ประสิทธิภาพของการเข้ารหัสสัญญาณแบบบีซีเอชโค้ด โดยมีการใช้อินเทอร์ลีฟ

PERFORMANCE OF BCH-ENCODED SIGNAL WITH INTERLEAVING

นายดำรงค์ศักดิ์ พลพิทักษ์ชัย รหัส 50360999

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2553

ใบรับรองปริญญานิพนธ์

ชื่อหัวข้อโครงงาน	**ประสิทธิภาพของการเข้ารหัสสัญญาณแบบบีซีเอชโค้ด โดยมีการใช้อินเทอร์ลีฟ**
ผู้ดำเนินโครงงาน	นายดำรงค์ศักดิ์ พลพิทักษ์ชัย รหัส 50360999
ที่ปรึกษาโครงงาน	ผู้ช่วยศาสตราจารย์ ดร.สุรเชษฐ์ กานต์ประชา
สาขาวิชา	วิศวกรรมไฟฟ้า
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2553

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้ปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า

.....ที่ปรึกษาโครงงาน

(ผู้ช่วยศาสตราจารย์ดร. สุรเชษฐ์ กานต์ประชา)

.....กรรมการ

(ดร. ชัยรัตน์ พินทอง)

.....กรรมการ

(ดร. อัครพันธ์ วงค์กังแห)

ชื่อหัวข้อโครงงาน	ประสิทธิภาพของการเข้ารหัสสัญญาณแบบบีซีเอชโค้ด โดยมีการใช้อินเทอร์ลีฟ
ผู้ดำเนินโครงงาน	นายดำรงค์ศักดิ์ พลพิทักษ์ชัย รหัส 50360999
ที่ปรึกษาโครงงาน	ผู้ช่วยศาสตราจารย์ ดร.สุรเชษฐ์ กานต์ประชา
สาขาวิชา	วิศวกรรมไฟฟ้า
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2553

บทคัดย่อ

โครงงานนี้เป็นการศึกษาประสิทธิภาพของการเข้ารหัส BCH Code และผลของการใช้ Interleaver โดยการจำลองการส่งสัญญาณแบบ BPSK ในการศึกษาประสิทธิภาพนั้นจะใช้โปรแกรม MATLAB ในการจำลองการเข้ารหัสและถอดรหัส BCH Code โดยอาศัยส่งสัญญาณแบบ BPSK ซึ่งการหาประสิทธิภาพของการเข้ารหัส BCH Code จะใช้ค่า Bit error rate ในการวิเคราะห์เปรียบเทียบเพื่อหาประสิทธิภาพของการเข้ารหัส BCH Code แบบต่างๆ เพื่อเป็นกรณีศึกษาให้เลือกใช้การเข้ารหัส BCH Code ให้เหมาะสมกับช่องส่งสัญญาณ

ผลจากการจำลองพบว่าการเข้ารหัส BCH Code ได้ค่า Bit error rate ดีกว่าการส่งแบบ BPSK ที่ไม่มีการเข้ารหัสและการเข้ารหัส BCH Code แบบความยาวบล็อกโค้ต 31 บิตและบิตข้อมูล 11 บิต ที่สามารถแก้ไขความผิดพลาดได้ 5 บิตมีประสิทธิภาพดีที่สุดโดยที่ผลของ Interleaver มีผลน้อยมาก

Project title	Performance of BCH-encoded Signal with Interleaving
Name	Mr.Damroungsak Pholphitakchai ID. 50360999
Project advisor	Asst.Prof. Surachet Kanprachar, Ph.D.
Major	Electrical Engineering
Department	Electrical and Computer Engineering
Academic year	2010

Abstract

This project is to study the performance of the BCH-encoding and the effect of BCH-encoded signal with interleaver using the simulated transmitter BPSK. In the performance of the BCH-encoding, MATLAB program is used to simulate the encoding and decoding by BPSK transmitter. The efficiency of BCH-encoding will use the BER for analysis to find the efficiency of various BCH encoding of various BCH-encoding as a case study of the use of BCH-encoding to fit the channel signals.

The results from the simulation found that BER from BCH-encoding is better than the BPSK without coding. The BCH-encode signal with a code length of 31 bit and a data length of 11 bit, which can correct up to 5 error bit, perforns the best among all studied cases. Additionally, in the study of interleaving with BCH-encoding technique, it is found that interleaving does not improve the system performance.

กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างยิ่งของ ผศ.ดร. สุรเชษฐ์ กานต์ประชา อาจารย์ที่ปรึกษาโครงงานในการให้ความรู้และคำปรึกษาเกี่ยวกับการค้นหาข้อมูลและแนวทางการวิเคราะห์ต่างๆ ตลอดจนสละเวลาให้คำแนะนำทั้งภาคทฤษฎีและภาคปฏิบัติ ผู้จัดทำขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ ดร. ชัยรัตน์ พินทอง และดร.อัครพันธ์ วงศ์กังแห ที่กรุณาสละเวลาเป็นอาจารย์สอบโครงงาน

ขอขอบพระคุณบิดามารดาที่คอยให้คำแนะนำและกำลังใจในการเรียน

ผู้จัดทำจึงขอกราบขอบพระคุณเป็นอย่างสูง มา ณ โอกาสนี้

ดำรงศักดิ์ พลพิทักษ์ชัย

ผู้จัดทำโครงงาน

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของโครงงาน

ในปัจจุบันการติดต่อสื่อสารมีความสำคัญมากเกี่ยวเนื่องกับในชีวิตประจำวัน เช่น ด้านการศึกษา ด้านความบันเทิง การประกอบอาชีพ การรับทราบข่าวสารต่างๆ สิ่งเหล่านี้เป็นผลทำให้เกิดองค์ความรู้ใหม่ๆ และความต้องการที่จะพัฒนาเทคโนโลยีทางด้านการสื่อสารก็ยิ่งมีมากขึ้นเพื่อให้การติดต่อสื่อสารเกิดประสิทธิภาพสูงสุดในการใช้งาน

การสื่อสารด้วยระบบดิจิตอล (Digital Communication) มักพบปัญหาผิดพลาดของสัญญาณอันเนื่องมาจากปัญหาสัญญาณรบกวน สภาพแวดล้อม อุปกรณ์ที่ใช้ในการสื่อสารเอง เป็นผลทำให้การตีความข้อมูลที่ได้มาผิดพลาด ถ้าเป็นข้อมูลทางการเงินของธนาคารการผิดพลาดของข้อมูลก็อาจจะเป็นเรื่องใหญ่หรือเป็นข้อมูลสุขภาพของโรงพยาบาลหนึ่งส่งไปให้อีกโรงพยาบาลหนึ่ง การผิดพลาดของข้อมูลและนำไปใช้อาจเกิดความเสียหายที่ร้ายแรงได้

การแก้ไขปัญหาความผิดพลาดของการรับส่งข้อมูลสามารถทำได้หลายวิธีเช่น การส่งข้อมูลชุดเดิมไปหลายๆครั้ง เปลี่ยนช่องส่งสัญญาณ ตรวจสอบความผิดพลาดที่ปลายทางแล้วแก้ไขที่ปลายทาง ซึ่งแต่ละวิธีมีข้อดีข้อเสียต่างกันเช่นการส่งข้อมูลชุดเดิมไปหลายๆครั้งก็จะเสียพลังงานในการส่งเป็นเท่าตัวและเสียเวลาในการนำข้อมูลไปใช้งาน การเปลี่ยนช่องส่งสัญญาณในทางปฏิบัติสามารถทำได้ยากมาก การตรวจสอบข้อมูลที่ผิดพลาดโดยการเพิ่มบิตพิเศษทำให้สามารถตรวจสอบและแก้ไขข้อมูลที่ผิดพลาดได้เป็นวิธีการที่น่าสนใจข้อดีคือสิ้นเปลืองพลังงานที่จะส่งน้อยลงกว่าวิธีส่งข้อมูลชุดเดิมไปหลายๆครั้งและประหยัดเวลาในการนำจ้อมูลไปใช้งานแต่ข้อเสียคือสิ้นเปลือง Bandwidth มากขึ้น

โครงงานนี้ได้นำเสนอวิธีการหนึ่งที่ใช้ในการตรวจสอบและแก้ไขข้อมูลที่ผิดพลาดที่ปลายทางเรียกว่า BCH (Bose, Chaudhuri, and Hocquenghem) Code โดยการสร้างแบบจำลองในโปรแกรม MATLAB และทำมอดดูเลชันแบบ BPSK(Binary Phase Shift Keying)ส่งผ่านช่องส่งสัญญาณและใช้ Interleaver ในการช่วยแก้ไขความผิดพลาดที่เกิดขึ้น

1.2 วัตถุประสงค์ของโครงงาน

1)เพื่อศึกษาการมอดดูเลชั่นแบบ BPSK

2)เพื่อศึกษาการเข้ารหัสและถอดรหัสแบบ BCH Code

3)เพื่อศึกษาผลของสัญญาณเมื่อส่งผ่านช่องส่งสัญญาณและผ่านสัญญาณรบกวน

4)เพื่อศึกษาผลของการใช้ BCH Code เพียงอย่างเดียวและความแตกต่างระหว่างการใช้ Interleaver กับไม่ใช้ Interleaver ว่าแตกต่างกันอย่างไร

5)เพื่อศึกษาการเขียนโปรแกรมด้วย MATLAB

1.3 ขอบข่ายของโครงงาน

1)ศึกษาการทำมอดดูเลชันแบบ BPSK

2)ศึกษาการทำมอดดูเลชันแบบ BPSK และนำไปเข้ารหัสและถอดรหัสแบบ BCH Code

3)ศึกษาการทำมอดดูเลชันแบบ BPSK และนำไปเข้ารหัสและถอดรหัสแบบ BCH Code และผลของการทำ Interleaver

4)ศึกษาการเขียนโปรแกรม MATLAB

ตารางที่ 1.1 แผนการดำเนินงาน

แผนการดำเนินโครงการ	ปี 2553							ปี 2554		
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1)ศึกษาการทำมอดดูเลชันแบบ BPSKและการเข้ารหัสและถอดรหัสแบบ BCH Code										
2)ศึกษาวิธีการทำ Interleaver										
3)สร้างแบบจำลองการทำมอดดูเลชัน แบบ BPSKและการเข้ารหัสและถอดรหัสแบบ BCH Code โดยใช้โปรแกรม MATLAB										
4)สร้างแบบจำลองการใช้ Interleaver และศึกษาผลที่ได้ด้วยโปรแกรม MATLAB										
5)วิเคราะห์ผลที่ได้จากการทดลอง										
6)สรุปผลที่ได้จากการศึกษา										

1.5 ประโยชน์ที่คาดว่าจะได้รับจากโครงงาน

1)มีความรู้ความเข้าใจในการทำมอดดูเลชันแบบ BPSK

2)มีความรู้ความเข้าใจในการเข้ารหัสและถอดรหัสแบบ BCH Code

3)มีความรู้ความเข้าใจในการทำ Interleaver และผลของ Interleaver

4)มีความรู้ความเข้าการเขียนโปรแกรมขั้นพื้นฐาน

5)มีทักษะกระบวนการคิดที่มีเหตุมีผล

1.6 งบประมาณ

1.ค่าหนังสือ	400	บาท
2.ค่าจัดทำเอกสาร	400	บาท
3.ค่าพิมพ์เอกสาร	200	บาท
รวมทั้งสิ้น(หนึ่งพันบาทถ้วน)	1000	บาท

หมายเหตุ:ถัวเฉลี่ยทุกรายการ

บทที่ 2

หลักการเข้ารหัสและถอดรหัสแบบ BCH Code

BCH (Bose, Chaudhuri, and Hocquenghem) Code เป็นรหัสบล็อกโค้ดประเภทหนึ่งที่นำข้อมูลที่จะส่งมาแบ่งเป็นชุดข้อมูลขนาด k บิต และเพิ่มบิตพิเศษเข้าไปในแต่ละชุดข้อมูลเพื่อให้สามารถตรวจสอบบิตผิดพลาดได้ บิตพิเศษที่เพิ่มเข้าไปหาได้มากจากพีชคณิตช่องส่งสัญญาณที่เรียกว่า ฟิลด์กาลัว(Galois field) ในการใช้งานรหัส BCH Code มีประโยชน์มากเพราะมีความหลากหลายให้เลือกใช้ตามต้องการโดยสามารถออกแบบรหัส BCH Code ได้ว่าจะให้สามารถแก้ไขข้อมูลได้กี่บิตและแบ่งเป็นบล็อกข้อมูลละกี่บิต

2.1 การเข้ารหัสช่องส่งสัญญาณแบบบล็อกโค้ต (block code)[1]

ระบบรหัสบล็อกโค้ตข้อมูลที่จะทำการเข้ารหัสจะถูกแบ่งออกเป็นบล็อกขนาดเท่ากันจำนวน k บิต ซึ่งเขียนแทนด้วย $m=(m_0,m_1,m_2,...,m_{k-1})$ ในการเข้ารหัสจะนำบล็อกข้อมูลทั้งหมด k บิต ไปใช้ในการสร้างบิตพาริตีจำนวน $n-k$ บิต ซึ่งเขียนแทนด้วย $b=(b_0,b_1,b_2,...,b_{n-k-1})$ และเมื่อนำบิตข้อมูลและบิตพารีตีมาประกอบกันจะได้เป็นคำรหัส $c=(c_0,c_1,c_2,...,c_{n-1})$ ซึ่งสามารถเขียนเป็นความสัมพันธ์ได้ดังนี้

$$c_i=\begin{cases} b_i, & i=0,1,2,...,n-k-1 \\ m_{i+k-n}, & i=n-k,n-k+1,...,n-1 \end{cases} \tag{2.1}$$

นั่นคือ

$$(c_0,c_1,...,c_{n-k-1},c_{n-k},...,c_{n-1})=(b_0,b_1,...b_{n-k-1},m_0,m_1,...,m_{k-1}) \tag{2.2}$$

กระบวนการเข้ารหัสบล็อกโค้ตเป็นการแปลงข้อมูลจำนวน k บิต ให้เป็นคำรหัสที่มีความยาวเพิ่มขึ้นเป็น n บิต พิจารณารหัสบล็อกโค้ตให้ดีพบว่าการเข้ารหัสแต่ละครั้งต้องมีการพิจารณาบิตข้อมูลครั้งละ k บิต ซึ่งมีรูปแบบที่เป็นไปได้ทั้งหมดมากถึง 2^k รูปแบบเพราะฉะนั้นถ้าเราต้องการบรรจุรูปแบบทั้งหมดไว้ในหน่วยความจำเพื่อแปลงให้ได้คำรหัสที่เหมาะสมที่มีขนาดความยาว n บิตจะต้องอาศัยวงจรที่ซับซ้อนและหน่วยความจำที่มีขนาดใหญ่มากทำให้มีการพัฒนารหัสของบล็อกโค้ตที่มีคุณสมบัติพิเศษที่เรียกว่า คุณสมบัติเชิงเส้น(linear property)

หลักการที่สำคัญของรหัสบล็อกโค้ตเชิงเส้นอยู่ที่กรรมวิธีการคำนวณค่าของบิตพาริตี ซึ่งอาศัยหลักเกณฑ์ที่ตายตัวคือ ให้คำนวณจากบิตข้อมูลในลักษณะของการบวกเชิงเส้นในรูปแบบดังต่อไปนี้

$$b_j=p_{0,j}m_0+p_{1,j}m_1+p_{2,j}m_2+...+p_{k-1,j}m_{k-1} \text{ สำหรับ } j=0,1,2,3,...,n-k-1 \tag{2.3}$$

โดยสัมประสิทธิ์ p_{ij} จะมีค่าได้ 2 แบบเท่านั้น คือ 0 หรือ 1 ทั้งนี้ค่าของ p_{ij} จะกำหนดให้สอดคล้องกับความต้องการที่จะให้บิตพาริตี b_j มีความเกี่ยวพันกับบิตข้อมูลที่ m_i หรือไม่ นั่นคือถ้าไม่ต้องการให้มีความสัมพันธ์หรือขึ้นแก่กันก็กำหนด $p_{ij} = 0$ เพราะฉะนั้นจุดสำคัญของการเข้ารหัสจึงอยู่ที่กำหนด p_{ij} ที่เหมาะสมเพื่อให้ได้คุณสมบัติตามต้องการ

2.2 ทฤษฎีพีชคณิตพื้นฐานช่องส่งสัญญาณ

2.2.1 เซต (set) [2]

เซต (set) หมายถึง การรวบรวมสิ่งที่ไม่เฉพาะเจาะจง วัตถุเรื่องราวหรือเหตุการณ์โดยไม่รวมการกำหนดโอเปอร์เรชัน (operation) ระหว่างอีลิเมนต์ เซตสามารถแบ่งได้เป็น 2 ประเภทคือ เซตจำกัด (finite set) และ เซตไม่จำกัด (infinite set) เซตจำกัด หมายถึง เซตที่มีจำนวนอีลิเมนต์ในเซตเป็นจำนวนจำกัด เช่น เซตของมหาวิทยาลัยในประเทศไทย เป็นต้น ส่วนเซตไม่จำกัด หมายถึง เซตที่มีจำนวนอีลิเมนต์ในเซตไม่จำกัด เช่น เซตของจำนวนเต็ม เป็นต้น

2.2.2 กรุ๊ป (group) [3]

กรุ๊ป (group) หมายถึง เซตของอีลิเมนต์ G ที่มีการกำหนดโอเปอร์เรชัน "*" ระหว่างอีลิเมนต์ภายในเซต โดยโอเปอร์เรชันที่กำหนดขึ้นต้องมีคุณสมบัติดังต่อไปนี้จึงจะจัดว่าเป็นกรุ๊ป

1. คุณสมบัติปิด (Closure): $\forall a,b \in G : a*b \in G$
2. คุณสมบัติการเปลี่ยนกลุ่ม (Associativity): $\forall a,b,c \in G : a*(b*c) = (a*b)*c$
3. คุณสมบัติการมีเอกลักษณ์ (Identity): มี $\exists e \in G$: ที่ทำให้ $a*e = e*a = a$ สำหรับ $\forall a \in G$
4. คุณสมบัติการมีอินเวอร์ส (Inverse): $\forall a, a^{-1} \in G : a*a^{-1} = a^{-1}*a = e$
5. คุณสมบัติการสลับที่ (Commutativity): $\forall a,b \in G : a*b = b*a$

ในการสร้างกรุ๊ปที่มีจำนวนสมาชิกจำกัดนั้น โดยทั่วไปจะใช้ตัวเลขจำนวนเต็มเป็นสมาชิกและอาศัยการบวกและการคูณแบบมอดูโลเป็นโอเปอร์เรชันในการทำให้เซตของจำนวนเต็มมีสมาชิกจำกัดไม่เกินค่าที่ต้องการจะเขียนแทนด้วย $a+b = c \bmod d$ สำหรับการบวกและ $a \cdot b = c \bmod d$ สำหับการคูณค่าของ c ได้จากการบวกหรือคูณ a,b แล้วหารด้วย d แล้วเหลือเศษคือ c

ตัวอย่างที่ 2.1 จงพิสูจน์ว่าเซต {1,2,3,4} จัดเป็นกรุ๊ปภายใต้โอเปอร์เรชันการคูณแบบมอดูโล 5

วิธีทำ

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

2.2.3 อันดับของอีลิเมนต์ในกรุ๊ป (order of a group element) [2]

ให้ g เป็นอีลิเมนต์หนึ่งในกรุ๊ป G ภายใต้โอเปอร์เรชัน "*" อันดับของ g หรือ $ord(g)$ ให้มีค่าเท่ากับจำนวนเต็มที่เล็กที่สุดที่ทำให้ $g^{ord(g)}$ มีค่าเท่ากับอีลิเมนต์ที่เป็นเอกลักษณ์ของกรุ๊ป

ตัวอย่างที่ 2.2 จงหาอันดับของสมาชิกหรืออีลิเมนต์แต่ละตัวในกรุ๊ปของเซตจำกัด {1,2,3,4} ภายใต้โอเปอร์ชันการคูณแบบมอดูโล 5

วิธีทำ
$$\begin{aligned} 1^1 &= 1 \bmod 5 \\ 2^4 &= 1 \bmod 5 \\ 3^2 &= 1 \bmod 5 \\ 4^2 &= 1 \bmod 5 \end{aligned} \tag{2.4}$$

ฉะนั้น อีลิเมนต์ $g = 1,2,3,4$ มีอันดับ $ord(g) = 1,4,2,2$ ตามลำดับ

2.2.4 ซับกรุ๊ป(Subgroups) [2]

ภายใต้กรุ๊ป G ถ้าพิจารณาเฉพาะอีลิเมนต์บางส่วนของ G ที่มีจำนวนสมาชิกน้อยกว่ากรุ๊ป G แล้วพบว่าการประกอบกันของอีลิเมนต์เหล่านั้นมีคุณสมบัติครบตามเงื่อนไขของความเป็นกรุ๊ปแล้ว เราเรียกเซตของอีลิเมนต์ย่อยนั้นว่าเป็นซับกรุ๊ป (subgroup) สมมติให้ S เป็นซับเซตหรือเซตย่อยของ G ในการพิจารณาว่า S มีคุณสมบัติเป็นกรุ๊ปหรือไม่นั้นให้ตรวจสอบคุณสมบัติเพียงสามข้อคือ คุณสมบัติปิด คุณสมบัติการมีเอกลักษณ์ และคุณสมบัติอินเวอร์ ถ้ามีคุณสมบัติสามข้อให้จัดได้ว่า S เป็นซับกรุ๊ปของ G

