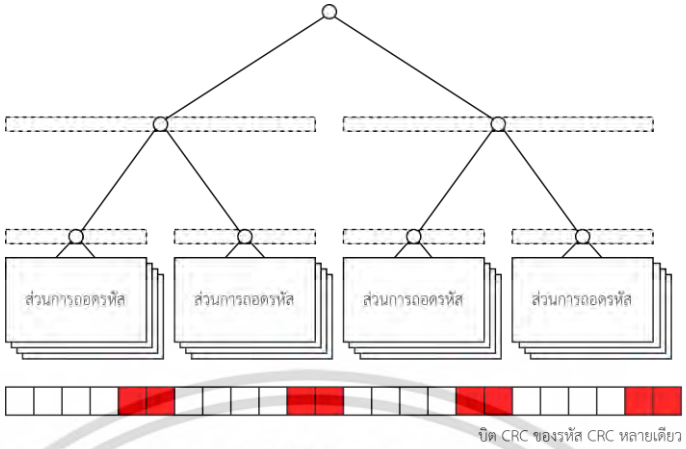
แม้การเข้ารหัสโพลาร์ร่วมกับ CRC ได้ถูกพิสูจน์ว่าสามารถช่วยเพิ่มสมรรถนะการถอดรหัสได้ แต่ก็มีการค้นพบว่าพหุนามที่ใช้งานกับรหัสโพลาร์นั้นเป็นพหุนามที่ไม่ได้ออกแบบมาสาหรับรหัสโพลาร์ กล่าวคือสามารถเลือกพหุนาม CRC ที่เหมาะสมต่อรหัสโพลาร์ได้ โดยเฉพาะให้เหมาะสมกับวิธีการถอดรหัสโพลาร์ ที่สามารถเพิ่มสมรรถนะการถอดรหัสโพลาร์ให้สูงสุดที่สุด การเข้ารหัสโพลาร์ร่วมกับ CRC ได้ถูกพิสูจน์ว่าสามารถลดจานวนคารหัสที่มีน้าหนักแฮมมิงต่าได้ ดังนั้นหนึ่งในวิธีการเลือกพนุนาม CRC คือการเลือกพนุนามที่ทาให้รหัสโพลาร์มีน้าหนักแฮมมิ่งต่าสุดที่เท่าที่เป็นไปได้ วิทยานิพนธ์นี้ได้นาเสนอการออกแบบรหัส CRC แบบอินเทอร์ลีฟสาหรับตัวถอดรหัสแบบแบ่งส่วน และเนื่องจากโครงสร้างของการถอดรหัสแบบแบ่งส่วนที่มีการตัดสินเส้นทางการถอดรหัสในแต่ละส่วนแยกกัน จึงได้น าเงื่อนไขการอินเทอร์ลีฟบิต CRC มาร่วมด้วย และเงื่อนไขการเลือกพหุนาม CRC คือการเลือกพหุนามที่สามารถกระจายบิต CRC ไปยังส่วนหน้าของชุดบิตข้อมูลให้ได้มากที่สุด เนื่องจากจะทาให้บิต CRC ถูกกระจายไปยังตัวถอดรหัสส่วนด้านหน้าได้มาก และช่วยในการตัดสินเส้นทางการถอดรหัสของตัวถอดรหัสส่วนนั้น ส่งผลให้เพิ่มสมรรถนะการถอดรหัสได้

เนื่องจากตัวถอดรหัสหักล้างต่อเนื่องที่มีการแบ่งส่วนจะมีการตัดเส้นทางการถอดรหัส ณ ตาแหน่งสุดท้ายของแต่ละส่วนเสมอ และรหัส CRC จะมีส่วนช่วยในการตัดเส้นทาง หากรหัส CRC แบบ

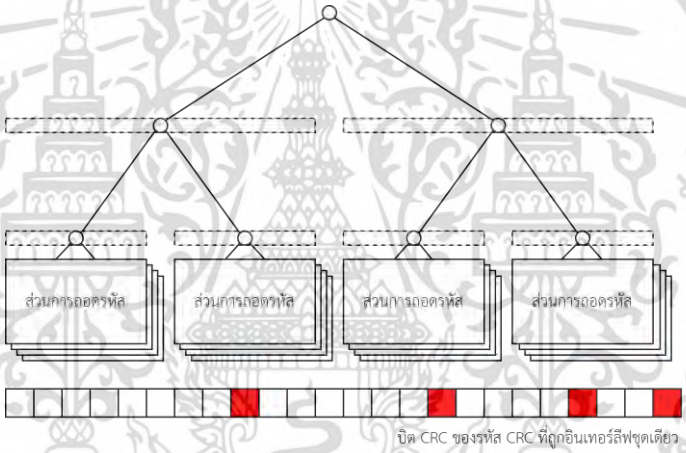
ทั่วไปที่ต าแหน่งบิต CRC จะต่อท้ายบิตข้อมูลภายใต้รหัสโพลาร์ ซึ่งมักจะเป็นต าแหน่งที่อยู่ภายในส่วนการถอดรหัสสุดท้ายดังภาพที่ 4.6 จะท าให้รหัสCRC ดังกล่าวไม่มีส่วนช่วยในการตัดเส้นทางการถอดรหัสในส่วนการถอดรหัสก่อนหน้า รหัส CRC จึงควรอยู่ในทุกส่วนการถอดรหัส ท าให้สามารถใช้งานรหัส CRC หลายชุดรหัสร่วมกับตัวถอดรหัสในทุกส่วนได้ แสดงดังภาพที่ 4.7 แต่การใช้รหัส CRC หลายชุด จะท าให้เสียต าแหน่งของบิตแช่แข็ง ในกรณีที่รหัส CRC ใช้งานร่วมกับรหัสโพลาร์ ซึ่งถ้าหากบิต CRC กินต าแหน่งบิตแช่แข็งมากเกินไป อาจส่งผลเสียต่อสมรรถนะการแก้ไขความผิดพลาดของรหัสโพลาร์ด้วย รวมทั้งยังเพิ่มความซับซ้อนในการเข้าและถอดรหัส CRC หลายชุดอีกเช่นกัน อีกทั้งในมาตรฐานการสื่อสารใช้งานรหัสโพลาร์ เช่น มาตรฐาน 5G ยังนิยมใช้งานรหัส CRC ชุดเดียว วิทยานิพนธ์นี้จึงพิจารณารหัส CRC ที่จะใช้งานร่วมกับเงื่อนไขการออกแบบพหุนาม CRC ที่น าเสนอเป็นรหัส CRC ชุดเดียว การอินเทอร์ลีฟรหัส CRC จึงเป็นทางเลือกแสดงดังภาพที่ 4.8 เพื่อที่จะให้บิต CRC ของรหัสชุดเดียวกระจายไปยังส่วนการถอดรหัสให้ได้มากที่สุด



ภาพที่ 4.6 รหัส CRC แบบทั่วไปชุดเดียวภายใต้ตัวถอดรหัสหักล้างต่อเนื่องที่มีการแบ่งส่วน



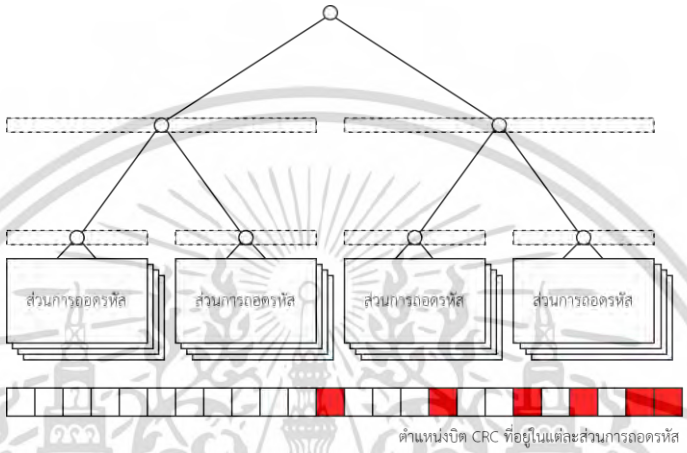
ภาพที่ 4.7 รหัส CRC หลายชุดภายใต้ตัวถอดรหัสหักล้างต่อเนื่องที่มีการแบ่งส่วน



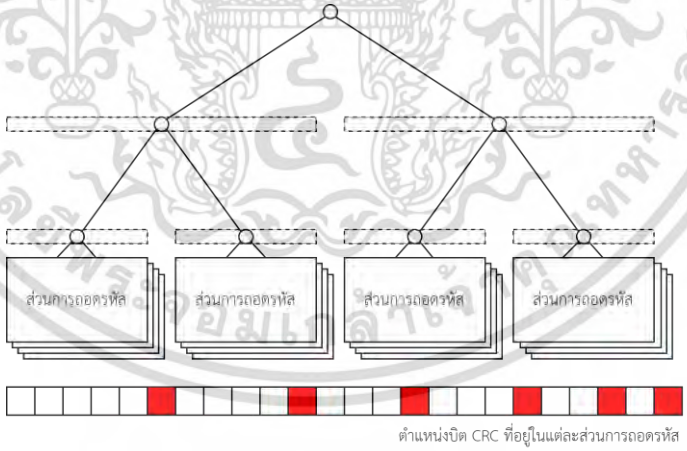
ภาพที่ 4.8 รหัส CRC แบบอินเทอร์ลีฟชุดเดียวภายใต้ตัวถอดรหัสหักล้างต่อเนื่องที่มีการแบ่งส่วน

