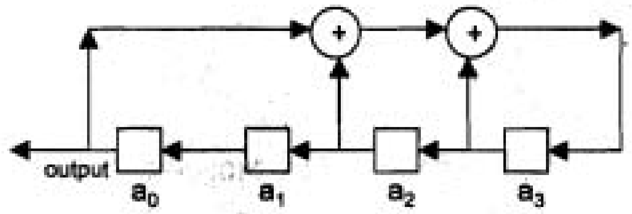
5 รหัสวัฏจักร
Cyclic Codes

E. Prange เป็นบุคคลแรกที่เริ่มศึกษารหัสวัฏจักรตั้งแต่ปี ค.ศ. 1957 รหัสวัฏจักรเป็นรหัสในตระกูลรหัสเชิงเส้น ที่มีสมบัติพิเศษ คือ "การเลื่อนวน (cyclic shift) ของคำรหัสยังคงเป็นคำรหัส" รหัสวัฏจักรเป็นรหัสที่สำคัญ เนื่องจากมีวิธีการเข้ารหัสที่มีประสิทธิภาพ สามารถเข้ารหัสโดยใช้สิ่งที่เรียกว่า shift register ดังในรูป 5.1



รูป 5.1 : ลักษณะของ shift register

นอกจากนี้รหัสที่สำคัญจำนวนมากสามารถแทนในรูปรหัสวัฏจักรได้ เช่น รหัสโกเลย์ รหัสแฮมมิง และรหัส-BCH เป็นต้น

ในบทนี้ เราจะศึกษาพหุนาม และจะแสดงให้เห็นความสัมพันธ์ของรหัสวัฏจักรกับพหุนาม ศึกษาโครงสร้างทางพีชคณิตของรหัสวัฏจักร พร้อมทั้งแสดงวิธีเข้ารหัสและถอดรหัสวัฏจักร

5.1 นิยามและตัวอย่าง

นิยาม 5.1.1 ถ้า $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ เป็นเวกเตอร์ใน F_q^n เราจะเรียกเวกเตอร์ $\mathbf{a}^1 = (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ ว่าเป็น ***การเลื่อนวน*** (cyclic shift) ของ **a** ไปทางขวา 1 ตำแหน่ง และจะแทนเวกเตอร์ที่เกิดจากการเลื่อนวน **a** ไปทางขวา i ครั้ง ด้วย $\mathbf{a}^i$

ตัวอย่าง 5.1.1 :

1. ให้ $a = 110 \in F_2^3$ ถ้าเราเลื่อนวน a ครั้งที่ 1, 2 และ 3 ตามลำดับ จะได้

$$a^1 = 011,\ a^2 = 101 \text{ และ } a^3 = 110 = a$$

2. ให้ $a = 1102210 \in F_3^7$ ถ้าเราเลื่อนวน a ครั้งที่ 1 และ 2 ตามลำดับ จะได้

$$a^1 = 0110221 \text{ และ } a^2 = 1011022$$

นิยาม 5.1.2 จะเรียกรหัสเชิงเส้น C ว่ารหัสวัฏจักร ถ้าการเลื่อนวนของคำรหัสใน C ยังคงเป็นคำรหัสใน C

ตัวอย่าง 5.1.2 :

1. C = {000, 011, 101, 110} เป็นรหัสวัฏจักรใน F_2^3 เพราะการเลื่อนวนของแต่ละเวกเตอร์ใน C ไปทางขวาแต่ละครั้ง ผลลัพธ์ยังคงเป็นเวกเตอร์ใน C ดังแสดงข้างล่างนี้

$$(011)^1 = 101 \in C,$$
$$(101)^1 = 110 \in C,$$
$$(110)^1 = 011 \in C$$

2. C = {0112, 1120, 1201, 2011} เป็นรหัสวัฏจักรใน F_3^4 (ตรวจสอบได้ไม่ยากนัก ลองทำเป็นแบบฝึกหัด)

3. C = {0000, 1001, 0110, 1111} ไม่เป็นรหัสวัฏจักร เพราะว่า ถ้าเลื่อนวนคำรหัส 1001 จะได้ 1100 ซึ่งไม่เป็นคำรหัสใน C

4. รหัสแฮมมิงในที่มี

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

เป็นเมทริกซ์ตรวจสอบภาวะเสมอ ไม่เป็นรหัสวัฏจักร ถ้า $x = 1110000$ จะเห็นว่า x เป็นคำรหัส ทั้งนี้เพราะว่า $xH^T = 0$ แต่ $y = 0111000$ ซึ่งเกิดจากการเลื่อนวนของเวกเตอร์ x ไปทางขวาหนึ่งครั้ง ไม่เป็นคำรหัส เพราะว่า $yH^T = 101 \neq 0$

เพื่อความสะดวกในการศึกษาโครงสร้างทางพีชคณิตของรหัสวัฏจักร เรานิยามรหัสวัฏจักรในรูปของพหุนาม โดยจะแทนเวกเตอร์ $a = a_0a_1 \ldots a_{n-1} \in F_q^n$ ด้วยพหุนาม $a(x)$ ซึ่งมีดีกรี $n - 1$ หรือน้อยกว่า ดังนี้

$$a = a_0a_1 \ldots a_{n-1} \leftrightarrow a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

ในกรณีนี้ เรากล่าวว่า a เป็นเวกเตอร์ที่สมนัยกับพหุนาม $a(x)$ หรือกลับกัน ในบทนี้ เราจะใช้เวกเตอร์ a กับพหุนาม $a(x)$ สลับกันตามความเหมาะสม ที่ผ่านมาเราเคยแทนคำรหัสในรูปของ n–สิ่งอันดับ $a_1a_2 \ldots a_n$ แต่เพื่อให้สอดคล้องกับสัมประสิทธิ์ของพหุนามซึ่งมักใช้ a_i เป็นสัมประสิทธิ์ของ x^i ดังนั้น เราจะเขียนเวกเตอร์ในรูปของ n–สิ่งอันดับ $a_0a_1 \ldots a_{n-1}$ ซึ่งเริ่มจาก a_0 ในตำแหน่งแรก และมี a_{n-1} เป็นตำแหน่งสุดท้าย

5.2 ริงของพหุนาม (Polynomial Ring)

ให้ F เป็นฟีลด์ พหุนามบนฟีลด์ F ได้แก่นิพจน์ที่อยู่ในรูป

$$f(x) = a_0 + a_1x + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix^i$$

เมื่อ n เป็นจำนวนเต็มที่ไม่เป็นลบ a_i, $0 \leq i \leq n$ เป็นสมาชิกของฟีลด์ F เรียก a_i ว่า***สัมประสิทธิ์*** ของ x^i เรียก x ว่า ***ตัวแปรที่ไม่กำหนดค่า*** (indeterminate) ***พหุนามศูนย์*** คือพหุนามที่มีสัมประสิทธิ์ a_i เป็น 0 ทั้งหมด เราจะแทนพหุนามศูนย์ด้วย 0 ถ้า $a_n \neq 0$ จะเรียก n ว่า ***ดีกรี*** ของพหุนาม $f(x)$ หรือเขียน $\deg f(x) = n$ และเรียก a_n ว่า

สัมประสิทธิ์นำ ของ f(x) เรียก a_0 ว่า ***พจน์ค่าคงตัว*** ถ้า f(x) เป็นพหุนามศูนย์ เรากำหนดให้ deg f(x) = $-\infty$ เรียกพหุนามซึ่งมีสัมประสิทธิ์นำ $a_n = 1$ ว่า ***พหุนามโมนิก*** เราอาจเขียนพหุนามโดยเรียงจากพจน์ที่มีกำลังสูงสุดไปหาพจน์ที่มีกำลังต่ำสุดก็ได้ เรามักเขียนพหุนามโดยละพจน์ที่มีสัมประสิทธิ์เป็นศูนย์ เช่นเขียน $1 + 2x^2 + x^5$ แทน $1 + 0x + 2x^2 + 0x^3 + 0x^4 + x^5$ เป็นต้น เราจะแทนเซตของพหุนามทั้งหลายบนฟิลด์ F ด้วย F[x] ให้

$$f(x) = \sum_{i=0}^{m} a_i x^i \quad \text{และ} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

เป็นพหุนามใน F[x] เราจะกล่าวว่าพหุนาม f(x) และ g(x) เท่ากัน หรือเขียน f(x) = g(x) ก็ต่อเมื่อ m = n และ $a_i = b_i$ สำหรับ $0 \le i \le n$ เรานิยามการบวกพหุนามและการคูณพหุนามดังนี้

การบวกพหุนาม

$$f(x) + g(x) = \sum_{i=0}^{k} (a_i + b_i) x^i \quad \text{เมื่อ } k = \max(m, n)$$

การคูณพหุนาม

$$f(x)g(x) = \sum_{i=0}^{m+n} c_i x^i = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_{i-j} b_j \right) x^i$$

เมื่อ $c_i = \sum_{j=0}^{i} a_{i-j} b_j = a_i b_0 + a_{i-1} b_1 + .. + a_0 b_i$

สำหรับ $0 \le i \le m + n$

ทฤษฎีบท 5.2.1

> ถ้า f(x) และ g(x) เป็นพหุนามใน F[x] ที่ไม่ใช่พหุนามศูนย์แล้ว
> deg f(x)g(x) = deg f(x) + deg g(x)

พิสูจน์ ให้ $f(x) = a_0 + a_1 x + \ldots + a_m x^m$ และ

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n \quad \text{เมื่อ } a_m, b_n \neq 0$$

พิจารณาผลคูณ $f(x)g(x) = \sum_{i=0}^{m+n} c_i x^i$ เราได้

$$c_{m+n} = (a_{m+n}b_0 + \ldots + a_{m+1}b_{n-1}) + a_m b_n + (a_{m-1}b_{n+1} + \ldots + a_0 b_{m+n})$$

จะเห็นว่าผลบวกในวงเล็บแรกเป็น 0 เพราะว่า $a_i = 0$ สำหรับ $i > m$ และผลบวกในวงเล็บที่สองเท่ากับ 0 เช่นกัน เพราะ $b_j = 0$ สำหรับ $j > n$ ดังนั้น

$$c_{m+n} = a_m b_n \neq 0 \text{ เพราะว่า } a_m \neq 0 \text{ และ } b_n \neq 0$$

และสำหรับ $k > m + n$ เราได้

$$c_k = (a_k b_0 + \ldots + a_{m+1} b_{k-m-1}) + (a_m b_{k-m} + \ldots + a_0 b_k)$$

เป็น 0 ทั้งหมด ดังนั้น $\deg f(x)g(x) = m + n$ ■

บทแทรก 5.2.1

> ถ้า $f(x)$ และ $g(x)$ เป็นพหุนามใน $F[x]$ ที่ไม่ใช่พหุนามศูนย์แล้ว $\deg f(x) \leq \deg f(x)g(x)$

ทฤษฎีบท 5.2.2

> $F[x]$ เป็นริงสลับที่ภายใต้การบวกและการคูณพหุนามและมี 1

พิสูจน์ จากนิยามของการบวกและการคูณพหุนาม เห็นได้ชัดว่า $F[x]$ มีสมบัติปิดภายใต้การบวกและการคูณพหุนาม พหุนามศูนย์ 0 เป็นเอกลักษณ์ภายใต้การบวก และสำหรับพหุนาม $f(x) = \sum_{i=0}^{n} a_i x^i$ ใด ๆ จะมีพหุนาม

$$-f(x) = \sum_{i=0}^{n} (-a_i) x^i = -\sum_{i=0}^{n} a_i x^i$$

เป็นพหุนามผกผันภายใต้การบวก สมบัติการเปลี่ยนหมู่และสมบัติการสลับที่ภายใต้การบวกเป็นจริงใน $F[x]$ ทั้งนี้เพราะว่าสมบัติการเปลี่ยนหมู่และสมบัติการสลับที่ภายใต้การบวกเป็นจริงในฟีลด์ F ดังนั้น $F[x]$ เป็นอาบีเลียนกรุปภายใต้การบวก ต่อไปจะแสดงว่า $F[x]$ มีสมบัติการเปลี่ยนหมู่ภายใต้คูณ ให้

$$f(x) = \sum_{i=0}^{m} a_i x^i \text{ , } g(x) = \sum_{i=0}^{n} b_i x^i \text{ และ } h(x) = \sum_{i=0}^{r} c_i x^i$$

ดังนั้น

$$\begin{aligned}
[f(x)g(x)]h(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{r} c_i x^i\right) \\
&= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_{i-j} b_j\right) x^i\right]\left(\sum_{i=0}^{r} c_i x^i\right) \\
&= \sum_{i=0}^{m+n+r}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{i-j} a_{j-k-k} b_k\right) c_j\right] x^i \\
&= \sum_{i=0}^{m+n+r}\left[\sum_{j=0}^{i} a_j\left(\sum_{k=0}^{i-j} b_{i-j-k} c_j\right)\right] x^i \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+r}\left(\sum_{j=0}^{i} b_{i-j} c_j\right) x^i\right] \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x^i\right)\left(\sum_{i=0}^{r} c_i x^i\right)\right] \\
&= f(x)[g(x)h(x)]
\end{aligned}$$