2.2.5 ทฤษฎีบทของลากรองจ์ (Lagrange's theorem)[2]

ถ้า S เป็นซับกรุ๊ปของ G แล้ว $ord(G)$ หารด้วย $ord(S)$ ลงตัวโดยที่ $ord(G)$ และ $ord(S)$ แทนอันดับของกรุ๊ป S และ G ตามลำดับ

2.2.6 ริง(ring) [2]

ริง คือ กลุ่มของอีลิเมนต์ R ที่กำหนดโอเปอร์เรชันระหว่างอีลิเมนต์ 2 แบบคือการบวก "+" และการคูณ "×" โดยต้องมีคุณสมบัติต่อไปนี้

1. R เป็นกรุ๊ปที่มีคุณสมบัติการสลับที่ ภายใต้โอเปอร์เรชันการบวก + โดยมีอีลิเมนต์ 0 เป็นเอกลักษณ์การบวก
2. คุณสมบัติปิด ภายใต้โอเปอร์เรชันการคูณ $\forall a,b \in R : a \times b \in R$
3. คุณสมบัติการจัดหมู่ ภายใต้โอเปอร์เรชันการคูณ; $\forall a,b,c \in R : a \times (b \times c) = (a \times b) \times c$
4. คุณสมบัติการแจกแจง: $\forall a,b,c \in R : a \times (b + c) = a \times b + a \times c$

ริงจะมีคุณสมบัติการสลับที่ด้วยเมื่อเป็นไปตามเงื่อนไขต่อไปนี้

5. คุณสมบัติสลับที่ภายใต้โอเปอร์เรชันการคูณ $a \times b = b \times a$
6. คุฯสมบัติการมีเอกลักษณ์การคูณ และอีลิเมนต์ 1 เป็นเอกลักษณ์

ดังนั้นริงที่มีคุณสมบัติในข้อ 5 และ 6 ก็จะเรียนกว่า ริงที่มีคุณสมบัติสลับที่และมีเอกลักษณ์

2.2.7 ฟิลด์ (field) [2]

ฟิลด์คือ กลุ่มของอีลิเมนต์ F ที่มีการกำหนดโอเปอร์เรชันระหว่างอีลิเมนต์ 2 แบบคือ การบวก "+" และการคูณ "×" โดยที่มีคุณสมบัติต่อไปนี้

1. F เป็นกรุ๊ปที่มีคุณสมบัติการสลับที่ ภายใต้โอเปอร์เรชันการบวก + โดยมีอีลิเมนต์ 0 เป็นเอกลักษณ์การบวก

2. F-{0} เป็นกรุ๊ปที่มีคุณสมบัติการสลับที่ ภายใต้โอเปอร์เรชันการคูณ

3. คุณสมบัติการแจกแจง: $\forall a,b,c \in F : a \cdot (b+c) = a \cdot b + a \cdot c$

2.2.8 ฟิลด์กาลัว (Galois field) [2]

ฟิลด์กาลัว คือเซตที่มีจำนวนจำกัดและมีคุณสมบัติของความเป็นฟิลด์โดยทั่วไปจะใช้สัญลักษณ์ $GF(q)$ แทนฟิลด์ที่มีอันดับเท่ากับ q ฟิลด์กาลัวแบบง่ายสุดคือ $GF(2)$ ซึ่งเป็นเซตที่ประกอบด้วยสมาชิกของเพียง 2 ตัวคือ $\{0,1\}$ โดยมีโอเปอร์เรชันการบวกและการคูณเลขฐานสองดังนี้

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

เซตที่ประกอบด้วยจำนวนเต็ม $\{0,1,2,...,q-1\}$ โดย q เป็นจำนวนเฉพาะ จัดเป็นฟิลด์ $GF(q)$ ภายใต้โอเปอร์เรชันการบวกและการคูณแบบมอดูโล q

2.2.9 คุณสมบัติพื้นฐานของฟิลด์กาลัว

ฟิลด์กาลัวมีเฉพาะในรูปของ $GF(p^m)$ โดย p เป็นจำนวนเฉพาะและ m เป็นจำนวนเต็มมากกว่าเท่ากับศูนย์ เช่น $GF(2), GF(3), GF(4), GF(5), GF(7), GF(8), GF(9), GF(11)$ และ $GF(13)$ เป็นต้น นั่นคือจะไม่มีฟิลด์กาลัวที่มีอันดับต่างไปจากนี้อยู่เลยและมีคุณสมบัติดังต่อไปนี้

1. ให้ β เป็นอีลิเมนต์หนึ่งในฟิลด์กาลัว $GF(q)$ อันดับของ β หรือ $ord(\beta)$ นิยามให้มีค่าเท่ากับตัวเลขจำนวนเต็ม m ที่น้อยที่สุดที่ทำให้ $\beta^m = 1$

2. ถ้า $t = ord(\beta)$ โดย $\beta \in GF(q)$ แล้ว t หาร $(q-1)$ ลงตัว

2.2.10 พริมีทีฟอีลิเมนต์ [3]

ใน $GF(q)$ จะมีอันดับจำกัดอยู่เพียงบางค่าเท่านั้น และสำหรับในส่วนนี้เราจะพิจารณาและให้ความสนใจเป็นพิเศษกับอีลิเมนต์ที่มีอันดับเท่ากับ $q-1$ เพราะเป็นอีลิเมนต์ที่มีประโยชน์ต่อการศึกษาในส่านต่อไป

สำหรับอีลิเมนต์ในฟิลด์กาลัว $GF(q)$ ใด ที่มีอันดับเท่ากับ $q-1$ เราเรียกอีลิเมนต์นั้นว่า พริมีทีฟอีลิเมนต์ (primitive element)

ตัวอย่างที่ 2.3 จงแสดงว่า 2 และ 3 เป็นพริมีทีฟอีลิเมนต์ของฟิลด์กาลัว $GF(5)$

วิธีทำ นำ 2 และ 3 มายกกำลังค่าต่างๆได้ดังนี้

$$\begin{aligned} 2^1 &= 2 & 3^1 &= 3 \\ 2^2 &= 4 & 3^2 &= 9 = 4 \bmod 5 \\ 2^3 &= 8 = 3 \bmod 5 & 3^3 &= 27 = 2 \bmod 5 \\ 2^4 &= 16 = 1 \bmod 5 & 3^4 &= 81 = 1 \bmod 5 \end{aligned} \tag{2.5}$$

ข้อสังเกตสำคัญที่ได้จากตัวอย่างที่ 2.3 สมการที่ (2.5) คืออีลิเมนต์ทุกค่ายกเว้น 0 สามารถเขียนอยู่ในรูปพริมีทีฟอีลิเมนต์ยกกำลังด้วยค่าต่างๆ ตั้งแต่ 1 ถึง $q-1$ ซึ่งการเขียนแบบนี้มีความสำคัญมาก

ให้ α เป็นพริมีทีฟอีลิเมนต์อีลิเมนต์ในฟิลด์กาลัว $GF(q)$ สมาชิกหรืออีลิเมนต์อื่นสามารถเขียนได้เป็นลำดับดังนี้

$$1, \alpha^1, \alpha^2, \alpha^3, ..., \alpha^{q-2}, \alpha^{q-1}, \alpha^q, ...$$

เมื่อยกกำลังไปเลื่อยๆจนถึง $q-1$ ค่าที่ได้จะซ้ำค่าเดิมเริ่มจากตัวที่ $q-1$ จะเท่ากับ 1

การหาจำนวนของพริมีทีฟอีลิเมนต์ภายในฟิลด์กาลัว $GF(q)$ หนึ่งก็เป็นอีกประเด็นหนึ่งที่น่าสนใจ และสำหรับการหาค่าดังกล่าวสามารถทำได้โดยอาศัยฟังก์ชัน Euler จะสามารถหาได้ดังนี้

2.2.11 ฟังก์ชัน Euler $\Phi(t)$

ฟังก์ชัน Euler $\Phi(t)$คือ จำนวนของตัวเลขจำนวนเต็มที่อยู่ในเซต $\{1,2,...,t-1\}$ ซึ่งไม่มีตัวประกอบร่วมกันกับ t เลยนอกจาก 1 ฟังก์ชัน Euler $\Phi(t)$ สามารถนิยามได้ดังนี้

สำหรับ t=1

$$\Phi(t) = 1 \tag{2.6}$$

และสำหรับ t>1

$$\Phi(t) = |\{1 \le i < t\} | \gcd(i,t) = 1| \tag{2.7}$$

โดย gcd(i,t) หมายถึงค่าหารร่วมมาก (greatest common divisor) ของ i และ t

เราสามารถหาได้จากสูตร

$$\Phi(t) = t \prod_{p|t} \left(1 - \frac{1}{p}\right) \text{เมื่อ } p \text{ เป็นตัวเลขจำนวนเฉพาะค่าบวกที่น้อยกว่าและหาร } t \text{ ลงตัว} \tag{2.8}$$

ตัวอย่างที่ 2.4 จงคำนวณหาฟังก์ชัน Euler $\Phi(t)$ ที่ $t = \{2,3,4,5,6,7,8\}$

วิธีทำ

$$\begin{aligned} \Phi(2) &= 1 \quad \Phi(3) = 2 \\ \Phi(4) &= 2 \quad \Phi(5) = 4 \\ \Phi(6) &= 2 \quad \Phi(7) = 6 \\ \Phi(8) &= 4 \end{aligned} \tag{2.9}$$

เช่น $\Phi(6) = |\{1 \le i < 6\} | \gcd(i,6) = 1| = |\{1,5\}|$ (2.10)

$\Phi(8) = |\{1 \le i < 8\} | \gcd(i,8) = 1| = |\{1,3,5,7\}| = 4$ (2.11)

ถ้าใช้สูตรจะได้

$$\Phi(2)=2\left(1-\frac{1}{2}\right)=1$$
$$\Phi(3)=3\left(1-\frac{1}{3}\right)=2$$
$$\Phi(4)=\Phi(2\cdot 2)=4\left(1-\frac{1}{2}\right)=2 \quad (2.12)$$
$$\Phi(6)=\Phi(2\cdot 3)=6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=2$$

เป็นต้น

พิจารณาฟิลด์กาลัว $GF(q)$

1. ถ้า t ไม่สามารถหาร $q-1$ ได้ลงตัวแล้ว ก็จะไม่มีอีลิเมนต์ที่มีอันดับ t ใน $GF(q)$
2. ถ้า t หาร $q-1$ ลงตัว $(t \mid q-1)$ แล้วจะมีอีลิเมนต์ที่มีอันดับ t ทั้งหมด $\Phi(t)$ ตัว

2.2.12 พหุนามพริมีทีฟ [1]

พหุนาม $p(x)$ ที่มีสัมประสิทธิ์เป็นตัวเลขไบนารีจาก $GF(2)$ จะจัดว่าเป็นพหุนามไม่ลดรูป (irreducible) ถ้าพหุนามดังกล่าวไม่สามารถแยกตัวประกอบออกเป็นพหุนามที่มีดีกรีต่ำกว่าได้

ในการพิจารณาว่าพหุนามหนึ่งเป็นพหุนามพริมีทีฟหรือไม่นั้น ยังไม่มีวิธีลัดที่ช่วยในการตรวจสอบได้อย่างรวดเร็ว แต่เราสามารถแจกแจงพหุนามที่มีคุณสมบัติพริมีทีฟที่ดีกรีไม่สูงมากนักได้ดังนี้

ตารางที่ 2.1 แสดงรายละเอียดของพหุนามพริเมทีฟที่มีดีกรีตั้งแต่3-6

ดีกรี (m)	พหุนามพริมีทีฟ	
3	x^3+x+1	x^3+x^2+1
4	x^4+x+1	x^4+x^3+1
5	x^5+x^2+1	x^5+x^3+1
	$x^5+x^3+x^2+x+1$	$x^5+x^4+x^2+x+1$
	$x^5+x^4+x^3+x+1$	$x^5+x^4+x^3+x^2+1$
6	x^6+x+1	$x^6+x^4+x^3+x+1$
	x^6+x^5+1	$x^6+x^5+x^2+x+1$
	$x^6+x^5+x^3+x^2+1$	$x^6+x^5+x^4+x+1$

2.2.13 คุณสมบัติของพหุนามบน $GF(2)$ [2]

สำหรับพหุนาม $f(x)$ บน $GF(2)$ จะได้ว่า

$$[f(x)]^{2^j} = f\left(x^{2^j}\right) \tag{2.13}$$

โดยที่ j เป็นค่าจำนวนเต็มที่มากกว่าศูนย์

2.2.14 การสร้างฟิลด์กาลัว $GF(2^m)$ จาก $GF(2)$ [1]

การสร้าง $GF(2^m)$ จาก $GF(2)$ จะขออธิบายเป็นตัวอย่างต่อไปนี้

ตัวอย่างที่ 2.5 จงสร้าง $GF(2^m)$ ในรูปของพหุนามพาริมีทีฟ $p(x)=1+x+x^4$ บน $GF(2)$

วิธีทำ

กำหนดให้ α เป็นรากของพหุนาม $p(x)=1+x+x^4$ ที่มีคุณสมบัติพริมีทีฟบน $GF(2)$ ฉะนั้น

$$p(\alpha)=1+\alpha+\alpha^4=0 \text{ หรือ } \alpha^4=1+\alpha \tag{2.14}$$

โดยที่ $\alpha_0,\alpha_1,\alpha_2,...,\alpha_{m-1}$ คือสัมประสิทธิ์ของพหุนาม $\alpha_0+\alpha_1\alpha+\alpha_2\alpha^2+...+\alpha_{m-1}\alpha^{m-1}$

ตารางที่ 2.2 แสดงวิธีการหา $GF(2^m)$

แสดงวิธีแบบยกกำลัง		แสดงวิธีแบบพหุนาม	วิธีคำนวณ	แสดงเป็นไบนารี
0	=	0		0000
α^0	=	1		1000
α^1	=	α		0100
α^2	=	α^2		0010
α^3	=	α^3		0001
α^4	=	$1+\alpha$		1100
α^5	=	$\alpha+\alpha^2$	$\alpha\cdot\alpha^4=\alpha\cdot(1+\alpha)$	0110
α^6	=	$\alpha^2+\alpha^3$	$\alpha^2\cdot\alpha^4=\alpha^2(1+\alpha)$	0011
α^7	=	$1+\alpha+\alpha^3$	$\alpha^3\cdot\alpha^4=\alpha^3\cdot(1+\alpha)$	1101
α^8	=	$1+\alpha^2$	$\alpha^4\cdot\alpha^4$	1010
α^9	=	$\alpha+\alpha^3$	$\alpha\cdot\alpha^8=\alpha(1+\alpha^2)$	0101
α^{10}	=	$1+\alpha+\alpha^2$	$\alpha^2\cdot\alpha^8=\alpha^2(1+\alpha^2)$	1110
α^{11}	=	$\alpha+\alpha^2+\alpha^3$	$\alpha\cdot\alpha^{10}=\alpha(1+\alpha+\alpha^2)$	0111
α^{12}	=	$1+\alpha+\alpha^2+\alpha^3$		1111
α^{13}	=	$1+\alpha^2+\alpha^3$		1011
α^{14}	=	$1+\alpha^3$		1001

2.2.15 คุณสมบัติของฟิลด์กาลัว $GF(2^m)$ [2]

1. อีลิเมนต์ที่ไม่ใช้ศูนย์จำนวนทั้งหมด 2^m-1 ตัวของฟิลด์ $GF(2^m)$ คือรากทั้งหมดของพหุนาม $x^{2^m-1}+1$

2. อีลิเมนต์ทั้งหมด 2^m-1 ตัวของฟิลด์ $GF(2^m)$ เป็นรากทั้งหมดของพหุนาม $x^{2^m}+x$

2.2.16 พหุนามต่ำสุด[1]

อีลิเมนต์ 1 เป็นรากของพหุนามมากมายเช่น $x+1, x^2+1, x^4+x$ เป็นต้นแต่ที่เราสนใจคือพหุนามที่มีดีกรีต่ำสุดคือ x+1 นั้นเองและเรียนกพหุนามนั้นว่า "พหุนามต่ำสุด $\phi(x)$ ของอีลิเมนต์ 1 "และจะสามารถหาพหุนามต่ำสุดได้ดังนี้

ให้ $\phi(x)$ เป็นพหุนามต่ำสุดของ β ซึ่งเป็นอีลิเมนต์หนึ่งในฟิลด์ GF(2m) และให้ e เป็นจำนวนเต็มที่เล็กที่สุดที่ทำให้ $\beta^{2^e}=\beta$ จะได้ว่า

$$\phi(x)=\prod_{j=0}^{e-1}\left(x+\beta^{2^j}\right) \tag{2.15}$$

ตัวอย่างที่ 2.6 พิจารณาฟิลด์กาลัว $GF(2^4)$ ในตัวอย่างที่ 5 สมมติให้อีลิเมนต์ β ตัวหนึ่งที่เราสนใจคือ α^7 จงหาพหุนามต่ำสุดของอีลิเมนต์ β

วิธีทำ

ขั้นแรกให้คำนวณสังยุคของ β ซึ่งประกอบด้วย

$$\beta^2=\alpha^{14}, \beta^4=\alpha^{28}=\alpha^{13}, \beta^8=\alpha^{56}=\alpha^{11} \tag{2.16}$$

อาศัยทฤษฎีที่ 2.8 จะได้ว่าพหุนามต่ำสุดของ β มีค่าเป็น

$$\begin{aligned}\phi(x)=\prod_{j=0}^{e-1}\left(x+\beta^{2^j}\right)&=\left(x+\alpha^7\right)\left(x+\alpha^{11}\right)\left(x+\alpha^{13}\right)\left(x+\alpha^{14}\right)\\&=\left[x^2+\left(\alpha^7+\alpha^{11}\right)x+\alpha^7\alpha^{11}\right]\left[x^2+\left(\alpha^{13}+\alpha^{14}\right)x+\alpha^{13}\alpha^{14}\right]\\&=\left[x^2+\left(1+\alpha^2\right)x+\alpha^3\right]\left[x^2+\left(\alpha^2\right)x+\alpha^{12}\right]\\&=x^4+x^3+1\end{aligned} \tag{2.17}$$

2.3 การเข้ารหัสและถอดรหัส BCH Code[3]

2.3.1 การเข้ารหัส BCH Code

การเข้ารหัสของ BCH Code มีความยุงยากซับซ้อนตรงที่คำนวณหาพหุนามตัวกำเนิด g(x) ในที่นี้จะไม่กล่าวถึงรายละเอียดในการหาพหุนามกำเนิด g(x) จะนำมาใช้สามารถดูพหุนามกำเนิดได้ที่ภาคผนวก ก. มีขั้นตอนดังนี้

ขั้นตอนที่ 1 กำหนดความสามารถแก้ไขบิตผิดพลาด t บิต ในหนึ่งบล็อกความยาว n บิตและบิตข้อมูล k บิตทั้งสามอย่างนี้จะเป็นตัวกำหนดพหุนามกำเนิด g(x)

ขั้นตอนที่ 2 นำข้อมูลที่จะส่งมาคูณกับพหุนามกำเนิด g(x) แสดงดังตัวอย่างที่ 2.7

ตัวอย่างที่ 2.7 การเข้ารหัส BCH(15,5) ให้ข้อมูลเป็น 10010 สามารถหาพหุนามกำเนิดได้จากตารางภาคผนวกสำหรับ BCH(15,5) จะได้พหุนามกำเนิดคือ 10100110111

วิธีทำ

$$\begin{array}{cccccccccccccc} & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & \\ & & & & & & & & & 1 & 0 & 0 & 1 & 0 & \times \\ \hline & & & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & + \\ \hline 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}$$

Code word ที่จะส่งคือ 101100100011110

2.3.2 การถอดรหัส BCH [1]

มีขั้นตอนดังนี้

ขั้นตอนที่ 1 คำนวณหาค่าซินโดรม $s=(s_1,s_2,s_3,...,s_{2t})$ จากสัญญาณที่รับมา $r(x)$

ขั้นตอนที่ 2 คำนวณพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ จากเซตของซินโดรมที่ได้จากข้อ 1 สามารถคำนวณได้ 2 วิธีคือ 1) Peterson-Gorenstein-Zierler และ 2) Berlekamp-Massey

ขั้นตอนที่ 3 หาหมายเลขระบุตำแหน่งของความผิดพลาด $\beta_1,\beta_2,...,\beta_v$ ได้จากส่วนกลับของรากของพหุนาม $\sigma(x)$

ขั้นตอนที่ 4 คำนวณตำแหน่งของความผิดพลาด $j_1,j_2,j_3,...,j_v$ จาก $\beta_1,\beta_2,...,\beta_v$ ที่ได้จากข้อ3

ขั้นตอนที่ 5 คำนวณค่าความผิดพลาด $e_1,e_2,e_3,...,e_v$ ณ ตำแหน่งของความผิดพลาด $j_1,j_2,j_3,...,j_v$

