4 รหัสที่สำคัญบางรหัส Some Special Codes

4.1 รหัสแฮมมิ่ง (Hamming Codes)

รหัสแฮมมิ่งเป็นรหัสที่สำคัญและเป็นที่รู้จักกันแพร่หลายรหัสหนึ่ง เป็นรหัสที่ใช้ใน computer RAM ค้นพบโดย Marcel Golay ในปี 1949 และโดย Richard Hamming ในปี 1950 ต่างคนต่างค้นพบโดยอิสระจากกัน รหัสแฮมมิ่งเป็นรหัสเชิงเส้น ที่เป็นรหัสสมบูรณ์ เป็นรหัสที่ออกแบบให้สามารถแก้ไขข้อผิดพลาดได้หนึ่งตำแหน่ง มีขั้นตอนการถอดรหัสที่ง่าย รหัสแฮมมิ่งเป็นรหัสที่นิยามโดยใช้ชุดตัวอักษรจากฟีลด์จำกัด F_q สำหรับ q ที่เป็นจำนวนเฉพาะยกกำลังใดๆ ซึ่งเราจะเรียกว่ารหัสแฮมมิ่งฐาน q แต่เราจะศึกษาวิธีสร้างเฉพาะกรณีที่ q เป็นจำนวนเฉพาะ (สำหรับกรณีที่ q เป็นจำนวนเฉพาะยกกำลัง เราสร้างได้ในทำนองเดียวกัน) เราจะสร้างรหัสแฮมมิ่งโดยการสร้างเมทริกซ์ตรวจสอบภาวะเสมอ ที่มีจำนวนหลักมากที่สุด และเพื่อความสะดวกในการอธิบาย เราจะเริ่มต้นจากรหัสแฮมมิ่งฐานสอง นั่นคือ จะเริ่มจากกรณีที่ $q = 2$

รหัสแฮมมิ่งฐานสอง

เป็นรหัสที่ใช้ฟีลด์ $F_2 = \{0, 1\}$ เป็นชุดตัวอักษร

นิยาม 4.1.1 ให้ r เป็นจำนวนเต็มบวกซึ่ง $r \geq 2$ และให้ H เป็นเมทริกซ์ขนาด $r \times (2^r - 1)$ ซึ่งแต่ละหลักของ H คือเวกเตอร์ที่ไม่ใช่ศูนย์ใน F_2^r ทั้งหลายที่แตกต่างกัน เรียกรหัสซึ่งมี H เป็นเมทริกซ์ตรวจสอบภาวะเสมอว่ารหัสแฮมมิ่ง(ฐานสอง) และจะแทนรหัสนี้ด้วย Ham(r, 2)

ตัวอย่าง 4.1.1 : พิจารณากรณีที่ $r = 2$ เวกเตอร์ที่ไม่ใช่เวกเตอร์ศูนย์ใน F_2^2 มีทั้งหมด 3 เวกเตอร์ คือ 01, 10, และ 11 ดังนั้น

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

เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(2, 2)

ตัวอย่าง 4.1.2 : พิจารณากรณีที่ $r = 3$ เวกเตอร์ที่ไม่ใช่เวกเตอร์ศูนย์ใน F_2^3 มีทั้งหมด 7 เวกเตอร์ คือ 001, 010, 100, 011, 101, 110, และ 111 ดังนั้น

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

เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(3, 2)

หมายเหตุ :

1. ความยาวของรหัส Ham(r, 2) คือ $n = 2^r - 1$
2. มิติของรหัส $\text{Ham}(r, 2)^\perp$ คือ r = จำนวนแถวของเมทริกซ์ H
3. ลำดับของแต่ละหลักใน H จะเรียงลำดับอย่างไรก็ได้
4. เพื่อประโยชน์ในการหาเมทริกซ์ก่อกำเนิด เราจะจัดเรียง H ให้อยู่ในรูปมาตรฐาน $H = [B \mid I]$ เช่น ในกรณี $r = 3$ เราอาจจัดเรียงแต่ละหลักใน H ในตัวอย่าง 4.1.2 ใหม่ได้เป็น

$$H_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

5. เพื่อประโยชน์ในการถอดรหัส (ซึ่งจะกล่าวถึงในภายหลัง) เราจะเรียงลำดับของแต่ละหลักใน H ตามลำดับธรรมชาติของตัวแทนฐานสอง เช่นในกรณี $r = 3$ เราอาจจัดเรียงแต่ละหลักใน H ในรูป

$$H_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

หลักแรกของ H_2 คือ 001^T ซึ่งเป็นจำนวนฐานสองที่แทนจำนวนเต็ม 1

หลักที่ 2 ของ H_2 คือ 010^T ซึ่งเป็นจำนวนฐานสองที่แทนจำนวนเต็ม 2 และต่อไปเรื่อย ๆ จะเห็นว่าหลักที่ 1 – 7 ของ H_2 เป็นตัวแทนฐานสองของจำนวนธรรมชาติ 1, 2, 3, 4, 5, 6, 7 ตามลำดับ

ทฤษฎีบท 4.1.1

(สมบัติของรหัสแฮมมิ่ง) สำหรับ $r \geq 2$

1. มิติของ Ham(r, 2) คือ $k = n - r = 2^r - 1 - r$
2. Ham(r, 2) เป็นรหัส – $[2^r - 1, 2^r - 1 - r]$
3. ระยะน้อยสุดของ Ham(r, 2) คือ $d = 3$
4. Ham(r, 2) เป็นรหัสสมบูรณ์

พิสูจน์

1. จากขนาดของเมทริกซ์ตรวจสอบภาวะเสมอ H ของรหัส Ham(r, 2) เรารู้ว่า $\text{Ham}(r, 2)^{\perp}$ มีมิติเท่ากับ r นั่นคือ $\text{Ham}(r, 2)^{\perp}$ เป็นรหัส – $[2^r - 1, r]$ ดังนั้น มิติของ Ham(r, 2) เท่ากับ $k = n - r = 2^r - 1 - r$
2. เนื่องจาก H ซึ่งเป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(r, 2) มีขนาด $r \times (2^r - 1)$ จากข้อ 1 เรารู้ว่ามิติของ Ham(r, 2) คือ $k = n - r = 2^r - 1 - r$ ดังนั้น Ham(r, 2) เป็นรหัส – $[2^r - 1, 2^r - 1 - r]$
3. เนื่องจาก Ham(r, 2) เป็นรหัสเชิงเส้น ดังนั้น เราจะพิสูจน์ให้เห็นว่าคำรหัสแต่ละคำใน Ham(r, 2) มีน้ำหนัก ≥ 3 ซึ่งสามารถพิสูจน์ได้โดยการแสดงว่าใน Ham(r, 2) ไม่มีคำซึ่งมีน้ำหนักเท่ากับ 1 และ 2 ดังนี้