เราเหลือเพียงแสดงว่าสมบัติการแจกแจงในข้อ 8 ของนิยาม 2.1.9 และการสลับที่ภายใต้การคูณเป็นจริง ซึ่งจะเว้นการแสดงไว้ให้เป็นแบบฝึกหัด เราสรุปได้ว่า F[x] เป็นริงสลับที่ และมี 1 เป็นเอกลักษณ์ภายใต้การคูณ ■

ทฤษฎีบท 5.2.3

ขั้นตอนวิธีการหาร (The Division Algorithm)

ถ้า f(x) และ g(x) เป็นพหุนามใน F[x] ซึ่ง $g(x) \neq 0$ แล้วจะมีพหุนาม q(x) และ r(x) ใน F[x] ซึ่ง

$$f(x) = g(x)q(x) + r(x)$$

เมื่อ $r(x) = 0$ หรือ $\deg r(x) < \deg g(x)$ เรียก q(x) ว่าผลหาร (quotient) และเรียก r(x) ว่าเศษ (remainder)

ตัวอย่าง 5.2.1 : ให้ $f(x) = x^3 + x + 1$ และ $g(x) = x^2 + x + 1$ ใน $F_2[x]$ ใช้วิธีตั้งหารยาว เราได้

$$
\begin{array}{rl}
 & x + 1 \qquad\qquad = q(x) \\
x^2 + x + 1 \,\big) & \overline{x^3 \qquad + x + 1} \\
 & \underline{x^3 + x^2 + x} \\
 & \qquad x^2 \qquad + 1 \\
 & \qquad \underline{x^2 + x + 1} \\
 & \qquad\qquad x \qquad\qquad = r(x)
\end{array}
$$

อย่าลืมว่า $-1 = 1$ ใน F_2 ดังนั้น

$$x^3 + x + 1 = (x^2 + x + 1)(x + 1) + x$$

ในที่นี้ ตัวหารคือ $x^2 + x + 1$ ผลหารคือ $q(x) = x + 1$ ส่วน $r(x) = x$ คือเศษที่เหลือจากการหาร

นิยาม 5.2.1

> ถ้า $f(x), g(x) \in F[x]$ และถ้ามีพหุนาม $q(x)$ ใน $F[x]$ ซึ่งทำให้ $f(x) = g(x)q(x)$ แล้วจะกล่าวว่า $g(x)$ หาร $f(x)$ ได้ลงตัว หรือเขียน $g(x) \mid f(x)$ หรือกล่าวว่า $f(x)$ เป็นพหุคูณของ $g(x)$

ตัวอย่าง 5.2.2 : พิจารณาพหุนาม $2 + x^2$ และ $2x + x^3 + x^4 + 2x^6$ ใน $F_3[x]$ จะเห็นว่า $2 + x^2$ หาร $2x + x^3 + x^4 + 2x^6$ ได้ลงตัว

$$
\begin{array}{rl}
 & 2x^4 + x \\
x^2 + 2 \,\big) & \overline{2x^6 \quad + x^4 + x^3 \quad + 2x} \\
 & \underline{2x^6 \quad + x^4} \qquad\qquad \text{เพราะว่า } 4 \equiv 1 \bmod 3 \\
 & \qquad\qquad x^3 \quad + 2x \\
 & \qquad\qquad \underline{x^3 \quad + 2x} \\
 & \qquad\qquad\qquad 0
\end{array}
$$

ดังนั้น $2x + x^3 + x^4 + 2x^6 = (2 + x^2)(x + 2x^4)$

ในกรณีนี้ เรากล่าวว่า $2x + x^3 + x^4 + 2x^6$ หาร $2 + x^2$ ได้ลงตัว เพราะเศษเป็น 0 หรือกล่าวว่าพหุนาม $2x + x^3 + x^4 + 2x^6$ เป็นพหุคูณของ $2 + x^2$ ใน $F_3[x]$

นิยาม 5.2.2 พหุนาม $f(x)$ ใน $F[x]$ เป็นพหุนามลดทอนได้ ถ้า $f(x) = a(x)b(x)$ เมื่อ $a(x), b(x) \in F[x]$ ซึ่งทั้ง $\deg a(x)$ และ $\deg b(x)$ น้อยกว่า $\deg f(x)$ มิฉะนั้น จะกล่าวว่า $f(x)$ ลดทอนไม่ได้

ตัวอย่าง 5.2.3 :

1. พหุนามดีกรีหนึ่งใน $F_2[x]$ มีเพียงสองพหุนามเท่านั้น คือพหุนาม x และ $1 + x$ เห็นได้ชัดว่าทั้งสองพหุนามนี้เป็นพหุนามลดทอนไม่ได้
2. พหุนามดีกรีสองใน $F_2[x]$ มีเพียง 4 พหุนามเท่านั้น คือ

$$x^2,\ x + x^2,\ 1 + x^2 \text{ และ } 1 + x + x^2$$

เนื่องจาก

$$x^2 = xx,\ x + x^2 = x(1 + x), \text{ และ}$$
$$1 + x^2 = (1 + x)(1 + x)$$

แสดงว่า x^2, $x + x^2$ และ $1 + x^2$ เป็นพหุนามดีกรีสองลดทอนได้ใน $F_2[x]$ ในตัวอย่าง 5.2.4 ข้อ 1 เราจะแสดงให้เห็นว่า $1 + x + x^2$ เป็นพหุนามลดทอนไม่ได้ และเป็นพหุนามลดทอนไม่ได้เพียงพหุนามเดียวใน $F_2[x]$ ที่มีดีกรีสอง

ทฤษฎีบท 5.2.4

1. $x - a$ เป็นตัวประกอบของ $f(x)$ ก็ต่อเมื่อ $f(a) = 0$
2. พหุนาม $f(x) \in F[x]$ ที่มีดีกรี 2 หรือ 3 เป็นพหุนามลดทอนไม่ได้ก็ต่อเมื่อ $f(a) \neq 0$ สำหรับทุก ๆ $a \in F$
3. $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$ บนฟีลด์ F ใด ๆ

พิสูจน์ 1 สมมุติให้ $x - a$ เป็นตัวประกอบเชิงเส้นของ $f(x)$ และสมมุติว่า $f(x) = (x - a)g(x)$ เห็นได้ชัดว่า $f(a) = 0$ ในทางกลับกัน สมมุติให้ $f(a) = 0$ จากขั้นตอนวิธีการหาร เรารู้ว่าจะต้องมีพหุนาม $q(x)$ และ $r(x)$ ซึ่ง

$$f(x) = (x - a)q(x) + r(x)$$

เมื่อ $r(x) = 0$ หรือ $\deg r(x) < 1$ ดังนั้น

$$f(a) = (a - a)q(a) + r(a) = r(a)$$

แสดงว่า $r(x)$ ต้องเป็นค่าคงตัว 0

พิสูจน์ 2. ถ้า $f(x)$ เป็นพหุนามที่มีดีกรี 2 หรือ 3 และเป็นพหุนามลดทอนได้แล้ว จะต้องมีพหุนามดีกรีหนึ่งหรือที่เราเรียกว่าพหุนามเชิงเส้นเป็นตัวประกอบหนึ่งของ $f(x)$ ดังนั้นทฤษฎีเป็นจริง ซึ่งเป็นผลมาจากข้อ 1

พิสูจน์ 3. ใช้วิธีตั้งหารยาวโดยให้ $x^n - 1$ เป็นตัวตั้ง และให้ $x - 1$ เป็นตัวหาร เราจะได้ $x^{n-1} + x^{n-2} + \ldots + x + 1$ เป็นผลหาร ∎

ตัวอย่าง 5.2.4 :

1. ให้ $f(x) = 1 + x + x^2$ เป็นพหุนามใน $F_2[x]$ จะเห็นว่า

   $f(0) = 1 + 0 + 0^2 = 1$ และ

   $f(1) = 1 + 1 + 1^2 = 1$

   จากทฤษฎี 5.2.4 ข้อ 1 แสดงว่า $f(x)$ ไม่มีตัวประกอบเชิงเส้น ดังนั้น $f(x) = 1 + x + x^2$ เป็นพหุนามลดทอนไม่ได้ใน $F_2[x]$ จากการตรวจสอบจะพบว่าพหุนามดีกรีสองที่เป็นพหุนามลดทอนไม่ได้ มีเพียงพหุนามเดียวเท่านั้น คือ $1 + x + x^2$ (ดูตัวอย่าง 5.2.3)

2. เราสามารถตรวจสอบได้ในทำนองเดียวกับในข้อ1 ว่า ทั้งพหุนาม

   $f(x) = 1 + x + x^3$ และ $g(x) = 1 + x^2 + x^3$

   เป็นพหุนามลดทอนไม่ได้ใน $F_2[x]$ เนื่องจาก

$$f(0) = 1 + 0 + 0^3 = 1 \neq 0$$

$$f(0) = 1 + 1 + 1^3 = 1 \neq 0$$

$$g(0) = 1 + 0^2 + 0^3 = 1 \neq 0$$

$$g(0) = 1 + 1^2 + 1^3 = 1 \neq 0$$

แสดงว่าทั้ง f(x) และ g(x) ไม่มีตัวประกอบเชิงเส้น เพราะไม่มีตัวประกอบเชิงเส้น นอกจากนี้เรายังสามารถตรวจสอบได้ไม่ยากนักว่าพหุนามดีกรี 3 ที่เป็นพหุนามลดทอนไม่ได้ใน $F_2[x]$ มีเพียงสองพหุนามเท่านั้น คือ $1 + x + x^3$ และ $1 + x^2 + x^3$

3. ให้ $f(x) = 1 + x + x^2$ เป็นพหุนามใน $F_3[x]$ จะเห็นว่า

$$f(0) = 1 + 0 + 0^2 = 1$$

$$f(1) = 1 + 1 + 1^2 = 0 \text{ และ}$$

$$f(2) = 1 + 2 + 2^2 = 1$$

แสดงว่า x – 1 เป็นตัวประกอบของ f(x) นอกจากนี้ จากการตั้งหารยาว เราพบว่า

$$f(x) = (x - 1)(x + 2) \text{ หรือ}$$

$$f(x) = (x - 1)(x - 1) = (x - 1)^2$$

เพราะว่า –1 = 2 ในฟิลด์ F_3 ดังนั้น $f(x) = 1 + x + x^2$ เป็นพหุนามลดทอนได้ใน $F_3[x]$

4. พิจารณาพหุนาม $f(x) = 1 + x^3 + x^4$ ใน $F_2[x]$ จะเห็นว่า

$$f(0) = 1 + 0^3 + 0^4 = 1$$

$$f(1) = 1 + 1^3 + 1^4 = 1$$

ไม่มีสมาชิกใดใน F_2 เป็นรากของ f(x) แสดงว่า f(x) ไม่มีตัวประกอบเชิงเส้น อาจเป็นไปได้ว่า f(x) มีตัวประกอบที่เป็นพหุนามกำลังสองที่ลดทอนไม่ได้ แต่เรารู้ว่าพหุนามดีกรีสองที่เป็นพหุนามลดทอนไม่ได้ใน $F_2[x]$ มีเพียงพหุนามเดียว คือ $1 + x + x^2$ และ

$$(1 + x + x^2)(1 + x + x^2) = 1 + x^2 + x^4 \neq 1 + x^3 + x^4$$

แสดงว่า $1 + x^3 + x^4$ เป็นพหุนามลดทอนไม่ได้บนฟิลด์ F_2

5. $x^3 - 1 = (x - 1)(x^2 + x + 1)$ บนฟิลด์ F ใด ๆ

6. $x^3 - 1 = (x - 1)^3$ ใน $F_3[x]$

ข้อสังเกต : จากข้อ 1 และ 3 ในตัวอย่าง 5.2.4 จะเห็นว่า $1 + x + x^2$ เป็นพหุนามลดทอนไม่ได้ในริง $F_2[x]$ แต่ลดทอนได้ในริง $F_3[x]$ แสดงว่าพหุนามที่ลดทอนไม่ได้ในริงหนึ่ง ไม่จำเป็นว่าพหุนามนั้นจะลดทอนไม่ได้ในริงอื่น ๆ ดังนั้น เมื่อกล่าวว่าพหุนามใดเป็นพหุนามที่ลดทอนไม่ได้ จะต้องระบุให้ชัดลงไปว่าลดทอนไม่ได้ในริงใด

