การเข้ารหัสควบคุมความผิดพลาดเชิงดิจิตอล ขั้นแนะนำ

ดร. วิระสิทธิ์ อิ่มถวิล
อาจารย์
ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น 40002

บทคัดย่อ

บทความนี้เป็นการแนะนำให้รู้จักเทคนิคการเข้ารหัสเพื่อควบคุมความผิดพลาด (Error control coding, ECC) ในระบบสื่อสารเชิงดิจิตอลและระบบการเก็บข้อมูลเชิงดิจิตอล การเข้ารหัสเพื่อควบคุมความผิดพลาดได้ถูกค้นพบประมาณปี ค.ศ. 1950 หลังจาก C. E. Shannon ได้ตีพิมพ์บทความ "A Mathematical Theory of Communications" ในปี ค.ศ. 1948 ในบทความนี้ Shannon ได้แสดงให้เห็นว่าระบบบสื่อสารเชิงดิจิตอลหนึ่งๆ สามารถทำให้ไม่มีความผิดพลาดร้อยเปอร์เซนต์ได้ด้วยการออกแบบตัวเข้ารหัสและถอดรหัสสัญญาณข้อมูลดิจิตอลอย่างเหมาะสม แต่ Shannon ไม่ได้แสดงให้เห็นว่าจะออกแบบตัวเข้ารหัสและถอดรหัสที่เหมาะสมอย่างไร จึงทำให้นักวิจัยทั่วโลกหันมาสนใจบทความนี้และพยายามค้นหาวิธีการที่จะทำให้ระบบสื่อสารเป็นระบบสื่อสารแบบปราศจากความผิดพลาดตั้งแต่นั้นเป็นต้นมาจนถึงปัจจุบัน

การเข้ารหัสควบคุมความผิดพลาดเป็นวิธีที่อาศัยหลักการรวมบิตข้อมูลเข้ากับกลุ่มของบิตที่ใช้ควบคุมความผิดพลาด (controlled bits) เพื่อป้องกันการรบกวนจากสัญญาณที่ไม่ต้องการ โดยวิธีการสร้างกลุ่มของบิตเหล่านี้มีหลายวิธี แต่ละวิธีนำมาซึ่งวิธีการเข้ารหัสแบบต่างๆ

An introduction to Error Control Coding

Dr. Virasit Imtawil

Lecturer

Department of Electrical Engineering

Faculty of Engineering, Khon Kaen University 40002

Abstract

This paper provides an introduction to Error Control Coding (ECC) widely used in digital communication and storage systems. ECC was discovered in 1950 after a great scientist named C. E. Shannon published his paper titled "A Mathematical Theory of Communications" in 1948 in which he theoretically showed we can make an error-free communication system given a suitable design of encoding and decoding processes. However, he did not tell us how to achieve such a great system in practice. This has made many researchers worldwide interested in the paper and trying to get to this goal since.

ECC is fundamentally based on the addition of redundancy to the digital data in order to protect the data from noise and interference. The process of determining this redundancy makes a variety of encoding methodologies.

บทนำ

ในระบบสื่อสารเชิงดิจิตอลหนึ่งๆ การหลีกเลี่ยงไม่ให้สัญญาณรบกวนมีผลกระทบต่อข้อมูลที่ส่งไปสามารถทำได้โดยการเพิ่มกำลังงานของเครื่องส่ง ซึ่งสามารถเป็นปัญหาได้ถ้าระบบมีกำลังงานที่จำกัด และผู้ส่งต้องการส่งสัญญาณเป็นระยะทางไกลๆ การเข้ารหัสควบคุมความผิดพลาด (ECC) เข้ามามีบทบาทในการเพิ่มภูมิต้านทานให้กับข้อมูลดิจิตอลต่อสัญญาณรบกวนโดยที่ไม่ต้องเพิ่มกำลังงานของเครื่องส่ง แต่สามารถส่งข้อมูลได้ไกลขึ้นหรือสามารถส่งข้อมูลให้มีความผิดพลาดน้อยลง