   สมมุติว่ามีคำที่มีน้ำหนักเท่ากับ 1 ใน Ham(r, 2) และสมมุติว่าคำที่มีน้ำหนักเท่ากับ 1 นั้นคือ $x = 00...010...0$ (โดยที่ 1 อยู่ในตำแหน่งที่ i) เนื่องจาก x ตั้งฉากกับทุก ๆ แถวของ H แสดงว่าตำแหน่งที่ i ของแต่ละแถวของ H ต้องเป็น 0 ทั้งหมด ดังนั้น

สมาชิกในหลักที่ i ของ H ต้องเป็น 0 ทั้งหมด ซึ่งเป็นไปไม่ได้ เพราะจากคำจำกัดความของรหัสแฮมมิ่ง H ต้องไม่มีหลักที่เป็นศูนย์

สมมุติว่ามีคำที่มีน้ำหนักเท่ากับ 2 ใน Ham(r, 2) สมมุติว่าคำที่มีน้ำหนักเท่ากับ 2 นั้นคือ $\mathbf{x}$ = 00...010...010...0 (โดยมี 1 อยู่ในตำแหน่งที่ i และ j) เนื่องจาก $\mathbf{x}$ ตั้งฉากกับทุก ๆ แถวของ H แสดงว่าตำแหน่งที่ i และ j ของแต่ละแถวของ H ต้องเหมือนกัน นั่นคือ หลักที่ i และ j ของเมทริกซ์ H ต้องเหมือนกัน ซึ่งเป็นไปไม่ได้เช่นกัน เพราะจากนิยาม 4.1.1 แต่ละหลักของ H ต้องแตกต่างกัน ดังนั้น d(Ham(r, 2)) $\geq$ 3

ต่อไปเราจะต้องแสดงว่าในรหัส Ham(r, 2) มีคำรหัสที่มีน้ำหนักเท่ากับ 3 เลือกเมทริกซ์ H ซึ่งสามหลักแรกของ H คือ

$$\begin{bmatrix}0\\ \vdots\\ 0\\ 1\end{bmatrix}, \begin{bmatrix}0\\ \vdots\\ 1\\ 0\end{bmatrix}, \text{ และ } \begin{bmatrix}0\\ \vdots\\ 1\\ 1\end{bmatrix}$$

จะเห็นว่าเวกเตอร์ $\mathbf{x}$ = 1110...0 ตั้งฉากกับทุกแถวของ H แสดงว่า $\mathbf{x}$ เป็นคำรหัสใน Ham(r, 2) ดังนั้น d(Ham(r, 2)) = 3

4. จากข้อ 1 เรารู้ว่ามิติของ Ham(r, 2) เท่ากับ $n - r$ ดังนั้น จำนวนคำรหัสของ Ham(r, 2) เท่ากับ 2^{n-r} และจากข้อ 3 เรามี

$$d(\text{Ham}(r, 2)) = 3 = 2t + 1$$

นั่นคือ t = 1 แทน t = 1 ในนิพจน์ทางซ้ายของสมการ (1.14.2) ในหัวข้อ 1.14 เราได้

$$2^{n-r}\left(1+\binom{n}{1}\right) = 2^{n-r}(1 + n) = 2^{n-r}(1 + 2^r - 1) = 2^n$$

แสดงว่า Ham(r, 2) เป็นรหัสสมบูรณ์ ∎

ขั้นตอนการถอดรหัส

ถ้า $\mathbf{x}$ = 0...010...0 (1 อยู่ในหลักที่ i) แล้วซินโดรม $S(x) = \mathbf{x}H^T$ จะตรงกับหลักที่ i ของเมทริกซ์ H ดังนั้น ถ้า H เป็นเมทริกซ์ซึ่งหลักของ H เป็นตัวแทนฐานสองของจำนวนซึ่งเรียงตามลำดับธรรมชาติ แล้วการถอดรหัสจะมีขั้นตอนง่าย ๆ คือ

ขั้นที่ 1 เมื่อได้รับเวกเตอร์ $\mathbf{x}$ คำนวณซินโดรม $S(\mathbf{x}) = \mathbf{x}H^T$

ขั้นที่ 2 ถ้า $S(\mathbf{x}) = \mathbf{0}$ ยอมรับว่า $\mathbf{x}$ เป็นคำรหัสที่ส่ง

ขั้นที่ 3 ถ้า $S(\mathbf{x}) \neq \mathbf{0}$ แสดงว่ามีข้อผิดพลาดเกิดขึ้นหนึ่งตำแหน่ง คือผิดพลาดในตำแหน่งที่เป็นจำนวนที่มี $S(\mathbf{x})$ เป็นตัวแทนฐานสอง

ตัวอย่าง 4.1.3 : ใช้เมทริกซ์

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

ถอดรหัสเวกเตอร์ต่อไปนี้

1. $\mathbf{x}$ = 0010111 2. $\mathbf{y}$ = 1111100

วิธีทำ 1 จะเห็นว่าหลักที่ 1 – 7 ของ H เป็นจำนวนฐานสองที่แทนจำนวนธรรมชาติ 1, 2, ..., 7 ตามลำดับ คำนวณหาซินโดรมของ $\mathbf{x}$ ดังนี้

$$S(\mathbf{x}) = \mathbf{x}H^T = (0,0,1,0,1,1,0)\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = (0,0,0)$$

เนื่องจาก S(**x**) = **0** = 000 เรายอมรับว่า **x** คือคำรหัสที่ส่ง

วิธีทำ 2 คำนวณหาซินโดรมของ **y**

$$S(\mathbf{y}) = \mathbf{y}H^T = (1,1,1,1,0,0,0)\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = (1,0,0)$$