ตัวอย่าง 5.2.5 : จงแยกตัวประกอบของ $x^4 - 1$ ใน $F_3[x]$

วิธีทำ จากข้อ 3 ของทฤษฎีบท 5.2.4 เราได้

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1)$$

ถ้าให้ $f(x) = x^3 + x^2 + x + 1$ จะเห็นว่า $x - 2$ เป็นตัวประกอบเชิงเส้นของ $f(x)$ เพราะว่า $f(2) = 0$ หาร $x^3 + x^2 + x + 1$ ด้วย $x - 2$ จะได้

$$x^3 + x^2 + x + 1 = (x - 2)(x^2 + 1)$$

ดังนั้น

$$x^4 - 1 = (x - 1)(x - 2)(x^2 + 1) = (x + 1)(x + 2)(x^2 + 1)$$

ทฤษฎีบท 5.2.5

> ถ้า $f(x)$ เป็นพหุนามที่ไม่ใช่ศูนย์ใน $F[x]$ และมีดีกรี n แล้ว $f(x)$ จะมีรากอย่างมาก n รากใน F

พิสูจน์ : เราจะพิสูจน์โดยวิธีอุปนัยเชิงคณิตศาสตร์บนดีกรี n ของ $f(x)$ เห็นได้ชัดว่าทฤษฎีเป็นจริงสำหรับ $n = 0$ และ 1 สมมุติว่า $n > 1$ และสมมุติว่าทฤษฎีเป็นจริงสำหรับพหุนามทั้งหลายที่มีดีกรีน้อยกว่า n พิจารณาพหุนาม $f(x)$ ที่มีดีกรี n ถ้า $f(x)$ ไม่มีรากใน F แสดงว่าทฤษฎีเป็นจริง (เพราะว่าจำนวนราก $= 0 < n = \deg f(x)$) ดังนั้น สมมุติว่า $f(x)$ มีรากอย่างน้อยหนึ่งราก และสมมุติว่ารากหนึ่งของ $f(x)$ คือ $a \in F$

จากทฤษฎีบท 5.2.4 เราได้ $f(x) = (x - a)q(x)$ เมื่อ $\deg q(x) = n-1$ ดังนั้นรากอื่นๆ ของ $f(x)$ ที่ไม่ใช่ a จะต้องเป็นรากของ $q(x)$ โดยการอุปนัยเชิงคณิตศาสตร์ $q(x)$ มีรากใน F อย่างน้อย $n - 1$ ราก และรากเหล่านี้ย่อมเป็นรากของ $f(x)$ ด้วย ดังนั้น เมื่อนับ a รวมด้วย เราสรุปได้ว่า $f(x)$ มีรากอย่างน้อย n ราก

∎

ทฤษฎีบท 5.2.6

Unique Factorization

ถ้า $f(x) \in F[x]$ แล้ว $f(x)$ สามารถแยกตัวประกอบได้ในรูป

$$f(x) = ap_1^{e_1}p_2^{e_2}\ldots p_k^{e_k} \qquad \ldots\ldots\ldots\ldots\ldots(5.2.1)$$

เมื่อ $a \in F$, $e_1, e_2, \ldots, e_k$ เป็นจำนวนเต็มบวก และ $p_1, p_2, \ldots, p_k$ เป็นพหุนามโมนิกที่แตกต่างกันและลดทอนไม่ได้ใน $F[x]$ และการแยกตัวประกอบนี้แยกได้เพียงแบบเดียวเท่านั้น ถ้าไม่คำนึงถึงลำดับของพหุนามที่เป็นตัวประกอบที่ปรากฏ

พิสูจน์ เราจะพิสูจน์โดยวิธีอุปนัยเชิงคณิตศาสตร์บนดีกรีของ $f(x)$ ทฤษฎีบทเป็นจริงสำหรับกรณี $\deg f(x) = 1$ เพราะพหุนามที่มีดีกรี 1 ใน $F[x]$ เป็นพหุนามลดทอนไม่ได้ ต่อไป สมมุติว่าพหุนามใน $F[x]$ ที่มีดีกรีน้อยกว่า n ทุกพหุนาม สามารถแยกตัวประกอบได้ในรูปดังกล่าว ถ้า $\deg f(x) = n$ และ $f(x)$ ลดทอนไม่ได้ใน $F[x]$ การพิสูจน์ก็จบลง เพราะเราสามารถเขียน $f(x) = a(a^{-1}f(x))$ เมื่อ a เป็นสัมประสิทธิ์นำของ $f(x)$ และ $a^{-1}f(x)$ เป็นพหุนามโมนิกใน $F[x]$ เพราะถ้า $f(x)$ เป็นพหุนามลดทอนได้แล้ว $f(x) = g(x)h(x)$ ซึ่ง

$$1 \le \deg g(x) < n \text{ และ } 1 \le \deg h(x) < n$$

โดยสมมุติฐานของการอุปนัย แสดงว่าทั้ง $g(x)$ และ $h(x)$ สามารถเขียนได้ในรูป (5.2.1) ดังนั้น $f(x)$ สามารถเขียนได้ในรูป (5.2.1) ตามต้องการ

ต่อไปจะแสดงว่าการแยกตัวประกอบของ f(x) แยกได้เพียงแบบเดียวเท่านั้น โดยจะสมมุติว่า f(x) แยกตัวประกอบได้สองแบบ คือ

$$f(x) = ap_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} = bq_1^{d_1}q_2^{d_2}\cdots q_r^{d_r} \qquad \cdots\cdots\cdots(5.2.2)$$

เมื่อ $b \in F$ และ $q_1, q_2, \ldots, q_r$ เป็นพหุนามโมนิกที่แตกต่างกันและลดทอนไม่ได้ใน F[x] จากการเปรียบเทียบสัมประสิทธิ์นำ จะได้ $a = b$ นอกจากนี้ พหุนามลดทอนไม่ได้ p_1 หารทางขวามือได้ลงตัว แสดงว่า p_1 ต้องหาร q_i สำหรับบาง i ซึ่ง $1 \le i \le r$ แต่ q_i เป็นพหุนามลดทอนไม่ได้ ดังนั้น $q_i = cp_1$ เมื่อ c เป็นค่าคงตัว และทั้ง p_1 และ q_i เป็นพหุนามโมนิก ดังนั้น $q_i = p_1$ ทำให้เราสามารถตัดทอน q_i และ p_1 ออกจากสมการ (5.2.2) ได้ ทำเช่นเดียวกันนี้ต่อไปเรื่อย ๆ ในที่สุดเราสามารถสรุปได้ว่า การแยกตัวประกอบทั้งสองแบบใน (5.2.2) เหมือนกัน อาจต่างกันเฉพาะลำดับของตัวประกอบที่ปรากฏเท่านั้น ▬

นิยาม 5.2.3

ถ้า $f_1(x), f_2(x), \ldots, f_k(x)$ เป็นพหุนามใน F[x] ที่ไม่ใช่ศูนย์แล้ว ตัวหารร่วมมากของ $f_1(x), f_2(x), \ldots, f_k(x)$ คือพหุนามโมนิกที่มีดีกรีมากที่สุดที่หาร $f_1(x), f_2(x), \ldots, f_k(x)$ ได้ลงตัว ซึ่งจะเขียนแทนด้วย

$$\gcd(f_1(x), f_2(x), \ldots, f_k(x))$$

และจะกล่าวว่า $f_1(x), f_2(x), \ldots, f_k(x)$ เป็นพหุนามเฉพาะสัมพัทธ์ต่อกัน ถ้า $\gcd(f_1(x), f_2(x), \ldots, f_k(x)) = 1$

ทฤษฎีบท 5.2.7

ขั้นตอนวิธีของยุคลิด(Euclidean Algorithm)

ให้ f(x) และ g(x) เป็นพหุนามใน F[x] ซึ่ง $g(x) \neq 0$

1. ทำกระบวนการแต่ละขั้นต่อไปนี้จนกระทั่ง $r_n(x) = 0$ สำหรับบางจำนวนเต็มบวก n :

$$f(x) = g(x)h_1(x) + r_1(x) \quad \text{เมื่อ } \deg r_1(x) < \deg g(x)$$

$g(x) = r_1(x)h_2(x) + r_2(x)$ เมื่อ $\deg r_2(x) < \deg r_1(x)$

$r_1(x) = r_2(x)h_3(x) + r_3(x)$ เมื่อ $\deg r_3(x) < \deg r_2(x)$

$\vdots$

$r_{n-3}(x) = r_{n-2}(x)h_{n-1}(x) + r_{n-1}(x)$ เมื่อ $\deg r_{n-1}(x) < \deg r_{n-2}(x)$

$r_{n-2}(x) = r_{n-1}(x)h_n(x) + r_n(x)$ เมื่อ $r_n(x) = 0$

แล้ว $\gcd(f(x), g(x)) = cr_{n-1}(x)$ เมื่อ $c \in F$ ซึ่งทำให้ $cr_{n-1}(x)$ เป็นพหุนามโมนิก

2. มีพหุนาม $a(x), b(x) \in F[x]$ ซึ่งทำให้

$$f(x)a(x) + g(x)b(x) = \gcd(f(x), g(x))$$

ตัวอย่าง 5.2.6 : จงใช้ขั้นตอนวิธีของยุคลิดหา $\gcd(x^5 + x^4 + x^2 + 1, x^3 + x^2 + x)$ ใน $F_2[x]$

วิธีทำ

$x^5 + x^4 + x^2 + 1 = (x^3 + x^2 + x)(x^2 + 1) + x + 1$

$x^3 + x^2 + x = (x + 1)(x^2 + 1) + 1$

$x + 1 = 1(x + 1) + 0$

ดังนั้น

$$\gcd(x^5 + x^4 + x^2 + 1, x^3 + x^2 + x) = 1$$

นั่นคือ $x^5 + x^4 + x^2 + 1$ และ $x^3 + x^2 + x$ เป็นพหุนามเฉพาะสัมพัทธ์ต่อกัน

นิยาม 5.2.4 ถ้า $f_1(x), f_2(x), \ldots, f_k(x)$ เป็นพหุนามใน $F[x]$ ที่ไม่ใช่ศูนย์แล้ว ตัวคูณร่วมน้อยของ $f_1(x), f_2(x), \ldots, f_k(x)$ คือพหุนามโมนิกที่มีดีกรีน้อยที่สุดที่เป็นพหุคูณของ $f_1(x), f_2(x), \ldots, f_k(x)$ ซึ่งจะเขียนแทนด้วย

$$\operatorname{lcm}(f_1(x), f_2(x), \ldots, f_k(x))$$

หมายเหตุ : ถ้า $f_1(x), f_2(x), \ldots, f_k(x)$ เป็นพหุนามใน $F[x]$ ซึ่งมีตัวประกอบดังนี้

$$f_i(x) = a_i p_1(x)^{e_{i,1}} p_2(x)^{e_{i,2}} \dots p_n(x)^{e_{i,n}}$$

สำหรับ $i = 1, 2, \dots, k$, $a_i \in F$ และ $p_i(x)$ เป็นพหุนามโมนิกที่แตกต่างกันและลดทอนไม่ได้ใน $F[x]$ แล้ว

$$\begin{aligned}&\operatorname{lcm}(f_1(x), f_2(x), \dots, f_k(x))\\ &= p_1(x)^{\max\{e_{1,1},\dots,e_{k,1}\}} \dots p_n(x)^{\max\{e_{1,n},\dots,e_{k,n}\}}\end{aligned}$$

ตัวอย่าง 5.2.7 : ให้ $f_1(x) = (1 + x)^2(1 + x + x^4)^3$

$f_2(x) = (1 + x)(1 + x + x^2)^2$

$f_3(x) = x^2(1 + x + x^4)$

เป็นพหุนามใน $F_2[x]$ ดังนั้น

$\operatorname{lcm}(f_1(x), f_2(x), f_3(x)) = x^2(1 + x)^2(1 + x + x^2)^2(1 + x + x^4)^3$

5.3 ริงของพหุนามมอดุโล f(x)

นิยาม 5.3.1 ให้ $f(x)$, $a(x)$ และ $b(x)$ เป็นพหุนามใน $F[x]$ เราจะกล่าวว่าพหุนาม $a(x)$ คอนกรูเอนซ์กับ $b(x)$ มอดุโล $f(x)$ หรือเขียน $a(x) \equiv b(x) \pmod{f(x)}$ ถ้า $f(x)$ หาร $a(x) - b(x)$ ได้ลงตัว

ตัวอย่าง 5.3.1 :

1. $x^3 + x + 1 \equiv x \pmod{(x + 1)}$ ใน $F_2[x]$
   เพราะว่า $(x^3 + x + 1) - x = x^3 + 1 = (x + 1)(x^2 + x + 1)$
   ซึ่งหารด้วย $x + 1$ ได้ลงตัว
2. $x^3 + x + 1 \equiv 0 \pmod{(x^3 + x + 1)}$ ใน $F_2[x]$ หรือ

   $$x^3 \equiv x + 1 \pmod{(x^3 + x + 1)}$$
3. $x^3 + 2x^2 + x + 1 \equiv x + 1 \pmod{(x + 2)}$ ใน $F_3[x]$
   เพราะว่า $(x^3 + 2x^2 + x + 1) - (x + 1) = x^3 + 2x^2 = x^2(x + 2)$