หลักการของ ECC ในการป้องกันข้อมูลดิจิตอลต่อสัญญาณรบกวนคือ การใส่กลุ่มของบิตจำนวนหนึ่ง (redundant bits, RBs) ซึ่งสามารถมีได้ตั้งแต่บิตเดียวหรือหลายบิตเข้าไปยังบิตข้อมูล ก่อนที่จะส่งข้อมูลผ่านช่องสื่อสาร หรือก่อนที่จะเขียนข้อมูลลงบนอุปกรณ์เก็บข้อมูล ซึ่งเรียกกระบวนการนี้ว่า กระบวนการเข้ารหัส (encoding process) และเรียกเอาท์พุทของกระบวนการนี้ว่า สัญลักษณ์รหัส (coded word) กลุ่มของ RBs จะถูกคำนวณมาจากกลุ่มของบิตข้อมูลที่จะเข้ารหัส ความสัมพันธ์ของบิตข้อมูลและ RBs จะถูกนำมาใช้ในกระบวนการนำเอาสัญญาณข้อมูลออกมาจากสัญญาณเข้ารหัสที่ปลายทาง และเรียกกระบวนการนี้ว่า กระบวนการถอดรหัส (decoding process)

สมมติว่าสัญญาณข้อมูลประกอบไปด้วยข้อมูลขนาด k บิต เมื่อทำการเข้ารหัสแล้วได้ข้อมูลออกมามีขนาดเป็น n บิต ดังนั้น อัตราการเข้ารหัส (code rate) $R = k/n \quad (n > k)$ ค่าของ R มีความสัมพันธ์กับประสิทธิภาพของการเข้ารหัสคือ ถ้า R ยิ่งน้อยกว่า 1 มากเท่าไร ประสิทธิภาพในการป้องกันสัญญาณรบกวนก็จะมากขึ้นเท่านั้น แต่สิ่งที่จะต้องเสียไปเพื่อแลกกับประสิทธิภาพที่เพิ่มขึ้นคือความต้องการของแบนด์วิทในการส่งหรือจัดเก็บข้อมูลที่มากขึ้น

ในอดีตสาขาวิชา ECC มักได้รับความสนใจน้อยในวงการผู้ผลิตอุปกรณ์สื่อสาร เนื่องจากความยากและการลงทุนสูงในอุปกรณ์ฮาร์ดแวร์ ประกอบกับวิธีการเข้ารหัสและถอดรหัสที่ให้ประสิทธิภาพสูงมักจะไม่สามารถทำให้เกิดเป็นอุปกรณ์ที่ใช้งานจริงได้ เนื่องจากข้อจำกัดของเทคโนโลยี แต่ในปัจจุบันวิวัฒนาการทางด้าน microelectronics และ digital signal processing ได้ก้าวหน้าไปมาก ทฤษฎีที่ไม่เคยสามารถทำให้เป็นอุปกรณ์จริงของการเข้ารหัสและ

ถอดรหัสได้ถูกนำมาสร้างเป็นวงจรหรืออุปกรณ์ฮาร์ดแวร์ให้ทำงานจริงได้ ปัจจุบัน ECC ถูกนำมาใช้กันอย่างแพร่หลายในระบบสื่อสารเชิงดิจิตอลรูปแบบต่างๆ รวมไปถึงการจัดเก็บข้อมูลเชิงดิจิตอล ตารางที่ 1 แสดงตัวอย่างการนำเอา ECC มาประยุกต์ใช้งาน

ตารางที่ 1

แสดงตัวอย่างการประยุกต์ใช้งานของ ECC

Communication systems	Broadcasting, Mobile phones, Networks, Power line, Satellite, Sonar, Space, Spread spectrum, Telemetry, Telex and Fax
Control systems	Aerospace, Automobile, Naval, Railway
Information security and retrieval systems	Account and card codes, Bar and dot codes, Crypto, ISBN, Product identification codes
Information storage systems	Compact discs, Magnetic tapes and discs, Semiconductor memories
Signal processing systems	Fault tolerance, Image coding, Speech coding