จะเห็นว่า 100 เป็นจำนวนฐานสองที่แทนจำนวนเต็ม 4 กล่าวคือ $(100)_2 = 4_{10}$ แสดงว่าเวกเตอร์ **y** = 1111000 ที่ได้รับ ผิดไปจากคำรหัสที่ส่งหนึ่งตำแหน่ง คือผิดในตำแหน่งที่ 4 ดังนั้น เราถอดรหัสเวกเตอร์ **y** = 1111000 ให้เป็นคำรหัส 1110000 คือแก้ไขตำแหน่งที่ 4 ของ **y** จาก 1 ให้เป็น 0

การขยายรหัสแฮมมิ่ง

ให้ Hâm(r,2) เป็นรหัสที่ได้จากการเพิ่มบิตตรวจสอบภาวะเสมอ (คู่) เข้าไปในคำรหัสทุกคำของ Ham(r, 2) จากทฤษฎีบท 1.12.1 เรารู้ว่าระยะน้อยสุดของ Hâm(r, 2) เท่ากับ 4 และจากแบบฝึกหัด 3 ข้อ 2 เรารู้ว่า Hâm(r, 2) เป็นรหัสเชิงเส้น ดังนั้น Hâm(r, 2) เป็นรหัสเชิงเส้นที่มีพารามิเตอร์ $[2^r, 2^r - 1 - r, 4]$ และถ้า H เป็นเมทริกซ์ตรวจสอบภาวะเสมอของ Ham(r, 2) แล้วเมทริกซ์ตรวจสอบภาวะเสมอของรหัสขยาย Hâm(r, 2) คือ

$$\hat{H} = \begin{bmatrix} & & & & 0 \\ & & & & 0 \\ & & H & & \vdots \\ & & & & 0 \\ 1 & 1 & \cdots & 1 & 1 \end{bmatrix}$$

แถวสุดท้ายของเมทริกซ์ $\hat{H}$ กำหนดสมการสำหรับตรวจสอบภาวะเสมอ กล่าวคือ ถ้า $x_1x_2 \ldots x_{n+1}$ เป็นคำรหัสของ $\hat{\mathrm{H}}\mathrm{am}(r, 2)$ แล้ว

$$x_1 + x_2 + \ldots + x_{n+1} = 0$$

ดังนั้น ถ้า H เป็นเมทริกซ์ตรวจสอบภาวะเสมอของ Ham(r, 2) ที่หลักของ H เป็นจำนวนฐานสองซึ่งเรียงตามลำดับธรรมชาติ แล้วการถอดรหัสสำหรับรหัส $\hat{\mathrm{H}}\mathrm{am}(r,2)$ จะมีขั้นตอนง่าย ๆ เช่นกัน เราจะอธิบายสำหรับกรณีที่ r = 3 เพื่อเป็นตัวอย่างสำหรับกรณี r ใด ๆ

ตัวอย่าง 4.1.4 : เมทริกซ์ตรวจสอบภาวะเสมอของ $\hat{\mathrm{H}}\mathrm{am}(r, 2)$ คือ

$$\hat{H} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

ซินโดรมของเวกเตอร์ $\mathbf{e}_i$ = (00 … 010…0) คือ $S(\mathbf{e}_i) = \mathbf{e}_i H^T$ ซึ่งก็คือหลักที่ i ของเมทริกซ์ $\hat{H}$ ถ้า **y** เป็นเวกเตอร์ที่ได้รับ เราคำนวณหาซินโดรม $S(\mathbf{y}) = \mathbf{y}\hat{H}^T$ สมมุติว่า

$$S(\mathbf{y}) = (s_1, s_2, s_3, s_4)$$

เราถอดรหัสตามขั้นตอนต่อไปนี้

ขั้นที่ 1 ถ้า $s_4 = 0$ และ $(s_1, s_2, s_3) = \mathbf{0}$ ให้คิดว่าไม่มีข้อผิดพลาดเกิดขึ้น ยอมรับว่า **y** คือคำรหัสที่ส่ง

ขั้นที่ 2 ถ้า $s_4 = 0$ แต่ $(s_1, s_2, s_3) \neq \mathbf{0}$ ให้คิดว่ามีข้อผิดพลาดเกิดขึ้นอย่างน้อยสองตำแหน่ง ในกรณีนี้ เราขอให้ต้นทางส่งมาใหม่

ขั้นที่ 3 ถ้า $s_4 = 1$ และ $(s_1, s_2, s_3) = \mathbf{0}$ ให้คิดว่ามีข้อผิดพลาดเกิดขึ้นหนึ่งตำแหน่งคือเกิดขึ้นในตำแหน่งสุดท้าย

ขั้นที่ 4 ถ้า $s_4 = 1$ แต่ $(s_1, s_2, s_3) \neq \mathbf{0}$ ให้คิดว่ามีข้อผิดพลาดเกิดขึ้นหนึ่งตำแหน่ง คือเกิดขึ้นในตำแหน่งที่ i เมื่อ i คือจำนวนซึ่งแทนด้วยจำนวนฐานสอง (s_1, s_2, s_3)

รหัสแฮมมิ่งฐาน q

จากทฤษฎีบท 3.8.2 ถ้า H เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสเชิงเส้น C เรารู้ว่าระยะน้อยสุดของ C เท่ากับ 3 ก็ต่อเมื่อสองหลักใด ๆ ของ H เป็นเซตอิสระเชิงเส้น นั่นคือต้องไม่มีหลักใดของ H เป็นพหุคูณของหลักอื่น ๆ ดังนั้นถ้าเราจะสร้างรหัส C ซึ่งเป็นรหัส-$[n, n - r, 3]$ สำหรับ r ซึ่ง $r \geq 2$ โดยให้ n มีค่ามากที่สุดเท่าที่จะทำได้แล้ว เราจะต้องหาเซตของเวกเตอร์ใน F_q^r ที่ไม่ใช่เวกเตอร์ศูนย์ซึ่งไม่มีเวกเตอร์ใดเป็นพหุคูณของเวกเตอร์อื่น ๆ