ซึ่งหารด้วย $x + 2$ ได้ลงตัว

4. ใน $F_3[x]$, $(x + 1)^3 + x + 1 = (x^3 + 1) + (x + 1) = x^3 + x + 2$

$$= x(x^2 + 1) + 2 \equiv 2 \pmod{(x^2 + 1)}$$

นิยาม 5.3.2

> ให้ $F[x]/f(x)$ แทนเซตของพหุนามใน $F[x]$ ซึ่งมีดีกรีน้อยกว่า $\deg f(x)$
> ถ้า $a(x), b(x) \in F[x]/f(x)$ กำหนดการดำเนินการใน $F[x]/f(x)$ ดังนี้
>
> **การบวกมอดุโล f(x)**
>
> $a(x) + b(x)$ ก็คือการบวกปกติใน $F[x]$
>
> **การคูณมอดุโล f(x)**
>
> $a(x)b(x)$ ก็คือเศษที่เหลือจากการหาร $a(x)b(x)$ ใน $F[x]$ ด้วย $f(x)$

ตัวอย่าง 5.3.2 : ให้ $a(x) = x^2 + 1$ และ $b(x) = x^2$ เป็นพหุนามใน $F_2[x] / (x^3 - 1)$ ผลคูณ $a(x)b(x) = (x^2+ 1)x^2 = x^4 + x^2$ หาร $a(x)b(x)$ ด้วย $x^3 - 1$ เราได้

$$\begin{array}{rll}
 & x & \text{พจน์ผลหาร} \\
x^3 - 1 \,\big) & \overline{x^4 \quad + x^2} & = a(x)b(x) \\
 & \underline{x^4 \qquad - x} & \\
 & x^2 + x & \text{พจน์เศษ}
\end{array}$$

นั่นคือ $a(x)b(x) = x^4 + x^2 = x(x^3 - 1) + (x^2 + x)$ ใน $F_2[x]$ ดังนั้น

$$a(x)b(x) \equiv x^2 + x \pmod{(x^3 - 1)}$$

หรือ $\quad a(x)b(x) = x^2 + x$ ใน $F_2[x] / (x^3 - 1)$

จะเห็นว่าวิธีการหาผลคูณในตัวอย่าง 5.3.2 ข้างบนนี้ เป็นวิธีที่ไม่สะดวกนัก เราสามารถใช้วิธีลดรูปพหุนามให้อยู่ในรูปที่ง่ายกว่าได้

ตัวอย่างเช่น เรารู้ว่า

$$x^3 - 1 \equiv 0 \pmod{x^3 - 1}$$

หรือ

$$x^3 \equiv 1 \pmod{x^3 - 1}$$

ดังนั้น เราจะแทน x^3 ด้วย 1 ซึ่งจะช่วยให้เราสามารถหาผลคูณในตัวอย่าง 5.3.2 ได้โดยไม่ต้องใช้ขั้นตอนวิธีการหาร จะใช้วิธีลดรูป ดังนี้

$$a(x)b(x) = x^4 + x^2 = x(x^3) + x^2 = x(1) + x^2 = x + x^2$$

ใน $F_2[x] / (x^3 - 1)$

ในกรณีทั่วไป ถ้า $f(x) = x^n - 1$ แล้ว $x^n \equiv 1 \pmod{x^n - 1}$ ดังนั้น ถ้า $r(x)$ เป็นพหุนามใด ๆ ใน $F[x] / (x^n - 1)$ แล้ว $\deg r(x) < n$ เพราะเราสามารถลดดีกรีของพหุนาม $r(x)$ ใน $F[x] / (x^n - 1)$ ด้วยการแทน x^n ด้วย 1

ทฤษฎีบท 5.3.1

$F[x] / f(x)$ เป็นริงภายใต้การบวกและการคูณมอดุโล $f(x)$

พิสูจน์ เว้นไว้ให้พิสูจน์เป็นแบบฝึกหัด

ตัวอย่าง 5.3.3 : ให้ $f(x) = x^3 - 1$ เป็นพหุนามใน $F_2[x]$ สมาชิกในริง $F_2[x] /(x^3 - 1)$ ได้แก่พหุนามดีกรีน้อยกว่า 3 ซึ่งอยู่ในรูป $r(x) = a + bx + cx^2$ เมื่อ a, b, $c \in F_2$ จะเห็นว่าเราสามารถเลือก a, b, c แต่ละตัวได้สองวิธี ดังนั้นจะมีสมาชิกใน $F_2[x] /(x^3 - 1)$ ได้แตกต่างกัน $2^3 = 8$ ตัว ซึ่งได้แก่

$$\{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}$$

ดังแสดงการเลือกเวกเตอร์ abc และพหุนามที่สมนัยกันข้างล่างนี้

abc	r(x)
000	0
100	1
010	x
001	x^2

abc	r(x)
110	$1 + x$
101	$1 + x^2$
011	$x + x^2$
111	$1 + x + x^2$

ข้อสังเกต :

1. ถ้า f(x) เป็นพหุนามดีกรี n สมาชิกใน $F_q[x]$ / f(x) ประกอบด้วยพหุนามดีกรีน้อยกว่า n ซึ่งมีสัมประสิทธิ์เป็นสมาชิกใน F_q ทั้งหลาย
2. ถ้า f(x) เป็นพหุนามดีกรี n จำนวนสมาชิกใน $F_q[x]$ / f(x) เท่ากับ q^n

ทฤษฎีบท 5.3.2

F[x] / f(x) เป็นฟิลด์ก็ต่อเมื่อ f(x) เป็นพหุนามลดทอนไม่ได้

พิสูจน์ เว้นไว้ให้พิสูจน์เป็นการบ้าน

5.4 พหุนามก่อกำเนิดและพหุนามตรวจสอบภาวะเสมอ

จากทฤษฎี 5.3.1 เรารู้ว่า F[x]/f(x) เป็นริงสำหรับพหุนาม f(x) ใดๆ ใน F[x] ในหัวข้อนี้ เราสนใจเฉพาะริง F[x] / f(x) เมื่อ $f(x) = x^n - 1$ และให้ $R_n = F[x]/(x^n - 1)$ ซึ่งเราสามารถแทน x^n ด้วย 1 ในการคำนวณทางพีชคณิตใน R_n

พิจารณาพหุนาม

$$a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \text{ ใน } R_n = F[x]/(x^n - 1)$$

ซึ่งสมนัยกับเวกเตอร์ $\mathbf{a} = a_0a_1 \dots a_{n-1}$ ถ้าเราคูณพหุนาม a(x) ด้วย x จะพบว่า

$$\begin{aligned} x\cdot a(x) &= x(a_0 + a_1x + \dots + a_{n-1}x^{n-1}) \\ &= a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} + a_{n-1}x^n \\ &= a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} \quad (\text{เพราะ } x^n = 1) \end{aligned}$$

ซึ่งเป็นพหุนามที่สมนัยกับเวกเตอร์ $a_{n-1}a_0a_1 \dots a_{n-2}$ ซึ่งเกิดจากการเลื่อนวนของเวกเตอร์ **a** แสดงว่าการเลื่อนวนเวกเตอร์ **a** หนึ่งครั้งไปทางขวา จะเหมือนกับการคูณพหุนาม a(x) ด้วย x นั่นเอง

ทฤษฎีบท 5.4.1 รหัส C ใน R_n เป็นรหัสวัฏจักรก็ต่อเมื่อ C มีสมบัติสอดคล้องกับเงื่อนไขสองข้อต่อไปนี้

1. ถ้า $a(x), b(x) \in C$ แล้ว $a(x) + b(x) \in C$
2. ถ้า $a(x) \in C$ และ $r(x) \in R_n$ แล้ว $r(x)a(x) \in C$

พิสูจน์ สมมุติให้ C เป็นรหัสวัฏจักรใน R_n แสดงว่า C เป็นรหัสเชิงเส้น ดังนั้น C สอดคล้องกับเงื่อนไขข้อ 1 และถ้า $a(x) \in C$ และ $r(x) = r_0 + r_1x + \ldots + r_{n-1}x^{n-1} \in R_n$ แล้ว

$$r(x)a(x) = r_0a(x) + r_1\,xa(x) + \ldots + r_{n-1}\,x^{n-1}a(x) \in C$$

แสดงว่าข้อ 2 เป็นจริง

ในทางกลับกัน สมมุติให้เงื่อนไขข้อ 1 และ 2 เป็นจริง จากเงื่อนไขข้อแรก แสดงว่า C มีสมบัติปิดภายใต้การบวก และจากข้อ 2 ถ้าเราเลือก $r(x)$ ให้เป็นสเกลาร์ใด ๆ จะเห็นว่า C มีสมบัติปิดภายใต้การคูณด้วยสเกลาร์ ดังนั้น C เป็นรหัสเชิงเส้น ต่อไปจะแสดงว่า C เป็นรหัสวัฏจักร นั่นคือจะแสดงว่าการเลื่อนวนของสมาชิกใน C เป็นสมาชิกใน C เราให้ $a(x)$ เป็นสมาชิกใน C และให้ $r(x) = x$ จากเงื่อนไขข้อ 2 แสดงว่า $xa(x) \in C$ นั่นคือ C เป็นรหัสวัฏจักรตามต้องการ ■

หมายเหตุ : สำหรับผู้ที่คุ้นเคยกับวิชาพีชคณิตนามธรรม จะเห็นว่ารหัส C ก็คือไอดีลของริง R_n นั่นเอง

นิยาม 5.4.1 ถ้า $f(x) \in R_n$ เราให้ $\langle f(x)\rangle$ แทนเซตของพหุนามใน R_n ที่เป็นพหุคูณของ $f(x)$ ทั้งหลายใน R_n กล่าวคือ

$$\langle f(x)\rangle = \{r(x)f(x) \mid r(x) \in R_n\}$$

ทฤษฎีบท 5.4.2 ถ้า $f(x)$ เป็นพหุนามใด ๆ ใน R_n แล้ว $\langle f(x)\rangle$ จะเป็นรหัสวัฏจักร ซึ่งจะเรียกว่ารหัสวัฏจักรที่ก่อกำเนิดโดย $f(x)$

พิสูจน์ ในการแสดงว่า C = <f(x)> เป็นรหัสเชิงเส้น เราเพียงแสดงว่าเงื่อนไขข้อ 1 และข้อ 2 ของทฤษฎีบท 5.4.1 เป็นจริงสำหรับ C ดังนี้

1. ถ้า $a(x)f(x)$ และ $b(x)f(x) \in \langle f(x)\rangle$ แล้ว

   $a(x)f(x) + b(x)f(x) = (a(x) + b(x))f(x) \in \langle f(x)\rangle$

2. ถ้า $a(x)f(x) \in \langle f(x)\rangle$ และ $r(x) \in R_n$ แล้ว

   $r(x)a(x)f(x) = (r(x)a(x))f(x) \in \langle f(x)\rangle$ ■

ตัวอย่าง 5.4.1 : จงหาคำรหัสทั้งหลายของรหัส $C = \langle 1 + x^2\rangle$ ในริง $F_2[x] / (x^3 - 1)$

วิธีทำ ในที่นี้ $f(x) = 1 + x^2$

จากตัวอย่าง 5.3.3 สมาชิกใน $F_2[x] / (x^3 - 1)$ ประกอบด้วย

$$0,\ 1,\ x,\ x^2,\ 1 + x,\ 1 + x^2,\ x + x^2,\ 1 + x + x^2$$

สมาชิกใน C เกิดจากการคูณพหุนาม f(x) ด้วยพหุนาม r(x) ทั้งหลายใน $F_2[x] / (x^3 - 1)$ ตัวอย่างเช่น ให้ $r(x) = 1 + x \in F_2[x] / (x^3 - 1)$ เราจะได้คำรหัส

$$r(x)f(x) = (1 + x)(1 + x^2) = 1 + x + x^2 + x^3 = x + x^2$$

เพราะว่า $x^3 = 1$ จะเห็นว่า $x + x^2$ เป็นคำรหัสใน C ซึ่งสมนัยกับเวกเตอร์ 011 ดังแสดงในแถวที่ 5 ของตาราง 5.4.1 ถ้าให้ $r(x) = x^2$ จะได้คำรหัส

$$r(x)f(x) = x^2 (1 + x^2) = x^2 + x^4 = x^2 + x$$

ซึ่งสมนัยกับเวกเตอร์ 011 เช่นเดียวกัน ดังปรากฏในแถวที่ 4 ของตาราง เราสามารถหาคำรหัสอื่น ๆ ใน C ได้ในทำนองเดียวกัน คำรหัสทั้งหลายใน C ปรากฏในหลักที่สองของตาราง 5.4.1 ซึ่งสมนัยกับเวกเตอร์ในหลักที่สามของตารางเดียวกัน