ก่อนอื่น เรามารู้จักกับทฤษฎีของข้อมูล (information theory) ในเบื้องต้น เพื่อลำดับแนวคิดและเป็นพื้นฐานต่อการทำความเข้าใจหลักการของ ECC ทฤษฎีของข้อมูลข่าวสาร ปริมาณของข้อมูล (information content) สามารถกำหนดจากค่าลอกอริทึมของส่วนกลับของความถี่ของการเกิดของข้อมูลนั้น เนื้อความหรือเอนโทรปี (entropy) ของกลุ่มของข้อมูลคือ ค่าเฉลี่ยทางสถิติของปริมาณของข้อมูลแต่ละชุด เพื่อให้เกิดความกระจ่างเกี่ยวกับปริมาณของข้อมูล ยกตัวอย่างประโยค 2 ประโยคเช่น "หนึ่งปีมีสิบสองเดือน" กับ "พรุ่งนี้ลาวจะบุกอเมริกา" เราจะเห็นว่าประโยคแรก โอกาสที่จะเกิดขึ้นคือ ร้อยเปอร์เซนต์ ประโยคนี้มีปริมาณของข้อมูลเป็นศูนย์ แต่ประโยคหลังโอกาสที่จะเกิดขึ้นมีน้อยมาก จึงมีปริมาณของข้อมูลมาก ดังนั้น เราจะเห็นได้ว่าความน่าจะเป็นของการเกิดของข้อมูลเกี่ยวข้องกับปริมาณของข้อมูลที่เราได้รับในลักษณะที่สวนทางกัน นั่นคือ ถ้าข้อมูลมีโอกาสเกิดขึ้นน้อยจะมีปริมาณของข้อมูลมาก แต่ถ้าข้อมูลมีโอกาสของการเกิดขึ้นมากจะมีปริมาณของข้อมูลน้อย ต่อไปมาทำความรู้จักกับคำว่า ความจุของช่องสื่อสาร (channel capacity) ความจุของช่องสื่อสารหนึ่งๆ คือ ปริมาณที่จะบอกว่าเราสามารถส่งข้อมูลด้วยความเร็วเฉลี่ยสูงสุดได้ไม่เกินเท่าไหร่ผ่านช่องสื่อสารนั้น Shannon[1] ได้ค้นพบว่า ความจุ

ของช่องสื่อสารหนึ่งๆ ที่มีสัญญาณรบกวนเป็นแบบ AWGN (additive white Gaussian noise) สามารถอธิบายได้ด้วยความสัมพันธ์ดังนี้

$$C = B\log_2(1+SNR) \quad (1)$$

เมื่อ C คือ ความจุของช่องสื่อสารในหน่วย บิตต่อวินาที B คือ แบนด์วิทของสัญญาณที่จะส่งผ่านช่องสื่อสาร และ SNR คือ อัตราส่วนกำลังงานของสัญญาณต่อกำลังงานของสัญญาณรบกวน (signal to noise ratio) จากสมการที่ (1) จะเห็นว่า วิธีการที่จะเพิ่มค่าของ C สามารถทำได้ 2 วิธีคือ การเพิ่มแบนด์วิทของสัญญาณโดยวิธีของ ECC หรือการเพิ่มกำลังงานของเครื่องส่ง จากประเด็นดังกล่าว เราจะเห็นว่า ระบบที่มีข้อจำกัดในเรื่องกำลังงานของเครื่องส่ง สามารถที่จะส่งสัญญาณไปได้ไกลๆ โดยการเพิ่มแบนด์วิทของสัญญาณโดยการใส่ redundancy ตามหลักการของ ECC โดยให้สัญญาณที่รับได้มีความผิดพลาดอยู่ในช่วงที่ยอมรับได้ เป็นต้น