ขั้นตอนที่ 6 แก้ไขคำรหัสให้ถูกต้องด้วยค่าความผิดพลาดที่คำนวณได้

จะแสดงเป็นตัวอย่างต่อไปนี้

ตัวอย่างที่ 2.8 จงหาพหุนามระบุตำแหน่งความผิดพลาดและถอดรหัส BCH (15,5) ซึ่งแก้ไขความผิดพลาดได้ 3 บิตที่ใช้พหุนามพริมีทีฟ $p(x)=1+x+x^4$ เมื่อพหุนามรหัสสที่รับคือ

$$r(x)=x^3+x^{10} \tag{2.18}$$

2.3.2.1 หาค่าของซินโดรม

หาซินโดรมจำนวนทั้งหมด $2t=2\times3=6$ ได้ดังนี้

$$\begin{aligned} s_1 &= r(\alpha)=\alpha^3+\alpha^{10}=\alpha^{12} \\ s_2 &= r(\alpha^2)=(\alpha^2)^3+(\alpha^2)^{10}=\alpha^6+\alpha^{20}=\alpha^9 \\ s_3 &= r(\alpha^3)=(\alpha^3)^3+(\alpha^3)^{10}=\alpha^9+\alpha^{30}=\alpha^7 \\ s_4 &= r(\alpha^4)=(\alpha^4)^3+(\alpha^4)^{10}=\alpha^{12}+\alpha^{40}=\alpha^3 \\ s_5 &= r(\alpha^5)=(\alpha^5)^3+(\alpha^5)^{10}=\alpha^{15}+\alpha^{50}=\alpha^{10} \\ s_6 &= r(\alpha^6)=(\alpha^6)^3+(\alpha^6)^{10}=\alpha^{18}+\alpha^{60}=\alpha^{14} \end{aligned} \tag{2.19}$$

2.3.2.2 คำนวณพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$

จากเซตของซินโดรมที่ได้จากข้อ 2.3.2.1 สามารถหาพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ แยกเป็นสองวิธี

2.3.2.2.1 Peterson-Gorenstein-Zierler

สมมติฐานว่าชุดสัญลักษณ์ที่รับมาได้มีจำนวนความผิดพลาด สูงสุด เท่ากับ $v = t = 3$ คือมีจำนวนสัญลักษณ์สูงสุดที่รหัสสามารถตรวจแก้ไขได้ จากนั้นคำนวณหาค่าดีเทอร์มิเนนต์ของเมทริกซ์ S

$$\begin{aligned}
\det(S) &= \det\begin{pmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \\ s_3 & s_4 & s_5 \end{pmatrix} = \det\begin{pmatrix} \alpha^{12} & \alpha^9 & \alpha^7 \\ \alpha^9 & \alpha^7 & \alpha^3 \\ \alpha^7 & \alpha^3 & \alpha^{10} \end{pmatrix} \\
&= \alpha^{12}\det\begin{pmatrix} \alpha^7 & \alpha^3 \\ \alpha^3 & \alpha^{10} \end{pmatrix} - \alpha^9\det\begin{pmatrix} \alpha^9 & \alpha^3 \\ \alpha^7 & \alpha^{10} \end{pmatrix} + \alpha^7\det\begin{pmatrix} \alpha^9 & \alpha^7 \\ \alpha^7 & \alpha^3 \end{pmatrix} \\
&= \alpha^{12}\left(\alpha^7\alpha^{10} - \alpha^3\alpha^3\right) - \alpha^9\left(\alpha^9\alpha^{10} - \alpha^7\alpha^3\right) + \alpha^7\left(\alpha^9\alpha^3 - \alpha^7\alpha^7\right) \\
&= \alpha^{29} + \alpha^{18} + \alpha^{28} + \alpha^{19} + \alpha^{19} + \alpha^{21} \\
&= \alpha^{14} + \alpha^3 + \alpha^{13} + \alpha^4 + \alpha^4 + \alpha^6 \\
&= \left(1 + \alpha^3\right) + \alpha^3 + \left(1 + \alpha^2 + \alpha^3\right) + \left(1 + \alpha\right) + \left(1 + \alpha\right) + \left(\alpha^2 + \alpha^3\right) \\
&= 0
\end{aligned} \tag{2.20}$$

จากการทดสอบพบว่าดีเทอร์มิเนนต์ที่ได้มีค่าเท่ากับ 0 ฉะนั้นความผิดพลาดที่เกิดขึ้นต้องน้อยกว่า 3 จึงสมมติฐานใหม่ให้ $v = 2$ จากนั้นหาค่าดีเทอร์มิเนนต์ของเมทริกซ์ S

$$\begin{aligned}
\det(S) &= \det\begin{pmatrix} s_1 & s_2 \\ s_2 & s_3 \end{pmatrix} = \det\begin{pmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & \alpha^7 \end{pmatrix} \\
&= \alpha^{12}\alpha^7 - \alpha^9\alpha^9 \\
&= \alpha^{19} - \alpha^{18} = \alpha^4 - \alpha^3 = 1 + \alpha + \alpha^3 \\
&= \alpha^7
\end{aligned} \tag{2.21}$$

ซึ่งพบว่ามีค่าไม่เป็นศูนย์ ฉะนั้นจึงสรุปว่าชุดสัญลักษณ์ที่รับได้มีความผิดพลาดเกิดขึ้น 2 สัญลักษณ์ จากนั้นให้หาเมทริกซ์ผกผันเพื่อแก้สมการหาค่าของ σ_1, σ_2 ตามความสัมพันธ์ต่อไปนี้

$$\begin{aligned}
\begin{bmatrix} s_1 & s_2 \\ s_2 & s_3 \end{bmatrix}\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} &= \begin{bmatrix} -s_3 \\ -s_4 \end{bmatrix} \\
\begin{bmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & \alpha^7 \end{bmatrix}\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} &= \begin{bmatrix} \alpha^7 \\ \alpha^3 \end{bmatrix}
\end{aligned} \tag{2.22}$$

โดยจะได้ผลดังนี้

$$\begin{aligned}
\sigma_1 &= \alpha^{12} \\
\sigma_2 &= \alpha^{13}
\end{aligned} \tag{2.23}$$

ฉะนั้นพหุนามระบุตำแหน่งความผิดพลาดมีค่าเท่ากับ

$$\sigma(x) = 1 + \alpha^{12}x + \alpha^{13}x^2 \tag{2.24}$$

2.3.2.2.2 Berlekamp-Massey

ตั้งค่าเริ่มเป็นดังนี้

$\mu = 0$

$\sigma(x) = 1$

$l = 0$

$\beta(x) = 0$

ขั้นตอนที่ 1 ให้ $\mu = \mu + 1$ และคำนวณกาค่า d จากสมการที่ (2.9)

$$d = s_{\mu} + s_{\mu+1}\sigma_1 + s_{\mu+2}\sigma_2 + \ldots + s_1\sigma_i \qquad (2.25)$$

ขั้นตอนที่ 2 ตรวจสอบถ้า $d = 0$ ไปทำขั้นตอนที่ 6 ถ้า $d \neq 0$ ทำขั้นตอนต่อไป

ขั้นตอนที่ 3 หา $\sigma'(x)$ จากสมการที่ (2.10)

$$\sigma'(x) = \sigma(x) + d\beta(x) \qquad (2.26)$$

ขั้นตอนที่ 4 ถ้า $2l < \mu$ ไปทำขั้นตอนที่ 5 ถ้าไม่ใช่ไปทำขั้นตอนที่ 6

ขั้นตอนที่ 5 ให้ $l = \mu - l$ และ $\beta(x) = d^{-1}\sigma(x)$ (2.27)

ขั้นตอนที่ 6 ให้ $\beta(x) = x\beta(x)$ (2.28)

ขั้นตอนที่ 7 ถ้า $\mu = 2t$ หยุดการทำงานไม่ใช้ไปทำขั้นตอนที่ 1 (2.29)

ตัวอย่างที่ 2.9 จากตัวอย่างที่ 2.8 หาค่าพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ โดยวิธีของ Berlekamp-Massey

กำหนดค่าเริ่มต้น

$\mu = 0$

$\sigma(x) = 1$

$l = 0$

$\beta(x) = 0$

$\mu = 1;$

$d = s_1 = \alpha^{12}$

$d \neq 0$ ต้องปรับ $\sigma(x)$

$\sigma'(x) = \sigma(x) + dx\beta(x)$

$\sigma'(x) = 1 + \alpha^{12}x[0]$

$\sigma'(x) = 1$

$2l = 0 < \mu = 1$

$\beta(x) = d^{-1}\sigma(x)$

$\beta(x) = \alpha^{3}$□1

$l = \mu - l = 1 - 0 = 1$

$\sigma(x) = \sigma'(x) = 1$

$\mu = 2;$

$d = s_2 + s_1\sigma_1$

$d = s_2 + s_1[0] = s_2 = \alpha^9$

$d \neq 0$ ต้องปรับ $\sigma(x)$

$\sigma'(x) = \sigma(x) + dx\beta(x)$

$\sigma'(x) = 1 + \alpha^9 x\alpha^3$

$\sigma'(x) = 1 + \alpha^{12}x$

$2l = 2 = \mu = 2$

$\beta(x) = x\beta(x)$

$\beta(x) = \alpha^3 x$

$l = \mu - l = 2 - 1 = 1$

$\sigma(x) = \sigma'(x) = 1 + \alpha^{12}x$

$\mu = 3;$

$d = s_3 + s_2\sigma_1$

$d = s_3 + s_2\alpha^{12} = \alpha^7 + \alpha^9\alpha^{12} = \alpha^{10}$

$d \neq 0$ ต้องปรับ $\sigma(x)$

$\sigma'(x) = \sigma(x) + dx\beta(x)$

$\sigma'(x) = 1 + \alpha^{12} + \alpha^{10}x[x\alpha^3]$

$\sigma'(x) = 1 + \alpha^{12}x + \alpha^{13}x^2$

$2l = 2 < \mu = 3$

$\beta(x) = d^{-1}\sigma(x)$

$\beta(x) = \alpha^5[1 + \alpha^{12}x] = \alpha^5 + \alpha^2 x$

$l = \mu - l = 3 - 1 = 2$

$\sigma(x) = \sigma'(x) = 1 + \alpha^{12}x + \alpha^{13}x^2$

$\mu = 4;$

$d = s_4 + s_3\sigma_1 + s_2\alpha_2$

$d = s_4 + s_3\alpha^{12} + s_2\alpha^{13} = \alpha^3 + \alpha^7\alpha^{12} + \alpha^9\alpha^{13} = 0$

$d = 0$ ไม่ต้องปรับ $\sigma(x)$

$\beta(x) = x\beta(x)$

$\beta(x) = x[\alpha^5 + \alpha^2 x] = \alpha^5 x + \alpha^2 x^2$

$\sigma(x) = \sigma'(x) = 1 + \alpha^{12}x + \alpha^{13}x^2$

$\mu = 5;$

$d = s_5 + s_4\sigma_1 + s_3\sigma_2$

$d = s_4 + s_4\alpha^{12} + s_3\alpha^{13} = \alpha^{10} + \alpha^{15} + \alpha^{20} = 0$

$d = 0$ ไม่ต้องปรับ $\sigma(x)$

$\beta(x) = x\beta(x)$

$\beta(x) = x[\alpha^5 x + \alpha^2 x^2] = \alpha^5 x^2 + \alpha^2 x^3$

$\sigma(x) = \sigma'(x) = 1 + \alpha^{12} x + \alpha^{13} x^2$

$\mu = 6$;

$d = s_6 + s_5\sigma_1 + s_4\sigma_2$

$d = s_4 + s_4\alpha^{12} + s_3\alpha^{13} = \alpha^{14} + \alpha^7 + \alpha = 0$

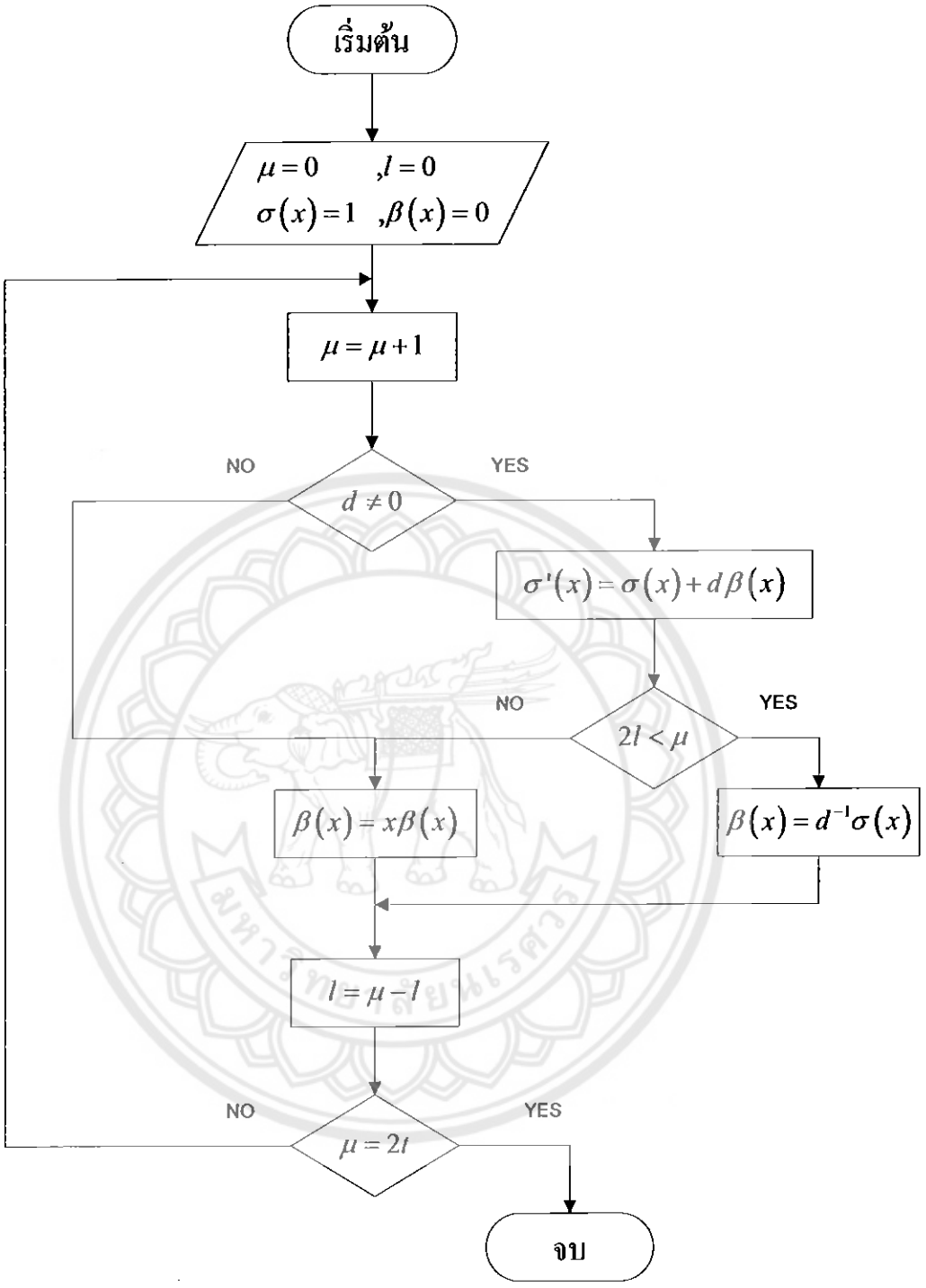
$d = 0$ ไม่ต้องปรับ $\sigma(x)$

$\beta(x) = x\beta(x)$

$\beta(x) = x[\alpha^5 x^2 + \alpha^2 x^3] = \alpha^5 x^3 + \alpha^2 x^4$

$\sigma(x) = \sigma'(x) = 1 + \alpha^{12} x + \alpha^{13} x^2$

จากตัวอย่างที่ 2.9 สามารถเขียน Flowchart วิธีการหาพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ ของ วิธี Berlekamp-Massey ได้แสดงดังรูปที่ 2.1



รูปที่ 2.1 แสดง Flowchart การหาพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ โดยวิธี Berlekamp-Massey

จากการหาสมการความผิดพลาดของข้อมูลทั้งสองวิธีจะเห็นได้ว่าวิธีของ Peterson-Gorenstein-Zierler นั้นง่ายต่อการคำนวณแต่หากความผิดพลาดเยอะขึ้นจะทำให้เกิดความยุ่งยากมากขึ้นวิธีการของ Berlekamp-Massey จะแก้ปัญหาเรื่องนี้ได้

2.3.2.3 การหาตำแหน่งความผิดพลาด

หารากพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)=1+\alpha^{12}x+\alpha^{13}x^2$ โดยการทดสอบหาว่าอีลิเมนต์ α^i ใดที่ทำให้ $\sigma(\alpha^i)$ มีค่าเท่ากับ 0 ดังนี้

$$\begin{aligned}\sigma(\alpha^0)&=1+\alpha^{12}\alpha^0+\alpha^{13}\alpha^0\\&=1+\alpha^{12}+\alpha^{13}=1+(1+\alpha+\alpha^2+\alpha^3)+(1+\alpha^2+\alpha^3)\\&=1+\alpha=\alpha^4\\\sigma(\alpha^1)&=1+\alpha^{12}\alpha^1+\alpha^{13}\alpha^2\\&=1+\alpha^{13}+\alpha^{15}=1+(1+\alpha^2+\alpha^3)+1\\&=1+\alpha^2+\alpha^3=\alpha^{13}\end{aligned} \tag{2.30}$$

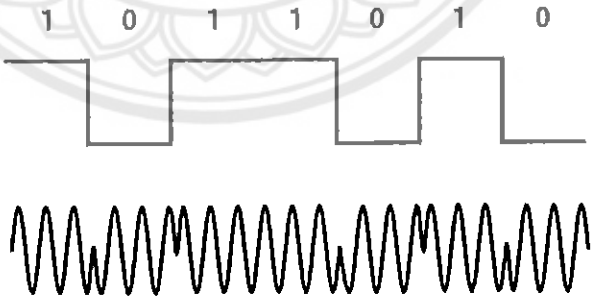
โดยการทดสอบเช่นนี้ไปเรื่อยจาก $i=0$ ถึง $i=14$ จะพบว่า α^5 และ α^{12} เท่านั้นที่ทำให้ $\sigma(x)$ มีค่าเป็น 0 จึงบอกได้ว่ามีความผิดพลาดเกิดขึ้นสองตำแหน่ง ซึ่งหาได้จากความสัมพันธ์ดังนี้

$$\begin{aligned}\beta_1&=\alpha^{-5}=\alpha^{15-5}=\alpha^{10}\\\beta_2&=\alpha^{-12}=\alpha^{15-12}=\alpha^3\end{aligned} \tag{2.31}$$

ดังนั้นตำแหน่งของความผิดพลาดของคำรหัสที่รับได้คือ ตำแหน่งที่ 3 และ 10

2.4 การมอดดูเลชั่นแบบ BPSK

หลักการการมอดดูเลชั่นแบบ BPSK คือค่าของขนาดและความถี่ของคลื่นพาห์จะไม่มีการเปลี่ยนแปลง แต่จะเปลี่ยนเฟสของสัญญาณเมื่อมีกาเปลี่ยนแปลงสภาวะของบิตจากบิต 0 ไปเป็นบิต 1 หรือจากบิต 1 ไปเป็นบิต 0 คลื่นจะเปลี่ยนเฟสไป 180° องศาแสดงดังรูปที่ 2.2



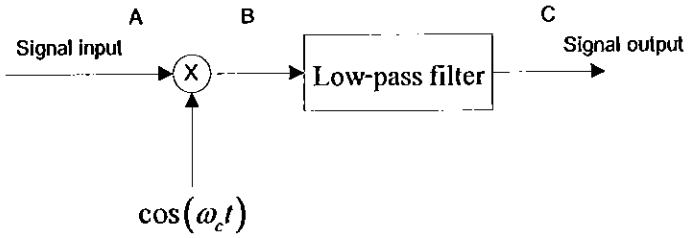
รูปที่ 2.2 แสดงการ Modulation แบบ BPSK

สมการของคลื่นพาห์แสดงดังสมการที่ (2.30)

$$v(t)=V\cos(\omega_c t+\phi(t)) \tag{2.32}$$

เมื่อ $\phi(t)$ คือเฟสของคลื่นพาห์มีค่าเปลี่ยนแปลงตามเวลา

หลักการดีมอดดูเลชั่นของ BPSK จะใช้ $\cos(\omega_c t)$ เข้ามาคูณกับสัญญาณและผ่าน Low-pass filter สามารถแสดงดังรูปที่ 2.3