ถ้า v เป็นเวกเตอร์ใน F_q^r ที่ไม่ใช่เวกเตอร์ศูนย์แล้ว จะมีเพียง $q - 1$ เวกเตอร์เท่านั้น ที่เป็นพหุคูณของ v เซตของเวกเตอร์เหล่านั้นได้แก่

$$\{av \mid a \in F_q \text{ และ } a \neq 0\}$$

จำนวนเวกเตอร์ที่ไม่ใช่ศูนย์ใน F_q^r ทั้งหมดเท่ากับ $|F_q^r| - 1 = q^r - 1$ จะถูกแบ่งออกเป็น $\frac{q^r - 1}{q - 1}$ กลุ่ม ๆ ละ $q - 1$ เวกเตอร์ โดยที่สมาชิกในกลุ่มเดียวกันเป็นพหุคูณของกันและกัน ดังนั้น ถ้าเราจะสร้างรหัสที่มีความยาว n มากที่สุด และมีระยะน้อยสุด d เท่ากับ 3 เราจะต้องสร้างเมทริกซ์ตรวจสอบภาวะเสมอ H ซึ่งแต่ละหลักของ H จะต้องไม่เป็น **0** และจะต้องเป็นเวกเตอร์ที่มาจากกลุ่มที่ต่างกัน เพราะจะทำให้ไม่มีเวกเตอร์ที่เป็นพหุคูณของกันเวกเตอร์อื่น

นิยาม 4.1.2 ให้ $r \geq 2$ เรียกรหัส C ว่ารหัสแฮมมิ่งฐาน q ถ้าเมทริกซ์ตรวจสอบภาวะเสมอของ C คือเมทริกซ์ H ซึ่งแต่ละหลักของ H เป็นเวกเตอร์ที่ไม่ใช่เวกเตอร์ศูนย์ และมาจากกลุ่มที่ต่างกันกลุ่มละหนึ่งเวกเตอร์เท่านั้น

หมายเหตุ : ในกรณีที่ $q = 2$ เราได้รหัสแฮมมิ่งฐานสอง

เพื่อความเข้าใจยิ่งขึ้น เราจะยกตัวอย่างสำหรับกรณีที่ $r = 2$, $q = 3$

ตัวอย่าง 4.1.5 : ในกรณีที่ $r = 2$, $q = 3$ เราแบ่งเวกเตอร์ใน F_3^2 ที่ไม่ใช่เวกเตอร์ศูนย์ออกเป็น $\frac{3^2-1}{3-1} = 4$ กลุ่ม โดยที่สมาชิกในกลุ่มเดียวกัน เป็นพหุคูณของกันและกัน ดังนี้

$$\left\{\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}0\\2\end{pmatrix}\right\},\ \left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}2\\0\end{pmatrix}\right\},\ \left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}2\\2\end{pmatrix}\right\},\text{ และ } \left\{\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}2\\1\end{pmatrix}\right\}$$

เลือกหนึ่งเวกเตอร์จากแต่ละกลุ่ม สมมุติว่าเลือกเวกเตอร์แรกของแต่ละกลุ่ม ให้เวกเตอร์ที่เลือกเหล่านี้เป็นหลักของเมทริกซ์ H เราได้

$$H = \begin{bmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 2\end{bmatrix}$$

เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(2, 3) หรือเราอาจเลือกเวกเตอร์ที่สองจากแต่ละกลุ่ม เราได้

$$H_1 = \begin{bmatrix}0 & 2 & 2 & 2\\ 2 & 0 & 2 & 1\end{bmatrix}$$

เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(2, 3) ด้วยเช่นกัน

ตัวอย่าง 4.1.6 : ในทำนองเดียวกับในตัวอย่าง 4.1.5 เราได้

1. เมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(2, 11) คือ

$$\begin{bmatrix}0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\end{bmatrix}$$

2. เมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(3, 3) คือ

$$\begin{bmatrix}0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2\\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2\end{bmatrix}$$

ทฤษฎีบท 4.1.2

> **สมบัติของรหัสแฮมมิ่งฐาน q**
> 1. Ham(r, q) เป็นรหัส – $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$
> 2. Ham(r, q) เป็นรหัสสมบูรณ์ซึ่งสามารถแก้ไขข้อผิดพลาดได้หนึ่งตำแหน่ง

พิสูจน์ 1 เป็นจริงตามนิยามของรหัสแฮมมิ่งฐาน q

พิสูจน์ 2 เนื่องจากระยะน้อยสุด d ของ Ham(r, q) คือ $3 = 2t + 1$ เมื่อ $t = 1$ จำนวนที่อยู่ทางด้านซ้ายของ sphere-packing bound คือ

$$q^{n-r}(1 + n(q - 1)) = q^{n-r}(1 + q^r - 1) = q^n$$

ซึ่งเท่ากับจำนวนทางขวามือของ sphere-packing bound ดังนั้น Ham(r, q) เป็นรหัสสมบูรณ์ และสามารถแก้ไขข้อผิดพลาดได้หนึ่งตำแหน่ง เพราะว่ามีระยะน้อยสุด $d = 3$ ▬

บทแทรก 4.1.1

> ถ้า q เป็นจำนวนเฉพาะยกกำลัง และถ้า $n = (q^r - 1)/(q - 1)$ สำหรับจำนวนเต็ม $r \geq 2$ แล้ว $A_q(n, 3) = q^{n-r}$

ตัวอย่าง 4.1.7 : จงหา $A_2(15, 3)$

ในที่นี้ $n = 15, d = 3$ และ $q = 2$

$$n = 15 = \frac{2^r - 1}{2 - 1} = 2^r - 1$$

แสดงว่า $r = 4$ ดังนั้น จากบทแทรก 4.1.1 เราได้

$$A_2(15, 3) = 2^{n-r} = 2^{11} = 2048$$

การถอดรหัสแฮมมิ่งฐาน q

เนื่องจากรหัสแฮมมิ่งเป็นรหัสสมบูรณ์ ซึ่งสามารถแก้ไขข้อผิดพลาดได้หนึ่งตำแหน่ง โคเซตนำของแถวลำดับมาตรฐานประกอบด้วยเวกเตอร์ศูนย์และเวกเตอร์ที่มีน้ำหนักเท่ากับ 1 ทั้งหมด และซินโดรม