หลักการเข้ารหัสและถอดรหัส

ECC สามารถแบ่งรูปแบบออกได้เป็น 2 วิธีใหญ่ๆคือ การเข้ารหัสแบบบล็อก (block coding, BC) และการเข้ารหัสแบบคอนโวลูชัน (convolutional coding, CC) รายละเอียดของการเข้ารหัสทั้ง 2 วิธีสามารถหาอ่านเพิ่มเติมได้จากเอกสารอ้างอิง[2-4] แต่ละวิธีจะมีข้อดีและข้อเสียที่แตกต่างกันขึ้นอยู่กับการนำไปใช้งาน การเข้ารหัสแบบ BC ยังมีวิธีการย่อยอีกหลายรูปแบบ ซึ่งไม่สามารถนำมาอธิบายในบทความนี้ทั้งหมดได้ สำหรับการเข้ารหัสแบบ CC จะมีหลักการที่ค่อนข้างแน่นอน สิ่งที่แตกต่างของวิธีการเข้ารหัสแบบ CC จะอยู่ที่การถอดรหัส เพื่อให้เห็นภาพและเข้าใจหลักการพื้นฐาน จะขอยกตัวอย่างวิธีการเข้ารหัสและถอดรหัสทั้ง 2 แบบอย่างง่ายๆ ดังนี้คือ

การเข้ารหัสแบบบล็อก

การเข้ารหัสแบบบล็อกมีหลักการคือ สัญญาณข้อมูลดิจิตอลจะถูกแบ่งออกเป็นบล็อกๆ สมมติให้แต่ละบล็อกประกอบไปด้วยข้อมูลขนาด k บิตผ่านตัวเข้ารหัส (encoder) หรือจำนวนของบิตอินพุท ได้สัญญาณที่เข้ารหัสแล้วออกมาเป็น n บิตหรือจำนวนของบิตเอาท์พุท โดยที่ $n > k$ เสมอ การเข้ารหัสสามารถเขียนด้วยตัวย่อ (n,k) นั่นหมายความว่า จำนวน

ของ RBs เป็น $n-k$ บิต ยกตัวอย่างเช่น $k=3$ และ $n=6$ เราเขียนแทนด้วย การเข้ารหัสบล็อกแบบ $(6,3)$ ซึ่งจะเห็นว่ารูปแบบของสัญญาณข้อมูลที่เป็นไปได้ทั้งหมดคือ $2^3=8$ รูปแบบใน 3-tuple vector space และแต่ละรูปแบบของข้อมูลจะถูกแปลงไปเป็นสัญญาณรหัสที่มีจำนวนบิตเป็น 6 ใน 6-tuple vector space ซึ่งจะมีเพียง 8 สมาชิกเท่านั้นจากทั้งหมด $2^6=64$ สมาชิก ที่จะถูกเลือกมาเป็นสัญญาณรหัส หลักการเลือกก็คือ จะเลือกสมาชิกที่มีความแตกต่างของบิตมากที่สุดมาเป็นสัญญาณรหัส หรือมีระยะทางของแฮมมิง (Hamming distance) มากที่สุด ระยะทางของแฮมมิงของเวกเตอร์ $\bar{u}$ และเวกเตอร์ $\bar{v}$ เขียนแทนด้วย $d(\bar{u},\bar{v})$ หมายถึง จำนวนบิตที่แตกต่างกันของ $\bar{u}$ และ $\bar{v}$ เช่น $\bar{u}=(100010)$ และ $\bar{v}=(010011)$ เราจะได้ $d(\bar{u},\bar{v})=3$ เป็นต้น ตารางที่ 2 แสดงเวกเตอร์ข้อมูลและเวกเตอร์ของสัญญาณรหัส เมื่อเข้ารหัสบล็อกแบบ $(6,3)$

สมมติให้สัญญาณข้อมูลคือ 101110101 สัญญาณรหัสที่ได้จะเป็น 011101101110011101 ในกรณีที่ k มีค่ามากๆ การใช้ตาราง (table look-up) จะไม่เหมาะเนื่องจากต้องใช้เนื้อที่ในหน่วยความจำมาก เช่น การเข้ารหัสบล็อกแบบ $(127,92)$ จะต้องใช้เนื้อที่ในหน่วยความจำถึงอย่างน้อย 2^{92} ซึ่งทำได้ยาก ดังนั้น โดยทั่วไปจะใช้ generator matrix เป็นตัวสร้างสัญญาณรหัสดังนี้คือ สมมุติให้ $\bar{m}$ เป็นเวกเตอร์สัญญาณข้อมูล $\bar{U}$ เป็นเวกเตอร์สัญญาณรหัส ซึ่ง $\bar{U}$ จะมีความสัมพันธ์กับ $\bar{m}$ ดังนี้[2]