หนึ่งในหลักการออกแบบที่สามารถให้บิต CRC กระจายไปยังส่วนการถอดรหัสด้านหน้าได้คือการพิจารณาค่าน้ำหนักแถวแรก (first-row weight) โดยค่าน้ำหนักหมายถึงจานวนเลขหนึ่งและแถวแรกหมายถึงแถวแรกของเมทริกซ์พาริตีตรวจสอบ $\mathbf{H}$ ซึ่งหากจานวนเลขหนึ่งในแถวแรกของเมทริกซ์ $\mathbf{H}$ มีจ านวนมาก เมื่อรหัส CRC ถูกอินเทอร์ลีฟ บิตแรกของ CRC จะมีโอกาสที่อยู่ในส่วนการถอดรหัสส่วนแรกน้อยลงแสดงดังภาพที่ 4.9 ในทางกลับกัน หากจ านวนเลขหนึ่งในแถวแรกของเมทริกซ์ $\mathbf{H}$ มีจ านวนน้อย เมื่อรหัส CRC ถูกอินเทอร์ลีฟ บิตแรกของ CRC จะมีโอกาสที่อยู่ในส่วนการถอดรหัสส่วนแรกมากขึ้นแสดงดังภาพที่ 4.10 แล้วจะส่งผลต่อตาแหน่งของบิต CRC ที่สองเหมือนกัน และหากจ านวนเลขหนึ่งในแถวที่สองของเมทริกซ์ $\mathbf{H}$ มีจ านวนน้อย ก็จะท าให้ต าแหน่งของบิต CRC ที่สองมีโอกาสอยู่ในส่วนการถอดรหัสด้านหน้ามากขึ้นเช่นกัน และเนื่องจากรหัส CRC มีคุณสมบัติ cyclic ซึ่งลักษณะเลขหนึ่งของแต่ละแถวใน

เมทริกซ์ **H** จะเกิดจากการเลื่อนทีละบิต ทาให้จานวนเลขหนึ่งในแต่ละแถวมีจานวนใกล้เคียงกัน แสดงตัวอย่างเมทริกซ์ **H** ที่มีคุณสมบัติ cyclic ดังภาพที่ 4.11 และเมทริกซ์ดังกล่าวเมื่อถูกอินเทอร์ลีฟ ตาแหน่งเลขหนึ่งของแต่ละแถวของเมทริกซ์จะท ให้ถูกอยู่ทางซ้ายให้ได้มากที่สุดดังภาพที่ 4.12 กล่าวคือ สามารถพิจารณาเพียงค่าน้ าหนักของแถวแรกได้ ส าหรับการออกแบบรหัส CRC ที่น าเสนอ



ภาพที่ 4.9 ตาแหน่งของบิต CRC ที่ถูกอินเทอร์ลีฟจะกระจายขึ้นไปยังส่วนการถอดรหัสด้านหน้าน้อยลง เมื่อเมทริกซ์ **H** มีค่าน้ าหนักแถวแรกมาก



ภาพที่ 4.10 ตาแหน่งของบิต CRC ที่ถูกอินเทอร์ลีฟจะกระจายขึ้นไปยังส่วนการถอดรหัสด้านหน้ามากขึ้น เมื่อเมทริกซ์ **H** มีค่าน้ าหนักแถวแรกน้อย

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \begin{matrix} \text{row weight} = 3 \\ \text{row weight} = 3 \\ \cdots \\ \text{row weight} = 2 \end{matrix}$$

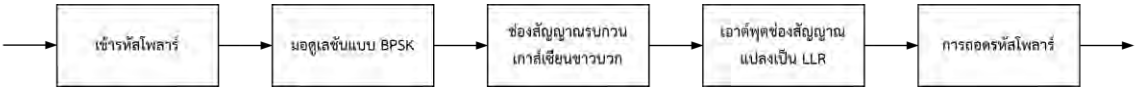
ภาพที่ 4.11 คุณสมบัติ cyclic ของรหัส CRC ที่ทาให้จานวนเลขหนึ่งในแต่ละแถวของเมทริกซ์ **H** มีจ านนวใกล้เคียงกัน

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{matrix} \text{row weight} = 3 \\ \text{row weight} = 3 \\ \cdots \\ \text{row weight} = 2 \end{matrix}$$

ภาพที่ 4.12 ตัวอย่างลักษณะของเมทริกซ์ **H** ที่มีคุณสมบัติ cyclic เมื่อถูกอินเทอร์ลีฟ

บทที่ 5
ผลการออกแบบและการจำลองสมรรถนะของรหัสโพลาร์ที่ใช้ตัวถอดรหัสแบบแบ่งส่วน

บทที่ 5 จะนาเสนอผลการออกแบบและการจาลองสมรรถนะของการถอดรหัสโพลาร์โดยใช้การวัดอัตราเฟรมผิดพลาด โดยแบ่งผลลัพธ์เป็น 3 ส่วนหลัก ส่วนแรกจะแสดงผลการจาลองสมรรถนะของตัวถอดรหัสแบบแบ่งส่วนที่ใช้งานกับรหัสโพลาร์ตามมาตรฐาน 5G ซึ่งตัวถอดรหัสดังกล่าวได้กล่าวถึงในบทที่ 2 จะสามารถช่วยลดความซับซ้อนเชิงพื้นที่หน่วยความจาที่ลดลงได้ แต่ก็ต้องแลกกับสมรรถนะที่ลดลงตั้งแต่เล็กน้อยยันมากตามรูปแบบของตัวถอดรหัส ผลการจาลองแสดงถึงสมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัสแบบแบ่งส่วนรูปแบบต่าง ๆ ที่เหมาะสมกับการใช้งานร่วมกับรหัสโพลาร์ตามมาตรฐาน 5G โดยพิจารณาว่าไม่เกิดการสูญเสียสมรรถนะอัตราเฟรมผิดพลาดที่มากเกินไป รวมถึงแสดงความซับซ้อนที่ลดลงในแต่ละรูปแบบของตัวถอดรหัสแบบแบ่งส่วน ในส่วนที่สองจะน าเสนอผลการจาลองของเทคนิคการถอดรหัสที่ได้นาเสนอ ได้แก่ วิธีการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทาง ซึ่งได้กล่าวในบทที่ 4 เป็นเทคนิคที่ใช้ร่วมกับการถอดรหัสหักล้างต่อเนื่องแบบลิสสาหรับรหัสโพลาร์ที่มีรหัส CRC แบบอินเทอร์ลีฟร่วม โดยเทคนิคดังกล่าวจะถูกใช้งานกับบิต CRC ที่ถูกอินเทอร์ลีฟ ช่วยให้ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสสามารถรักษาเส้นทางการถอดรหัสที่ถูกต้องอยู่ได้ ส่งผลให้สมรรถนะการแก้ไขความผิดพลาดดีขึ้น โดยในส่วนนี้จะแสดงให้เห็นว่าเทคนิคดังกล่าวสามารถเพิ่มสมรรถนะได้ทั้งตัวถอดรหัสหักล้างต่อเนื่องแบบทั่วไปและที่ถูกแบ่งส่วน และส่วนสุดท้าย ได้นาเสนอพหุนาม CRC ที่เหมาะสมกับเทคนิคการถอดรหัสด้วยวิธีการปรับค่าความน่าเชื่อถือเส้นทางจากเกณฑ์การเลือกด้วยการพิจารณาค่าน้าหนักแถวแรกของเมทริกซ์พาริตีตรวจสอบของพหุนาม CRC นั้น ซึ่งได้กล่าวถึงในบทที่ 4 โดยส่วนนี้จะยกตัวอย่างพหุนาม CRC ขึ้นมาที่มีค่าน้าหนักแถวแรกที่แตกต่างกันและจาลองสมรรถนะอัตราเฟรมผิดพลาดเปรียบเทียบกัน โดยพนุนาม CRC ที่มีค่าน้าหนักแถวแรกต่าจะให้แนวโน้มของสมรรถนะอัตราเฟรมผิดพลาดที่ดีกว่าพนุนาม CRC ที่มีค่าน้าหนักแถวแรกสูง ในทุกการจาลองภายในวิทยานิพนธ์นี้จะจาลองสมรรถนะอัตราเฟรมผิดพลาดภายใต้ช่องสัญญาณอุดมคติ ซึ่งคือช่องสัญญาณ AWGN แบบไบนารีและใช้การมอดูเลชันแบบ BPSK สาหรับรหัสโพลาร์ ระบบการจ าลองจะถูกแสดงเป็นแผนภาพบล็อกดังภาพที่ 5.1