ของโคเซตนำ $f_i = 0 \ldots 0b0 \ldots 0$ เมื่อ b อยู่ในตำแหน่งที่ i คือ

$$S(f_i) = S(0 \ldots 0b0 \ldots 0)$$
$$= (0 \ldots 0b0 \ldots 0)H^T = bh_i$$

เมื่อ h_i คือเวกเตอร์สลับเปลี่ยนของหลักที่ i ของ H

ด้วยเหตุนี้ เราสรุปขั้นตอนการถอดรหัสแฮมมิ่งฐาน q ได้ดังนี้

ขั้นที่ 1 เมื่อได้รับเวกเตอร์ **x** คำนวณหาซินโดรม S(**x**)

ขั้นที่ 2 ถ้า S(**x**) = **0** ให้คิดว่า **x** คือคำรหัสที่ส่ง

ขั้นที่ 3 ถ้า S(**x**) ≠ **0** แล้ว S(**x**) = bh_i สำหรับบาง b และ i ให้คิดว่ามีข้อผิดพลาดเกิดขึ้นหนึ่งตำแหน่ง คือผิดพลาดในตำแหน่งที่ i ซึ่งสามารถแก้ไขให้ถูกต้องได้โดยนำ b ไปหักออกจากตำแหน่งที่ i ของ **x**

ตัวอย่าง 4.1.8 : พิจารณารหัสฐาน q = 5 ซึ่งมี

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

เป็นเมทริกซ์ตรวจสอบภาวะเสมอ สมมุติให้ **x** = 221031 เป็นเวกเตอร์ที่ได้รับ คำนวณหาซินโดรมของ **x** จะได้

$$S(\mathbf{x}) = \mathbf{x}H^T = (2,2,1,0,3,1)\begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{bmatrix} = (2, 6) = 2(1, 3)$$

จะเห็นว่า $(1, 3)^T$ ก็คือหลักที่ 5 ของ H และ b = 2 นำ b ไปหักออกจากตำแหน่งที่ 5 ของ 221031 เราได้ 221011 ดังนั้น เราถอดรหัสเวกเตอร์ **x** = 221031 ที่ได้รับให้เป็นคำรหัส 221011

4.2 รหัสโกเลย์ (Golay Codes)

รหัสโกเลย์เป็นรหัสสมบูรณ์อีกตระกูลหนึ่ง ที่ค้นพบโดย M. J. E.

Golay ในปี ค.ศ. 1949 จากสมการ (1.14.1) ในหัวข้อ 1.14 เรารู้ว่ารหัสฐาน q ที่มีความยาว n จะเป็นรหัสสมบูรณ์ที่สามารถแก้ไขข้อผิดพลาดได้ถึง t ตำแหน่ง ก็ต่อเมื่อ

$$M\left\{1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t\right\}=q^n$$

ในการค้นหารหัสสมบูรณ์ เราจะต้องหาจำนวนเต็ม M, n, q, และ t ซึ่งสอดคล้องกับสมการนี้ นั่นคือหา n, q, และ t ซึ่งทำให้

$$1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t$$

เป็นจำนวนซึ่งอยู่ในรูป q^s เมื่อ s เป็นจำนวนเต็มบวกบางจำนวน ในช่วงเวลานั้นโกเลย์พบพารามิเตอร์ (n, M, d) สามชุด ที่นอกเหนือจากพารามิเตอร์ของรหัสสมบูรณ์ที่กล่าวไปแล้วทั้งหลาย พารามิเตอร์สามชุดนี้คือ

(23, 2^{12}, 7) และ (90, 2^{78}, 5) สำหรับ q = 2 และ
(11, 3^6, 5) สำหรับ q = 3

โกเลย์สนใจเฉพาะรหัสเชิงเส้น เขาสามารถแสดงได้ว่ามีรหัสไบนารีเชิงเส้น-[23, 12, 7] และรหัสเทอร์นารีเชิงเส้น-[11, 6, 5] โกเลย์สร้างรหัสเหล่านี้โดยการสร้างเมทริกซ์ก่อกำเนิด ซึ่งเขาแสดงไว้ในบทความของเขาเพียงหนึ่งหน้ากระดาษ โดยไม่ได้อธิบายว่าเขาได้เมทริกซ์เหล่านั้นมาได้อย่างไร อย่างไรก็ตาม ยังมีวิธีอื่นอีกในการสร้างรหัสเหล่านี้ แต่อาจจะต้องใช้โครงสร้างทางคณิตศาสตร์ที่ซับซ้อนกว่า ในขณะเดียวกันโกเลย์สามารถแสดงได้ว่ารหัสไบนารีเชิงเส้น-[90, 78, 5] ไม่มี

รหัสโกเลย์ G_{24} และ G_{23}

รหัสโกเลย์ไบนารีขยาย (extended binary Golay code) หรือ G_{24} คือรหัสที่มี G = [I_{12} | A] เป็นเมทริกซ์ก่อกำเนิด เมื่อ I_{12} คือ

เมทริกซ์เอกลักษณ์ขนาด 12x12 และ A คือเมทริกซ์ขนาด 12 x 24 ข้างล่างนี้

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

ข้อสังเกต : พิจารณาเมทริกซ์ก่อกำเนิด G ของรหัส G_{24} จะพบว่า

1. ความยาวของ G_{24} เท่ากับ 24
2. $\dim(G_{24}) = 12$
3. แต่ละแถวของเมทริกซ์ G มีน้ำหนักเท่ากับ 8 หรือ 12
4. A เป็นเมทริกซ์สมมาตร กล่าวคือ $A^T = A$
5. แต่ละแถวของเมทริกซ์ G ตั้งฉากกัน

ทฤษฎีบทประกอบ 4.2.1

G_{24} เป็นคู่ของตัวเอง กล่าวคือ $(G_{24})^{\perp} = G_{24}$

พิสูจน์ พิจารณาเทริกซ์ก่อกำเนิด G จากข้อสังเกต เราพบว่าแต่ละแถวของ G ตั้งฉากกัน กล่าวคือ ถ้า r_i และ r_j เป็นสองแถวใด ๆ ของ G แล้ว $r_i \cdot r_j = 0$ เรารู้ว่า ถ้า c เป็นคำรหัสใน G_{24} แล้ว c ต้องเป็นการรวมเชิงเส้นของแถวของ G สมมุติว่า

$$c = a_1 r_1 + a_2 r_2 + \ldots + a_{12} r_{12}$$

สำหรับ $a_1, a_2, \ldots, a_{12}$ ที่เป็นสเกลาร์บางตัว ดังนั้น

$$c \cdot r_j = (a_1 r_1 + a_2 r_2 + \ldots + a_{12} r_{12}) \cdot r_j$$
$$= a_1(r_1 \cdot r_j) + a_2(r_2 \cdot r_j) + \ldots + a_{12}(r_{12} \cdot r_j) = 0$$