รูปที่ 2.3 แสดงการดีมอดดูเลชั่นของ BPSK

จากรูปที่ 2.3 เมื่อรับสัญญาณมาทางจุด A จะเป็นดังสมการที่ (2.31)

$$signal\ input = A_c m(t)\cos(\omega_c t) \tag{2.33}$$

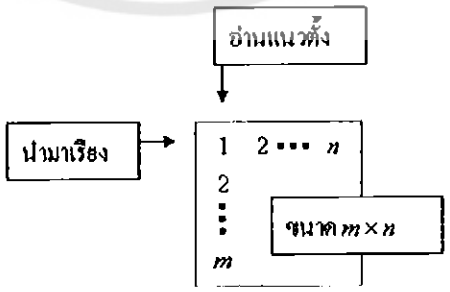
นำ $\cos(\omega_c t)$ มาคูณกับสัญญาณที่รับมา ที่จุด B จะได้เป็นสมการที่ (2.32)

$$\begin{aligned} s(t) &= A_c m(t)\cos(\omega_c t)\cos(\omega_c t) \\ &= A_c m(t)\cos^2(\omega_c t) \\ &= A_c m(t)\left[\frac{1}{2}+\frac{\cos(2\omega_c t)}{2}\right] \\ &= \frac{A_c m(t)}{2}+\frac{\cos(\omega_c t)}{2} \end{aligned} \tag{2.34}$$

จะเห็นได้ว่าพจน์ที่สองเป็นความถี่สูงเมื่อผ่าน Low-pass filter ก็จะได้สัญญาณที่จุด C ที่ต้องการ

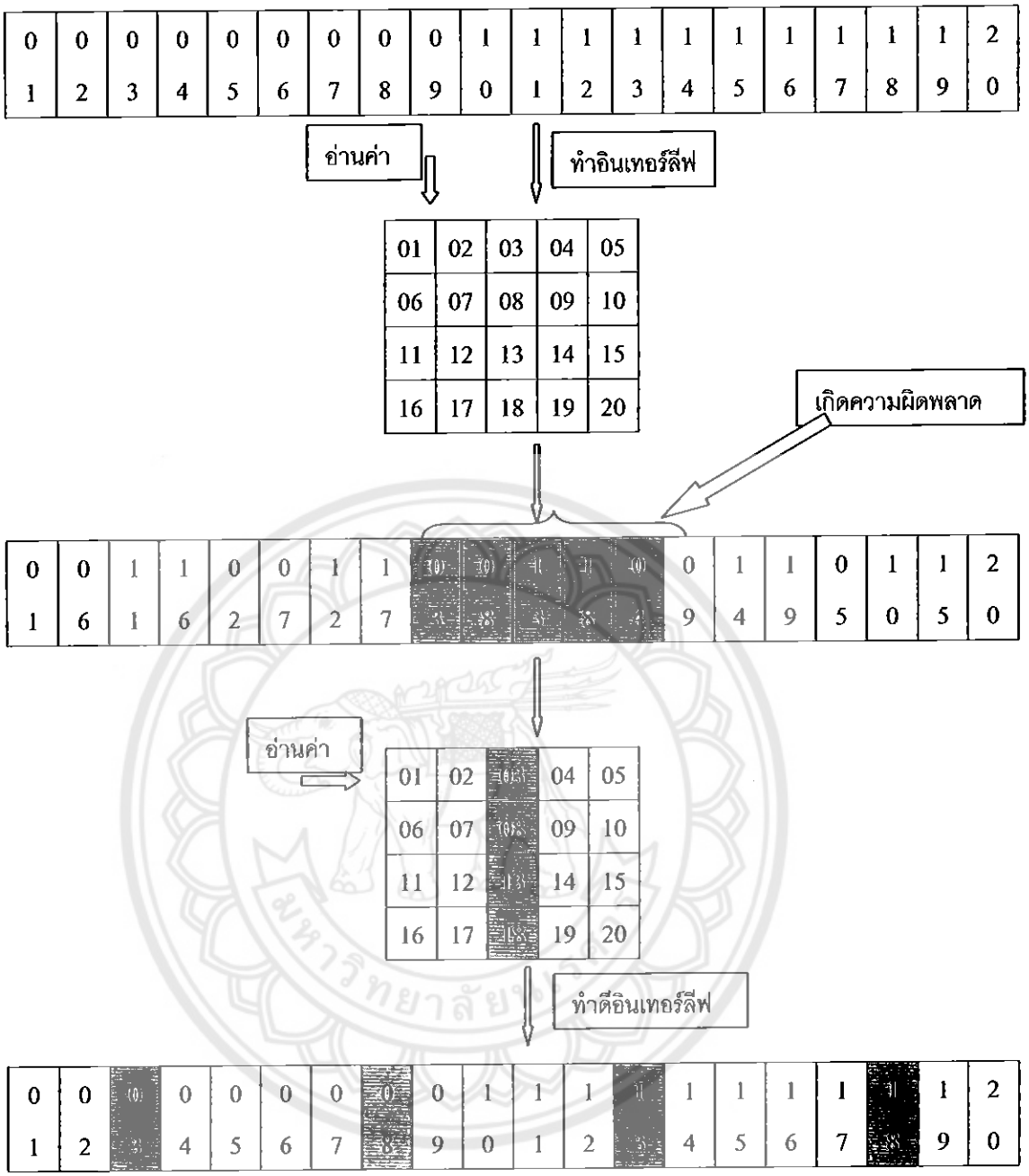
2.5 อินเทอร์ลีฟวิง(Interleaving)[1]

อินเทอร์ลีฟเป็นวิธีการช่วยแก้ไขบิตผิดพลาดอย่างต่อเนื่องวิธีการคือจะนำข้อมูลมาแบ่งเป็นบล็อกเล็กๆขนาด $m \times n$ บิต โดย m คือจำนวนแถวและ n คือจำนวนหลักแล้วนำข้อมูลที่จะส่งมาเรียงใส่ในบล็อกทีละแถวจนครบแล้วอ่านข้อมูลทีละหลักส่งออกไปสามารถแสดงดังรูปที่ 2.4



รูปที่ 2.4 แสดงการทำอินเทอร์ลีฟ

เมื่อมีการทำอินเทอร์ลีฟกับสัญญาณจากรูปที่ 2.4 เมื่อข้อมูลเกิดผิดพลาดติดกันยาวๆ และทำการดีอินเทอร์ลีฟออกมาข้อมูลที่เกิดผิดพลาดก็จะกระจายออกไปเมื่อใช้ร่วมกับการเข้ารหัสก็จะสามารถแก้ไขข้อมูลได้สามารถแสดงเป็นตัวอย่างได้ดังรูปที่ 2.5



รูปที่ 2.5 แสดงตัวอย่างการทำอินเทอร์ลีฟ

จากรูปที่ 2. 5 จะเห็นได้ว่าความผิดพลาดที่เกิดขึ้นจะมีการกระจายตัวออกไปเมื่อมีการเข้ารหัส BCH Code ร่วมด้วยจากที่จะผิดพลาดติดกันยาวๆแล้วไม่สามารถแก้ไขได้แต่เมื่อมีการทำอินเทอร์ลีฟก็จะสามารถแก้ไขได้เช่นถ้าข้อมูลมีการเข้ารหัส BCH(7,4) บิตข้อมูลที่ 03 และ 18 ก็จะสามารถแก้ไขได้จากข้อมูลชุดนี้จะผิดทั้งหมด 4 บิตโดยที่การเข้ารหัส BCH(7,4) ไม่สามารถแก้ไขความผิดพลาดได้เลยก็จะเหลือความผิดพลาดทั้งหมด 2 บิต ที่การเข้ารหัส BCH(7,4) สามารถแก้ไขความผิดพลาดนั้นได้แต่ผลของการทำอินเทอร์ลีฟนี้จะสามารถช่วยแก้ไขข้อมูลที่เกิดความผิดพลาด

ติดกันยาวๆ เท่านั้นถ้าเกิดข้อมูลมีการกระจายตัวอย่างอยู่แล้วผลของการทำอินเทอร์ลีฟจะไม่มีผลหรือมีผลของการทำอินเทอร์ลีฟน้อยมาก

ในบทที่ 2 ได้แสดงหลักการและทฤษฎีที่ใช้ในการเข้ารหัส BCH Code ในบทต่อไปจะแสดงวิธีการออกแบบโปรแกรมจำลองการส่งสัญญาณเพื่อหาประสิทธิภาพของการเข้ารหัส BCH Code และวิธีการที่ใช้ในการเปรียบเทียบเพื่อศึกษาการเข้ารหัส BCH Code

บทที่ 3
การออกแบบโครงงาน และวิธีการดำเนินงาน

จากบทที่ 2 เราได้ศึกษาพีชคณิตฯของช่องส่งสัญญาณและการเข้ารหัสและถอดรหัส BCH Code ในบทนี้จะกล่าวถึงการออกแบบและเขียนโปรแกรมเพื่อจำลองการเข้ารหัสและถอดรหัส BCH Code โดยใช้โปรแกรม MATLAB เพื่อศึกษาประสิทธิภาพของการเข้ารหัสและถอดรหัส BCH Code

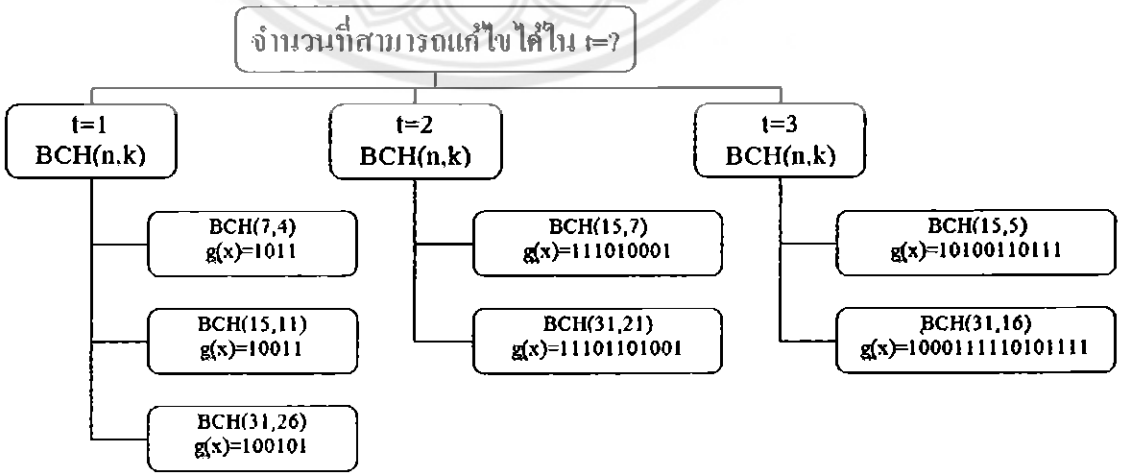
3.1 ขั้นตอนการออกแบบเขียนโปรแกรมเพื่อศึกษาการเข้ารหัส BCH Code

3.1.1 เขียนโปรแกรมสร้างสัญญาณ

ขั้นตอนที่ 1 ในระบบการสื่อสารระบบหนึ่งจะมีการส่งข้อมูลจากต้นทางไปยังปลายทาง และในการศึกษาประสิทธิภาพของการเข้ารหัส BCH Code จะสมมติข้อมูลที่จะส่งขึ้นมาโดยสร้างสัญญาณดิจิตอลและให้ความน่าจะเป็นที่มีบิต 0 หรือ บิต 1 มีโอกาสเกิดเท่าๆกัน

3.1.2 การออกแบบการเข้ารหัส BCH Code

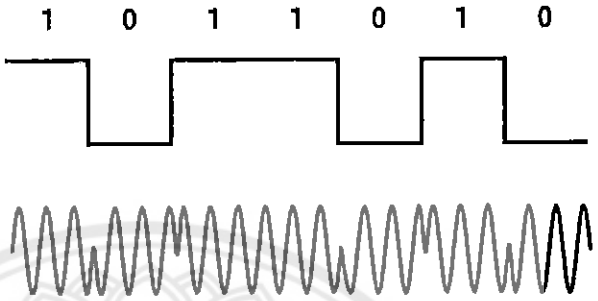
ขั้นตอนที่ 2 กำหนดจำนวนบิตที่จะสามารแก้ไขได้และเลือกความยาวของข้อมูลที่จะส่งแต่ละบล็อกขนาด n บิต ทั้งสองอย่างนี้จะเป็นตัวกำหนดจำนวนข้อมูลที่จะส่งในแต่ละบล็อกขนาด k บิตและพหุนามกำเนิดรหัส แล้วจะใช้ข้อมูลที่สร้างขึ้นจากขั้นตอนที่ 1 มาแบ่งเป็นบล็อกขนาด k บิตและนำไปคูณกับพหุนามกำเนิดรหัสเพื่อทำการเข้ารหัส BCH Code สามารถการออกแบบการเข้ารหัสแบบ BCH Code เป็นแผนภาพได้ดังรูปที่ 3.1



รูปที่ 3.1 แสดงการออกแบบการเข้ารหัส BCH Code

3.1.3 การมอดดูเลชั่นแบบ BPSK

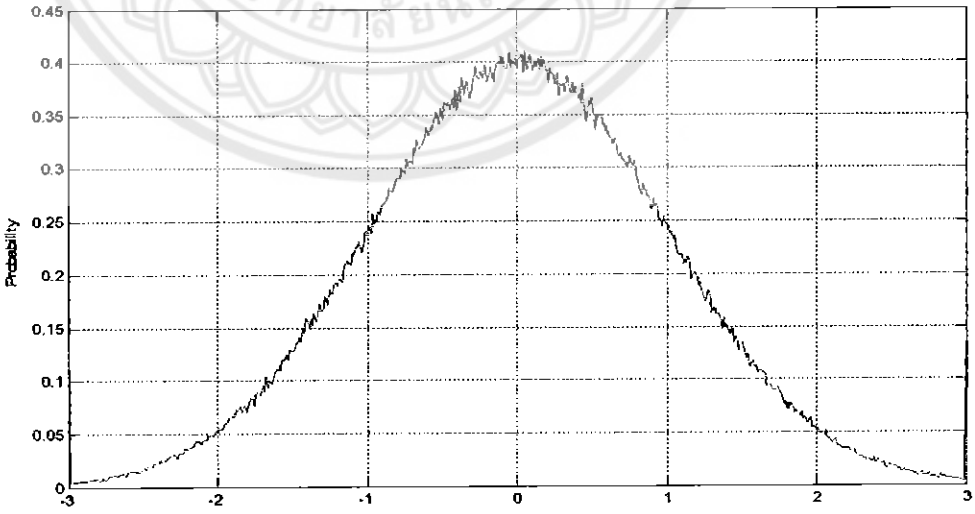
ขั้นตอนที่ 3 นำสัญญาณที่มีการเข้ารหัสแล้วมา Modulation เพื่อส่งข้อมูลออกไป การ Modulation นี้เราจะใช้การ Modulation แบบ BPSK คือเมื่อมีการกลับค่าบิตจากบิต 0 เป็นบิต 1 หรือจากบิต 1 เป็นบิต 0 เฟสก็จะกลับ 180 องศาแสดงดังรูปที่ 3.2



รูปที่ 3.2 แสดงการ Modulation แบบ BPSK

3.1.4 สร้างสัญญาณรบกวน

ขั้นตอนที่ 4 ในการศึกษาประสิทธิภาพของการเข้าแบบ BCH Code จำเป็นต้องเกิดการผิดพลาดของข้อมูลเพื่อจะดูว่าสามารถแก้ไขความผิดพลาดนั้นได้ดีหรือไม่ จะให้ความน่าจะเป็นที่ข้อมูลจะผิดพลาดมีการกระจายตัวแบบเกาเซียนแสดงดังรูปที่ 3.3 โดยการสุ่มแล้วนำไปบวกกับสัญญาณที่ทำการส่งออกมา



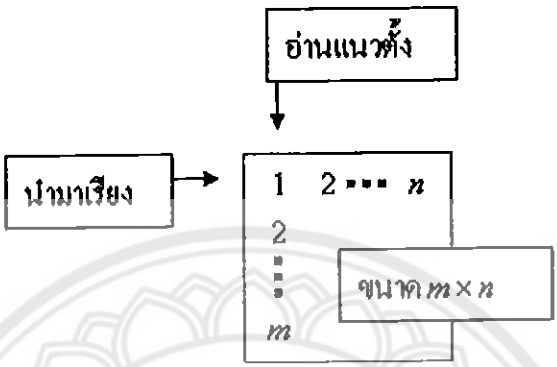
รูปที่ 3.3 แสดงความน่าจะเป็นของความผิดพลาดของข้อมูล

3.1.5 แก้ไขบิตผิดพลาดปลายทาง

ขั้นตอนที่ 5 ในภาครับสัญญาณมาจะทำการ Demodulation สัญญาณก่อนจากนั้นก็จะถอดรหัส BCH Code และแก้ไขข้อมูลที่ผิดพลาด

3.1.6 ทำ Interleave

ขั้นตอนที่ 6 ทำการทดสอบผลของการทำ Interleave โดยจะนำข้อมูลมาแบ่งเป็นบล็อกเล็กๆขนาด $m \times n$ บิต โดย m คือจำนวนแถวและ n คือจำนวนหลักแล้วนำข้อมูลที่จะส่งมาเลียงใส่ในบล็อกทีละแถวจนครบแล้วอ่านข้อมูลทีละหลักส่งออกไปสามารถแสดงได้ดังรูปที่ 3.4

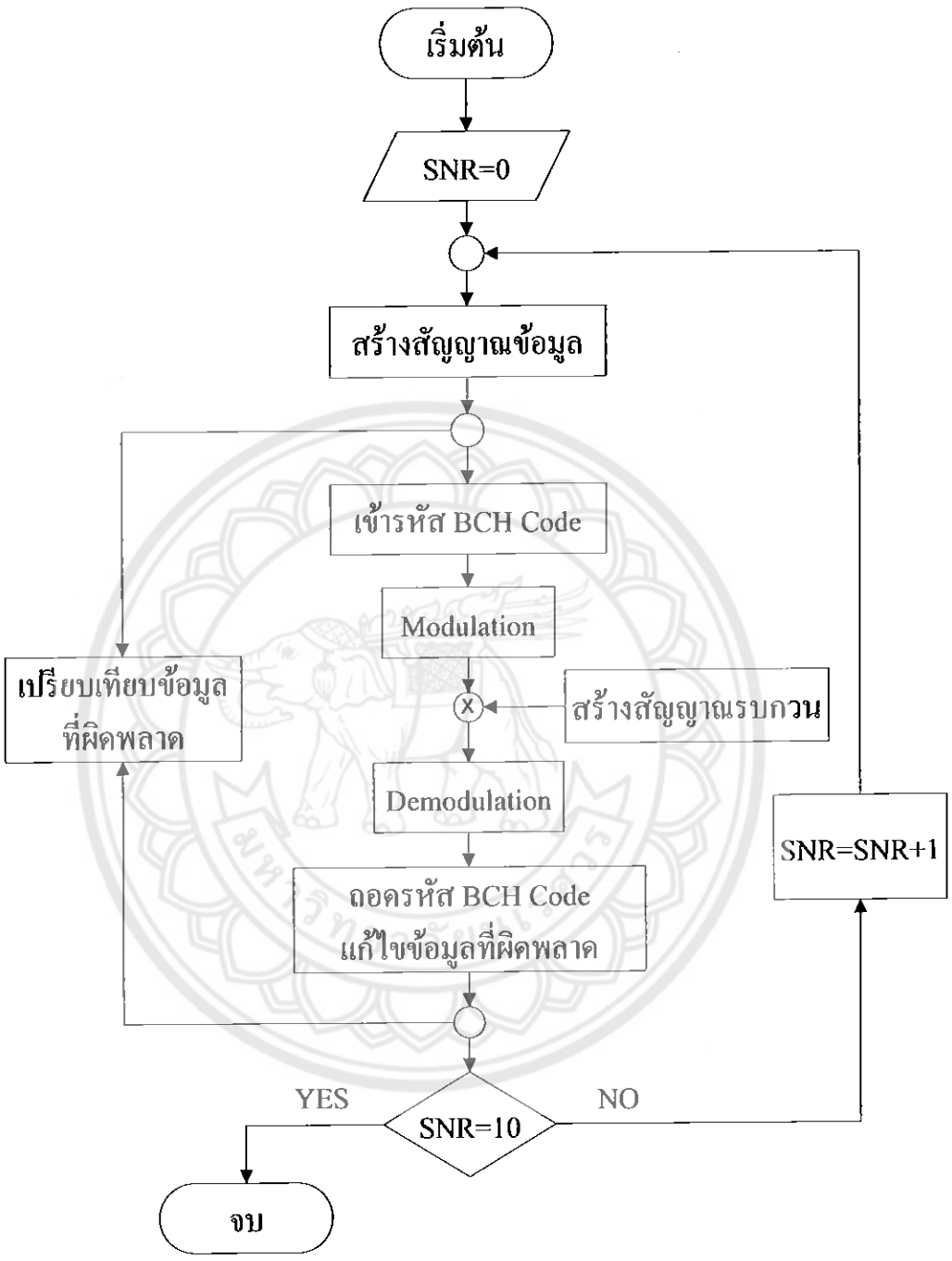


รูปที่ 3.4 แสดงการทำอินเทอร์ลีฟ

3.1.7 Flowchart แสดงการออกแบบโปรแกรมเพื่อจำลองการเข้ารหัส BCH Code

จากขั้นตอนการออกแบบโปรแกรมที่กล่าวมาแล้วสามารถเขียนเป็น Flowchart แสดงการออกแบบโปรแกรมทั้งหมดได้แสดงดังรูปที่ 3.5