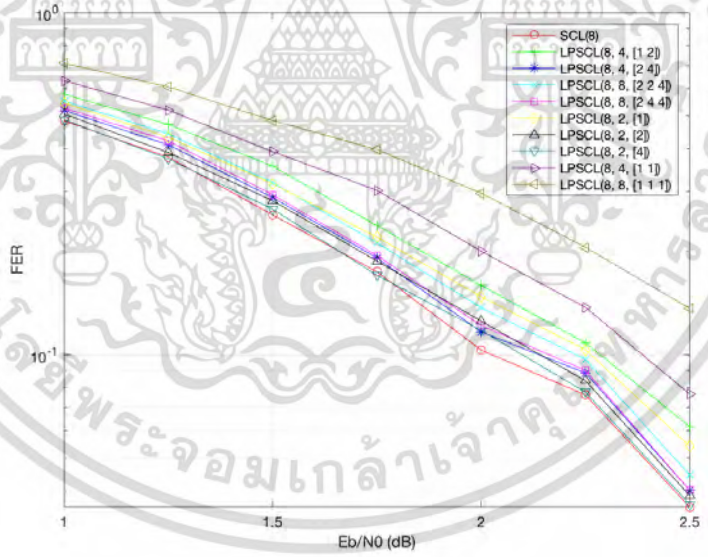
ภาพที่ 5.1 ระบบการจ าลองที่ใช้งานช่องสัญญาณอุดมคติ

5.1 ผลการทดสอบตัวถอดรหัสแบบแบ่งสำหรับรหัสโพลาร์ในมาตรฐาน 5G

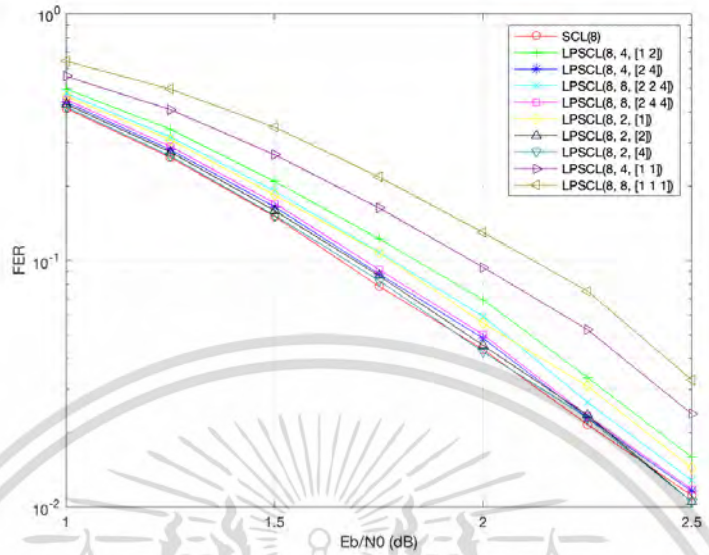
ผลการทดสอบในส่วนนี้จะเป็นตัวถอดรหัสแบบแบ่งส่วนที่ใช้งานภายใต้รหัสโพลาร์ตามมาตรฐาน 5G สาหรับช่องสัญญาณ UCI รหัสโพลาร์ใช้อัตรารหัส $R=1/2$ ที่ความยาวคารหัส $N=\{256, 512, 1024\}$ ส าหรับช่องสัญญาณ DCI รหัสโพลาร์ใช้อัตรารหัสสองค่าที่ $R=\{0.55, 0.27\}$ และความยาวค ารหัส $N=\{256, 512\}$ ซึ่งเป็นไปตามมาตรฐาน 5G ที่อนุญาตให้ใช้

5.1.1 สมรรถนะของตัวถอดรหัสแบบแบ่งสำหรับรหัสโพลาร์ในมาตรฐาน 5G

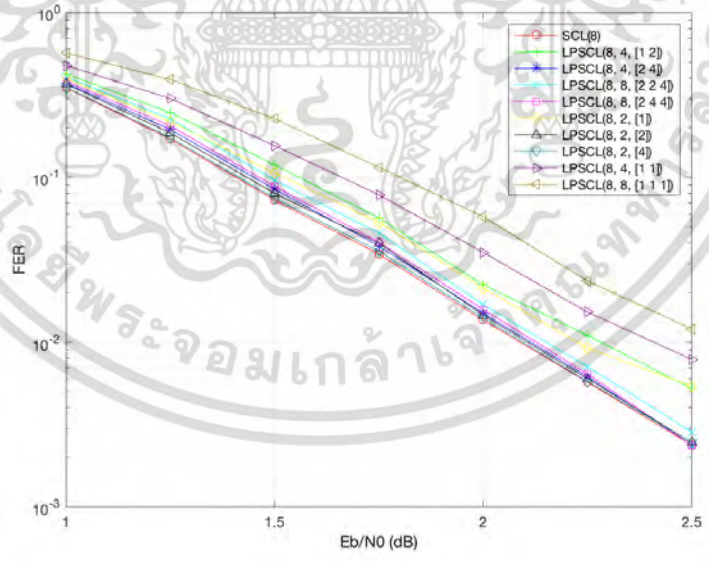
หัวข้อย่อยนี้จะแสดงสมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL สาหรับรหัสโพลาร์ตามมาตรฐาน 5G โดยสองช่องสัญญาณ UCI และ DCI จะใช้งานรหัส CRC ที่แตกต่างกันโดยที่ช่องสัญญาณ UCI จะใช้งานพหุนาม CRC ที่ไม่มีการอินเทอร์ลีฟ ซึ่งกราฟสมรรถนะอัตราเฟรมผิดพลาดของช่องสัญญาณ UCI ที่ความยาวค ารหัส 256 512 และ 1024 จะแสดงดังภาพที่ 5.2 ถึง 5.4 ตามล าดับ



ภาพที่ 5.2 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL สาหรับช่องสัญญาณ UCI ที่ $N=256$ และ $R=1/2$



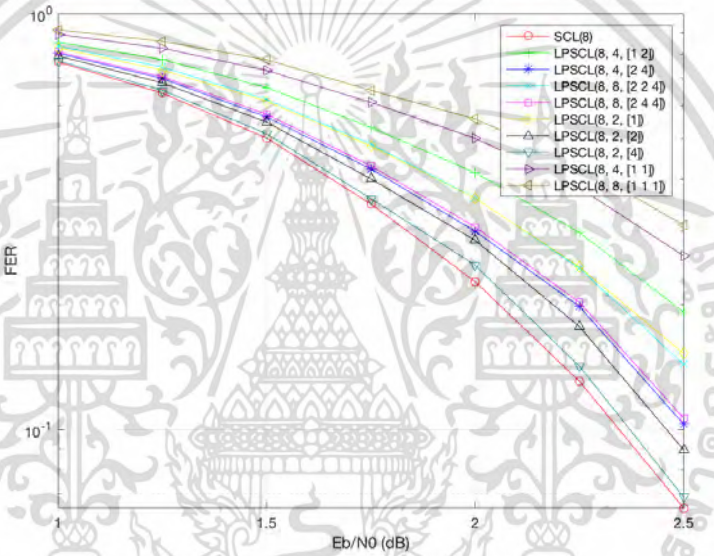
ภาพที่ 5.3 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL สาหรับช่องสัญญาณ UCI ที่ $N = 512$ และ $R = 1/2$



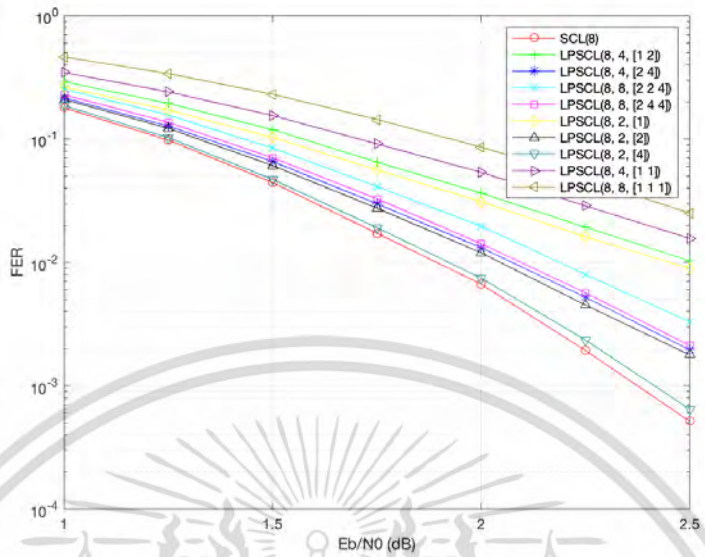
ภาพที่ 5.4 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL ส าหรับช่องสัญญาณ UCI ที่ $N = 1024$ และ $R = 1/2$

โดยสมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส SCL(8) และ LPSCL(8, 2, [4]) นั้นใกล้เคียงกันมาก ขณะที่ตัวถอดรหัส LPSCL(8, 2, [4]) สามารถลดขนาดหน่วยความจาได้กว่าร้อยละ 25 ขณะที่สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL(8, 4, [2, 4]) และ LPSCL(8, 8, [2, 2, 4]) แย่กว่าตัวถอดรหัส SCL(8) เล็กน้อย แต่สามารถลดขนาดหน่วยความจ าได้กว่าร้อยละ 42.62 และ 46.31 ตามล าดับ

ส าหรับช่องสัญญาณ DCI จะใช้งานพหุนาม CRC $g_{24C}(x)$ ตามหัวข้อที่ 3.1 ที่มีการอินเทอร์ลีฟ ซึ่งกราฟสมรรถนะอัตราเฟรมผิดพลาดของช่องสัญญาณ DCI ที่ความยาวคารหัส 256 และ 512 จะแสดงดังภาพที่ 5.5 และ 5.6



ภาพที่ 5.5 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL สาหรับช่องสัญญาณ DCI ที่ $N=256$ $R=0.55$ และพหุนาม CRC $g_{24C}(x)$



ภาพที่ 5.6 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส LPSCL สำหรับช่องสัญญาณ DCI $N = 512$ $R = 0.27$ และพหุนาม CRC $g_{24C}(x)$

โดยตัวถอดรหัส LPSCL(8, 2, [4]) ยังให้สมรรถนะอัตราเฟรมผิดพลาดที่ใกล้เคียงกับตัวถอดรหัส SCL(8) ในทางกลับกัน ตัวถอดรหัส LPSCL(8, 4, [2, 4]) และ LPSCL(8, 8, [2, 2, 4]) ในช่องสัญญาณ DCI กลับให้สมรรถนะที่ลดลงจากตัวถอดรหัส SCL(8) ค่อนข้างมากหากเทียบกับช่องสัญญาณ UCI

5.1.2 ขนาดหน่วยความจำของตัวถอดรหัสแบบแบ่งสำหรับรหัสโพลาร์ในมาตรฐาน 5G

หัวข้อย่อยนี้จะแสดงถึงผลลัพธ์การลดขนาดหน่วยความจำของตัวถอดรหัสแบบแบ่งส่วนรูปแบบต่าง ๆ หากใช้งานกับรหัสโพลาร์ตามมาตรฐาน 5G ซึ่งเป็นที่ทราบแล้วว่าเทคนิคการแบ่งส่วนตัวถอดรหัสสามารถลดจำนวนค่าที่ต้องเก็บในการถอดรหัสแบบ SCL ซึ่งจะส่งผลให้ใช้งานขนาดหน่วยความจำลดลง ขณะเดียวกันก็ส่งผลต่อสมรรถนะการแก้ไขความผิดพลาดที่ลดลง โดยขนาดของหน่วยความจำที่ลดลงสามารถคำนวณได้โดยตรงจากพารามิเตอร์ต่าง ๆ ของตัวถอดรหัสแบบแบ่งส่วน สามารถสรุปเป็น 3 ตารางดังต่อไปนี้

ตารางที่ 5.1 ร้อยละของขนาดหน่วยความจ ที่ลดลงของตัวถอดรหัสแบบแบ่งส่วนสำหรับรหัสโพลาร์ที่มีขนาดลิส $L = 8$ และ $Q_{llr} = Q_{PM} = 8$

ตัวถอดรหัส	หน่วยความจ ำ[บิต]	

	$N=512$	$N=1024$	หน่วยความจ า ที่ลดลง
$\mathrm{SCL}(8)$	45048	90104	-
$\mathrm{LPSCL}(8,2,[1])$	26872	53752	40.34%
$\mathrm{LPSCL}(8,2,[2])$	29176	58360	35.23%
$\mathrm{LPSCL}(8,2,[4])$	33784	67576	25.00%
$\mathrm{LPSCL}(8,4,[1,1])$	17784	35576	60.52%
$\mathrm{LPSCL}(8,4,[1,2])$	20088	40184	55.40%
$\mathrm{LPSCL}(8,4,[2,4])$	25848	51704	42.62%
$\mathrm{LPSCL}(8,8,[1,1,1])$	13240	26488	70.60%
$\mathrm{LPSCL}(8,8,[2,2,4])$	21880	43768	51.43%
$\mathrm{LPSCL}(8,8,[2,4,4])$	24184	48376	46.31%
$\mathrm{LPSCL}(8,8,[8,8,8])$	41464	82936	7.96%

ตารางที่ 5.2 ร้อยละของขนาดหน่วยความจ ที่ลดลงของตัวถอดรหัสแบบแบ่งส่วนส าหรับรหัสโพลาร์ที่มีขนาดลิส $L=16$ และ $Q_{llr}=Q_{PM}=8$

ตัวถอดรหัส	หน่วยความจ า[บิต]		หน่วยความจ า ที่ลดลง
	$N=512$	$N=1024$	
$\mathrm{SCL}(16)$	86000	172016	-
$\mathrm{LPSCL}(16,2,[1])$	47344	94704	44.95%
$\mathrm{LPSCL}(16,2,[2])$	49648	99312	42.27%
$\mathrm{LPSCL}(16,2,[4])$	54256	108528	36.91%
$\mathrm{LPSCL}(16,4,[1,1])$	28016	56048	67.42%
$\mathrm{LPSCL}(16,4,[1,2])$	30320	60656	64.74%
$\mathrm{LPSCL}(16,4,[2,4])$	36080	72176	58.05%
$\mathrm{LPSCL}(16,8,[1,1,1])$	18352	36720	78.66%
$\mathrm{LPSCL}(16,8,[2,2,4])$	26992	54000	68.61%

$\mathrm{LPSCL}(16,8,[2,4,4])$	29296	58608	65.93%
$\mathrm{LPSCL}(16,8,[8,8,8])$	46576	93168	45.84%

ตารางที่ 5.3 ร้อยละของขนาดหน่วยความจ ที่ลดลงของตัวถอดรหัสแบบแบ่งส่วนส าหรับรหัสโพลาร์ที่มีขนาดลิส $L=16$ และ $Q_{llr}=Q_{PM}=8$

ตัวถอดรหัส	หน่วยความจ า[บิต]		หน่วยความจ า ที่ลดลง
	$N=512$	$N=1024$	
$\mathrm{SCL}(16)$	86000	172016	-
$\mathrm{LPSCL}(16,2,[2])$	49648	99312	42.27%
$\mathrm{LPSCL}(16,2,[4])$	54256	108528	36.91%
$\mathrm{LPSCL}(16,2,[8])$	63472	126960	26.19%
$\mathrm{LPSCL}(16,4,[2,2])$	31472	62960	63.40%
$\mathrm{LPSCL}(16,4,[2,4])$	36080	72176	58.04%
$\mathrm{LPSCL}(16,4,[4,8])$	47600	95216	44.65%
$\mathrm{LPSCL}(16,8,[2,2,2])$	22384	44784	73.97%
$\mathrm{LPSCL}(16,8,[4,4,8])$	39664	79344	53.87%
$\mathrm{LPSCL}(16,8,[4,8,8])$	44272	88560	48.52%
$\mathrm{LPSCL}(16,8,[16,16,16])$	78832	157680	8.33%

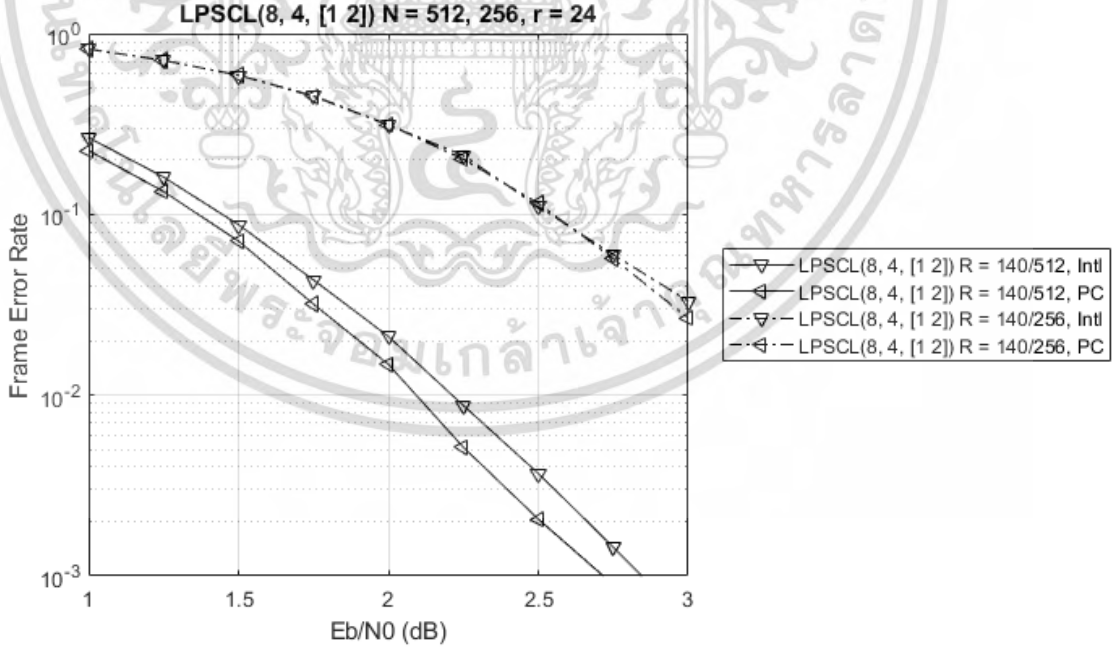
หากพิจารณาที่ตัวถอดรหัส LPSCL ที่มีขนาดลิส $L=8$ ตัวถอดรหัส $\mathrm{LPSCL}(8,8,[1,1,1])$ สามารถลดขนาดพื้นที่หน่วยความจาได้สูงสุดถึงร้อยละ 70.60 แต่ก็เกิดความสูญเสียของสมรรถนะการแก้ไขความผิดพลาดพอสมควร ขณะที่ตัวถอดรหัส $\mathrm{LPSCL}(8,8,[2,4,4])$ ที่สูญเสียสมรรถนะการแก้ไขความผิดพลาดเพียงเล็กน้อย สามารถลดขนาดพื้นที่หน่วยความจ าได้ถึงร้อยละ 46.31