แสดงว่าสมาชิกใน G_{24} ต้องเป็นสมาชิกของ $(G_{24})^{\perp}$ นั่นคือ $G_{24} \subseteq (G_{24})^{\perp}$ แต่

$$\dim(G_{24}) = \dim(G_{24})^{\perp}$$

ดังนั้น $G_{24} = (G_{24})^{\perp}$ ■

ทฤษฎีบทประกอบต่อไปนี้ แสดงให้เห็นว่า $[A \mid I_{12}]$ ก็เป็นเมทริกซ์ก่อกำเนิดของ G_{24} ด้วย

ทฤษฎีบทประกอบ 4.2.2

$G' = [A \mid I_{12}]$ เป็นเมทริกซ์ก่อกำเนิดของ G_{24}

พิสูจน์ จากทฤษฎีบท 3.7.7 เรามี $H = [A^T \mid I]$ เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัส G_{24} และ $(G_{24})^{\perp} = G_{24}$ จากทฤษฎีบทประกอบ 4.2.1 แสดงว่าเมทริกซ์

$$H = [A^T \mid I] = [A \mid I]$$

เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัส $(G_{24})^{\perp}$ และเนื่องจากเมทริกซ์ตรวจสอบภาวะเสมอของ $(G_{24})^{\perp}$ เป็นเมทริกซ์ก่อกำเนิดของ G_{24} นั่นคือ $H = [A \mid I] = G'$ เป็นเมทริกซ์ก่อกำเนิดของ G_{24} ด้วย ■

ทฤษฎีบทประกอบ 4.2.3

น้ำหนักของคำรหัสแต่ละคำใน G_{24} เป็นพหุคูณของ 4

พิสูจน์ ให้ c เป็นคำรหัสใน G_{24} เราจะแสดงว่า $wt(c)$ เป็นพหุคูณของ 4 เรารู้ว่า c เป็นการรวมเชิงเส้นของแต่ละแถวของเมทริกซ์ก่อกำเนิด G ถ้าให้ r_i เป็นแถวที่ i ของ G เราแยกพิจารณาดังนี้ ขั้นแรกสมมุติว่า c เป็นแถวใดแถวหนึ่งของ G เห็นได้ชัดว่า $wt(c)$ เป็นพหุคูณของ 4 เพราะว่าแถวใด ๆ ของ G มีน้ำหนักเป็น 8 หรือ 12 ต่อไปพิจารณา

กรณีที่ c เป็นผลบวกของสองแถวใด ๆ ของ G สมมุติว่า $c = r_i + r_j$ เนื่องจาก G_{24} เป็นรหัสคู่ของตัวเอง แต่ละแถวของ G_{24} ตั้งฉากกัน นั่นคือ $r_i \cdot r_j = 0$ แสดงว่าแถว r_i และแถว r_j มีจำนวนเลข 1 ที่อยู่ในตำแหน่งที่ตรงกันเป็นจำนวนคู่ กล่าวคือ $wt(r_i \cap r_j)$ เป็นจำนวนคู่ เนื่องจาก $wt(r_i + r_j) = d(r_i, r_j)$ และจากทฤษฎีบท 1.9.2 เราได้

$$wt(r_i + r_j) = wt(r_i) + wt(r_j) - 2wt(r_i \cap r_j)$$

ซึ่งเป็นพหุคูณของ 4 ต่อไปเราพิจารณากรณีที่ c เป็นผลรวมของสามแถวใด ๆ ของเมทริกซ์ G เช่น $c = r_i + r_j + r_k$ เนื่องจาก $wt(r_i + r_j)$ และ $wt(r_k)$ เป็นพหุคูณของ 4 ดังนั้น โดยเหตุผลเดียวกับข้างบนนี้ เราสามารถสรุปได้ว่า $wt(c) = wt(r_i + r_j + r_k)$ เป็นพหุคูณของ 4 และจากการอุปนัยเชิงคณิตศาสตร์ เราสรุปได้ว่า $wt(c)$ เป็นพหุคูณของ 4 สำหรับ c ที่เป็นคำรหัสใด ๆ ของ G_{24} ■

ทฤษฎีบทประกอบ 4.2.4

ไม่มีคำรหัสที่มีน้ำหนักเท่ากับ 4 ใน G_{24}

พิสูจน์ สมมุติว่ามีคำรหัส $c = c_1c_2 \ldots c_{24}$ ใน G_{24} ซึ่ง $wt(c) = 4$ เพื่อความสะดวกในการอธิบาย เราจะเขียน c ในรูป (L | R) เมื่อ $L = c_1c_2 \ldots c_{12}$ และ $R = c_{13}c_{14} \ldots c_{24}$ ดังนั้น จะเกิดกรณีใดกรณีหนึ่งต่อไปนี้

กรณี 1 $wt(L) = 0$ และ $wt(R) = 4$ จะเห็นว่ากรณีนี้เป็นไปไม่ได้ เพราะเมื่อพิจารณาจากเมทริกซ์ก่อกำเนิด G จะพบว่ามีคำรหัสเพียงคำเดียวเท่านั้นที่มี $wt(L) = 0$ คำรหัสนั้นคือ $\mathbf{0} = 00 \ldots 0$

กรณี 2 $wt(L) = 1$ และ $wt(R) = 3$ ถ้า $wt(L) = 1$ แสดงว่า L ต้องเป็นแถวใดแถวหนึ่งของ G ซึ่งเป็นไปไม่ได้ เพราะแต่ละแถวของ G มีน้ำหนัก 8 หรือ 12 เท่านั้น

กรณี 3 $wt(L) = wt(R) = 2$ ถ้า $wt(L) = 2$ แสดงว่า c ต้องเป็นผลบวกของสองแถวของ $G = [I \mid A]$ เมื่อตรวจดูจากเมทริกซ์ A จะไม่พบว่ามีสองแถวใดที่ผลบวกมีน้ำหนักเท่ากับ 2 ดังนั้น กรณีนี้จึงเป็นไปไม่ได้