ตารางที่ 2

แสดงเวกเตอร์ข้อมูลและเวกเตอร์ของสัญญาณรหัส

เวกเตอร์ข้อมูล	เวกเตอร์รหัส
000	000000
100	110100
010	011010
110	101110
001	101001
101	011101
011	110011
111	000111

$$\vec{U} = \vec{m}G \tag{2}$$

เมื่อ G เป็น generator matrix หาค่าได้จากสมการดังต่อไปนี้

$$G = \begin{bmatrix} \vec{V}_1 \\ \vec{V}_2 \\ - \\ - \\ \vec{V}_k \end{bmatrix} \tag{3}$$

เมื่อ $\vec{V}_1$, $\vec{V}_2$, ..., $\vec{V}_3$ เลือกมาจากเซตของเวกเตอร์ฐาน (set of basis vectors) n เวกเตอร์ใน n-tuple space ซึ่งสามารถเลือกได้ $\binom{n}{k}$ วิธี ยกตัวอย่างเช่น generator matrix ที่สร้างเวกเตอร์รหัสในตารางที่ 2 คือ

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

จะเห็นว่าแต่ละแถวของ generator matrix เป็นสมาชิกของเซตของเวกเตอร์ฐานใน 6-tuple vector space ในกรณีการเข้ารหัสบล็อกตามตัวอย่างในตารางที่ 2 เป็นตัวอย่างหนึ่งการเข้ารหัสบล็อกแบบเป็นระบบ (systematic block code) นั่นคือแต่ละรหัสจะประกอบไปด้วยสัญญาณข้อมูล (message bits) เดิมและ RBs ดังนั้น เราสามารถที่จะเขียน G ในรูปของ

$$G = [P, I_k] \tag{4}$$

เมื่อ P คือ matrix ในส่วนที่จะสร้าง parity-check bits ซึ่งเป็น matrix ขนาด $k \times (n-k)$ ส่วน I_k คือ identity matrix มีขนาดเป็น $k \times k$ วิธีการถอดรหัส-การเข้ารหัสโดยวิธีนี้ใช้วิธีที่เรียกว่า syndrome test โดยมีหลักการคือ สมมติให้ $\vec{r}$ คือ เวกเตอร์สัญญาณที่รับได้ที่เครื่องรับ ขั้นแรกคำนวณหาค่า

$$S = \vec{r}H^T \tag{5}$$

เมื่อ S เรียกว่า ค่า syndrome H คือ parity-check matrix หาจาก $H=\left[I_{n-k}, P^T\right]$ ถ้าสัญญาณที่รับได้ไม่มีความผิดพลาดเกิดขึ้น ค่าของ S จะเป็นศูนย์ แต่ถ้ามีความผิดพลาดเกิดขึ้นค่าของ S จะไม่เป็นศูนย์และให้นำค่าของ S ที่ได้ไปเปรียบเทียบกับรูปแบบของความผิดพลาดที่คำนวณเอาไว้แล้ว ยกตัวอย่างเช่นจากการเข้ารหัส $(6,3)$ ข้างต้นจะมีรูปแบบของความผิดพลาดและค่าของ S ที่สอดคล้องกัน ดังแสดงในตารางที่ 3

ถ้ารับสัญญาณได้ $\bar{r}=001110$ ค่า $S=\bar{r}H^T=100$ ซึ่งตรงกับรูปแบบของความผิดพลาด 100000 ดังนั้น แสดงว่าสัญญาณรหัสที่ส่งมาเกิดความผิดพลาดขึ้นในบิตที่ 6 จึงได้ $U=101110$ เป็นต้น

การเข้ารหัสแบบคอนโวลูชัน

การเข้ารหัสแบบคอนโวลูชันจะแตกต่างการเข้ารหัสแบบบล็อกคือ ใน BC ข้อมูลที่ถูกแบ่งออกเป็นบล็อก แต่ละบล็อกประกอบไปด้วย k บิตนั้นเมื่อเข้ารหัสแล้วจะได้สัญลักษณ์รหัส n บิต โดยกระบวนการเข้ารหัสจะเกิดขึ้นอย่างเป็นอิสระต่อกันในแต่ละ