5.2 ผลการทดสอบรหัส CRC แบบอินเทอร์ลีฟสำหรับตัวถอดรหัสแบบแบ่งส่วน

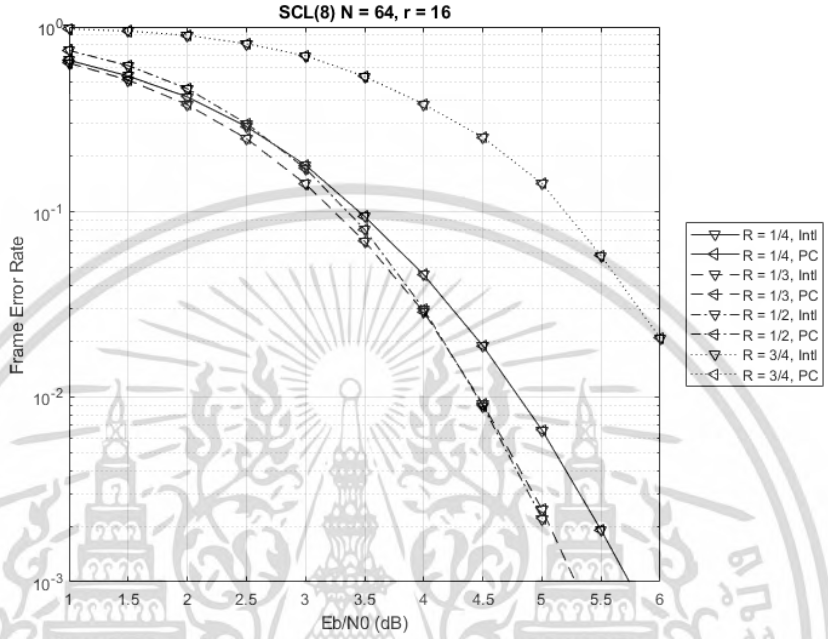
ผลการทดสอบในส่วนนี้จะใช้งานรหัส CRC แบบอินเทอร์ลีฟหลากหลายรูปแบบภายใต้ตัวถอดรหัสแบบแบ่งส่วนสาหรับรหัสโพลาร์ โดยรหัส CRC แบบอินเทอร์ลีฟจะถูกถอดรหัสด้วยวิธีการตัดเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทาง

5.2.1 สมรรถนะของรหัส CRC แบบอินเทอร์ลีฟสำหรับตัวถอดรหัสแบบแบ่งส่วนโดยวิธีการตัดเส้นทาง

สมรรถนะอัตราเฟรมผิดพลาดของรหัสโพลาร์ร่วมกับ CRC ทั้งแบบทั่วไปและแบบอินเทอร์ลีฟภายใต้ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสหรือ $\mathrm{LPSCL}(8,4,[1,2])$ หรือ SCL(8) ร่วมกับวิธีการตัดเส้นทางจะถูกจ ลอง สาหรับ $\mathrm{LPSCL}(8,4,[1,2])$ จะใช้งานรหัส CRC พหุนามความยาว $r=24$ บิต $g(x)=[1,1,0,1,1,0,0,1,0,1,0,1,1,0,0,0,1,0,0,0,1,0,1,1,1]$ โดยรหัสโพลาร์จะความยาวคารหัส $N=512$ และ $N=256$ อัตรารหัส $R=140/512$ และ $R=140/256$ และขนาดลิส $L=8$ และจะใช้งานรหัส CRC พหุนาม $g(x)=[1,1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1]$ โดยรหัสโพลาร์จะความยาวคารหัส $N=64$ อัตรารหัส $R=1/2$ และขนาดลิส $L=8$ สาหรับ SCL(8) และแสดงกราฟสมรรถนะอัตราเฟรมผิดพลาดภายใต้ตัวถอดรหัส $\mathrm{LPSCL}(8,4,[1,2])$ และ SCL(8) ดังภาพที่ 5.7 และ 5.9 ตามล าดับ



ภาพที่ 5.7 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{LPSCL}(8,4,[1,2])$ ร่วมกับวิธีการตัดเส้นทาง

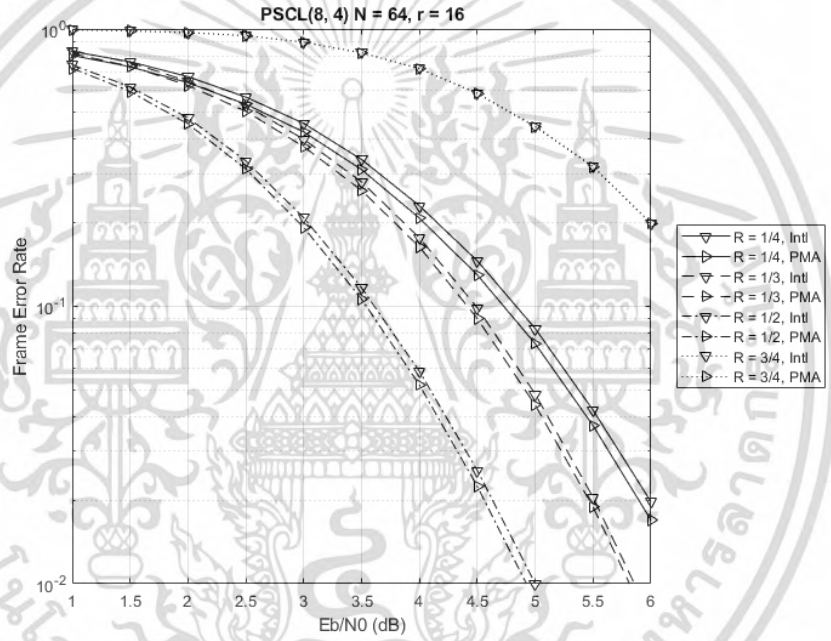


ภาพที่ 5.8 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส SCL(8) ร่วมกับวิธีการตัดเส้นทาง

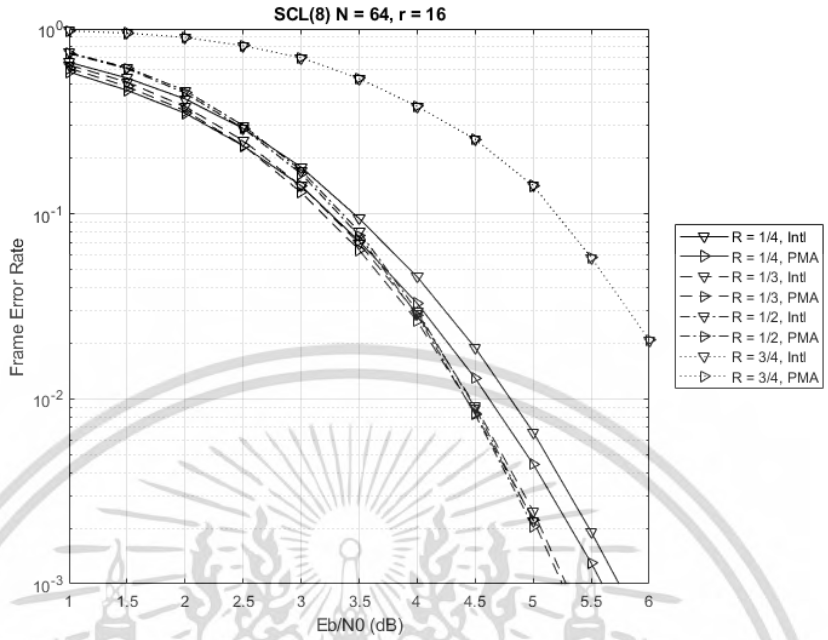
โดยจะแสดงสมรรถนะอัตราเฟรมผิดพลาดของการนาวิธีการตัดเส้นทางมาใช้งานภายใต้ตัวถอดรหัส $\mathrm{LPSCL}(8,4,[1,2])$ และ SCL(8) โดยวิธีการตัดเส้นทางสามารถปรับปรุงสมรรถนะได้ภายใต้ตัวถอดรหัสแบบแบ่งส่วน แต่ไม่เกิดการปรับปรุงสมรรถนะภายใต้ตัวถอดรหัสแบบทั่วไป เนื่องจากบิต CRC ที่ถูกอินเทอร์ลีฟจะถูกกระจายไปยังภายใต้แต่ละส่วนของตัวถอดรหัสที่ถูกแบ่งส่วน เมื่อการถอดรหัสมาถึงจุดสิ้นสุดของแต่ละส่วนตัวถอดรหัส บิต CRC ที่ถูกอินเทอร์ลีฟจะมีส่วนช่วยในการเลือกเส้นทางการถอดรหัสที่จะถูกส่งต่อไปยังส่วนของตัวถอดรหัสถัดไปของ ขณะที่ตัวถอดรหัส SCL(8) ไม่มีกระบวนการดังกล่าว ทาให้ไม่เกิดการปรับปรุงของสมรรถนะ สาหรับตัวถอดรหัส $\mathrm{LPSCL}(8,4,[1,2])$ วิธีการดังกล่าวสามารถให้สมรรถนะที่ดีกว่าวิธีการถอดรหัสทั่วไป 0.2 dB และตัวถอดรหัส SCL(8) วิธีการทั้งสองให้สมรรถนะที่เท่ากัน ผลของการเพิ่มสมรรถนะภายใต้วิธีการปรับค่าความน่าเชื่อถือเส้นทางนั้นขึ้นอยู่กับคุณสมบัติของตัวถอดรหัส ทั้งความยาวค ารหัส ความยาวบิตพาริตี และอื่น ๆ