กรณี 4 $wt(L) = 3$ และ $wt(R) = 1$ เนื่องจาก $[A \mid I]$ เป็นเมทริกซ์ก่อกำเนิดของรหัส G_{24} ด้วยเช่นกัน ถ้า $wt(R) = 1$ เมื่อพิจารณาเมทริกซ์นี้จะเห็นว่า c ต้องเป็นแถวใดแถวหนึ่งของเมทริกซ์ $[A \mid I]$ ซึ่งเป็นไปไม่ได้ เพราะแต่ละแถวของ $[A \mid I]$ มีน้ำหนักเท่ากับ 8 หรือ 12

กรณี 5 $wt(L) = 4$ และ $wt(R) = 0$ เมื่อพิจารณาโดยใช้เมทริกซ์ก่อกำเนิด $[A \mid I]$ จะเห็นว่าเป็นไปไม่ได้เช่นกัน

จากทั้ง 5 กรณี แสดงว่าไม่มีคำรหัสใดใน G_{24} ที่มีน้ำหนักเท่ากับ 4 ■

ทฤษฎีบท 4.2.1

รหัสโกเลย์ G_{24} เป็นรหัสฐานสองซึ่งมีพารามิเตอร์ [24, 12, 8]

พิสูจน์ พิจารณาเมทริกซ์ก่อกำเนิดของรหัส G_2 เรารู้ว่าความยาวของ G_{24} เท่ากับ 24 และ $\dim(G_{24}) = 12$ เราเหลือเพียงแสดงว่า

$$d(G_{24}) = wt(G_{24}) = 8$$

จากการสังเกตเมทริกซ์ก่อกำเนิด G ของรหัส G_{24} เราพบว่า

$$d(G_{24}) = wt(G_{24}) = 4 \text{ หรือ } 8$$

จากทฤษฎีบทประกอบ 4.2.4 เรารู้ว่าไม่มีคำรหัสใดใน G_{24} ที่มีน้ำหนักเท่ากับ 4 ดังนั้น $d(G_{24}) = wt(G_{24}) = 8$ ตามต้องการ ■

จากทฤษฎีบท 1.12.1 เรารู้ว่า ถ้า d เป็นจำนวนเต็มคี่แล้ว จะมีรหัส–(n, M, d) ก็ต่อเมื่อมีรหัส–(n + 1, M, d + 1) ดังนั้น ถ้าเราตัดบิตสุดท้ายของคำรหัสแต่ละคำใน G_{24} ซึ่งเป็นรหัสไบนารี–(24, 2^{12}, 8) เราจะได้รหัสไบนารี–(23, 2^{12}, 7) เราเรียกกระบวนการสร้างรหัสในลักษณะนี้ว่า ***การเจาะรหัส*** (puncturing the code) เราแทนรหัสที่เกิดจากการเจาะรหัส G_{24} ด้วย G_{23}

ในทางกลับกัน ถ้าเรามีรหัส G_{23} เราสามารถสร้างรหัส G_{24} ได้โดยการเพิ่มบิตตรวจสอบภาวะเสมอ (หรือที่เรียกว่า overall parity check) เข้าไปในคำรหัสทุกคำของ G_{23} จากตัวอย่าง 1.14.4(2) G_{23} เป็นรหัสสมบูรณ์

รหัสโกเลย์เทอร์นารี G_{12}

G_{12} เป็นรหัสโกเลย์เทอร์นารี ซึ่งก่อกำเนิดโดยเมทริกซ์ $G = [I_6 \mid B]$ เมื่อ

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

ทฤษฎีบท 4.2.2

1. G_{12} เป็นรหัสซึ่งเป็นคู่ของตัวเอง กล่าวคือ $(G_{12})^{\perp} = G_{12}$
2. $[B \mid I_6]$ เป็นเมทริกซ์ก่อกำเนิดของ G_{12} ด้วย
3. G_{12} เป็นรหัสเทอร์นารี-$(12, 3^6, 6)$

ดังนั้น ถ้าเราเจาะรหัส G_{12} กล่าวคือ ถ้าเราตัดตำแหน่งสุดท้ายของคำรหัสทุกคำใน G_{12} เราจะได้รหัสเทอร์นารี–$(11, 3^6, 5)$ ซึ่งจะแทนด้วย G_{11} จากตัวอย่าง 1.14.4(3) จะเห็นว่า G_{11} เป็นรหัสสมบูรณ์

ในปี ค.ศ. 1973 นักคณิตศาสตร์ชื่อ Tietävainen และ van Lint ได้แสดงให้เห็นว่า รหัสสมบูรณ์ทั้งหลายที่ไม่ชัด (nontrivial perfect code) จะมีพารามิเตอร์เหมือนกับรหัสแฮมมิ่งหรือรหัสโกเลย์เท่านั้น

ทฤษฎีบท 4.2.3

รหัสสมบูรณ์ฐาน q เมื่อ q เป็นจำนวนเฉพาะยกกำลังที่ไม่ใช่ trivial perfect code แล้ว จะมีพารามิเตอร์เหมือนพารามิเตอร์ของรหัสแฮมมิ่งหรือรหัสโกเลย์เท่านั้น

4.3 รหัส ISBN

ดังได้เห็นในหัวข้อ 1.1 แล้วว่า รหัส ISBN เป็นรหัสฐาน 11 ซึ่งมีความยาว 10 หลัก ที่อยู่ในรูป $\mathbf{c} = c_1c_2 \ldots c_{10}$ ซึ่งสอดคล้องกับสมการ

$$\sum_{i=1}^{10} ic_i \equiv 0 \pmod{11}$$

หรือ

$$c_{10} \equiv \sum_{i=1}^{9} ic_i \pmod{11}$$

ดังนั้น เราใช้ c_{10} เป็นตัวตรวจสอบภาวะเสมอ รหัส ISBN เป็นรหัสซึ่งออกแบบให้สามารถตรวจสอบข้อผิดพลาดได้ ดังในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.3.1