Flowchart



รูปที่ 3.5 แสดง Flowchart การออกแบบโปรแกรม

จากรูปที่ 3.5 เป็นการออกแบบโปรแกรมเพื่อสร้างแบบจำลองในการเข้ารหัส BCH Code เพื่อหาประสิทธิภาพของการเข้ารหัส BCH Code โดยเริ่มจากการสร้างบิตข้อมูลก่อนจากนั้นทำการเข้ารหัส BCH Code แบบต่างๆจากนั้นจะทำการมอดดูเลชั่นแบบ BPSK และทำการส่งไปในช่องส่งสัญญาณ เมื่อถึงภาครับจะทำการดีมอดดูเลชั่นของ BPSK จากนั้นจะถอดรหัสและตรวจสอบข้อมูล

ต้นทางและปลายทางหาจำนวนบิตข้อมูลที่ผิดพลาดไปจากนั้นทำการเพิ่มค่าของ SNR แล้วก็จะสร้างบิตข้อมูลใหม่อีกครั้งทำเช่นนี้ไปจนครบตามที่กำหนด SNR ไวในที่นี้กำหนดไวที่ $10dB$

3.2 ออกแบบการทดลองเพื่อศึกษาประสิทธิภาพของการเข้ารหัส BCH Code

จากข้อที่ 3.1 ได้สร้างแบบจำลองเพื่อหาประสิทธิภาพของการเข้ารหัสแล้ว สำหรับการวิเคราะห์เปรียบเทียบเพื่อหาประสิทธิภาพของการเข้ารหัส BCH Code และผลของการใช้ อินเทอร์ลีฟสามารถแบ่งการพิจารณาออกเป็น 4 กรณีดังนี้

3.2.1 ออกแบบเปรียบเทียบประสิทธิภาพการแก้ไข 1 บิต

การเข้ารหัส BCH Code ที่สามารถแก้ไขความผิดได้ 1 บิต มีอยู่มากมายเพื่อหาประสิทธิภาพของการเข้ารหัส BCH Code ในจะทดสอบทั้งมด 3 กรณี โดยวิเคราะห์เปรียบเทียนความสามารถของการเข้ารหัส BCH Code ที่สามารถแก้ไขได้ 1 บิตทั้งหมด 3 กรณีคือ 1. BCH Code (7,4) 2. BCH Code (15,11) 3. BCH Code (31,26) โดยใช้กราฟ BER ในการเปรียบเทียบ

3.2.2 ออกแบบเปรียบเทียบประสิทธิภาพความยาวของบล็อกโค้ต 15 บิต

การเข้ารหัส BCH Code ที่มีความยาวของบล็อกโค้ต 15 บิต มีด้วยกัน 3 แบบคือ 1 BCH Code (15,11)ที่สามารถแก้ไขความผิดพลาดได้ 1 บิต 2. BCH Code (15,7)ที่สามารถแก้ไขความผิดพลาดได้ 2 บิต 3. BCH Code (15,5)ที่สามารถแก้ไขความผิดพลาดได้ 3 บิต เพื่อศึกษาประสิทธิของการเข้ารหัส BCH Code ที่มีความยาวของบล็อกโค้ต 15 บิต โดยวิเคราะห์เปรียบเทียนความสามารถของการเข้ารหัส BCH Code ที่ $n = 15$ บิต ทั้งหมด 3 กรณี คือ 1 BCH Code (15,11) 2. BCH Code (15,7) 3. BCH Code (15,5) โดยใช้กราฟ BER ในการเปรียบเทียบ

3.2.3 ออกแบบเปรียบเทียบประสิทธิภาพความยาวของบล็อกโค้ต 31 บิต

การเข้ารหัส BCH Code ที่มีความยาวของบล็อกโค้ต 31 บิต มีด้วยกัน 5 แบบคือ 1 BCH Code (31,26))ที่สามารถแก้ไขความผิดพลาดได้ 1 บิต 2. BCH Code (31,21))ที่สามารถแก้ไขความผิดพลาดได้ 2 บิต 3. BCH Code (31,16))ที่สามารถแก้ไขความผิดพลาดได้ 3 บิต 4. BCH Code (31,11))ที่สามารถแก้ไขความผิดพลาดได้ 5 บิต 5. BCH Code (31,6))ที่สามารถแก้ไขความผิดพลาดได้ 7 บิต เพื่อศึกษาประสิทธิของการเข้ารหัส BCH Code ที่มีความยาวของบล็อกโค้ต 31 บิต โดยวิเคราะห์เปรียบเทียนความสามารถของการเข้ารหัส BCH Code ที่ $n = 31$ บิต ทั้งหมด 5 กรณี คือ 1 BCH Code (31,26) 2. BCH Code (31,21) 3. BCH Code (31,16) 4. BCH Code (31,11) 5. BCH Code (31,6)โดยใช้กราฟ BER ในการเปรียบเทียบ

3.2.4 ออกแบบเปรียบเทียบผลของ Interleave

ในการสื่อสารมักพบปัญหาข้อมูลเกิดผิดพลาดติดกันยาวๆ จนเกินความสามารถของการเข้ารหัสBCH Code วิธีการที่นำมาแก้ไขปัญหานี้คือการทำ Interleave การใช้ Interleave นี้จะมีผลมากหรือน้อยจะศึกษาเปรียบเทียบการเข้ารหัส BCH Code ที่มีการใช้ Interleave และการเข้ารหัส

BCH Code ที่ไม่มีการใช้ Interleave โดยวิเคราะห์เปรียบเทียบกรณีที่ใช้ Interleave และไม่ใช้ Interleave ในกรณีความยาวบล็อกโค้ด 7 บิต และ 15 บิตโดยใช้กราฟ BER ในการเปรียบเทียบ

ในบทที่ 3 ได้แสดงหลักการออกแบบโปรแกรมจำลองการส่งสัญญาณเพื่อศึกษาประสิทธิภาพของการเข้ารหัส BCH Code ในบทต่อไปจะแสดงผลจากการทดลองโปรแกรมที่จำลองการส่งสัญญาณเพื่อทดสอบประสิทธิภาพของการเข้ารหัส BCH Code ที่ได้ออกแบบไว้ในบทนี้และวิเคราะห์เปรียบเทียบผลจากการคำนวณตามทฤษฎี

บทที่ 4
ผลการดำเนินโครงงาน

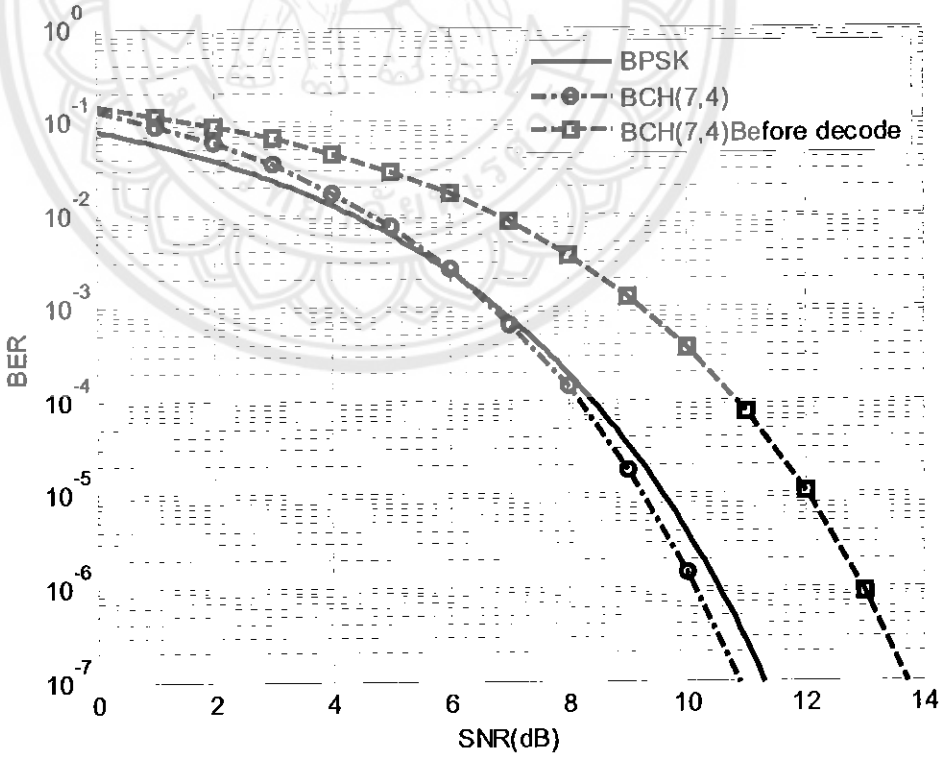
ในบทนี้จะกล่าวถึงผลจากการ Simulate การเข้ารหัส BCH Code เพื่อวิเคราะห์เปรียบเทียบประสิทธิภาพของการเข้า BCH Code ที่สามารถแก้ไขบิตผิดพลาดได้ 1 บิต ความยาวบล็อกโค้ต 15 บิต 31 บิตและผลของการใช้ Interleaver โดยใช้กราฟของ Bit error rate ในการวิเคราะห์เปรียบเทียบระหว่างค่าของ Bit error rate ของกราฟที่ยังไม่ได้ถอดรหัสกับกราฟที่ถอดรหัสแล้ว

4.1 ประสิทธิภาพของ BCH Code ที่สามารถแก้ไขได้ 1 บิต

การวิเคราะห์เปรียบเทียบเพื่อหาประสิทธิภาพการเข้ารหัส BCH จะเริ่มจากความสามารถของ BCH Code ที่สามารถแก้ไขได้ 1 บิตที่มีความยาวบล็อกโค้ต 7 บิต 15 บิต 31 บิต

4.1.1 ประสิทธิภาพของ BCH(7,4)

ผลจากการ Simulate การเข้ารหัส BCH(7,4) ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.1

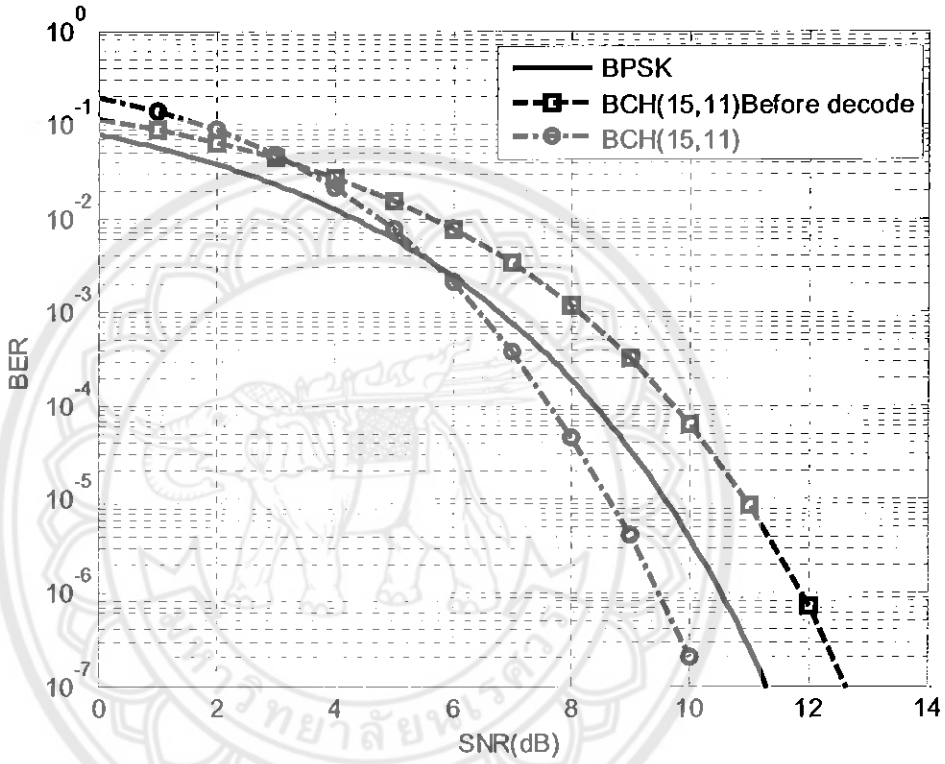


รูปที่ 4.1 แสดง Bit error rate การเข้ารหัส BCH(7,4)

จากกราฟรูปที่ 4.1 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $3dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.1.2 ประสิทธิภาพของ BCH(15,11)

ผลจากการ Simulate การเข้ารหัส BCH(15,11) ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.2

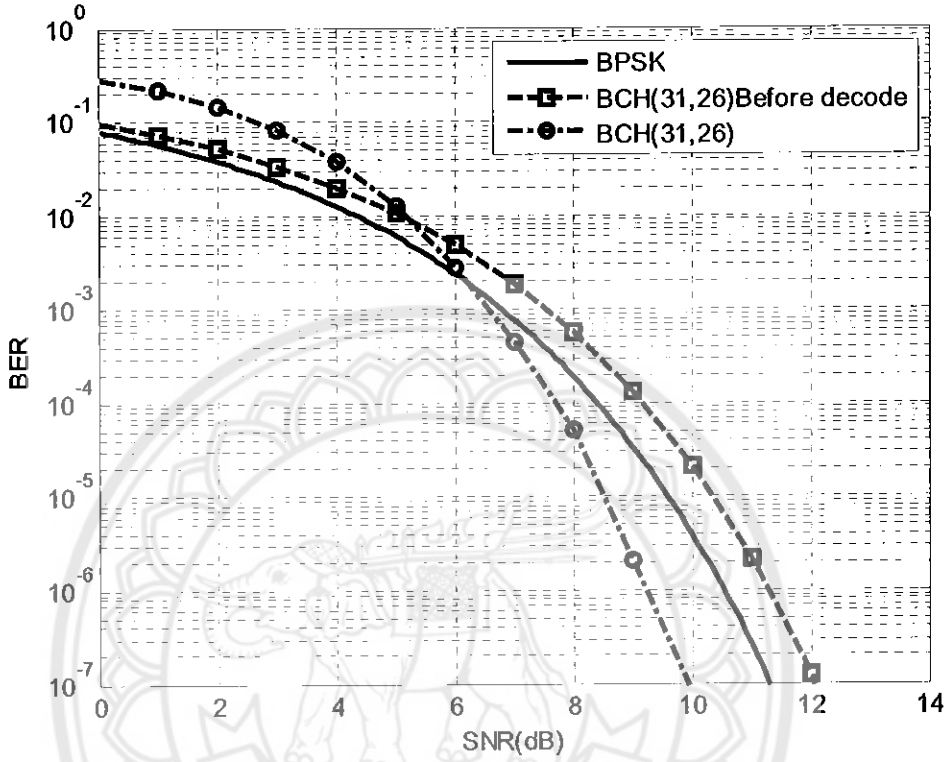


รูปที่ 4.2 แสดง Bit error rate การเข้ารหัส BCH(15,11)

จากกราฟรูปที่ 4.2 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $2.5dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.1.3 ประสิทธิภาพของ BCH(31,26)

ผลจากการ Simulate การเข้ารหัส BCH(31,26) ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.3



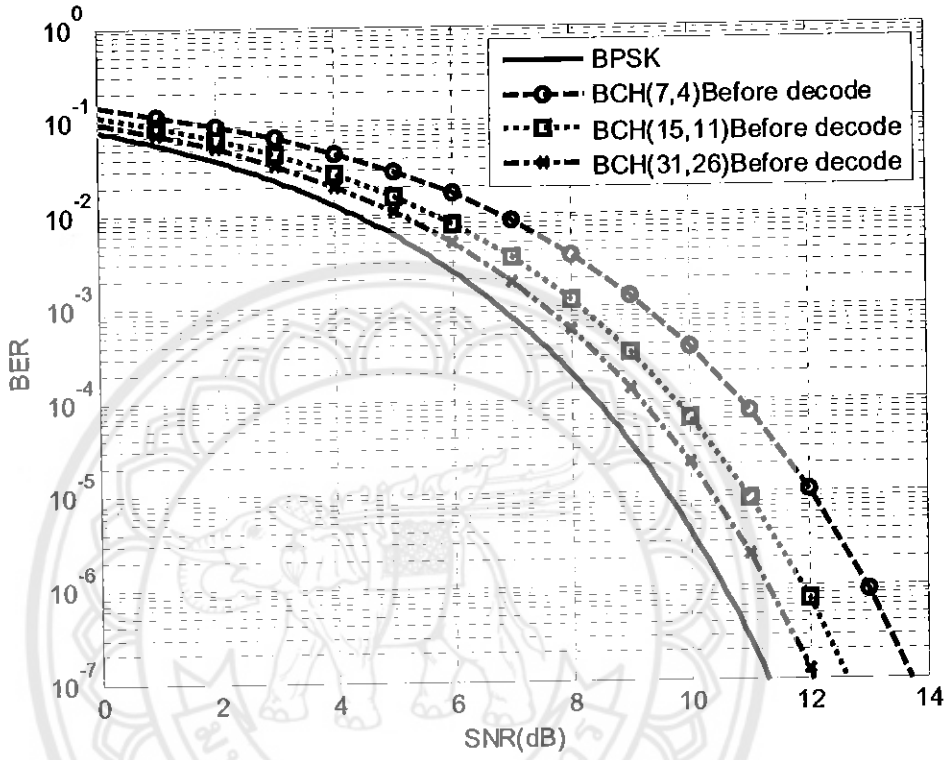
รูปที่ 4.3 แสดง Bit error rate การเข้ารหัส BCH(31,26)

จากกราฟรูปที่ 4.3 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $2dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

จากการ simulate การเข้ารหัส BCH (7,4) (15,11)และ(31,26) พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit- error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสสำหรับ BCH(7,4) ลดลงมากที่สุดและ BCH(15,11) BCH(31,26)ตามลำดับ

4.1.4 เปรียบเทียบการเข้ารหัส BCH Code สำหรับกรณีแก้ไขบิตผิดพลาดได้ 1 บิต

ผลจากการ Simulate การเข้ารหัส BCH Code ก่อนถอดรหัสสำหรับกรณีแก้ไขบิตผิดพลาดได้ 1 บิตแสดงดังรูปที่ 4.4



รูปที่ 4.4 แสดง Bit error rate ที่ยังไม่มีการถอดรหัสของ BCH (7,4) (15,11)และ(31,26)

จากกราฟรูปที่ 4.4 เปรียบเทียบทั้งสามกรณีพบว่า BCH (31,26) มีค่า BER ต่ำที่สุดและตามด้วย BCH (15,11)และ(7,4) แย่ที่สุด สามารถคำนวณค่าของ BER ของ BPSK ได้จาก Q function ตามสมการที่ 4.1

$$BER = Q\left(\sqrt{2 \times \frac{E_b}{N_0}}\right) \tag{4.1}$$

$$E_b = \frac{V_T^2}{2R_b} \tag{4.2}$$

สามารถหาค่าของ Q function ได้จากภาคผนวก ข.