5.2.2 สมรรถนะของรหัส CRC แบบอินเทอร์ลีฟสำหรับตัวถอดรหัสแบบแบ่งส่วนโดยวิธีการปรับค่าความน่าเชื่อถือเส้นทาง

สมรรถนะอัตราเฟรมผิดพลาดของรหัสโพลาร์ร่วมกับ CRC แบบอินเทอร์ลีฟ ภายใต้ตัวถอดรหัสหักล้างต่อเนื่องแบบลิสหรือ $\mathrm{PSCL}(8,4)$ และ SCL(8) ร่วมกับวิธีการปรับความน่าเชื่อถือเส้นทางจะถูกจ าลองเพื่อเปรียบเทียบกับวิธีการถอดรหัสร่วมกับบิต CRC แบบอินเทอร์ลีฟแบบปกติ ซึ่งจะใช้งานรหัส CRC พหุนาม $g(x)=[1,1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1]$ ความยาวบิต CRC $r=16$ โดยรหัสโพลาร์จะความยาวคารหัส $N=64$ อัตรารหัส $R=1/2$ และขนาดลิส $L=8$ และแสดงกราฟสมรรถนะอัตราเฟรมผิดพลาดภายใต้ตัวถอดรหัส $\mathrm{PSCL}(8,8)$ และ SCL(8) ดังภาพที่ 5.9 และ 5.10 ตามล าดับ



ภาพที่ 5.9 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{PSCL}(8,4)$ ร่วมกับวิธีการปรับความน่าเชื่อถือเส้นทาง



ภาพที่ 5.10 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส SCL(8) ร่วมกับวิธีการปรับความน่าเชื่อถือเส้นทาง

โดยจะแสดงสมรรถนะอัตราเฟรมผิดพลาดของการนาวิธีการปรับค่าความน่าเชื่อถือเส้นทางมาใช้งานภายใต้ตัวถอดรหัส $\mathrm{PSCL}(8,4)$ และ SCL(8) โดยวิธีการปรับค่าความน่าเชื่อถือเส้นทางสามารถปรับปรุงสมรรถนะได้ ภายใต้ตัวถอดรหัสทั้งแบบแบ่งส่วนและแบบทั่วไป เนื่องจากมีการตัดสินใจบิต ณ ตาแหน่งบิตพาริตี แทนที่การแยกเส้นทางการถอดรหัส การตัดสินใจนี้สามารถเกิดขึ้นได้ทุกจุดภายใต้ตัวถอดรหัสทั้งแบบแบ่งส่วนและแบบทั่วไป โดยตัวถอดรหัส $\mathrm{PSCL}(8,4)$ วิธีการดังกล่าวสามารถให้สมรรถนะที่ดีกว่าวิธีการถอดรหัสทั่วไป 0.01 dB และตัวถอดรหัส SCL(8) สามารถให้สมรรถนะที่ดีกว่าวิธีการทั่วไปเล็กน้อย ผลของการเพิ่มสมรรถนะภายใต้วิธีการปรับค่าความน่าเชื่อถือเส้นทางนั้นขึ้นอยู่กับคุณสมบัติของตัวถอดรหัส ทั้งความยาวค ารหัส ความยาวบิตพาริตี และอื่น ๆ

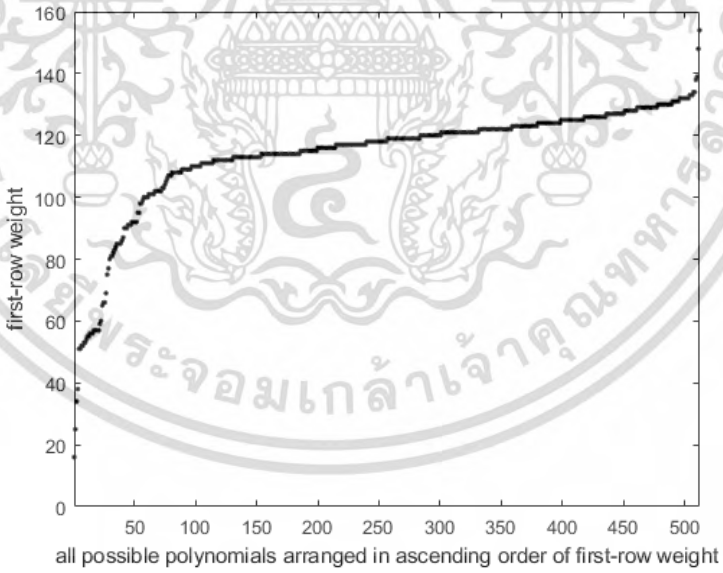
5.3 การออกแบบรหัส CRC แบบอินเทอร์ลีฟสำหรับตัวถอดรหัสแบบแบ่งส่วนและใช้วิธีการปรับค่าความน่าเชื่อถือเส้นทาง

เนื่องจากรหัส CRC แบบอินเทอร์ลีฟสามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดให้แก่ตัวถอดรหัสหักล้างต่อเนื่องแบบลิส รวมทั้งตัวถอดรหัสแบบแบ่งส่วนได้เช่นกันแล้ว วิทยานิพนธ์ได้นาเสนอการออกแบบพหุนาม CRC จากค่าน้าหนักแถวแรก เพื่อให้บิต CRC สามารถถูกกระจายไปยังส่วน

ด้านหน้าของตัวถอดรหัสได้มากขึ้น สาหรับรหัส CRC แบบอินเทอร์ลีฟ โดยตารางที่ 5.4 และได้แสดงกราฟเปรียบเทียบค่าน้าหนักแถวแรกของพหุนาม CRC ที่เป็นไปได้ทั้งหมดของรหัส CRC ความยาวบิต CRC $r=10$ บิต และความยาวบิตข้อมูล $m=256$ บิต ซึ่งมีความเป็นไปได้ทั้งหมดของพหุนาม CRC เท่ากับ $2^{r-1}=2^9=512$ รูปแบบ ดังภาพที่ 5.11

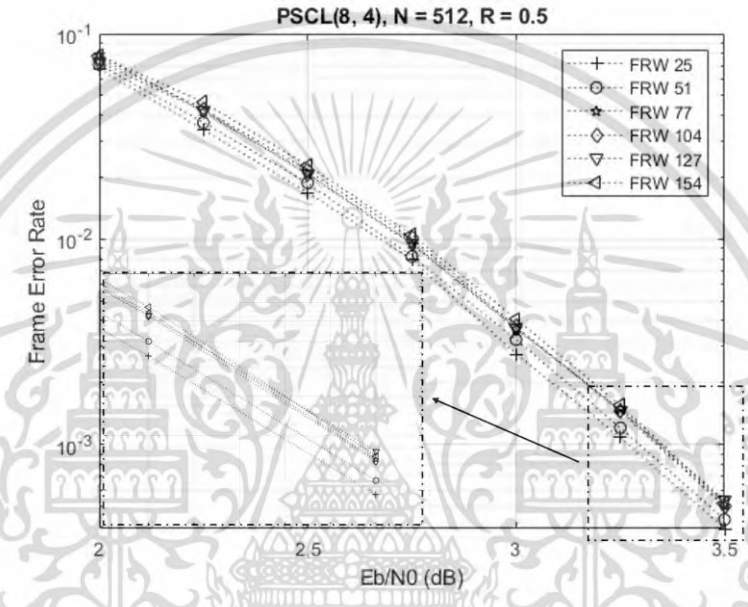
ตารางที่ 5.4 ตัวอย่างค่าน้าหนักแถวแรกของพหุนามกาเนิด CRC $g(x)$ ที่ความยาวบิต CRC $r=10$