จากตาราง 5.4.1 จะเห็นว่าคำรหัสทั้งหลายใน C ที่อยู่ในรูปของพหุนามใน $F_2[x]/(x^3 - 1)$ มีเพียง 4 พหุนามเท่านั้นที่แตกต่างกัน คือ

$$0,\ x + x^2,\ 1 + x^2,\ \text{และ}\ 1 + x$$

และคำรหัสที่อยู่ในรูปของเวกเตอร์หรือ 3-สิ่งอันดับที่สมนัยกันคือ

000, 011, 101, และ 110

ซึ่งก็คือรหัส C_2 ในตัวอย่าง 1.7.1 นั่นเอง

ตาราง 5.4.1 : คำรหัสของ $C = \langle 1 + x^2 \rangle$ ใน $F_2[x]/(x^3 - 1)$

$r(x)$	$c(x) = r(x)f(x)$	เวกเตอร์ c
0	0	000
1	$1 + x^2$	101
x	$1 + x$	110
x^2	$x + x^2$	011
$1 + x$	$x + x^2$	011
$1 + x^2$	$1 + x$	110
$x + x^2$	$1 + x^2$	101
$1 + x + x^2$	0	000

ข้อสังเกต : จะเห็นว่า $c(x) = r(x)f(x)$ เป็นพหุนามดีกรีน้อยกว่า 3 ซึ่งเป็นผลให้คำรหัส **c** เป็นเวกเตอร์ที่มีความยาวเท่ากับ 3 ในกรณีทั่วไป คำรหัส $c(x) = r(x)f(x)$ เป็นพหุนามดีกรีน้อยกว่า n ใน R_n ดังนั้น **c** จะเป็นเวกเตอร์ที่มีความยาว n ใน F_q^n

ทฤษฎีบท 5.4.3

ถ้า C เป็นรหัสวัฏจักรใน R_n ที่ $C \neq \{0\}$ แล้ว

1. จะมีพหุนามโมนิก $g(x)$ ที่มีดีกรีน้อยที่สุด ใน C เพียงพหุนามเดียว
2. $C = \langle g(x) \rangle$
3. $g(x)$ เป็นตัวประกอบของ $x^n - 1$ (หรือ $g(x)$ หาร $x^n - 1$ ลงตัว)

พิสูจน์ 1. สมมุติให้ $g(x)$ และ $h(x)$ เป็นพหุนามโมนิกที่มีดีกรีน้อยที่สุด

ใน C เนื่องจาก C เป็นรหัสเชิงเส้น เราได้ $g(x) - h(x) \in C$ และมีดีกรีน้อยกว่า $\deg g(x) = \deg h(x)$ ซึ่งขัดแย้งกับที่เราสมมุติให้ $g(x)$ และ $h(x)$ มีดีกรีเล็กที่สุด แสดงว่า $g(x) - h(x) = 0$ ดังนั้น $g(x) = h(x)$

พิสูจน์ 2. สมมุติให้ $a(x) \in C$ จากขั้นตอนวิธีการหาร แสดงว่าจะมีพหุนาม $q(x)$ และ $r(x)$ ใน $F[x]$ ซึ่งทำให้

$$a(x) = g(x)q(x) + r(x)$$

เมื่อ $r(x) = 0$ หรือ $\deg r(x) < \deg g(x)$ เราได้

$$r(x) = a(x) - g(x)q(x) \in C \quad \text{(C เป็นรหัสเชิงเส้น)}$$

ดังนั้น $r(x) = 0$ เพราะว่าเป็นไปไม่ได้ที่ $\deg r(x) < \deg g(x)$ เนื่องจาก $g(x)$ เป็นพหุนามที่มีดีกรีน้อยที่สุดใน C

พิสูจน์ 3. จากขั้นตอนวิธีการหารเช่นกัน เราได้

$$x^n - 1 = g(x)q(x) + r(x)$$

เมื่อ $r(x) = 0$ หรือ $\deg r(x) < \deg g(x)$ แต่

$$r(x) = (x^n - 1) - g(x)q(x) \equiv - g(x)q(x) \pmod{(x^n - 1)}$$

จะเห็นว่า $r(x)$ เป็นพหุคูณของ $g(x)$ ดังนั้น $r(x) \in \langle g(x) \rangle$ เนื่องจาก $g(x)$ มีดีกรีเล็กที่สุด ดังนั้น $r(x) = 0$ นั่นคือ $x^n - 1 = g(x)q(x)$ กล่าวคือ $g(x)$ เป็นตัวประกอบของ $x^n - 1$ ■

ข้อสังเกต : จากตัวอย่าง 5.4.1 เราพบว่าพหุนาม $1 + x^2$ ก่อกำเนิดรหัส C แต่ $1 + x^2$ ไม่ใช่พหุนามที่มีดีกรีน้อยที่สุดใน พหุนามที่มีดีกรีน้อยที่สุดใน C คือ $1 + x$ ซึ่งมีเพียงพหุนามเดียวเท่านั้น นอกจากนี้ $1 + x$ เป็นตัวประกอบของ $x^3 - 1$ หรือกล่าวว่า $1 + x$ หาร $x^3 - 1$ ได้ลงตัว

การแยกตัวประกอบของ $x^n - 1$ ออกเป็นผลคูณของพหุนามลดทอนไม่ได้ ไม่ใช่เรื่องง่ายนัก แต่เนื่องจากการแยกตัวประกอบของ $x^n - 1$ จะมีบทบาทสำคั มากต่อการศึกษารหัสวัฏจักร เราจึงแสดงตัวประกอบของ $x^n - 1$ บนฟิลด์ F_2 สำหรับ $n = 1, 2, \ldots, 25$ ในตาราง 5.4.2

ตาราง 5.4.2 : ตัวประกอบของ $x^n - 1$ บนฟิลด์ GF(2)

n	ตัวประกอบ
1	$1 + x$
2	$(1 + x)^2$
3	$(1 + x)(1 + x + x^2)$
4	$(1 + x)^4$
5	$(1 + x)(1 + x + x^2 + x^3 + x^4)$
6	$(1 + x)^2(1 + x + x^2)^2$
7	$(1 + x)(1 + x + x^3)(1 + x^2 + x^3)$
8	$(1 + x)^8$
9	$(1 + x)\ (1 + x + x^2)(1 + x^3 + x^6)$
10	$(1 + x)^2(1 + x + x^2 + x^3 + x^4)^2$
11	$(1 + x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10})$
12	$(1 + x)^4(1 + x + x^2)^4$
13	$(1 + x)(1 + x + \ldots + x^{12})$
14	$(1 + x)^2(1 + x + x^3)^2(1 + x^2 + x^3)^2$
15	$(1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4)$
16	$(1 + x)^{16}$
17	$(1 + x)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x^3 + x^4 + x^5 + x^8)$
18	$(1 + x)^2(1 + x + x^2)^2(1 + x^3 + x^6)^2$
19	$(1 + x)(1 + x + x^2 + \ldots + x^{18})$
20	$(1 + x)^4(1 + x + x^2 + x^3 + x^4)^4$
21	$(1+x)(1+x+x^2)(1+x^2+x^3)(1+x+x^3)(1+x+x^2+x^4+x^5+x^6)(1+x+x^2+x^4+x^6)$
22	$(1 + x)^2(1 + x + x^2 + \ldots + x^{10})^2$
23	$(1+x)(1+x+x^5+x^6+x^7+x^9+x^{11})(1+x^2+x^4+x^5+x^6+x^{10}+x^{11})$
24	$(1 + x)^8(1 + x + x^2)^8$
25	$(1 + x)(1 + x + x^2 + x^3 + x^4)(1 + x^5 + x^{10} + x^{15} + x^{20})$

นิยาม 5.4.2 จะเรียกพหุนามโมนิกที่มีดีกรีเล็กที่สุดใน $C \neq \{0\}$ ว่า ***พหุนามก่อกำเนิด*** ของรหัส C

ตัวอย่าง 5.4.2 : จงหารหัสวัฏจักรบนฟีลด์ F_2 ที่มีความยาวเท่ากับ 3 ทั้งหมด

วิธีทำ ในที่นี้ $n = 3$, $q = 2$ จากตัวอย่าง 5.3.3 เรารู้ว่าจำนวนสมาชิกใน $R_3 = F_2[x]/(x^3 - 1)$ เท่ากับ $2^3 = 8$ และ

$$F_2[x] / (x^3 - 1) = \{0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2\}$$

ซึ่งสมนัยกับเซตของเวกเตอร์

$$\{000, 100, 010, 001, 110, 101, 011, 111\}$$

ก่อนอื่น เราแยกตัวประกอบของ $x^3 - 1$ ใน $F_2[x]$ จะได้

$$x^3 - 1 = x^3 + 1 = (x + 1)(x^2 + x + 1)$$

ดังนั้น ตัวประกอบของ $x^3 - 1$ ได้แก่พหุนาม 1, $x + 1$, $x^2 + x + 1$ และ $x^3 - 1$ ที่ปรากฏในหลักแรกของตาราง 5.4.3 พหุนามเหล่านี้จะเป็นพหุนามก่อกำเนิดของรหัสวัฏจักรที่มีความยาว 3 และคำรหัสใน C คือพหุคูณของพหุนามก่อกำเนิด $g(x)$ นั่นคือ คำรหัสใน C เกิดจากการคูณพหุนามก่อกำเนิดของ C ด้วยพหุนามต่าง ๆ ใน $R_3 = F_2[x]/(x^3 - 1)$ ตัวอย่างเช่นถ้า C ก่อกำเนิดโดย $g(x) = 1 + x$ กล่าวคือ $C = \langle 1 + x \rangle$ สมาชิกใน C เกิดจากการคูณ $g(x) = 1 + x$ ด้วยสมาชิกใน R_3 ซึ่งได้แก่

$0(1+ x) = 0,$

$1(1 + x) = 1 + x,$

$x(1+ x) = x + x^2,$

$(1 + x)(1 + x) = 1 + x^2,$

$x^2(1 + x) = x^2 + x^3 = x^2 + 1$ เนื่องจาก $x^3 = 1$

$(1 + x^2)(1 + x) = 1 + x + x^2 + x^3 = x + x^2$

$(x + x^2)(1 + x) = x + x^2 + x^2 + x^3 = 1 + x$

$(1 + x + x^2)(1 + x) = 1 + x + x + x^2 + x^2 + x^3 = 0$

นั่นคือ

$$C = \{0, 1 + x, x + x^2, 1 + x^2\}$$

ซึ่งปรากฏในหลักที่สองของตาราง 5.4.3 ในแถวเดียวกับพหุนามก่อกำเนิด 1 + x เมื่อเขียนคำรหัสของ C ในรูปเวกเตอร์จะได้

$$C = \{000, 110, 011, 101\}$$

ซึ่งปรากฏในหลักที่สามของตาราง 5.4.3 เราสามารถหารหัส C ที่ก่อกำเนิดโดยพหุนามอื่นๆ ได้ในทำนองเดียวกัน ดังนั้น รหัสวัฏจักรบนฟีลด์ F_2 ที่มีความยาวเท่ากับ 3 ทั้งหมดคือรหัสที่ปรากฏในตาราง 5.4.3

ตาราง 5.4.3 : รหัสวัฏจักรไบนารีที่มีความยาวเท่ากับ 3

พหุนามก่อกำเนิด	รหัสใน R_3	รหัสใน F_2^3
1	R_3	F_2^3
$1 + x$	$\{0, 1+x, x+x^2, 1+x^2\}$	{000, 110, 011, 101}
$1 + x + x^2$	$\{0, 1 + x+ x^2\}$	{000, 111}
$x^3 - 1 = 0$	{0}	{000}

หมายเหตุ : จากตัวอย่าง 5.4.1 และ 5.4.2 จะเห็นว่าทั้ง $1 + x^2$ และ $1 + x$ ก่อให้เกิดรหัส C เดียวกัน แต่เราจะไม่เรียก $1 + x^2$ ว่าพหุนามก่อกำเนิดของ C พหุนามก่อกำเนิดตามนิยาม 5.4.2 คือพหุนาม 1 + x ที่มีดีกรีน้อยที่สุดใน C เพียงพหุนามเดียวเท่านั้น

เนื่องจาก g(x) เป็นพหุนามโมนิกซึ่งเป็นตัวประกอบของ $x^n - 1$ นั่นคือ

$$x^n - 1 = g(x)h(x)$$

ดังนั้น h(x) ย่อมเป็นพหุนามโมนิกที่เป็นตัวประกอบของ $x^n - 1$ ด้วย

นิยาม 5.4.3 ถ้า $x^n - 1 = g(x)h(x)$ และ g(x) เป็นพหุนามก่อกำเนิดของรหัส C จะเรียก h(x) ว่า ***พหุนามตรวจสอบภาวะเสมอ*** ของรหัส C

ตัวอย่าง 5.4.3 : พิจารณารหัส C ใน R_7 บนฟิลด์ F_2 ที่ก่อกำเนิดโดยพหุนาม $g(x) = 1 + x + x^3$ จากตาราง 5.4.2 เรามี