ตารางที่ 3

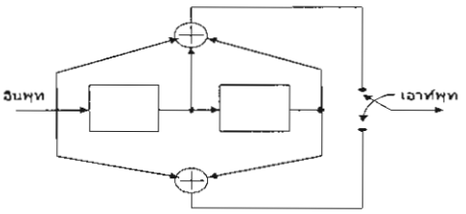
Syndrome Look-up table ของรหัส (6,3)

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

บล็อก ในขณะที่ใน CC การได้มาของสัญญาณรหัส n บิตจะขึ้นอยู่กับทั้ง ข้อมูล k บิต ณ ขณะปัจจุบันและกลุ่มของข้อมูล k บิตก่อนหน้านั้น โดยที่จะขึ้นอยู่กับกี่กลุ่มก่อนหน้า

นั้นแล้วแต่ผู้ออกแบบจะกำหนด ถ้าจำนวนกลุ่มก่อนหน้านั้นมีมาก ประสิทธิภาพของการเข้ารหัสก็จะสูงแต่ก็จะใช้หน่วยความจำมาก โดยทั่วไป CC จะถูกกำหนดด้วย 3 ตัวแปร โดยสามารถเขียนเป็นตัวย่อได้คือ (n,k,K) เมื่อ k คือจำนวนบิตอินพุท n คือ จำนวนบิตเอาท์พุท และ K เรียกว่า code constraint length ซึ่งจะสัมพันธ์กับหน่วยความจำของตัวเข้ารหัส รูปที่ 1 แสดงตัวอย่างของการเข้ารหัสคอนโวลูชันแบบ $(2,1,3)$ ซึ่งจะประกอบไปด้วย 1) 3-stage shift register นั่นหมายความว่าสัญลักษณ์ รหัสปัจจุบันขึ้นอยู่กับบิตข้อมูลปัจจุบันและ 2 บิตข้อมูลก่อนหน้านั้น 2) modulo-2 adder หรือ exclusive OR gate 2 ชุด (เท่ากับจำนวนของบิตเอาท์พุท) 3) multiplexer หรือ commutator ซึ่งทำหน้าที่มัลติเพล็กซ์บิตเอาท์พุต

การรวมกันของบิตข้อมูลใน register ถูกควบคุมด้วย generator polynomial $\bar{g}_1$ และ $\bar{g}_2$ เมื่อ $\bar{g}_1$ แทนการต่อกันของบิตข้อมูลในซีกบน และ $\bar{g}_2$ แทนการต่อกันของ

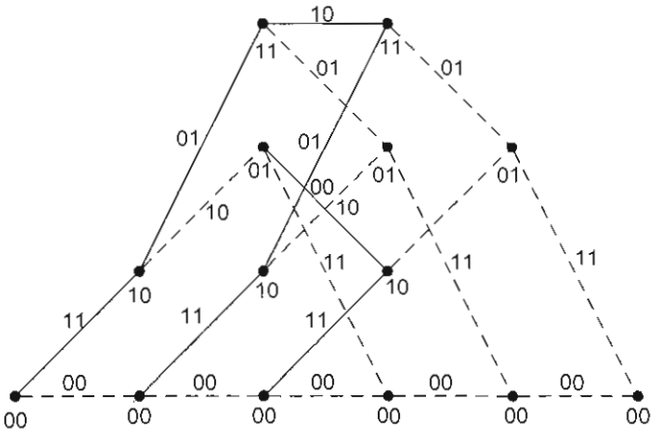


รูปที่ 1 แสดงตัวเข้ารหัสคอนโวลูชันแบบ (2,1,3)