ค่าสัมประสิทธิ์ของพหุนามก าเนิด $g(x)$	ค่าน้าหนักแถว (first row weight: FRW)
[1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1]	25
[1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1]	51
[1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1]	77
[1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1]	104
[1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1]	127
[1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1]	154

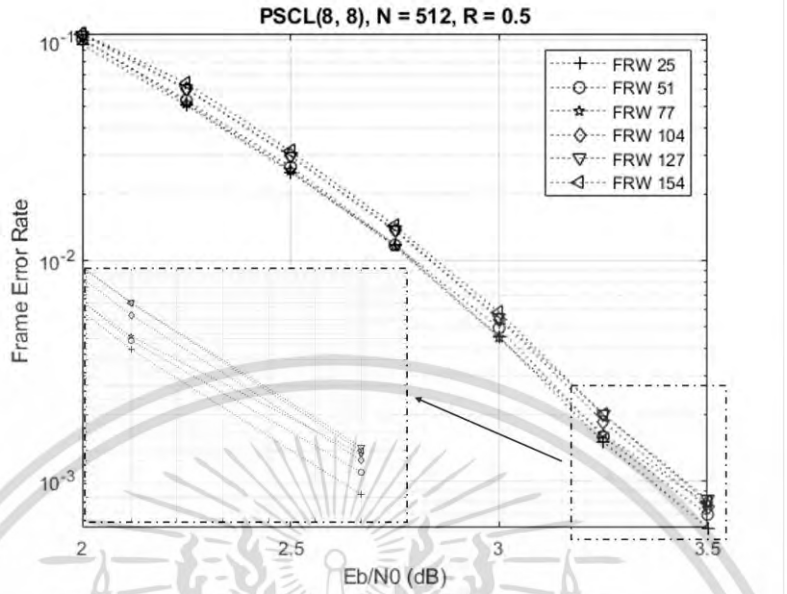


ภาพที่ 5.11 ค่าน้าหนักแถวแรกของพหุนามก าเนิด CRC ที่เป็นไปได้ทั้งหมดของรหัส CRC ที่มีความยาวบิต CRC $r=10$ บิต และความยาวบิตข้อมูล $m=256$ บิต

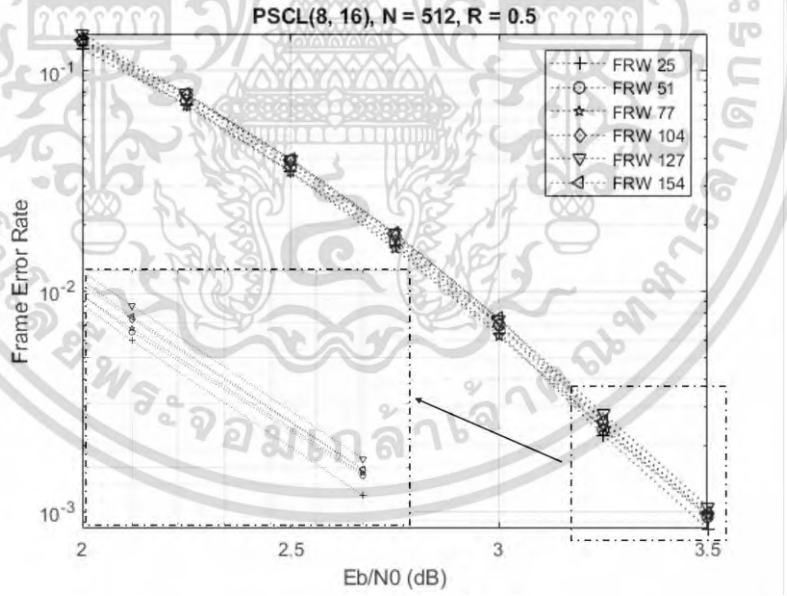
โดยจะแสดงสมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส PSCL ร่วมกับวิธีการปรับความน่าเชื่อถือ สาหรับรหัสโพลาร์ ซึ่งจะใช้งานรหัส CRC ที่มีค่าน้ำหนักแถวแรกแตกต่างกันตามตารางที่ 5.4 โดยรหัสโพลาร์จะความยาวค ารหัส $N=512$ อัตรารหัส $R=1/2$ และขนาดลิส $L=8$ และแสดงกราฟสมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{PSCL}(8,4)$ $\mathrm{PSCL}(8,8)$ และ $\mathrm{PSCL}(8,16)$ ดังภาพที่ 5.12 ถึง 5.14 ตามล าดับ



ภาพที่ 5.12 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{PSCL}(8,4)$ ที่ความยาวคารหัส $N=512$ อัตรารหัส $R=1/2$ ขนาดลิส $L=8$ และความยาวบิต CRC $r=10$ บิต



ภาพที่ 5.13 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{PSCL}(8,8)$ ที่ความยาวคารหัส $N=512$ อัตรารหัส $R=1/2$ ขนาดลิส $L=8$ และความยาวบิต CRC $r=10$ บิต



ภาพที่ 5.14 สมรรถนะอัตราเฟรมผิดพลาดของตัวถอดรหัส $\mathrm{PSCL}(8,16)$ ที่ความยาวคารหัส $N=512$ อัตรารหัส $R=1/2$ ขนาดลิส $L=8$ และความยาวบิต CRC $r=10$ บิต

โดยที่พหุนามที่มีค่าน้ำหนักแถวแรกต่ำนั้นให้สมรรถนะอัตราเฟรมผิดพลาดที่ดีกว่าพหุนามที่มีค่าน้ำหนักแถวแรกสูง โดยพหุนามที่มีค่าน้ำหนักแถวแรกเท่ากับ 25 ให้สมรรถนะที่ดีกว่าพหุนามที่มีค่าน้ำหนักแถวแรกเท่ากับ 154 กว่า 0.08 dB ที่อัตราเฟรมผิดพลาดเท่ากับ 10^{-3} ภายใต้ตัวถอดรหัสแบบแบ่งส่วนทั้งสามรูปแบบ $\mathrm{PSCL}(8,4)$ $\mathrm{PSCL}(8,8)$ และ $\mathrm{PSCL}(8,16)$ ร่วมกับวิธีการปรับความน่าเชื่อถือเส้นทาง

บทที่ 6
สรุปผลการวิจัย

6.1 สรุปผลการวิจัย

รหัสโพลาร์เป็นรหัสช่องสัญญาณที่ใช้แก้ไขความผิดพลาดของข้อมูลที่เกิดการรบกวนจากช่องสัญญาณ รหัสโพลาร์เป็นรหัสที่สามารถพิสูจน์ว่ามีสมรรถนะการแก้ไขความผิดพลาดเข้าใกล้ขีดจ ากัดของแชนนอน เช่นเดียวกับรหัสอื่น ๆ ทั้งรหัสแอลดีพีซีและรหัสเทอร์โบ อีกทั้งยังมีโครงสร้างแบบรีคลูซีฟที่เรียบง่าย จึงได้รับความสนใจในการวิจัยตั้งแต่นั้นมา รหัสโพลาร์ภายใต้การถอดรหัสหักล้างต่อเนื่องแบบลิสที่มี CRC ร่วมยังถูกนาเสนอว่าให้สมรรถนะที่เทียบเท่าหรือดีกว่ารหัสที่ทันสมัยอย่างเช่น รหัสแอลดีพีซี ในกรณีที่มีความยาวคารหัสสั้นถึงปานกลาง รหัสโพลาร์ดังกล่าวจึงถูกนาไปใช้งานในมาตรฐานการสื่อสารไร้สายยุคที่ 5 หรือมาตรฐาน 5G อย่างไรก็ตาม เมื่อความยาวคารหัสมีขนาดที่ยาวขึ้น รหัสโพลาร์ภายใต้การอดรหัสหักล้างต่อเนื่องแบบลิสจะมีความซับซ้อนเพิ่มขึ้นอย่างมาก ทั้งความซับซ้อนทางเวลา (คานวณนานขึ้น) และพื้นที่ (วงจรขนาดใหญ่ขึ้น ทั้งวงจรคานวณและหน่วยความจา) จึงมีหัวข้อการวิจัยเพื่อที่จะลดความซับซ้อนของการถอดรหัสโพลาร์เหล่านี้