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

$$= g(x)(1 + x)(1 + x^2 + x^3)$$

ดังนั้น พหุนามตรวจสอบภาวะเสมอของ C คือพหุนาม

$$h(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$$

จะเห็นว่า $\deg g(x) = n - k = 7 - 4 = 3$ และ $\deg h(x) = 4$

หมายเหตุ : เนื่องจากพหุนามตรวจสอบภาวะเสมอ $h(x)$ เป็นตัวประกอบของ $x^7 - 1$ ดังนั้น รหัสที่ก่อกำเนิดโดย $h(x)$ เป็นรหัสวัฏจักรที่มีความยาว 7 ด้วยเช่นกัน เราจะได้เห็นต่อไปว่ารหัสที่ก่อกำเนิดโดยพหุนาม $h(x)$ สมมูลกับรหัส $C^{\perp}$

ทฤษฎีบท 5.4.4

> ให้ C เป็นรหัสวัฏจักรใน R_n ซึ่งมี $g(x)$ เป็นพหุนามก่อกำเนิด และมี $h(x)$ เป็นพหุนามตรวจสอบภาวะเสมอ ดังนั้น $c(x)$ ใน R_n เป็นคำรหัสก็ต่อเมื่อ $c(x)h(x) = 0$

พิสูจน์ สมมุติให้ $c(x) \in C$ ดังนั้น $c(x)$ เป็นพหุคูณของ $g(x)$ นั่นคือ

$$c(x) \equiv a(x)g(x) \pmod{x^n - 1}$$

สำหรับบาง $a(x) \in R_n$ ดังนั้น

$$c(x)h(x) \equiv a(x)g(x)h(x) \equiv 0 \pmod{x^n - 1}$$

เนื่องจาก $g(x)h(x) = x^n - 1 = 0$ ในทางกลับกัน สมมุติให้

$$c(x)h(x) \equiv 0 \pmod{x^n - 1}$$

หาร $c(x)$ ด้วย $g(x)$ เราได้

$$c(x) = g(x)q(x) + r(x)$$

สำหรับบาง $q(x)$ และ $r(x)$ ใน R_n และ $r(x) = 0$ หรือ

$$\deg r(x) < \deg g(x) = n - k$$

จาก $c(x)h(x) \equiv 0 \pmod{x^n - 1}$ เราได้

$$c(x)h(x) = g(x)q(x)h(x) + r(x)h(x) \equiv r(x)h(x) \pmod{x^n - 1}$$

ดังนั้น

$$r(x)h(x) \equiv 0 \pmod{x^n - 1}$$

นั่นคือ $r(x)h(x)$ เป็นพหุคูณของพหุนาม $x^n - 1$ แต่ $\deg r(x) < n - k$ และ $\deg h(x) = k$ แสดงว่า $r(x)h(x) = 0$ แต่ $h(x) \neq 0$ ดังนั้น $r(x) = 0$ ซึ่งเป็นผลให้ $c(x) = g(x)q(x)$ นั่นคือ $c(x) \in C$ ■

5.5 เมทริกซ์ก่อกำเนิดและเมทริกซ์ตรวจสอบภาวะเสมอของรหัสวัฏจักร

เนื่องจากรหัสวัฏจักรเป็นรหัสเชิงเส้น ดังนั้นย่อมต้องกำหนดโดยเมทริกซ์ก่อกำเนิดได้ เราจะแสดงวิธีหาเมทริกซ์ก่อกำเนิดจากพหุนามก่อกำเนิด และจะแสดงวิธีหาเมทริกซ์ตรวจสอบภาวะเสมอจากพหุนามก่อกำเนิดนี้

ทฤษฎีบท 5.5.1

ถ้า $g(x) = g_0 + g_1x + \ldots + g_{n-k}x^{n-k}$ เป็นพหุนามก่อกำเนิดของรหัสวัฏจักรแล้ว g_0 จะไม่เป็นศูนย์

พิสูจน์ เราจะพิสูจน์โดยวิธีหาข้อขัดแย้ง โดยสมมุติว่า $g_0 = 0$ ดังนั้น

$$x^{n-1}g(x) = x^{-1}g(x)$$

เป็นคำรหัสใน C ซึ่งมีดีกรี $n - k - 1$ ซึ่งขัดแย้งกับความจริงที่ว่า $g(x)$ เป็นคำรหัสที่มีดีกรีต่ำสุด ดังนั้น $g_0 \neq 0$ ■

ทฤษฎีบท 5.5.2

ถ้า C เป็นรหัสวัฏจักรที่มี $g(x) = g_0 + g_1x + \ldots + g_{n-k}x^{n-k}$ เป็นพหุนามก่อกำเนิดแล้ว $\dim(C) = k$ และเมทริกซ์ก่อกำเนิดของ C จะอยู่ในรูป

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & & g_{n-k} & & \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & & g_{n-k} \end{bmatrix}$$

$$= \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

พิสูจน์ เห็นได้ชัดว่า

$$\{ g(x), xg(x), x^2g(x), \ldots, \text{และ } x^{k-1}g(x) \}$$

เป็นเซตอิสระเชิงเส้น เพราะถ้าไม่เป็นเซตอิสระเชิงเส้นแล้ว จะมีสเกลาร์ a_i สำหรับ $0 \leq i \leq k-1$ ซึ่งทำให้

$$a_0g(x) + a_1g(x)x + a_2g(x)x^2 + \ldots + a_{k-1}g(x)x^{k-1} = 0$$

นั่นคือ

$$(a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1})g(x) = 0$$

ซึ่งเป็นไปไม่ได้ เพราะทางซ้ายมือเป็นพหุนามที่มีดีกรีน้อยกว่า n ดังนั้นเป็นไปไม่ได้ที่จะเท่ากับ 0 (mod $(x^n - 1)$) นอกจาก a_i จะเป็น 0 ทั้งหมด

ต่อไป เราจะแสดงว่า $\{g(x), xg(x), x^2g(x), \ldots,$ และ $x^{k-1}g(x)\}$ แผ่ทั่ว C นั่นคือจะแสดงว่าคำรหัสใน C แต่ละคำสามารถเขียนในรูปการรวมเชิงเส้นของพหุนามเหล่านี้

ถ้า a(x) เป็นคำรหัสใน C แล้ว a(x) = g(x)q(x) สำหรับบางพหุนาม q(x) เนื่องจาก deg a(x) < n ดังนั้น deg q(x) < k สมมุติให้

$$q(x) = q_0 + q_1x + \ldots + q_{k-1}x^{k-1}$$

จะได้

$$g(x)q(x) = g(x)(q_0 + q_1x + \dots + q_{k-1}x^{k-1})$$

$$= q_0g(x) + q_1\,xg(x) + \dots + q_{k-1}x^{k-1}g(x)$$

นั่นคือ $a(x) = g(x)q(x)$ เป็นการรวมเชิงเส้นของพหุนาม

$$g(x), xg(x), x^2g(x), \dots, x^{k-1}g(x)$$

ดังนั้น $\{ g(x), xg(x), x^2g(x), \dots, x^{k-1}g(x) \}$ เป็นฐานหลักของ C และ dim (C) = k เขียนค่าพหุนามในฐานหลักในรูป n –สิ่งอันดับ เราได้เมทริกซ์ก่อกำเนิด G ในรูปที่ต้องการ ■

ตัวอย่าง 5.5.1 : จงหาพหุนามก่อกำเนิดของรหัสวัฏจักรบนฟิลด์ F_2 ทั้งหลายที่มีมิติ 3 และมี ความยาวเท่ากับ 7

วิธีทำ ในที่นี้ เราต้องการหารหัสที่มีความยาวเท่ากับ n = 7 ดังนั้น พหุนามก่อกำเนิดของรหัสที่มีความยาว 7 นี้ จะต้องเป็นตัวประกอบของ $x^7 - 1$ จากตาราง 5.4.2 เรามี

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

และเนื่องจากเราต้องการหารหัสที่มีมิติเท่ากับ 3 ดังนั้นเราสนใจเฉพาะพหุนามดีกรี n – k = 7 – 3 = 4 ที่เป็นตัวประกอบของ $x^7 - 1$ เท่านั้น ซึ่งได้แก่

1. $g_1(x) = (1 + x)(1 + x + x^3) = 1 + x^2 + x^3 + x^4$ และ
2. $g_2(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$

ตัวอย่าง 5.5.2 : จงหารหัสวัฏจักรเทอร์นารี C ที่ dim(C) = 3 และมีความยาว 4 พร้อมทั้งเขียนเมทริกซ์ก่อกำเนิดของรหัส C

วิธีทำ จากตัวอย่าง 5.2.5 เรามี $x^4 - 1 = (1 + x)(2 + x)(1 + x^2)$ และเนื่องจาก dim(C) = 3 พหุนามก่อกำเนิดของ C จะต้องมีดีกรี n – k = 4 – 3 = 1 และเป็นตัวประกอบของ $x^4 - 1$ ซึ่งมีสองพหุนาม ได้แก่ $g_1(x) = 1 + x$ และ $g_2(x) = 2 + x$ จะได้

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ และ } G_2 = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix}$$

เป็นเมทริกซ์ก่อกำเนิดของ C ที่เกิดจากพหุนามก่อกำเนิด $g_1(x) = 1 + x$ และ $g_2(x) = 2 + x$ ตามลำดับ

ตัวอย่าง 5.5.3 : จงหาเมทริกซ์ก่อกำเนิดของรหัสวัฏจักร C บนฟิลด์ F_2 ที่มีความยาว 7 ที่ก่อกำเนิดโดยพหุนาม $g(x) = 1 + x + x^3$

วิธีทำ เมทริกซ์ก่อกำเนิดของ C คือ

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

ดังได้เห็นในบทที่ 3 แล้วว่า ถ้าเมทริกซ์ก่อกำเนิดของ C อยู่ในรูปมาตรฐาน [I | A] แล้วเราสามารถหาเมทริกซ์ตรวจสอบภาวะเสมอของ C ได้โดยง่าย เพราะเมทริกซ์ตรวจสอบภาวะเสมอของ C จะอยู่ในรูป $[-A^T \mid I]$ ในกรณีที่เมทริกซ์ก่อกำเนิด G ไม่อยู่ในรูปมาตรฐาน การหาเมทริกซ์ตรวจสอบภาวะเสมอค่อนข้างจะซับซ้อนกว่า เช่นในตัวอย่างต่อไปนี้

ตัวอย่าง 5.5.4 : จงหาเมทริกซ์ตรวจสอบภาวะเสมอ ของรหัสไบนารี C ที่มีความยาว 7 ที่ก่อกำเนิดโดยพหุนาม $g(x) = 1 + x + x^3$

วิธีทำ เมทริกซ์ก่อกำเนิด G ของ C คือเมทริกซ์ในตัวอย่าง 5.5.3 ให้ $x = x_0x_1x_2x_3$ เป็นสารที่จะเข้ารหัส ซึ่งจะได้

$$xG = (x_0, x_0 + x_1, x_1 + x_2, x_0 + x_2 + x_3, x_1 + x_3, x_2, x_3)$$

เป็นคำรหัสใน C

สมมุติให้ $(a_0, a_1, a_2, a_3, a_4, a_5, a_6)$ เป็นแถวของเมทริกซ์ตรวจสอบภาวะเสมอของ C เมื่อ $a_i \in F_2$ สำหรับ $i = 0, 1, \ldots, 6$ ดังนั้น

$$a_0x_0 + a_1(x_0 + x_1) + a_2(x_1 + x_2) + a_3(x_0 + x_2 + x_3)$$

$$+ a_4(x_1 + x_3) + a_5x_2 + a_6x_3 = 0$$

$$x_0(a_0 + a_1 + a_3) + x_1(a_1 + a_2 + a_4) + x_2(a_2 + a_3 + a_5)$$

$$+ x_3(a_3 + a_4 + a_6) = 0$$

สมการข้างบนนี้เป็นจริงสำหรับทุก ๆ $x = x_0x_1x_2x_3 \in F_2^4$ ดังนั้น

$$a_0 + a_1 + a_3 = 0, \qquad a_2 + a_3 + a_5 = 0$$

$$a_1 + a_2 + a_4 = 0, \qquad a_3 + a_4 + a_6 = 0$$

สมมุติว่า $a_0 = 1$ แสดงว่า $a_1 + a_3 = 1$

เลือก $a_1 = 0$ เราได้ $a_3 = 1$ ซึ่งเป็นผลให้

$$a_2 = a_4,\ a_2 + a_5 = 1 = a_4 + a_5 \text{ และ } a_4 + a_6 = 1$$

ดังนั้น $a_5 + a_6 = 0$ หรือ $a_5 = a_6$

สมมุติว่าเลือก $a_2 = a_4 = 1$ และ $a_5 = a_6 = 0$ เราได้

$$a_0 = 1,\ a_1 = 0,\ a_2 = 1,\ a_3 = 1,\ a_4 = 1,\ a_5 = a_6 = 0$$

เลือก $a_1 = 1$ เราได้ $a_3 = 0$ ซึ่งเป็นผลให้

$$a_4 + a_6 = 0 \text{ หรือ } a_4 = a_6$$

ถ้าเลือก $a_4 = a_6 = 0$ เราได้

$$a_0 = 1,\ a_1 = 1,\ a_2 = 1,\ a_3 = 0,\ a_4 = 0,\ a_5 = 1,\ a_6 = 0$$

สมมุติให้ $a_0 = 0$ ทำในทำนองเดียวกัน เราได้

$$a_0 = 0,\ a_1 = 1,\ a_2 = 1,\ a_3 = 1,\ a_4 = 0,\ a_5 = 0,\ a_6 = 1$$

ดังนั้น เมทริกซ์ตรวจสอบภาวะเสมอของ C คือ

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

หมายเหตุ : จะเห็นว่าการหาเมทริกซ์ตรวจสอบภาวะเสมอในตัวอย่าง 5.5.4 ข้างบนนี้เป็นวิธีที่ไม่สะดวกนัก ถ้าเราสามารถหาพหุนามก่อกำเนิดของ $C^{\perp}$ ซึ่งเป็นรหัสคู่เสมอกันของ C จะทำให้เราสามารถหาเมทริกซ์ตรวจสอบภาวะเสมอของ C ได้ง่ายกว่า