ค่า BER ของ BCH(7,4) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{4}{7}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{4}{7}\times10^{(10/10)}}\right) \tag{4.3}$$

$$Q(3.38) = 3.6162\times10^{-4}$$

ค่า BER ของ BCH(15,11) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{11}{15}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{11}{15}\times10^{(10/10)}}\right) \tag{4.4}$$

$$Q(3.83) = 6.4072\times10^{-5}$$

ค่า BER ของ BCH(31,26) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{26}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{26}{31}\times10^{(10/10)}}\right) \tag{4.5}$$

$$Q(4.096) = 2.1017\times10^{-5}$$

จากการคำนวณหาค่า BER พบว่าค่าของ BER ที่คำนวณได้ของการเข้ารหัส BCH(31,26) ก่อนถอดรหัสดีที่สุดรองลงมาคือ BCH(15,11) และBCH(7,4) ตามลำดับ ซึ่งตรงกับผลจากการ Simulate แสดงดังรูปที่4.4

สามารถคำนวณหาค่า BER ที่มีการถอดรหัสแล้วได้จากสมการที่ (4.6)

$$BER = \sum_{i=t+1}^{n}\binom{n}{i}p^i(1-p)^{n-i} \tag{4.6}$$

เมื่อ n คือ ความยาวบล็อกโค้ต

t คือ จำนวนบิตที่ผิดพลาดที่ความสามารถของ BCH Code สามารถแก้ไขได้

p คือ ความน่าจะเป็นที่บิตผิดพลาด

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(7,4)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.3) $p = 3.6162\times10^{-4}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.7)

$$BER = \binom{7}{2}p^2(1-p)^5 + \binom{7}{3}p^3(1-p)^4 + \ldots + \binom{7}{7}p^7(1-p)^0 \tag{4.7}$$

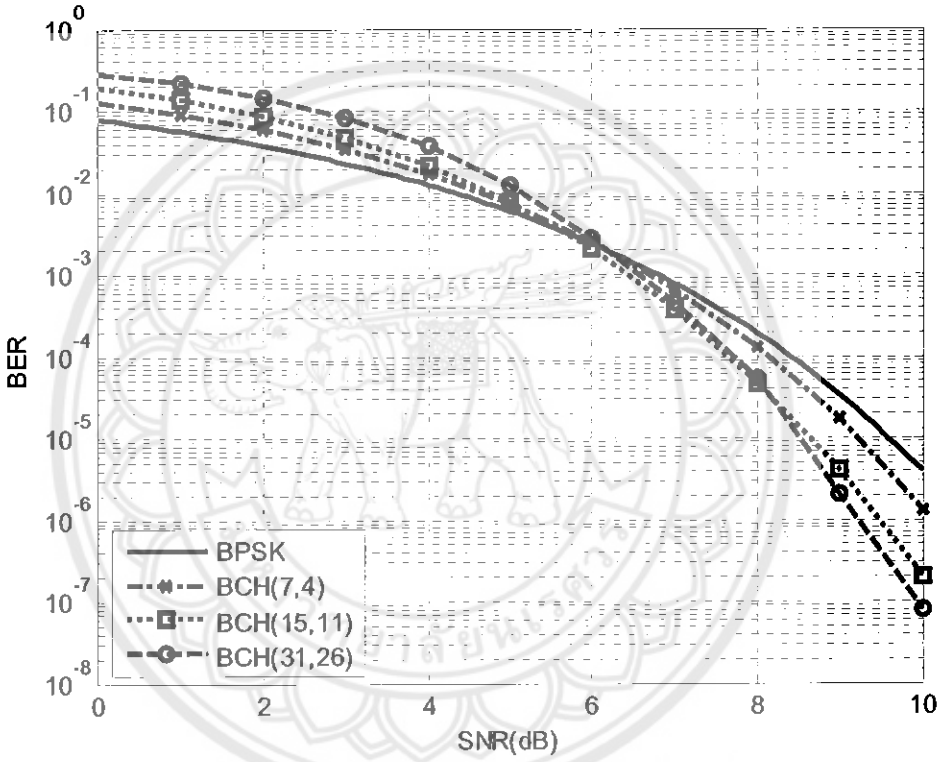
$$= 2.7428\times10^{-6}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(15,11)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.4) $p = 6.4072\times10^{-5}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.8)

$$BER = \binom{15}{2} p^2 (1-p)^{13} + \binom{15}{3} p^3 (1-p)^{12} + \ldots + \binom{15}{15} p^{15} (1-p)^0 \qquad (4.8)$$
$$= 4.3183 \times 10^{-7}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,26)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.5) $p = 2.1017 \times 10^{-5}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.9)

$$BER = \binom{31}{2} p^2 (1-p)^{29} + \binom{31}{3} p^3 (1-p)^{28} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \qquad (4.9)$$
$$= 2.0598 \times 10^{-7}$$



รูปที่ 4.5 แสดง Bit error rate ที่มีการถอดรหัสของ BCH (7,4) (15,11)และ(31,26)

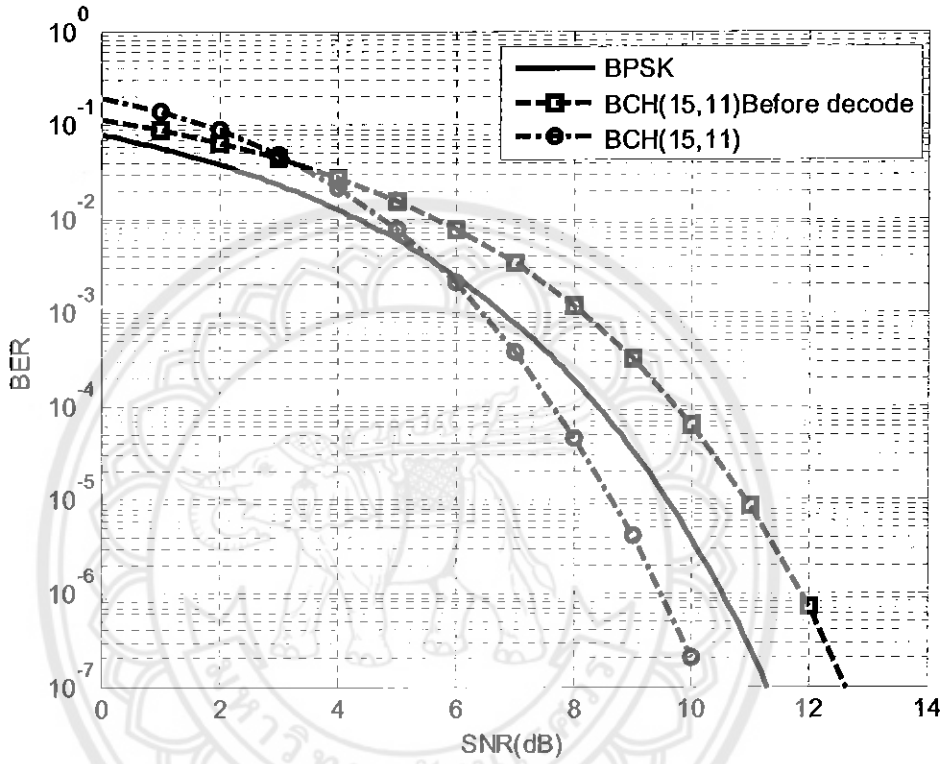
ผลจากการ Simulate แสดงดังรูปที่ 4.5 กับผลจากการคำนวณที่ได้จากสมการที่ (4.7) (4.8)และ(4.9)มีค่าใกล้เคียงกัน

จากการเปรียบเทียบการเข้ารหัส BCH Code แสดงดังรูปที่ 4.5 ภายหลังการถอดรหัสแล้ว พบว่าที่ SNR เท่ากันค่าของ BER ของ BCH (31,26) ดีที่สุดถึงแม้ว่าการลดลงของค่า SNR ที่ BER เท่ากันจะแย่ที่สุดเพราะค่าของ BER เริ่มต้นต่ำที่สุดที่ได้จากกราฟรูปที่ 4.4 และการคำนวณที่แสดงตามสมการที่ (4.3) (4.4)และ(4.5)

4.2 เปรียบเทียบประสิทธิภาพการเข้ารหัส BCH Code ที่ความยาวบล็อกข้อมูล 15 บิต

4.2.1 ประสิทธิภาพของ BCH(15,11) ที่สามารถแก้ไขบิตผิดพลาดได้ 1 บิต

ผลจากการ Simulate การเข้ารหัส BCH(15,11) ที่สมมารถแก้ไขบิตผิดพลาดได้ 1 บิต ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.6

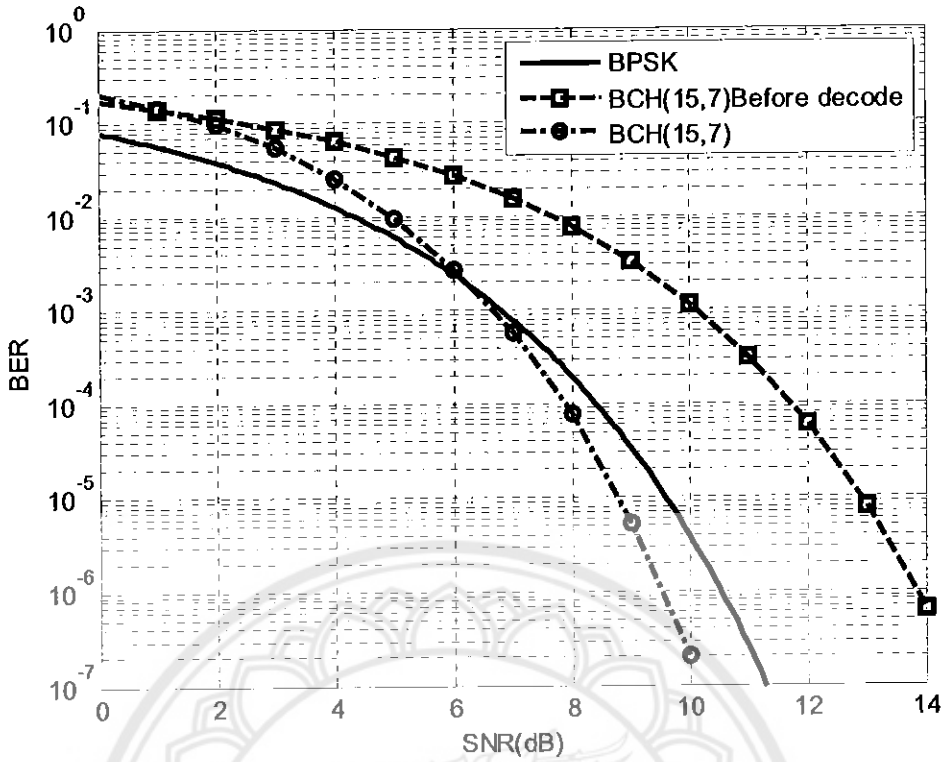


รูปที่ 4.6 แสดง Bit error rate การเข้ารหัส BCH(15,11)

จากกราฟรูปที่ 4.6 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $2.5dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.2.2 ประสิทธิภาพของ BCH(15,7) ที่สามารถแก้ไขบิตผิดพลาดได้ 2 บิต

ผลจากการ Simulate การเข้ารหัส BCH(15,7) ที่สมมารถแก้ไขบิตผิดพลาดได้ 2 บิตก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.7

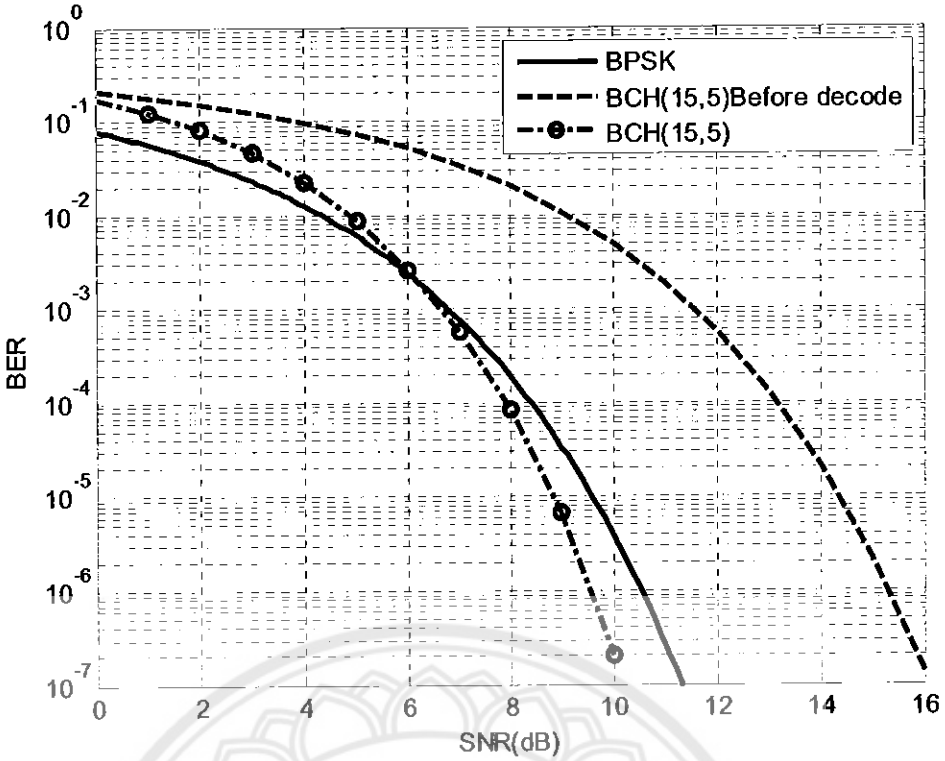


รูปที่ 4.7 แสดง Bit error rate การเข้ารหัส BCH(15,7)

จากกราฟรูปที่ 4.7 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $4.2dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.2.3 ประสิทธิภาพของ BCH(15,5) ที่สามารถแก้ไขบิตผิดพลาดได้ 3 บิต

ผลจากการ Simulate การเข้ารหัส BCH(15,5) ที่สมมารถแก้ไขบิตผิดพลาดได้ 3 บิตก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.8



รูปที่ 4.8 แสดง Bit error rate การเข้ารหัส BCH(15,5)

จากกราฟรูปที่ 4.8 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $6dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

จากกราฟรูปที่ 4.9 เปรียบเทียบทั้งสามกรณีพบว่า BCH (15,11) มีค่า BER ต่ำที่สุดและตามด้วย BCH (15,7)และ(15,5) แย้ที่สุด สามารถคำนวณค่าของ BER ของ BPSK ได้จาก Q function ตามสมการที่4.1

ค่า BER ของ BCH(15,11) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{11}{15}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2 \times \frac{11}{15} \times 10^{(10/10)}}\right) \tag{4.10}$$

$$Q(3.83) = 6.4072 \times 10^{-5}$$

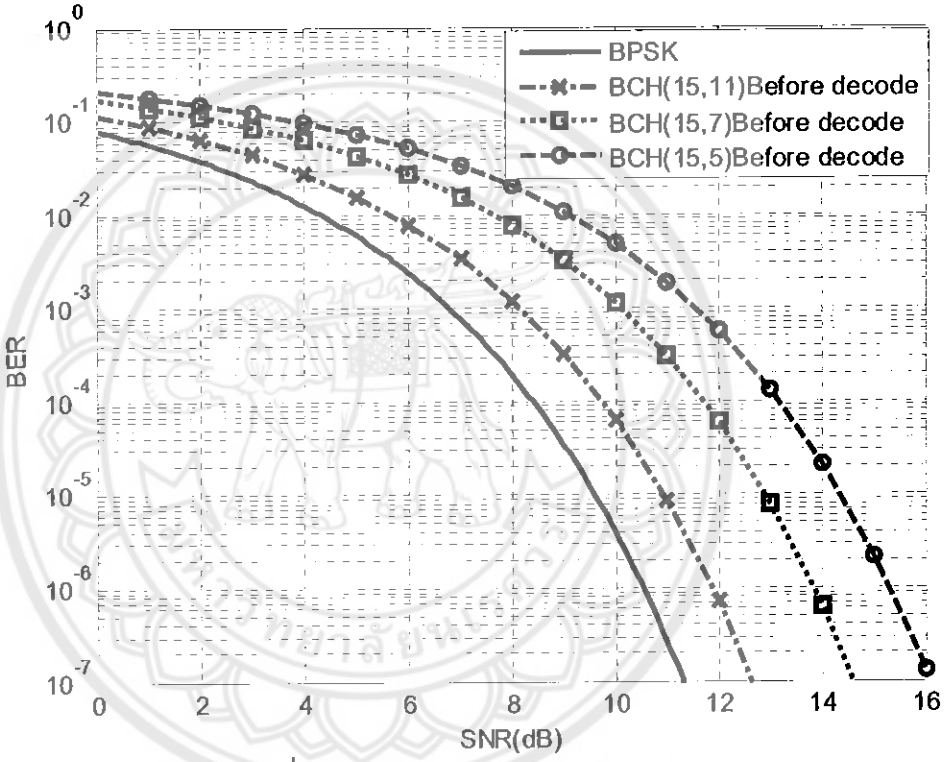
ค่า BER ของ BCH(15,7) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{7}{15}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2 \times \frac{7}{15} \times 10^{(10/10)}}\right) \tag{4.11}$$

$$Q(3.055) = 1.1 \times 10^{-3}$$

ค่า BER ของ BCH(15,5) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{5}{15}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{5}{15}\times10^{(10/10)}}\right) \tag{4.12}$$
$$Q(2.582) = 4.9\times10^{-3}$$



รูปที่ 4.9 แสดง Bit error rate ที่ยังไม่มีการถอดรหัสของ BCH (15,11) (15,7)และ(15,5)

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(15,11)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.10) $p = 6.4072\times10^{-5}$ แทนค่าลงในสมการที่ (4.6) จะได้แสดงดังสมการที่ (4.13)

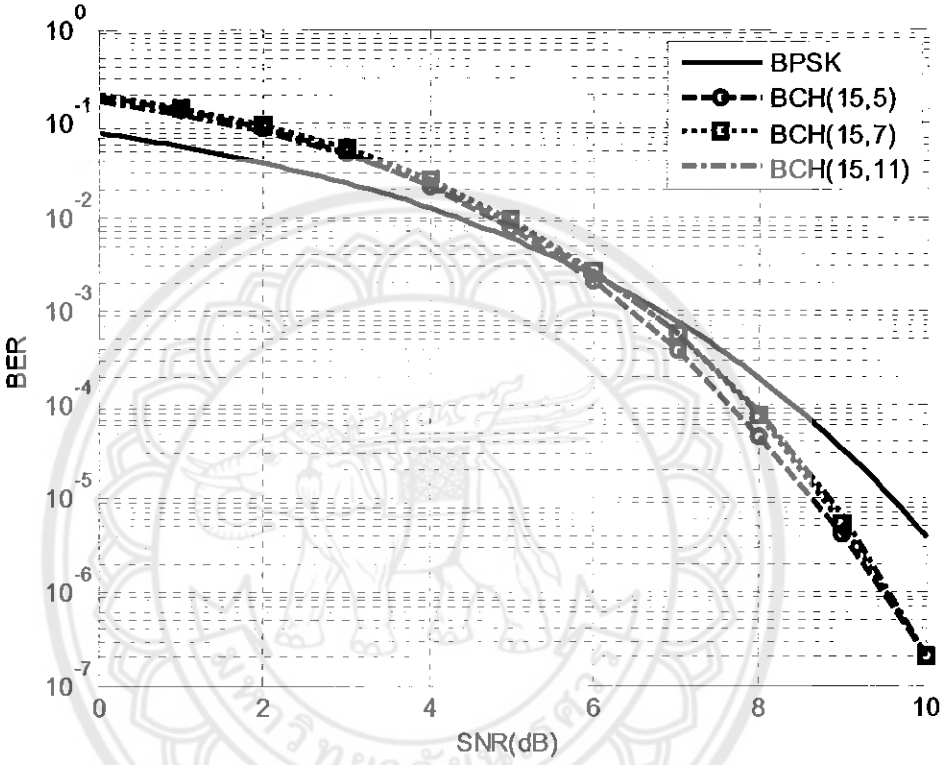
$$BER = \binom{15}{2}p^2(1-p)^{13} + \binom{15}{3}p^3(1-p)^{12} + \ldots + \binom{15}{15}p^{15}(1-p)^0 \tag{4.13}$$
$$= 4.3183\times10^{-7}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(15,7)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.11) $p = 1.1\times10^{-3}$ แทนค่าลงในสมการที่ (4.6) จะได้แสดงดังสมการที่ (4.14)

$$BER = \binom{15}{3}p^3(1-p)^{12} + \binom{15}{4}p^4(1-p)^{11} + \ldots + \binom{15}{15}p^{15}(1-p)^0 \tag{4.14}$$
$$= 6.4151\times10^{-7}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(15,5)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.12) $p = 4.9 \times 10^{-3}$ แทนค่าลงในสมการที่ (4.6) จะได้แสดงดังสมการที่ (4.15)

$$BER = \binom{15}{4} p^4 (1-p)^{11} + \binom{15}{5} p^5 (1-p)^{10} + \ldots + \binom{15}{15} p^{15} (1-p)^0 \qquad (4.15)$$
$$= 7.6076 \times 10^{-7}$$



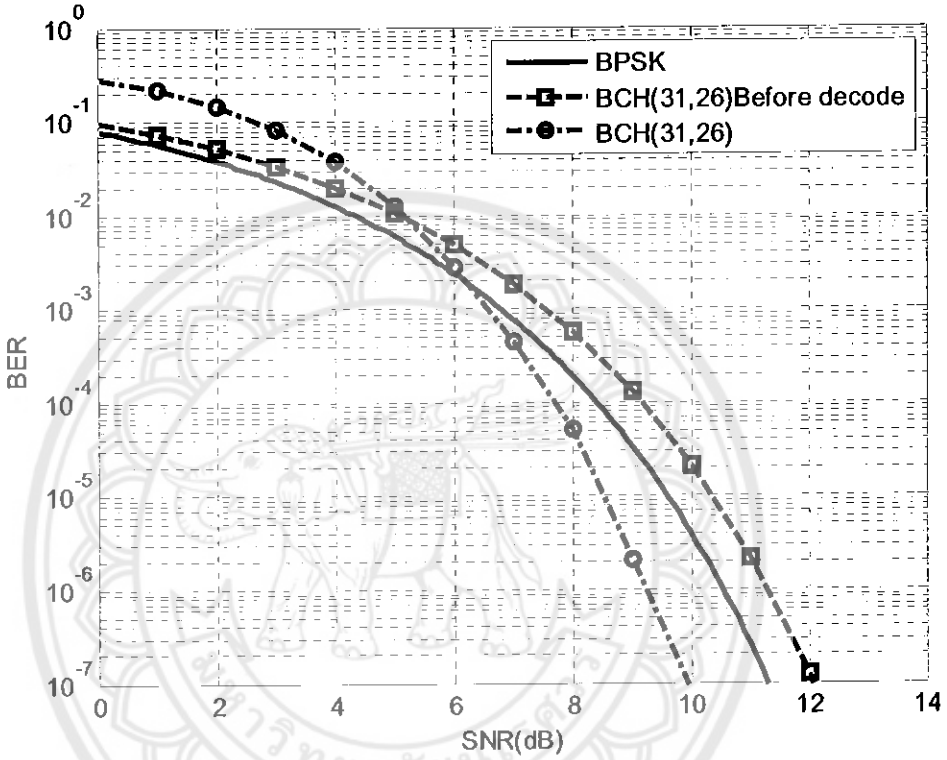
รูปที่ 4.10 แสดง Bits error rate ที่มีการถอดรหัสของ BCH (15,11) (15,7)และ(15,5)