1. รหัส ISBN สามารถตรวจจับข้อผิดพลาดได้หนึ่งตำแหน่ง
2. รหัส ISBN สามารถตรวจจับข้อผิดพลาดที่เกิดจากการสลับที่ของสองตำแหน่งใด ๆ

พิสูจน์ 1. สมมุติว่า $\mathbf{x} = x_1x_2 \ldots x_{10}$ เป็นเวกเตอร์ที่ได้รับ เราคำนวณหาผลบวก

$$X = \sum_{i=1}^{10} ix_i$$

ถ้า $X \not\equiv 0 \pmod{11}$ แสดงว่าต้องมีข้อผิดพลาดเกิดขึ้น

สมมุติว่า $\mathbf{c} = c_1c_2 \ldots c_{10}$ เป็นคำรหัสที่ส่ง และสมมุติว่าเราได้รับเวกเตอร์ $\mathbf{x} = x_1x_2 \ldots x_{10}$ ซึ่งเหมือนกับคำรหัส $\mathbf{c}$ ทุกตำแหน่ง ยกเว้นตำแหน่งที่ j สมมุติว่า $x_j = c_j + a$ เมื่อ $a \neq 0$ ดังนั้น

$$X = \sum_{i=1}^{10} ix_i = \sum_{i=1}^{10} ic_i + ja = ja \not\equiv 0 \pmod{11}$$

แสดงว่า $\mathbf{x}$ ไม่ใช่คำรหัส นั่นคือ สามารถตรวจจับได้ว่ามีข้อผิดพลาดเกิดขึ้น

พิสูจน์ 2. สมมุติว่า $c = c_1c_2 \ldots c_{10}$ เป็นคำรหัสที่ส่ง และสมมุติว่า $x = x_1x_2 \ldots x_{10}$ เป็นเวกเตอร์ที่ได้รับซึ่งเหมือนกับคำรหัส c แต่มีตำแหน่งที่ j และ k สลับที่กัน กล่าวคือ $x_j = c_k$ และ $x_k = c_j$ เมื่อ $c_k \neq c_j$ ดังนั้น

$$X = \sum_{i=1}^{10} ix_i = x_1 + 2x_2 + \ldots + jx_j + \ldots + kx_k + \ldots + 10x_{10}$$

$$= c_1 + 2c_2 + \ldots + jc_k + \ldots + kc_j + \ldots + 10c_{10}$$

$$= c_1 + 2c_2 + \ldots + jc_k + (jc_j - jc_j) + \ldots + kc_j + (kc_k - kc_k) \ldots + 10c_{10}$$

$$= \sum_{i=1}^{10} ic_i + (j-k)c_k + (k-j)c_j$$

$$= \sum_{i=1}^{10} ic_i + (j-k)c_k - (j-k)c_j$$

$$= \sum_{i=1}^{10} ic_i + (j-k)(c_k - c_j)$$

$$= (j-k)(c_k - c_j) \not\equiv 0 \pmod{11}$$ $\blacksquare$

หมายเหตุ : รหัส ISBN ไม่สามารถแก้ไขข้อผิดพลาดได้ ยกเว้นในกรณีที่รู้ว่าผิดที่ตำแหน่งใด เช่นในตัวอย่างต่อไปนี้

ตัวอย่าง 4.3.1 : สมมุติว่า 02011x5027 คือเวกเตอร์ที่ได้รับ เมื่อ x คือตำแหน่งหนึ่งที่เราไม่รู้ว่าคือจำนวนใด เราคำนวณ

$$1\cdot0 + 2\cdot2 + 3\cdot0 + 4\cdot1 + 5\cdot1 + 6\cdot x + 7\cdot5 + 8\cdot0 + 9\cdot2\ 10\cdot7 = 0$$

หรือ $6x + 4 = 0$ ดังนั้น

$$x = \frac{-4}{6} = 7\cdot6^{-1} = 7\cdot2 = 14 = 3$$

นั่นคือ เราสามารถบอกได้ว่า x ในตำแหน่งที่หกของเวกเตอร์ 02011x5027 คือ 3

แบบฝึกหัด 4

1. จงเขียนเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(4, 2)
2. จงใช้รหัสแฮมมิ่ง Ham(3, 2) ถอดรหัสคำต่อไปนี้

   2.1 1101001 2.2 1111111
3. จงใช้รหัสแฮมมิ่ง Ham(3, 3) ถอดรหัสคำต่อไปนี้

   3.1 0011121222012 3.2 111222000220
4. จงเขียนเมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(2, 3) แล้วใช้เมทริกซ์นี้ในการถอดรหัสคำต่อไปนี้

   4.1 2011 4.2 1122
5. ใช้เมทริกซ์ตรวจสอบภาวะเสมอของรหัสแฮมมิ่ง Ham(4, 2) ในข้อ 1 ในการถอดรหัสคำ 111000110010101
6. จงใช้การดำเนินการตามแถว บนเมทริกซ์ตรวจสอบภาวะเสมอของรหัส Ham(4, 2) เพื่อแปลงเมทริกซ์ดังกล่าวให้อยู่ในรูปมาตรฐาน $[A \mid I_6]$ แล้วใช้เมทริกซ์ที่ได้ใหม่นี้ เพื่อหาเมทริกซ์ก่อกำเนิดของรหัส Ham(4, 2)
7. จงแสดงว่าพารามิเตอร์ของ G_{11} สอดคล้องกับ sphere-packing bound
8. จงหา

   8.1 ตัวผกผันภายใต้การบวกของสมาชิกแต่ละตัวใน F_{11}

   8.2 ตัวผกผันภายใต้การคูณของสมาชิกแต่ละตัวใน F_{11} ที่ไม่ใช่ศูนย์
9. จงตรวจสอบว่าคำต่อไปนี้เป็นคำรหัส ISBN หรือไม่

   9.1 0 – 13 – 625007 – 5

   9.2 0 – 07 – 100893 – 4

10. ถ้าจำนวนต่อไปนี้เป็นส่วนหนึ่งของคำรหัส ISBN จงหาตัวตรวจสอบของแต่ละจำนวน

    10.1 007536212

    10.2 091961116

11. ถ้าจำนวนต่อไปนี้เป็นคำรหัส ISBN จงหา x ในคำเหล่านั้น

    11.1 0471x00105

    11.2 007012xx77