ถ้าเราแยกตัวประกอบ $x^n - 1$ ออกเป็นผลคูณของพหุนามลดทอนไม่ได้บนฟีลด์ F แล้ว เราจะรู้ทันทีว่ามีรหัสวัฏจักรบนฟีลด์ F ที่มีความยาว n เป็นจำนวนเท่าใด และยังรู้มิติของรหัสเหล่านั้นได้จากดีกรีของพหุนามก่อกำเนิด จะเป็นการดีมาก ถ้าเราสามารถหาพหุนามก่อกำเนิดของ $C^{\perp}$ ได้จากตัวประกอบของ $x^n - 1$ นอกจากนี้ยังชี้ให้เห็นว่ารหัส $C^{\perp}$ ก็เป็นรหัสวัฏจักรด้วยเช่นกัน

ถ้า $x^n - 1 = g(x)h(x)$ และ $\deg g(x) = n - k$ แล้วมิติของ $C = \langle g(x) \rangle$ จะเท่ากับ k และ $\deg h(x) = k$ เนื่องจาก h(x) เป็นตัวประกอบของ $x^n - 1$ ดังนั้น h(x) เป็นพหุนามก่อกำเนิดของรหัสวัฏจักร C' ที่มีมิติ $n - k$ ซึ่งเท่ากับมิติของ $C^{\perp}$ จึงอาจทำให้เข้าใจได้ว่ารหัส C' ก็คือ $C^{\perp}$ ซึ่งจริง ๆ แล้วไม่เป็นเช่นนั้น จะเป็นจริงเฉพาะบางกรณีเท่านั้น

นิยาม 5.5.1 ถ้า $h(x) = h_0 + h_1x + \ldots + h_kx^k$ เป็นพหุนามดีกรี k บนฟีลด์ F ส่วนกลับ(reciprocal) ของ h(x) คือพหุนาม

$$h_R(x) = h_k + h_{k-1}x + \ldots + h_0x^k = x^kh(x^{-1})$$

ตัวอย่าง 5.5.5 : ถ้า $h(x) = 1 + x + 2x^3 + x^4$ เป็นพหุนามบนฟีลด์ F_3 เราได้

$$h_R(x) = x^4h(x^{-1}) = x^4(1 + x^{-1} + 2x^{-3} + x^{-4}) = 1 + 2x + x^3 + x^4$$

จะเห็นว่าสัมประสิทธิ์ของ $h_R(x)$ ก็คือสัมประสิทธิ์ของ $h(x)$ แต่เรียงในลำดับที่ตรงกันข้ามกัน

ทฤษฎีบท 5.5.3 ถ้า C เป็นรหัสวัฏจักร-[n, k] ใน R_n ซึ่งมี

$$h(x) = h_0 + h_1x + \dots + h_kx^k$$

เป็นพหุนามตรวจสอบภาวะเสมอแล้ว

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & & h_0 & 0 & & 0 \\ & & \ddots & \ddots & & \ddots & & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & & h_k \end{bmatrix}$$

จะเป็นเมทริกซ์ตรวจสอบภาวะเสมอของ C นั่นคือ เป็นเมทริกซ์ก่อกำเนิดของ $C^{\perp}$

พิสูจน์ จากความสัมพันธ์ $g(x)h(x) = x^n - 1$ แสดงว่าพจน์ค่าคงตัว $h_0 \neq 0$ ให้

$$c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

เป็นคำรหัสใน C จากทฤษฎีบท 5.4.4 แสดงว่า $c(x)h(x) = 0$ นั่นคือ

$$c(x)h(x) = (c_0 + c_1x + \dots + c_{n-1}x^{n-1})(h_0 + h_1x + \dots + h_kx^k) = 0$$

ดังนั้นสัมประสิทธิ์ของทุกพจน์ใน $c(x)h(x)$ ต้องเป็นศูนย์ทั้งหมด โดยเฉพาะสัมประสิทธิ์ของ $x^k, x^{k+1}, \dots, x^{n-1}$ ในผลคูณ $c(x)h(x)$ ต้องเป็น 0 นั่นคือ

$$\begin{aligned} c_0h_k + c_1h_{k-1} + \dots + c_kh_0 &= 0 \\ c_1h_k + c_2h_{k-1} + \dots + c_{k+1}h_0 &= 0 \\ &\vdots \\ c_{n-k-1}h_k + c_{n-k}h_{k-1} + \dots + c_{n-1}h_0 &= 0 \end{aligned}$$

จากสมการแรก ชี้ให้เห็นว่าเวกเตอร์ $(c_0, c_1, \dots, c_{n-1})$ ตั้งฉากกับเวก

เตอร์ $(h_k, h_{k-1}, \ldots, h_0, 0, \ldots, 0)$ และจากสมการที่เหลือ จะเห็นว่าเวกเตอร์ $(c_0, c_1, \ldots, c_{n-1})$ ตั้งฉากกับเวกเตอร์ที่เกิดจากการเลื่อนวนของเวกเตอร์ $(h_k, h_{k-1}, \ldots, h_0, 0, \ldots, 0)$ ดังนั้น แต่ละแถวของเมทริกซ์ H เป็นคำรหัสใน $C^{\perp}$ นอกจากนี้ เนื่องจาก h(x) เป็นพหุนามโมนิกที่มีดีกรี k ดังนั้น $h_k \neq 0$ และเมทริกซ์ H อยู่ในรูปเมทริกซ์ขั้นบันได ดังนั้นเซตของแถวของ H เป็นเซตอิสระเชิงเส้น และจำนวนแถวของ H เท่ากับ n – k ซึ่งเท่ากับ $\dim(C^{\perp})$ แสดงว่า H เป็นเมทริกซ์ก่อกำเนิดของ $C^{\perp}$ นั่นคือเป็นเมทริกซ์ตรวจสอบภาวะเสมอของ C ■

บทแทรก 5.5.1

ถ้า $h(x) = h_0 + h_1x + \ldots + h_kx^k$ เป็นพหุนามตรวจสอบภาวะเสมอของรหัสวัฏจักร C แล้ว $C^{\perp}$ เป็นรหัสวัฏจักรซึ่งก่อกำเนิดโดยพหุนาม

$$h_R(x) = h_k + h_{k-1}x + \ldots + h_0x^k$$

พิสูจน์ เราจะแสดงได้ว่า $h_R(x)$ เป็นตัวประกอบของ $x^n - 1$ เนื่องจาก $g(x)h(x) = x^n - 1$ เราได้

$$g(x^{-1})h(x^{-1}) = (x^{-1})^n - 1$$

และ

$$x^{n-k}g(x^{-1})\, x^k h(x^{-1}) = x^n((x^{-1})^n - 1) = 1 - x^n$$

นั่นคือ $h_R(x) = x^k h(x^{-1})$ เป็นตัวประกอบของ $x^n - 1$ ดังนั้น $h_R(x)$ เป็นพหุนามก่อกำเนิดของรหัสวัฏจักร ซึ่งมี H ข้างบนนี้เป็นเมทริกซ์ก่อกำเนิด แสดงว่า $h_R(x)$ เป็นพหุนามก่อกำเนิดของ $C^{\perp}$ ตามต้องการ ■

หมายเหตุ : เนื่องจากสัมประสิทธิ์ของพหุนาม $h_R(x)$ เหมือนกับสัมประสิทธิ์ของพหุนามตรวจสอบภาวะเสมอ h(x) แต่เรียงในลำดับกลับกัน แสดงว่ารหัสที่ก่อกำเนิดโดย h(x) สมมูลกับรหัสที่ก่อกำเนิดโดย $h_R(x)$

ตัวอย่าง 5.5.5 : จาก $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ บนฟีลด์ F_2 จงหาเมทริกซ์ตรวจสอบภาวะเสมอของรหัส $C = <1 + x + x^3>$

วิธีทำ ในที่นี้

$$h(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$$

เป็นพหุนามตรวจสอบภาวะเสมอของรหัส C และพหุนามส่วนกลับของ h(x) คือ

$$h_R(x) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = 1 + x^2 + x^3 + x^4$$

ดังนั้น เมทริกซ์ตรวจสอบภาวะเสมอของ C คือ

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

เราสามารถตรวจสอบโดยการคำนวณโดยตรงได้ว่า H เป็นเมทริกซ์ตรวจสอบภาวะเสมอของ C จริง และ dim(C) = 3 (ดูแบบฝึกหัด 5 ข้อ 17 และ 18)

5.6 การเข้ารหัสวัฏจักร

คุณสมบัติที่สำคัญอย่างหนึ่งของรหัสวัฏจักร ก็คือเข้ารหัสและถอดรหัสได้ง่าย ถ้า C คือรหัสวัฏจักรบนฟีลด์ F ที่มี g(x) เป็นพหุนามก่อกำเนิด สมมุติให้ $\mathbf{m} = m_0m_1 \ldots m_{k-1}$ เป็นสารซึ่งสมนัยกับพหุนาม

$$m(x) = m_0 + m_1x + m_2x^2 + \ldots + m_{k-1}x^{k-1}$$

เราได้เห็นวิธีเข้ารหัสวัฏจักรแล้วสองวิธี วิธีแรกคือวิธีที่ใช้พหุนามก่อกำเนิด g(x) เช่นในตัวอย่าง 5.4.2 เราคูณ g(x) ด้วยสาร m(x) จะได้คำรหัส c(x) = m(x)g(x) ที่อยู่ในรูปพหุนาม ซึ่งสามารถแปลงให้อยู่ในรูปของ n-สิ่งอันดับที่สมนัยกับพหุนามได้ เนื่องจากรหัสวัฏจักรเป็นรหัสเชิงเส้น มีเมทริกซ์ก่อกำเนิด G เป็นตัวกำหนดคำรหัส ดังนั้นการเข้า

รหัสอีกวิธีหนึ่งคือการเข้ารหัสโดยการคูณเมทริกซ์ก่อกำเนิด G ด้วยสาร m จะได้คำรหัส mG

ให้ C = <g(x)> เรารู้ว่า m(x)g(x) เป็นคำรหัส แต่ถ้ากำหนดให้ m(x)g(x) เป็นคำรหัส ไม่ชัดเจนว่าตำแหน่งใดในคำรหัสเป็นสาร และตำแหน่งใดเป็นตัวตรวจสอบาวะเสมอ แต่ถ้าเมทริกซ์ก่อกำเนิดอยู่ในรูปมาตรฐาน $G = [\, I_k \mid A]$ แล้วสาร $m_0 m_1 \ldots m_{k-1}$ จะปรากฏใน k ตำแหน่งแรกของคำรหัสที่เกิดจากการคูณ G ด้วยสาร m ในหัวข้อนี้เราจะแนะนำวิธีเข้ารหัสวัฏจักรอีกวิธีหนึ่ง ซึ่งจะให้คำรหัสที่อยู่ในรูปแบบที่เรียกว่า ***รูปแบบที่เป็นระบบ*** (systematic form) ซึ่งก็คือรูปแบบที่มีสารปรากฏใน k ตำแหน่งสุดท้ายของคำรหัส

ถ้า g(x) เป็นพหุนามก่อกำเนิดของรหัสวัฏจักรที่มีมิติเท่ากับ k ดังนั้น

$$\deg g(x) = n - k$$

เราจะสร้างเมทริกซ์ก่อกำเนิดของ C ที่อยู่ในรูป $G = [R \mid I_k]$ ซึ่งจะเรียกว่าเมทริกซ์ในรูปแบบนี้ว่าเมทริกซ์ที่เป็นระบบ เพราะคำรหัสที่ได้จากการเข้ารหัสสารโดยใช้เมทริกซ์ที่อยู่ในรูป $G = [R \mid I_k]$ นี้ จะเป็นคำรหัสที่มีสารปรากฏใน k ตำแหน่งสุดท้ายของคำรหัส เมทริกซ์ในรูปแบบ $G = [R \mid I_k]$ นี้ไม่ใช่เมทริกซ์มาตรฐาน แต่เป็นเมทริกซ์ที่อยู่ในรูปแบบที่เกือบจะเป็นเมทริกซ์มาตรฐาน ต่างกันที่มี I_k อยู่ข้างหลัง