จากการเปรียบเทียบการเข้ารหัส BCH Code แสดงดังรูปที่ 4.10 ที่มีการถอดรหัสแล้วพบว่าค่าของ BER มีค่าไม่ต่างกันถึงแม้ว่าจะสามารถแก้ไขบิตได้ไม่เท่ากันเพราะค่าของ BER เริ่มต้นไม่เท่ากันที่ได้จากกราฟรูปที่ 4.9 และการคำนวณที่แสดงตามสมการที่ (4.10),(4.11)และ(4.12)โดยค่า BER ของ BCH (15,5)สูงที่สุดรองลงมาคือ BCH(15,7)และBCH(15,11)ตามลำดับและผลจากการคำนวณที่ BER=10dB BCH(15,11)ได้ค่า BER ดีที่สุดแต่ไม่แตกต่างจากกรณี BCH(15,7)และ BCH(15,5)มากนักเมื่อพิจารณากราฟรูปที่ 4.10 ก็ได้ค่าไม่แตกต่างกันมากและมีค่าใกล้เคียงกับผลที่ได้จากการคำนวณ

4.3 เปรียบเทียบประสิทธิภาพการเข้ารหัส BCH Code ที่ความยาวบล็อกข้อมูล 31 บิต

4.3.1 ประสิทธิภาพของ BCH(31,26) ที่สามารถแก้ไขบิตผิดพลาดได้ 1 บิต

ผลจากการ Simulate การเข้ารหัส BCH(31,26) ที่สมมารถแก้ไขบิตผิดพลาดได้ 1 บิต ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.11

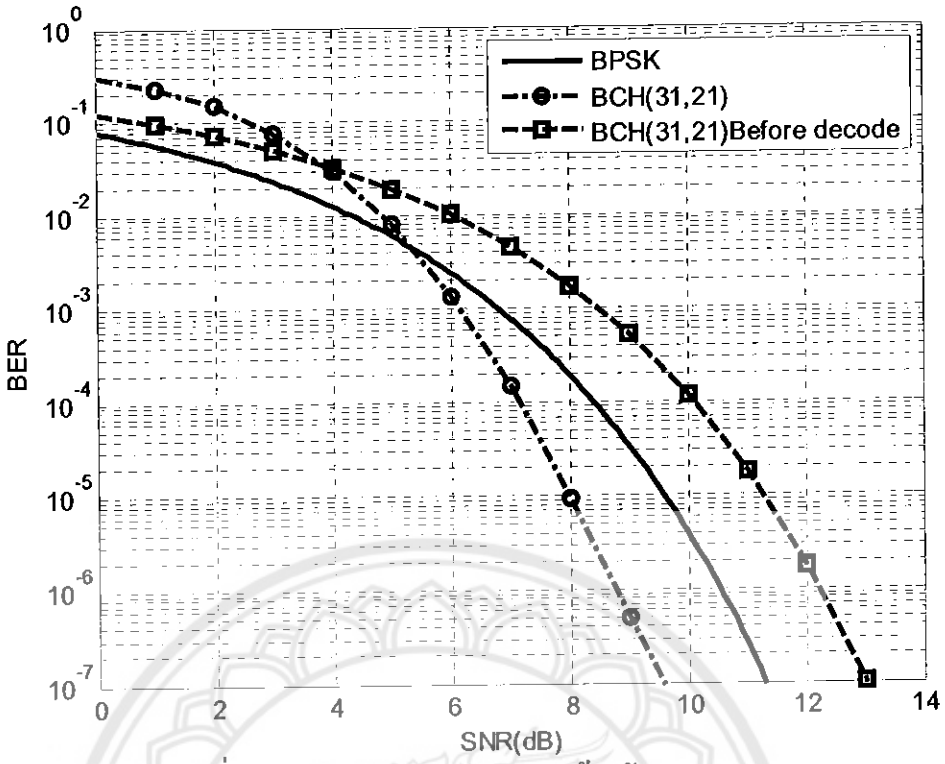


รูปที่ 4.11 แสดง Bit error rate การเข้ารหัส BCH(31,26)

จากกราฟรูปที่ 4.11 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $2dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.3.2 ประสิทธิภาพของ BCH(31,21) ที่สามารถแก้ไขบิตผิดพลาดได้ 2 บิต

ผลจากการ Simulate การเข้ารหัส BCH(31,21) ที่สมมารถแก้ไขบิตผิดพลาดได้ 2 บิตก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.12

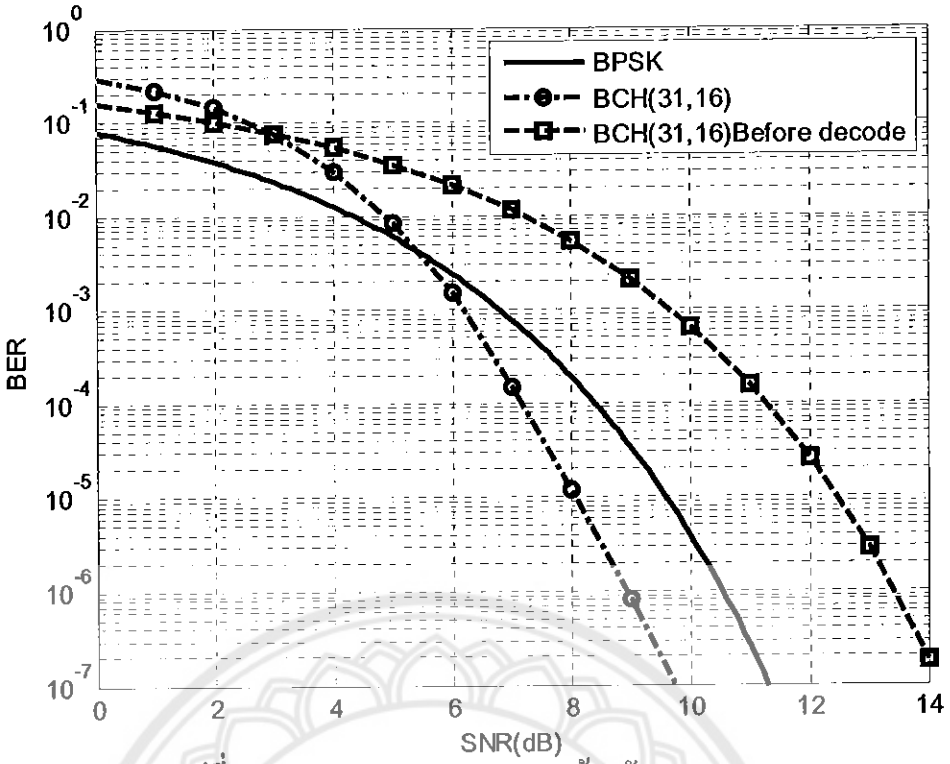


รูปที่ 4.12 แสดง Bit error rate การเข้ารหัส BCH(31,21)

จากกราฟรูปที่ 4.12 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $3.5dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.3.3 ประสิทธิภาพของ BCH(31,16) ที่สามารถแก้ไขบิตผิดพลาดได้ 3 บิต

ผลจากการ Simulate การเข้ารหัส BCH(31,16) ที่สมมารถแก้ไขบิตผิดพลาดได้ 3 บิตก่อถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.13

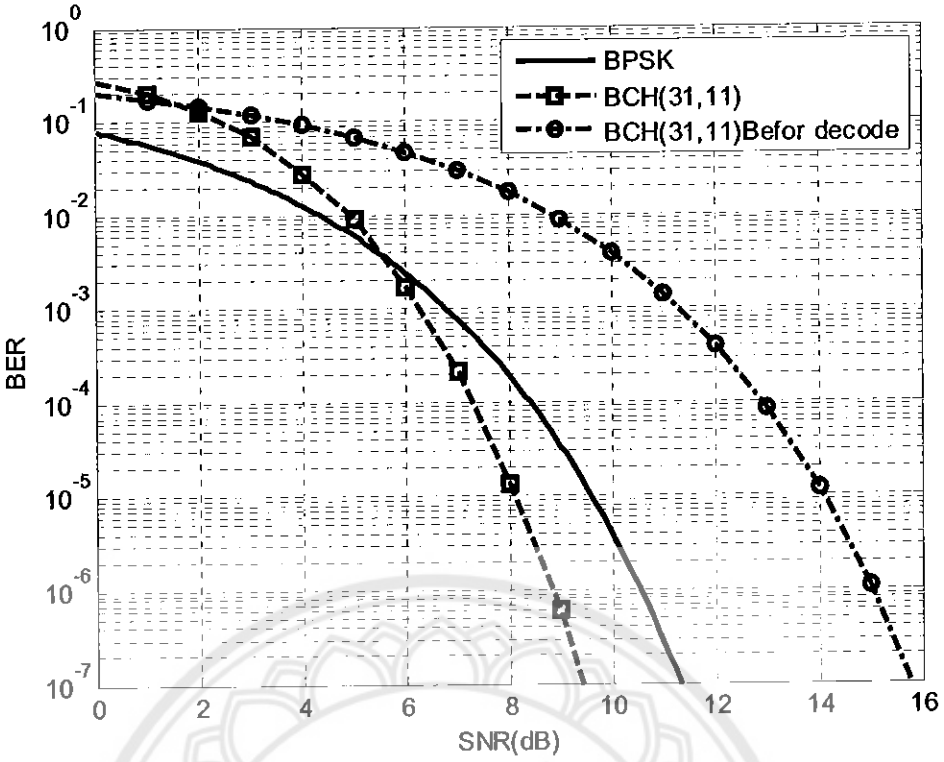


รูปที่ 4.13 แสดง Bit error rate การเข้ารหัส BCH(31,16)

จากกราฟรูปที่ 4.13 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $4.2dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.3.4 ประสิทธิภาพของ BCH(31,11) ที่สามารถแก้ไขบิตผิดพลาดได้ 5 บิต

ผลจากการ Simulate การเข้ารหัส BCH(31,11) ที่สมมารถแก้ไขบิตผิดพลาดได้ 5 บิต ก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.14

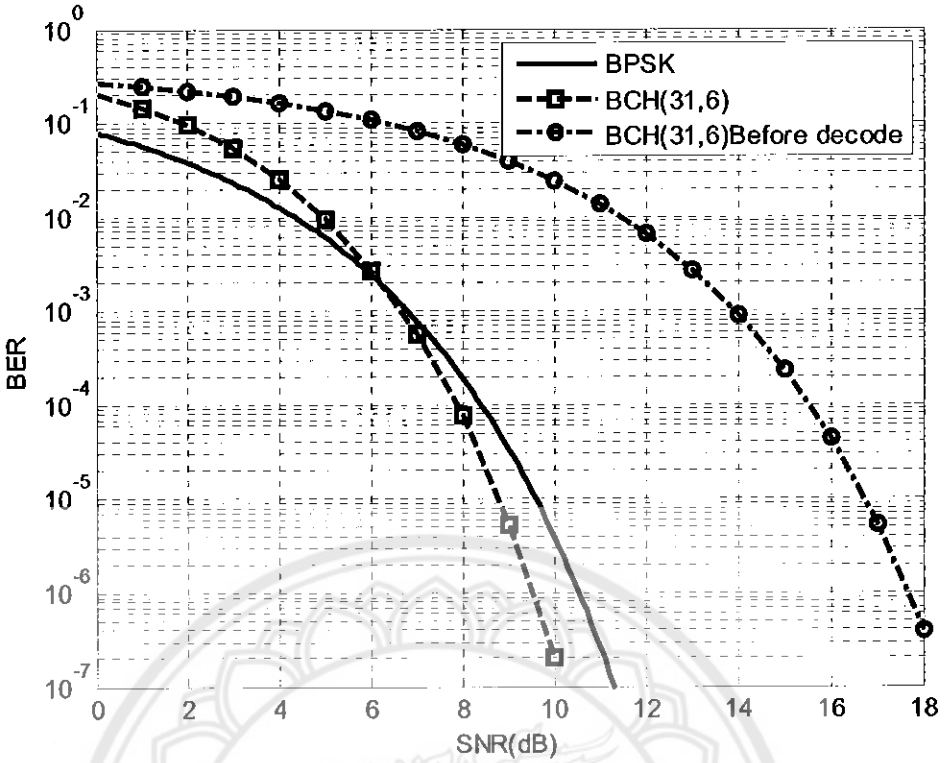


รูปที่ 4.14 แสดง Bit error rate การเข้ารหัส BCH(31,11)

จากกราฟรูปที่ 4.14 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $6dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

4.3.4 ประสิทธิภาพของ BCH(31,6) ที่สามารถแก้ไขบิตผิดพลาดได้ 7 บิต

ผลจากการ Simulate การเข้ารหัส BCH(31,6) ที่สามารถแก้ไขบิตผิดพลาดได้ 7 บิตก่อนถอดรหัสและหลังถอดรหัสแสดงดังรูปที่ 4.15



รูปที่ 4.15 แสดง Bit error rate การเข้ารหัส BCH(31,6)

จากกราฟรูปที่ 4.15 พบว่าที่ $BER = 10^{-6}$ ค่าของกราฟ Bit error rate ผ่านการถอดรหัสแล้วมีค่า SNR ลดลงจากกราฟ Bit error rate ที่ยังไม่ผ่านการถอดรหัสประมาณ $8dB$ และค่าของกราฟ Bit error rate ที่ผ่านการถอดรหัสแล้วดีกว่าการส่งข้อมูลแบบ BPSK ปกติ

จากกราฟรูปที่ 4.16 เปรียบเทียบทั้งสามกรณีพบว่า BCH (31,26) มีค่า BER ต่ำที่สุดและตามด้วย BCH (31,21) (31,16) (31,11)และ(31,6) แย่ที่สุด สามารถคำนวณค่าของ BER ของ BPSK ได้จาก Q function ตามสมการที่ 4.1

ค่า BER ของ BCH(31,26) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{26}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{26}{31}\times 10^{(10/10)}}\right) \tag{4.16}$$

$$Q(4.096) = 2.1017\times 10^{-5}$$

ค่า BER ของ BCH(31,21) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{21}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{21}{31}\times10^{(10/10)}}\right) \tag{4.17}$$

$$Q(3.68) = 1.1662\times10^{-4}$$

ค่า BER ของ BCH(31,16) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{16}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{16}{31}\times10^{(10/10)}}\right) \tag{4.18}$$

$$Q(3.213) = 6.5678\times10^{-4}$$

ค่า BER ของ BCH(31,11) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{11}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

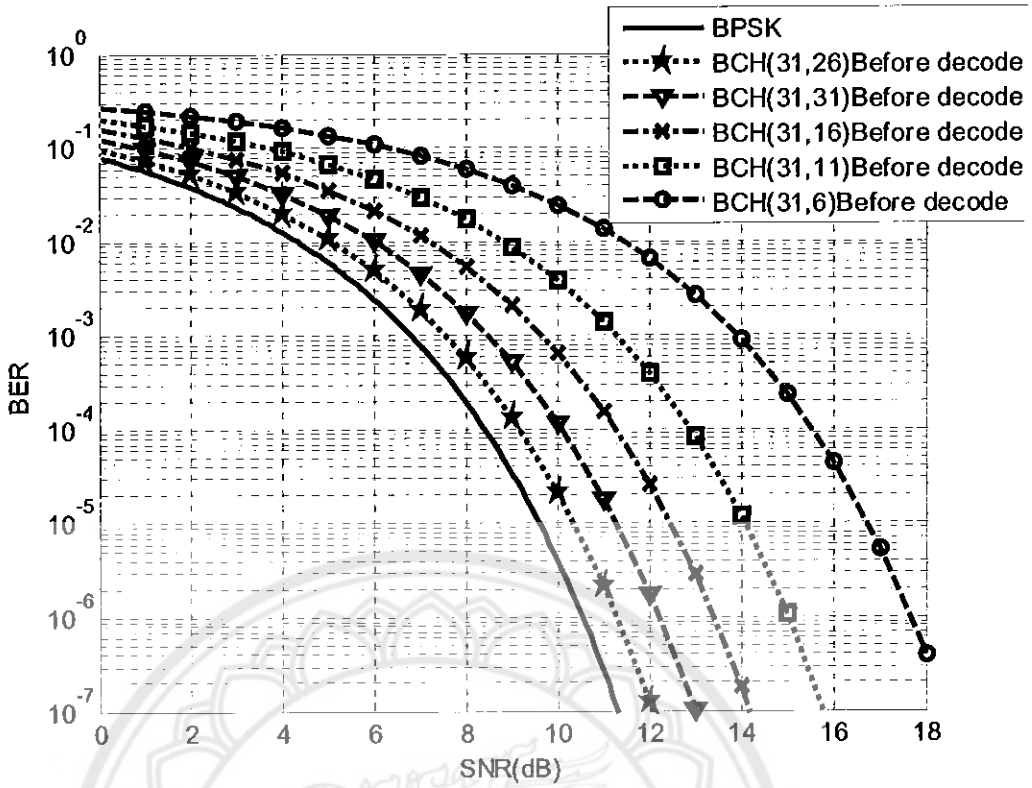
$$BER = Q\left(\sqrt{2\times\frac{11}{31}\times10^{(10/10)}}\right) \tag{4.19}$$

$$Q(2.66) = 3.9\times10^{-3}$$

ค่า BER ของ BCH(31,6) จะสามารถหาได้จากสมการที่ (4.1) แต่เนื่องจากการเข้ารหัสจะทำให้ Bit rate ค่าเพิ่มขึ้นส่งผลให้ค่าของ E_b เป็นไปตามสมการที่ (4.2) มีค่าลดลงเป็น $\frac{6}{31}E_b$ แทนค่าลงในสมการที่ (4.1) พิจารณาที่ $SNR = 10dB$ จะได้

$$BER = Q\left(\sqrt{2\times\frac{6}{31}\times10^{(10/10)}}\right) \tag{4.20}$$

$$Q(1.967) = 2.46\times10^{-2}$$



รูปที่ 4.16 แสดง Bit error rate ที่ยังไม่มีการถอดรหัสของ BCH (31,26) (31,21) (31,16) (31,11)และ(31,6)

ผลจากการ Simulate ค่าของ BER ที่ $SNR = 10dB$ ก่อนถอดรหัสพบว่าค่าของ BER ของ BCH(31,6)มีค่าแย่ที่สุดและรองลงมาคือ (31,21) (31,16) (31,11)และ(31,6) และการคำนวณตามสมการที่ (4.16)ถึง(4.20) มีค่าตรงกัน

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,26)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.16) $p = 2.1017 \times 10^{-5}$แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.21)

$$BER = \binom{31}{2} p^2 (1-p)^{29} + \binom{31}{3} p^3 (1-p)^{28} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \qquad (4.21)$$

$$= 2.0598 \times 10^{-7}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,21)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.17) $p = 1.1662 \times 10^{-4}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.22)

$$BER = \binom{31}{3} p^3 (1-p)^{28} + \binom{31}{4} p^4 (1-p)^{27} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \qquad (4.22)$$

$$= 7.0437 \times 10^{-9}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,16)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.18) $p = 6.5678 \times 10^{-4}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.23)

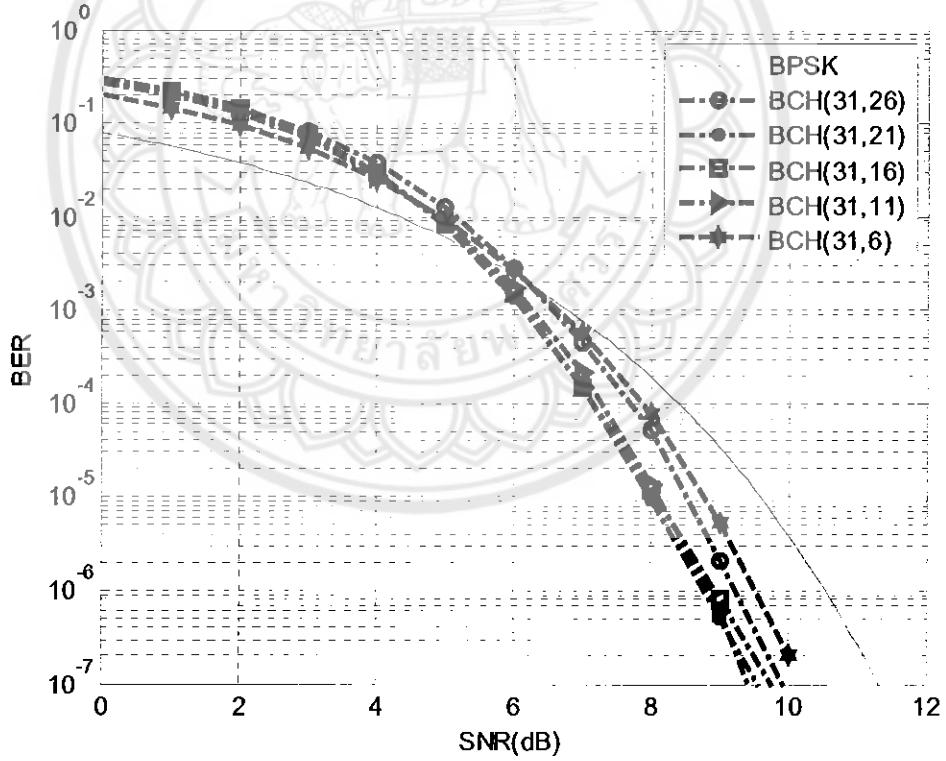
$$BER = \binom{31}{4} p^4 (1-p)^{27} + \binom{31}{5} p^5 (1-p)^{26} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \quad (4.23)$$
$$= 5.7822 \times 10^{-9}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,11)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.19) $p = 3.9 \times 10^{-3}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.24)

$$BER = \binom{31}{6} p^6 (1-p)^{25} + \binom{31}{7} p^7 (1-p)^{24} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \quad (4.24)$$
$$= 2.2458 \times 10^{-9}$$