บิตข้อมูลในซีกล่าง ซึ่งจะเห็นว่า $\bar{g}_1 = [1\ 1\ 1]$ และ $\bar{g}_2 = [1\ 0\ 1]$ ในการเข้ารหัสแบบ CC จะต้องมีการรีเซท register ด้วยบิตศูนย์ ซึ่งจะมีจำนวนเท่ากับ $K-1$ ก่อนที่จะทำการเข้ารหัสในครั้งต่อๆ ไป ตัวอย่างเช่น ในรูปที่ 1 ค่า $K=3$ ดังนั้น เราต้องการบิตศูนย์จำนวน 2 บิตเพื่อล้าง register ก่อนที่จะทำการเข้ารหัสในครั้งต่อไป สมมติให้ข้อมูลเป็น 101 จะได้บิตเอาท์พุทออกมาเป็น 1110001011 โดยที่ 6 บิตแรกของเอาท์พุทเกิดจากข้อมูลและ 4 บิตหลังเกิดจากบิตศูนย์ จำนวน 2 บิตเพื่อใช้ล้าง regsiter

การถอดรหัส CC สามารถทำได้หลายวิธี ในที่นี้จะขอยกตัวอย่างการถอดรหัสที่นิยมใช้กันมากที่สุดคือ การถอดรหัสแบบ Viterbi (Viterbi algorithm, VA) ซึ่งถูกค้นพบโดย Viterbi ในปี 1967[3] หลักการทำงานของ VA จะอาศัยหลักการของ MLD (maximum likelihood decoding) ซึ่งจะเกี่ยวข้องกับการวัดความเหมือนสูงสุดระหว่างสัญญาณที่รับได้กับ

สัญญาณรหัสซึ่งถูกเขียนบน trellis diagram รูปที่ 2 แสดง trellis diagram ของ CC ในรูปที่ 1 เมื่อกำหนดข้อมูลเป็น 101

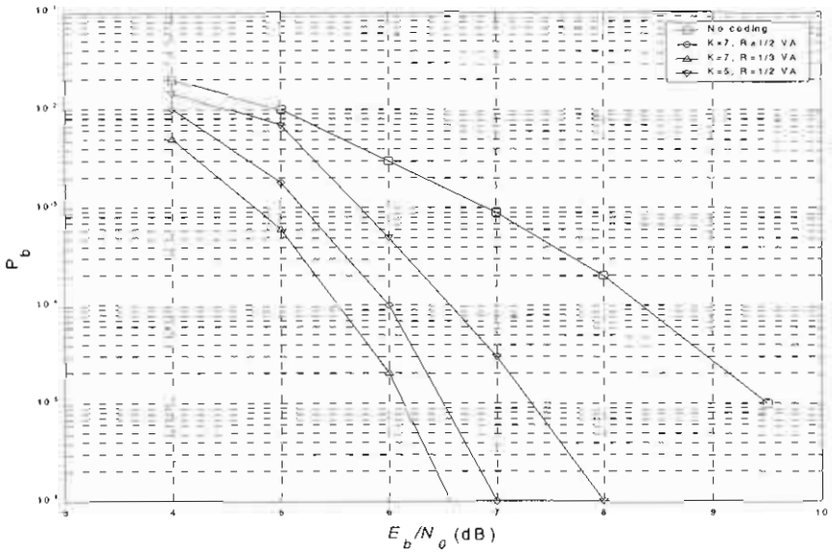


รูปที่ 2 แสดง trellis diagram ของ CC ในรูปที่ 1

จากรูปที่ 2 อธิบายได้ว่า สัญลักษณ์รหัสจะถูกเขียนบนเส้นที่เชื่อมต่อระหว่างโหนดของ trellis ตัวเลขกำกับบนโหนดแสดงสถานะของ register หรือสถานะของตัวเข้ารหัส (encoder state) เส้นประแสดงว่า บิตอินพุทเป็นศูนย์ เส้นทึบแสดงว่าบิตอินพุทเป็นหนึ่ง สมมติว่าสัญญาณที่รับได้เป็น 1101111100 VA จะทำการเปรียบเทียบสัญญาณที่รับได้กับทางเดินใน trellis ว่าเหมือนกับทางเดินไหนมากที่สุด ทางเดินใน trellis นั้นก็จะเป็น decoded path ซึ่งจากรูปก็จะเห็นว่าทางเดิน 1101011100 เหมือนกับสัญญาณที่รับได้มากที่สุด ซึ่งเมื่อดูจาก trellis ก็จะได้ข้อมูลที่ส่งมาเป็น 110 เป็นต้น