หนึ่งในวิธีการที่จะลดความซับซ้อนในการถอดรหัสโพลาร์คือการถอดรหัสแบบแบ่งส่วน [] ซึ่งสามารถนามาใช้เพื่อลดขนาดหน่วยความจาของตัวถอดรหัสหักล้างต่อเนื่องแบบลิส โดยจะมีการลดเส้นทางการถอดรหัสในระหว่างขั้นตอนการถอดรหัส รวมทั้งมีเทคนิคการเก็บข้อมูลการถอดรหัสซ้าในพื้นที่เดิม โดยผลลัพธ์แสดงให้เห็นว่ามีการลดขนาดหน่วยความจาอย่างมาก แต่ก็แลกกับสมรรถนะการแก้ไขความผิดพลาดที่ลดลง ดังนั้นเพื่อที่จะชดเชยสมรรถนะที่สูญเสียไป วิทยานิพนธ์นี้ได้นาเสนอเทคนิคการใช้งานรหัส CRC ที่มีการอินเทอร์ลีฟกับตัวถอดรหัสแบบแบ่งส่วน เพื่อเพิ่มสมรรถนะการแก้ไขความผิดพลาด โดยบิต CRC จะมีตาแหน่งอยู่ในแต่ละส่วนตัวถอดรหัสช่วยในการเลือกตัดเส้นทางการถอดรหัส วิทยานิพนธ์ฉบับนี้ยังได้นาเสนอวิธีการถอดรหัสบิต CRC 2 วิธี ได้แก่ วิธีการตรวจสอบเส้นทางและวิธีการปรับค่าความน่าเชื่อถือเส้นทางที่สามารถเพิ่มสมรรถนะการแก้ไขความผิดพลาดจากการถอดรหัสบิต CRC รูปแบบดั้งเดิม นอกจากนี้การเลือกใช้งานพหุนาม CRC ยังส่งผลต่อตาแหน่งของบิต CRC อินเทอร์ลีฟในแต่ละส่วนตัวถอดรหัส ซึ่งจะส่งผลต่อสมรรถนะการแก้ไขความผิดพลาดเช่นเดียวกัน วิทยานิพนธ์ฉบับนี้ได้นาเสนอการเลือกใช้งานพหุนาม CRC จากค่าน้าหนักแถวแรกของเมทริกซ์พาริตีตรวจสอบของรหัส CRC ที่จะทาให้บิต CRC อินเทอร์ลีฟกระจายไปอยู่ในส่วนตัวถอดรหัสด้านหน้ามากขึ้น บิต CRC ที่กระจายไปยังส่วนด้านหน้าจะช่วยเลือกตัดเส้นทางการถอดรหัสของการถอดรหัสแบบแบ่งส่วนส่วนด้านหน้าได้ ช่วยให้ได้สมรรถนะที่ดีขึ้น

6.2 ข้อเสนอแนะ

สาหรับรหัส CRC ที่ใช้ภายใต้การถอดรหัสแบบแบ่งส่วนคาดว่าพิจารณาคุณสมบัติอื่นร่วมกันในการเลือกพหุนาม เช่น ค่าน้ำหนักแฮมมิง ที่ส่งผลต่อการปรับค่าความน่าเชื่อถือเส้นทางของเส้นทางการถอดรหัส ซึ่งส่งผลให้สมรรถนะการถอดรหัสดีขึ้นอย่างมาก นอกจากรหัส CRC แล้ว รหัสพาริตีตรวจสอบคาดว่าสามารถนามาใช้งานภายใต้การถอดรหัสแบบแบ่งส่วนได้อย่างดี เนื่องจากบิตพาริตีจะสามารถวางไว้ที่ตาแหน่งที่ต้องการได้อย่างยืดหยุ่น แต่ยังจาเป็นในการหาตาแหน่งที่เหมาะสมที่สุดในการวางตาแหน่ง รวมถึงความสัมพันธ์ระหว่างบิตพาริตีและบิตข้อมูลเช่นกัน

เอกสารอ้างอิง

[1] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal,* vol. 27, no. 3, pp. 379-423, 1948.

[2] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *Proceedings of ICC '93 - IEEE International Conference on Communications,* vol. 2, pp. 1064-1070, 1993.

[3] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory,* vol. 8, no. 1, pp. 21-28, 1962.

[4] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," *IEEE Transactions on Information Theory,* vol. 55, no. 7, pp. 3051-3073, 2009.

[5] K. Niu and K. Chen, "CRC-Aided Decoding of Polar Codes," *IEEE Communications Letters,* vol. 16, no. 10, pp. 1668-1671, 2012.

[6] I. Tal and A. Vardy, "List Decoding of Polar Codes," *IEEE Transactions on Information Theory,* vol. 61, no. 5, pp. 2213-2226, 2015.

[7] A. Alamdar-Yazdi and F. R. Kschischang, "A Simplified Successive-Cancellation Decoder for Polar Codes," *IEEE Communications Letters,* vol. 15, no. 12, pp. 1378-1380, 2011.

[8] C. Condo, V. Bioglio and I. Land, "Generalized Fast Decoding of Polar Codes," *2018 IEEE Global Communications Conference (GLOBECOM),* pp. 1-6, 2018.

[9] B. L. H. S. J. J. a. D. T. K. Chen, "Reduce the Complexity of List Decoding of Polar Codes by Tree-Pruning," *IEEE Communications Letters,* vol. 20, no. 2, pp. 204-207, 2016.

[10] L. L. J. Y. X. T. Z. Z. X. Y. a. C. Z. Yifei Shen, "Low-Latency Segmented List-Pruning Software Polar List Decoder," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 4, pp. 3575-3589, 2020.

[11] S. A. Hashemi, A. Balatsoukas-Stimming, P. Giard, C. Thibeault and W. J. Gross, "Partitioned successive-cancellation list decoding of polar codes," *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* pp. 957-960, 2016.

[12] S. A. Hashemi, M. Mondelli, S. H. Hassani, C. Condo, R. L. Urbanke and W. J. Gross, "Decoder Partitioning: Towards Practical List Decoding of Polar Codes," *IEEE Transactions on Communications,* vol. 66, no. 9, pp. 3749-3759, 2018.

[13] 3. G. P. Project, "Multiplexing and channel coding," 3GPP TS 38.212 v15.0.0, 2018.

[14] A. a. B. P. M. a. B. A. Balatsoukas-Stimming, "LLR-based successive cancellation list decoding of polar codes," *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* pp. 3903-3907, 2014.

[15] R. a. T. T. Mori, "Performance of Polar Codes with the Construction using Density Evolution," *IEEE Communications Letters,* vol. 13, no. 7, pp. 519-521, 2009.

[16] P. Trifonov, "Efficient Design and Decoding of Polar Codes," *IEEE Transactions on Communications,* vol. 60, no. 11, pp. 3221-3227, 2012.

[17] G. He, J.-C. Belfiore, I. Land, G. Yang, X. Liu, Y. Chen, R. Li, J. Wang, Y. Ge, R. Zhang and W. Tong, "Beta-Expansion: A Theoretical Framework for Fast and Recursive Construction of Polar Codes," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference,* pp. 1-6, 2017.

[18] W. W. Peterson and D. T. Brown, "Cyclic Codes for Error Detection," *Proceedings of the IRE,* vol. 49, no. 1, pp. 228-235, 1961.

[19] T. Wang, D. Qu and T. Jiang, "Parity-Check-Concatenated Polar Codes," *IEEE Communications Letters,* vol. 20, no. 12, pp. 2342-2345, 2016.

[20] H. Zhang, R. Li, J. Wang, S. Dai, G. Zhang, Y. Chen, H. Luo and J. Wang, "Parity-Check Polar Coding for 5G and Beyond," *2018 IEEE International Conference on Communications (ICC),* pp. 1-7, 2018.

[21] P. a. M. V. Trifonov, "Polar Subcodes," *IEEE Journal on Selected Areas in Communications,* vol. 34, no. 2, pp. 254-266, 2016.

[22] G. Sarkis, P. Giard, A. Vardy, C. Thibeault and W. J. Gross, "Fast Polar Decoders: Algorithm and Implementation," *IEEE Journal on Selected Areas in Communications,* vol. 32, no. 5, pp. 946-957, 2014.

[23] M. Hanif and M. Ardakani, "Fast Successive-Cancellation Decoding of Polar Codes: Identification and Decoding of New Nodes," *IEEE Communications Letters,* vol. 21, no. 11, pp. 2360-2363, 2017.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายอนุสรณ์ วงค์ษา
วัน เดือน ปีเกิด	09 มีนาคม พ.ศ. 2541 ที่นนทบุรี
ที่อยู่	47/345 ซอยงามวงศ์วาน 47 แยก 12 แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร
ประวัติการศึกษา	2561 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม (เกียรตินิยมอันดับหนึ่ง) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ผลงานวิจัยที่ได้นำเสนอในงานประชุมวิชาการ	1) A. Wongsa, W. Phakphisut, L. M. Min Myint and P. Supnithi, “Design of Partition Decoding for Polar Codes in 5G New Radio,” 2020 International Conference on Advanced Technologies for Communications (ATC), Nha Trang, Vietnam, 2020, pp. 199-204 2) A. Wongsa, L. M. M. Myint, P. Supnithi and W. Phakphisut, “Interleaved CRC Codes for Polar Codes with Partitioned List Decoding,” 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 2021, pp. 512-515