จากสมการที่ (4.6) สามารถหาค่า BER ของ BCH(31,6)ที่มีการถอดรหัสแล้ว ที่ $SNR = 10dB$ จากสมการที่ (4.20) $p = 2.46 \times 10^{-2}$ แทนค่าลงในสมการที่ (4.6) แสดงดังสมการที่ (4.25)

$$BER = \binom{31}{8} p^8 (1-p)^{23} + \binom{31}{9} p^9 (1-p)^{22} + \ldots + \binom{31}{31} p^{31} (1-p)^0 \quad (4.25)$$
$$= 6.3037 \times 10^{-7}$$



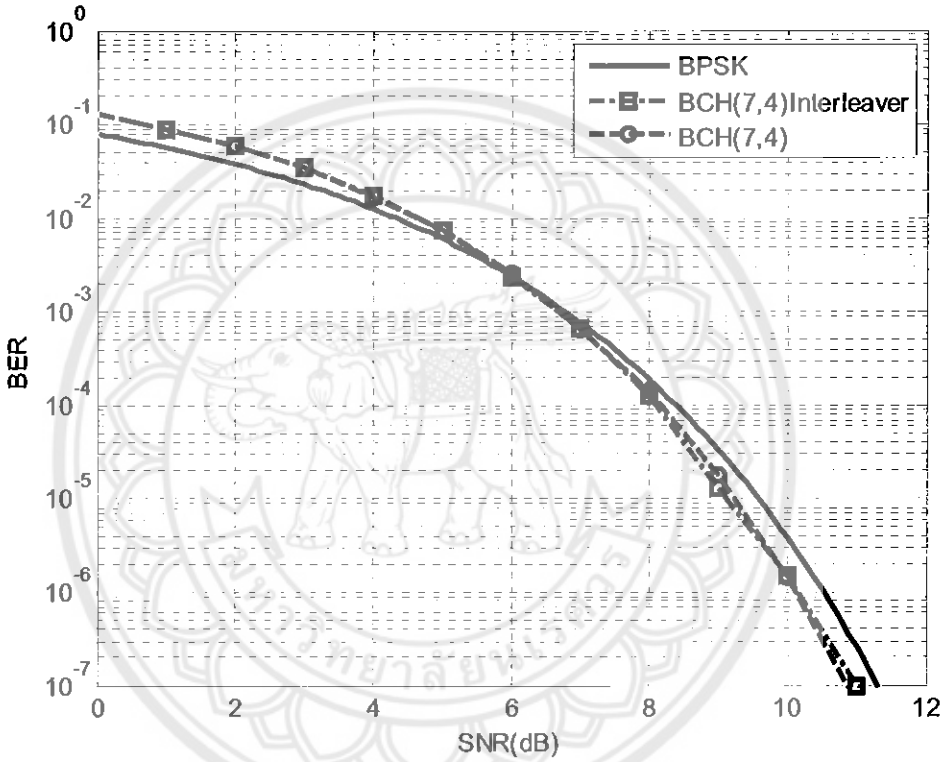
รูปที่ 4.17 แสดง Bit error rate ที่มีการถอดรหัสของ BCH (31,26) (31,21) (31,16) (31,11)และ(31,6)

ผลจากการ Simulate การเข้ารหัส BCH Code ความยาวบล็อกโค้ด 31บิตได้ค่า BER ของ BCH(31,6)แย่ที่สุดซึ่งตรงกับการคำนวณตามสมการที่ (4.21)ถึง(4.25) เนื่องจาก BCH (31,6) มีค่าของ BER ก่อนถอดรหัสที่สูงมากและผลจากการ Simulate ได้ BCH(31,11) แก้ไขได้ 5บิต มีค่าของ

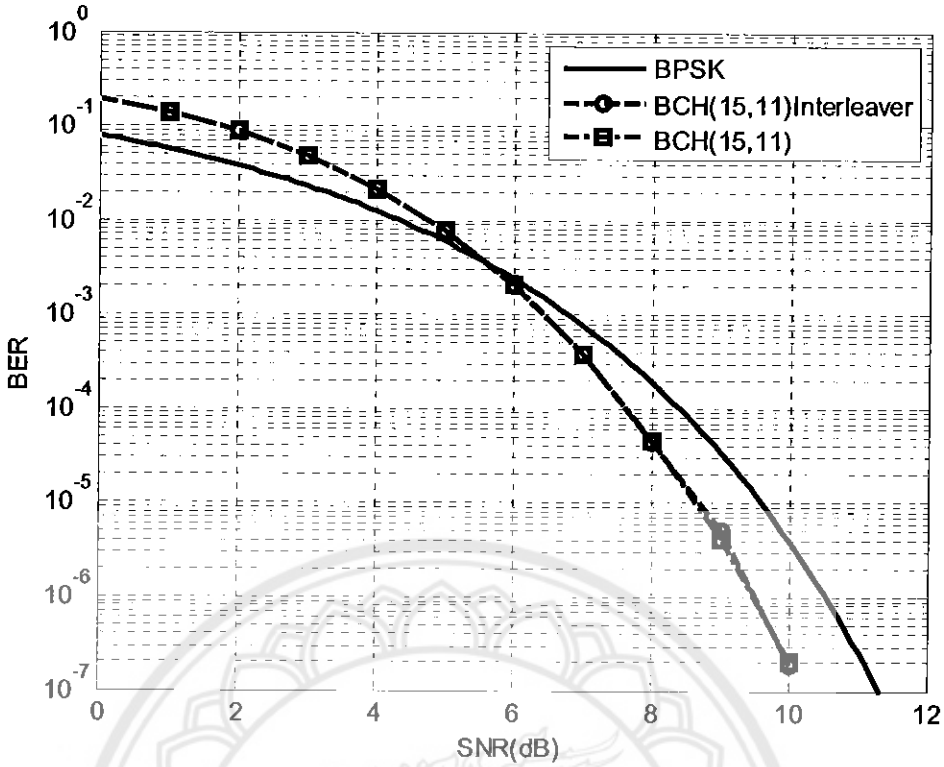
กราฟ BER ดีที่สุดซึ่งไม่แตกต่างกับ BCH(31,16)และBCH(31,21) มากนักและตรงกับการคำนวณตามสมการที่ (4.22)ถึง(4.24)

4.3 เปรียบเทียบการเข้ารหัส BCH Code โดยใช้ Interleaver และไม่ใช้ Interleaver

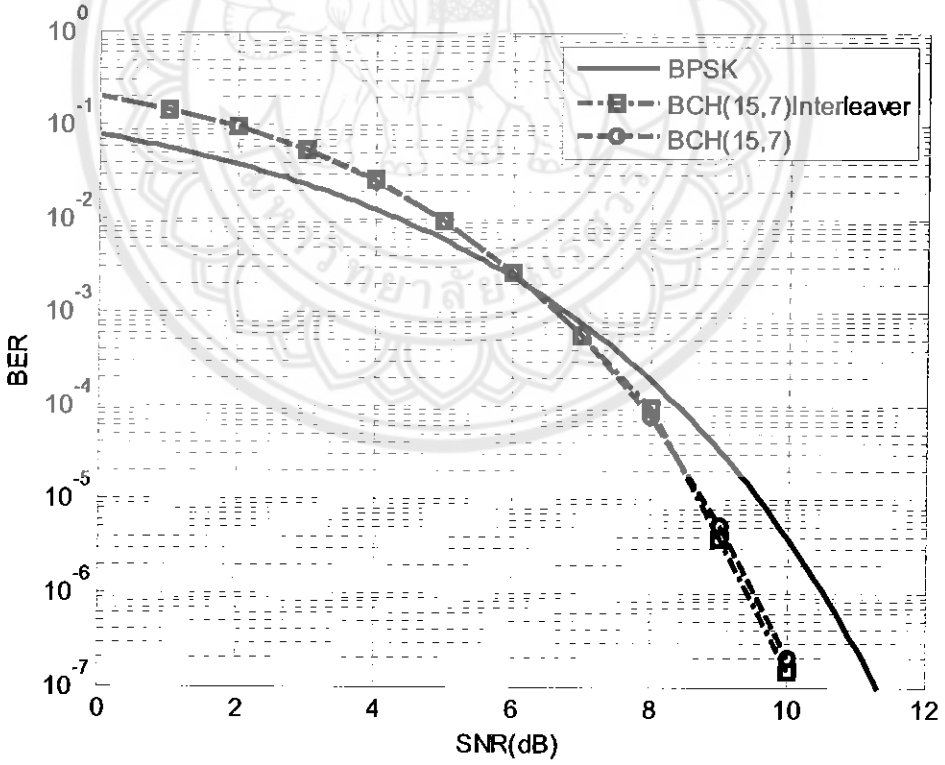
ผลจากการ Simulate การเข้ารหัส BCH Code ที่มีความยาวบล็อกโค้ต 7 บิตและ 15 บิตที่มีการใช้ Interleaver กับไม่ใช้ Interleaver แสดงดังรูปที่ 4.18 ถึง รูปที่ 4.21



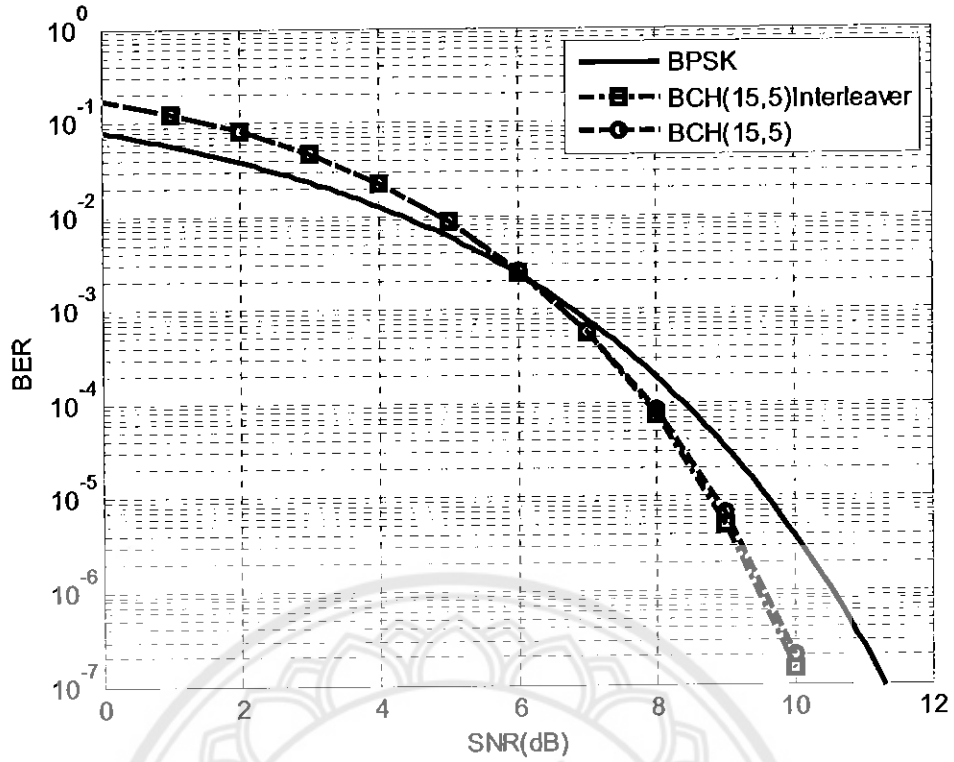
รูปที่ 4.18 แสดงการเข้ารหัส BCH(7,4)และBCH(7,4)ที่มีการใช้ Interleaver



รูปที่ 4.19 แสดงการเข้ารหัส BCH(15,11)และBCH(15,11)ที่มีการใช้ Interleaver



รูปที่ 4.20 แสดงการเข้ารหัส BCH(15,7)และBCH(15,7)ที่มีการใช้ Interleaver



รูปที่ 4.21 แสดงการเข้ารหัส BCH(15,5)และBCH(15,5)ที่มีการใช้ Interleaver

จากกราฟของ BER รูปที่ 4.18 ถึง 4.21 พบว่าผลของการเข้ารหัส BCH Code ที่ใช้ Interleaver และการเข้ารหัส BCH Code เพียงอย่างเดียวให้ผลลัพธ์ไม่แตกต่างกันเนื่องจากแบบจำลองนี้ได้กำหนดความน่าจะเป็นของความผิดพลาดมีการกระจายตัวแบบเกาส์เซียนจึงไม่มีผลของการทำ Interleaver เพราะการสลับบิตข้อมูลความผิดพลาดของข้อมูลยังคงมีการกระจายตัวของความน่าจะเป็นเหมือนเดิม การ Interleaver สามารถใช้กับความผิดพลาดของข้อมูลที่เกิดผิดพลาดขึ้นติดกันยาวๆ แต่เนื่องด้วยความน่าจะเป็นของความผิดพลาดของข้อมูลมีการกระจายตัวแบบเกาส์เซียน จึงส่งผลให้ค่าของ BER ของการเข้ารหัส BCH Code ที่มีการใช้ Interleaver ไม่มีผลหรือมีผลน้อยมากเมื่อเทียบกับการเข้ารหัส BCH Code เพียงอย่างเดียว

บทที่ 5
สรุปผลการดำเนินโครงงาน

5.1 ผลการดำเนินโครงงาน

จากการจำลองการเข้ารหัส BCH Code และการกล้ำสัญญาณแบบ BPSK โดยการใช้โปรแกรม MATLAB เพื่อศึกษาประสิทธิภาพของการของการเข้ารหัส BCH Code แสดงให้เห็นว่ากระบวนการที่ภาคส่งได้เพิ่มบิตพิเศษเข้าไปเพื่อช่วยให้ภาครับสามารถแก้ไขข้อมูลที่ผิดพลาดได้ดีกว่าการส่งสัญญาณปกติและผลจากการจำลองพบว่าการเข้ารหัส BCH Code ที่มีความยาวบล็อกโค้ต 31 บิต และบิตข้อมูล 11 บิต ที่สามรถแก้ไขความผิดพลาดได้ 5บิต มีประสิทธิภาพดีที่สุดและค่าของ BER ลดลงจากการส่งแบบ BPSK ที่ไม่มีการเข้ารหัส ผลจากการใช้ Interleaver ไม่มีผลมากนักเนื่องจากความผิดพลาดมีการกระจายตัวอยู่แล้วเมื่อใช้ Interleaver ความผิดพลาดก็ยังคงมีการกระจายตัวอยู่เหมือนเดิม สำหรับ Interleaver จะใช้ได้ผลก็ต่อเมื่อเกิดความผิดพลาดของข้อมูลติดกันยาวเท่านั้น การเลือกใช้การเข้ารหัส BCH(31,11) มีประสิทธิภาพมากแต่ก็ต้องสิ้นเปลือง Bandwidth มากขึ้นตามไปด้วยเพราะฉะนั้นควรเลือกให้เหมาะสมกับการสื่อสาร

5.2 ปัญหาที่พบขณะทำโครงงาน

1. เนื่องจากผู้ดำเนินโครงงานไม่มีความเข้าใจลักษณะของการดำเนินโครงงานตลอดจนทฤษฎีที่เกี่ยวข้องมากนักจึงเสียเวลาไปมาก
2. ผู้ดำเนินโครงงานขาดทักษะด้านการเขียนโปรแกรมจึงทำให้โปรแกรมที่เขียนขึ้นมาเสียเวลาในการประมวลผลมาก

5.3 ข้อเสนอแนะ

1. ควรศึกษารายละเอียดเกี่ยวกับโปรแกรมและทฤษฎีที่เกี่ยวข้องเพื่อให้เกิดความว่องไวในการประมวลผลให้มากที่สุด
2. ควรมีความตรงต่อเวลาในการส่งงานและความละเอียดรอบครอบ

เอกสารอ้างอิง

[1] พิสิฐ วนิชชานันท์. "ทฤษฎีรหัสช่องสัญญาณ (Channel Coding Theory)". พิมพ์ครั้งที่ 1 ;บริษัท แอ็ปป้า พริ้นติ้ง กรุ๊ป จำกัด. 2552.

[2] Stephen B. Wicker. "Error Control Systems for Digital Comunication and Storage". Prentice-Hall. 1995

[3] R.F. Churchhouse,W.F. MeColl,andA.B. tayler. "Error-Correcting Codes and Finite Fields". Clarendon Press. 1992

[4] Daniel J. Costello. "Error Control Coding Fundamentals and Applications". Pearson Prentice Hell. 1983.

[5] Couch, L. W., Digital and Analog Communication Systems, 7th ed., Prentice-Hall, Ine., New Jersey,2007.

ภาคผนวก ก

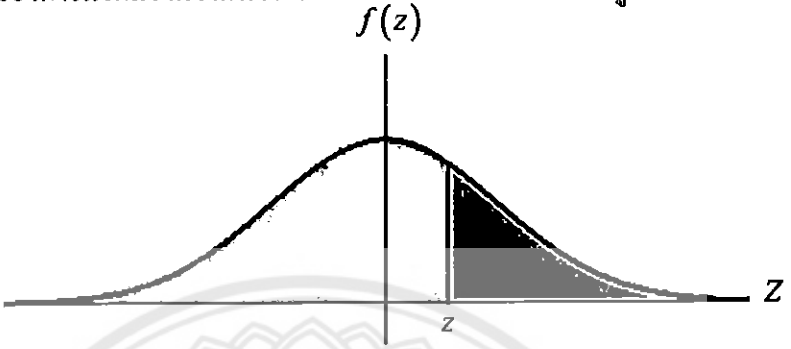
ตารางที่ ก-1 แสดงพหุนามกำเนิดรหัส BCH Code

n	k	t	พหุนามกำเนิด BCH Code g(x)
7	4	1	1011
15	11	1	1001 1
15	7	2	1110 1000 1
15	5	3	1010 0110 111
31	26	1	1001 01
31	21	2	0111 0110 1001
31	16	3	1000 1111 1010 1111
31	11	5	1011 0001 0011 0110 1010 1
31	6	7	1100 1011 0111 1010 1000 1001 01

ภาคผนวก ข

Q function[5]

ถ้าให้ Z เป็นตัวแปรสุ่มที่มีการกระจายแบบปกติซึ่งค่าเฉลี่ยเป็น 0 และมีความแปรปรวนเท่ากับ 1 กราฟของการแจกแจงความน่าจะเป็น สามวาดเป็นกราฟได้ดังรูปที่ ก-1



รูปที่ ก-1 รูปการแจกแจงความน่าจะเป็นของตัวแปรสุ่มที่มีการแจกแจงปกติ

สมการหาพื้อนที่ใต้กราฟเมื่อ $Z > z$ ได้ดังนี้

$$P(Z > z) = \int_{z}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-(z-\mu)^2/2\sigma^2} dz \qquad \text{(ก-1)}$$

กำหนดให้ $\lambda = (z-\mu)/\sigma$ จะได้

$$P(Z > z) = \int_{z}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\lambda^2/2} \sigma d\lambda \qquad \text{(ก-2)}$$

$$P(Z > z) = \frac{1}{\sqrt{2\pi}} \int_{z}^{\infty} e^{-\lambda^2/2} d\lambda \qquad \text{(ก-3)}$$

กำหนดให้สมการที่(ก-3) แทนด้วย Q function เมื่อ $Z \geq 3$ จะได้ Q function แสดงดังสมการที่ (ก-4)

$$Q(z) \approx \frac{1}{\sqrt{2\pi}z} e^{-\lambda^2/2} \qquad \text{(ก-4)}$$

ตารางที่ ข-1 ตาราง Q function

z	$Q(z)$	z	$Q(z)$
0.0	0.50000	2.1	0.01786
0.1	0.46017	2.2	0.01390
0.2	0.42074	2.3	0.01072
0.3	0.38209	2.4	0.00082
0.4	0.34458	2.5	0.00621
0.5	0.30854	2.6	0.00466
0.6	0.27425	2.7	0.00347
0.7	0.21186	2.8	0.00256
0.8	0.24196	2.9	0.00187
0.9	0.18406	3.0	0.00135
1.0	0.15866	3.1	0.00097
1.1	0.13567	3.2	0.00069
1.2	0.11507	3.3	0.00048
1.3	0.09680	3.4	0.00034
1.4	0.08076	3.5	0.00023
1.5	0.06681	3.6	0.00016
1.6	0.05480	3.7	0.00011
1.7	0.04457	3.8	0.00007
1.8	0.03593	3.9	0.00005
1.9	0.02872	4.0	0.00003
2.0	0.02275		