เพื่อให้เห็นถึงประสิทธิภาพของ ECC รูปที่ 3 แสดงผลการจำลองในคอมพิวเตอร์ของการถอดรหัสแบบ VA เมื่อใช้ CC ที่อัตราการเข้ารหัสต่างๆ และที่ K ค่าต่างๆ ในระบบที่มีการรบกวนแบบ AWGN และใช้วิธีการมอดูเลตแบบ BPSK จะเห็นว่า ประสิทธิภาพของระบบดีขึ้นเมื่ออัตราส่วนของการเข้ารหัสลดลงจาก 1/2 มาเป็น 1/3 และค่าของ code constraint length เพิ่มขึ้นจาก 5 มาเป็น 7 เราสามารถนิยาม coding gain ได้จากค่าผลต่างของ Eb/N0 (dB) ที่ค่า P_b (probability of bit error) เดียวกันของระบบที่ไม่มีการเข้ารหัสและระบบที่มีการ

เข้ารหัส เช่น จากรูป coding gain เมื่อ $R = 1/2$ และ $K = 7$ ที่ค่า $P_b = 10^{-5}$ มีค่าประมาณ 2 dB นั่นหมายความว่า เราสามารถประหยัดกำลังงานของเครื่องส่งได้ถึง 2 dB ที่ประสิทธิภาพเท่ากัน



รูปที่ 3 แสดงประสิทธิภาพของ ECC

สรุป

ECC คือ เทคนิคหนึ่งที่ใช้ในการตรวจจับและควบคุมความผิดพลาดในระบบสื่อสารและจัดเก็บข้อมูลเชิงดิจิตอล โดยใช้หลักการของการเพิ่ม redundancy ให้กับข้อมูลเปรียบเสมือนเป็นการเพิ่มภูมิคุ้มกันให้กับข้อมูลจากการถูกรบกวนด้วยสัญญาณที่เราไม่ต้องการ กระบวนการใส่ RBs ให้กับข้อมูลมีหลายวิธี แต่ละวิธีนำมาซึ่งการเข้ารหัสแต่ละแบบ การเลือกใช้วิธีการเข้ารหัสและถอดรหัส ขึ้นอยู่กับการประยุกต์ใช้งาน [4] อย่างไรก็ตาม การเพิ่มประสิทธิภาพโดยวิธีของ ECC ก็มีสิ่งที่ต้องแลกเปลี่ยนกับการได้มาซึ่งประสิทธิภาพที่ดีขึ้น นั่นก็คือการเพิ่มของแบนด์วิทของสัญญาณที่จะส่งไปเนื่องจากสัญญาณมี redundancy เพิ่มขึ้น แต่การแลก

เปลี่ยนแบนด์วิทกับประสิทธิภาพ ไม่ได้เป็นการแลกเปลี่ยนแบบเท่าทุน การแลกเปลี่ยนเป็นไปในลักษณะที่ได้กำไร นั่นคือ ประสิทธิภาพที่เพิ่มขึ้นได้มากกว่าการชดเชยด้วยแบนด์วิท[5]

เอกสารอ้างอิง

1. C. E. Shannon, ***A Mathematical Theory of Communications***, Bell Syst. Tech. J., vol. 27, pp. 379-423, 1948
2. B. Sklar, ***Digital Communications: Fundamentals and Applications***, Prentice-Hall, 1988
3. S. Lin and D.J. Costello, Jr., ***Error-Control Coding: Fundamentals and Applications***, Prentice-Hall, 1983
4. Daniel J. Costello, Jr., Joachim Hagenauer, Hideki Imai, Stephen B. Wicker, ***Applications of Error-Control Coding,*** IEEE Transactions on Information Theory, Vol.44, No.6, pp. 2531-2560, Oct 1998.
5. Stephen B. Wicker, ***Error Control Systems for Digital Communication and Storage***, Prentice-Hall, 1995