เราหารพหุนาม x^{n-k+i} สำหรับ i = 0, 1, ..., k − 1 ด้วย g(x) จะได้

$$x^{n-k+i} = g(x)q_i(x) + r_i(x)$$

เมื่อ $r_i(x) = 0$ หรือ $\deg r_i(x) < \deg g(x) = n - k$ ดังนั้น

$$x^{n-k+i} - r_i(x) = g(x)q_i(x) \in C$$

จะเห็นว่า $x^{n-k+i} - r_i(x)$ เป็นคำรหัสใน C ที่มีสัมประสิทธิ์ของ $-r_i(x)$ อยู่ใน k ตำแหน่งแรก เพราะ $\deg r_i(x) < \deg g(x) = n - k$ และมี 1 อยู่ในตำแหน่งที่ i ส่วนตำแหน่งอื่น ๆ เป็น 0 ดังนั้น ถ้าให้ r_i เป็นเวกเตอร์ใน F_q^{n-k} ที่สมนัยกับพหุนาม $r_i(x)$ เป็นแถวที่ i ของเมทริกซ์ R เราได้

$$G = [R \mid I_k] = \begin{bmatrix} -r_0 & \\ -r_1 & \\ \vdots & I_k \\ -r_{k-2} & \\ -r_{k-1} & \end{bmatrix}$$

เป็นเมทริกซ์ก่อกำเนิดของรหัส C เมื่อ

$$R = \begin{bmatrix} -r_0 \\ -r_1 \\ \vdots \\ -r_{k-2} \\ -r_{k-1} \end{bmatrix} = \begin{bmatrix} -r_0(x) \\ -r_1(x) \\ \vdots \\ -r_{k-2}(x) \\ -r_{k-1}(x) \end{bmatrix}$$

เพราะว่าแต่ละแถวของเมทริกซ์ G เป็นคำรหัส จะเห็นว่าแต่ละแถวประกอบกันเป็นเซตอิสระเชิงเส้น และจำนวนแถวของเมทริกซ์ G เท่ากับ dim(C) = k ดังนั้น k แถวของ G เป็นฐานหลักของรหัส C ซึ่งยืนยันว่า $G = [R \mid I_k]$ เป็นเมทริกซ์ก่อกำเนิดของ C จริง นอกจากนี้ เราสามารถตรวจสอบได้ไม่ยากนักว่า $H = [I_{n-k} \mid -R^T]$ เป็นเมทริกซ์ตรวจสอบภาวะเสมอของ C ทั้งนี้เพราะว่า $GH^T = 0$

ตัวอย่าง 5.6.1 : พิจารณารหัสวัฏจักร-[7, 4] บนฟิลด์ F_2 ซึ่งก่อกำเนิดโดยพหุนาม

$$g(x) = 1 + x + x^3$$

ในที่นี้ $n - k = 3$ หาร x^{3+i} ด้วย g(x) สำหรับ i = 0, 1, 2, 3 จะได้

$x^3 = (1)(1 + x + x^3) + (1 + x)$

$x^4 = (x)(1 + x + x^3) + (x + x^2)$

$x^5 = (1 + x^2)(1 + x + x^3) + (1 + x + x^2)$

$x^6 = (1 + x + x^3)(1 + x + x^3) + (1 + x^2)$

สรุปผลลัพธ์ดังในตาราง 5.6.1 ข้างล่างนี้

ตาราง 5.6.1 ฐานหลักของรหัส C $= \langle 1 + x + x^3 \rangle$

n	x^{3+i}	$r_i(x)$	$c_i(x) = x^{3+i} - r_i(x)$	c_i
0	x^3	$1 + x$	$1 + x + x^3$	1101000
1	x^4	$x + x^2$	$x + x^2 + x^4$	0110100
2	x^5	$1 + x + x^2$	$1 + x + x^2 + x^5$	1110010
3	x^6	$1 + x^2$	$1 + x^2 + x^6$	1010001

เนื่องจาก $x^3 = (1)(1 + x + x^3) + (1 + x)$ แสดงว่า $r_0(x) = 1 + x$ ดังนั้น

$$c_0(x) = x^3 - (1 + x) = 1 + x + x^3$$

ซึ่งสมนัยกับคำรหัส c_0 = 1101000 ในแถวแรกของตาราง 5.6.1 เราหา c_1, c_2, c_3 ได้ในทำนองเดียวกัน ใช้คำรหัส c_i เป็นแถวที่ i ของเมทริกซ์ G เราได้เมทริกซ์ก่อกำเนิด G ที่อยู่ในรูป $G = [R \mid I_4]$

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

และเมทริกซ์ตรวจสอบภาวะเสมอ H ในรูปแบบที่เป็นระบบที่สมนัยกัน คือ

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

จากการคูณเมทริกซ์โดยตรง จะพบว่า $GH^T = 0$ นั่นคือ H เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัส C ที่ก่อกำเนิดโดย $g(x) = 1 + x + x^3$

เราสามารถหาคำรหัสที่สมนัยกับสาร $m(x)$ โดยใช้การดำเนินการกับพหุนามได้ดังนี้ หารพหุนาม $x^{n-k}m(x)$ ด้วย $g(x)$ จะได้

$$x^{n-k}m(x) = g(x)q(x) + r(x)$$

เมื่อ $r(x) = 0$ หรือ $\deg r(x) < \deg g(x) = n - k$ ดังนั้น

$$x^{n-k}m(x) - r(x) = g(x)q(x)$$

เป็นคำรหัสใน C เพราะว่า $x^{n-k}m(x) - r(x)$ เป็นพหุคูณของ $g(x)$

ตัวอย่าง 5.6.2 : พิจารณารหัส C บนฟีลด์ F_2 ที่มีความยาว 7 ซึ่งก่อกำเนิดโดยพหุนาม $g(x) = 1 + x + x^3$ ถ้าเราให้ **m** = 1001 เป็นสารซึ่งสมนัยกับพหุนาม $m(x) = 1 + x^3$ แล้ว $x^3m(x) = x^3 + x^6$ หาร $x^3m(x)$ ด้วย $g(x)$ เราได้

$$\begin{array}{rl} & x^3 + x \qquad = q(x) \\ x^3 + x + 1 \,\big) & \overline{x^6 + x^3} \\ & \underline{x^6 + x^4 + x^3} \\ & x^4 \\ & \underline{x^4 + x^2 + x} \\ & x^2 + x \quad = r(x) \end{array}$$

เศษที่เหลือจากการหารคือ $r(x) = x^2 + x$ เราได้

$$x^3m(x) = x^3 + x^6 = (1 + x + x^3)(x + x^3) + x^2 + x$$

ดังนั้น

$$x^{n-k}m(x) - r(x) = x^3m(x) - (x^2 + x) = x^6 + x^3 + x^2 + x$$

เป็นคำรหัสใน C ซึ่งสมนัยกับเวกเตอร์ 0111001 จะเห็นว่าส่วนที่เป็นสารปรากฏใน k = 4 ตำแหน่งสุดท้าย และ

$$\deg r(x) < n - k = 7 - 4 = 3$$

ส่วน $\deg(x^{n-k} m(x))$ เริ่มจาก n – k = 3 และเพิ่มขึ้นถึง n – 1 = 6 ดังนั้นพหุนาม $x^{n-k} m(x)$ และ $r(x)$ จึงไม่มีพจน์ร่วมกันเลย

5.7 ซินโดรมและการถอดรหัสวัฏจักร

หลังจากที่เราได้เมทริกซ์ก่อกำเนิด ที่อยู่ในรูปเกือบจะมาตรฐานแล้ว เราสามารถคำนวณหาเมทริกซ์ตรวจสอบภาวะเสมอได้ จากเมทริกซ์ก่อกำเนิด และเมทริกซ์ตรวจสอบภาวะเสมอที่อยู่ในรูปพิเศษนี้ เราจะหาซินโดรม หาพหุนามที่สมนัยกับซินโดรมและแสดงวิธีถอดรหัส

สมมุติให้ C เป็นรหัสวัฏจักรบนฟิลด์ F_q ที่ก่อกำเนิดโดยพหุนาม $g(x)$ ซึ่งมีดีกรี n – k ในหัวข้อที่แล้ว เราสามารถหาเมทริกซ์ก่อกำเนิดที่อยู่ในรูป $G = [R \mid I_k]$ เมื่อ R คือเมทริกซ์ขนาด $k \times (n-k)$ ซึ่งมี

$$-r_0(x), -r_1(x), \ldots, -r_{k-1}(x)$$

เป็นแต่ละแถวของ R และ I_k คือเมทริกซ์เอกลักษณ์ขนาด $k \times k$ ส่วนเมทริกซ์ตรวจสอบภาวะเสมอคือ $H = [I_{n-k} \mid -R^T]$

ถ้า **w** ซึ่งเป็น n-สิ่งอันดับใด ๆ ใน F_q^n เรารู้แล้วว่าซินโดรมของ **w** คือ **s** = **w**H^T ในทฤษฎีบทข้างล่างนี้ ชี้ให้เห็นประโยชน์ที่เลือกพหุนามก่อกำเนิดและพหุนามตรวจสอบภาวะเสมอในรูปแบบพิเศษนี้ ซึ่งมี

ทฤษฎีบท 5.7.1 ถ้า $w(x)$ เป็นพหุนามดีกรีไม่เกิน n – 1 ที่สมนัยกับเวกเตอร์ **w** ที่ได้รับ และ $s(x)$ เป็นพหุนามที่สมนัยกับซินโดรม **s** ของ **w** แล้ว $s(x)$ จะเป็นพหุนามที่เป็นเศษที่เหลือจากการหาร $w(x)$ ด้วย $g(x)$ กล่าวคือ $s(x) \equiv w(x) \pmod{g(x)}$

พิสูจน์ สมมุติให้

$$w(x) = w_0 + w_1x + \dots + w_{n-1}x^{n-1}$$

จะเห็นว่าหลักที่ i สำหรับ $0 \le i \le n-k-1$ ของ H สมนัยกับพหุนาม x^i และหลักที่ i สำหรับ $n-k \le i \le n-1$ สมนัยกับพหุนาม $r_{i-n+k}(x)$ เนื่องจาก

$$\mathbf{s} = \mathbf{w}H^T = w_0\mathbf{h}_0 + w_1\mathbf{h}_1 + \dots + w_{n-1}\mathbf{h}_{n-1}$$

เมื่อ $\mathbf{h}_i$ คือหลักที่ i ของ H แทนแต่ละหลักของ H ด้วยพหุนามที่สมนัยกัน เราได้

$$\begin{aligned}
s(x) &= w_0 1 + w_1x + w_2x^2 + \dots + w_{n-k-1}x^{n-k-1} \\
&\quad + w_{n-k}r_0(x) + w_{n-k+1}r_1(x) + \dots + w_{n-1}r_{k-1}(x) \\
&= w_0 + w_1x + \dots + w_{n-k-1}x^{n-k-1} \\
&\quad + w_{n-k}(x^{n-k} - q_0(x)g(x)) + \dots + w_{n-1}(x^{n-1} - q_{k-1}(x)g(x)) \\
&= w(x) - [w_{n-k}q_0(x)\,g(x) + \dots + w_{n-1}q_{k-1}(x)g(x)] \\
&= w(x) - g(x)[w_{n-k}q_0(x) + \dots + w_{n-1}q_{k-1}(x)] \\
&= w(x) - g(x)Q(x)
\end{aligned}$$

เมื่อ $Q(x) = w_{n-k}q_0(x) + \dots + w_{n-1}q_{k-1}(x)$ ดังนั้น

$$w(x) = g(x)Q(x) + s(x)$$

แต่เนื่องจาก $\deg r_i(x) < n-k$ จะได้ $\deg s(x) < n-k$ จากขั้นตอนวิธีการหาร แสดงว่า $s(x)$ เป็นเศษที่เหลือจากการหาร $w(x)$ ด้วย $g(x)$ ตามต้องการ ∎

ตัวอย่าง 5.7.1 : ให้ $g(x) = 1 + x + x^3$ เป็นพหุนามก่อกำเนิดของรหัสวัฏจักร-[7, 4] บนฟีลด์ F_2 จากตัวอย่าง 5.6.1 เราได้

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

และ

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

สมมุติว่า **w** = 1011011 เป็นเวกเตอร์ที่ได้รับ ซึ่งสมนัยกับพหุนาม

$$w(x) = 1 + x^2 + x^3 + x^5 + x^6$$

ถ้าเราหารพหุนาม $w(x)$ ด้วย $g(x) = 1 + x + x^3$ จะได้

$$w(x) = (x^3 + x^2 + x + 1)g(x) + x^2$$

เศษที่เหลือจากการหารคือ $s(x) = x^2$ ซึ่งสมนัยกับซินโดรม **s** = 001 ดังนั้น เราถอดรหัสให้เป็นคำรหัส

$$w(x) - s(x) = 1 + x^2 + x^3 + x^5 + x^6 - x^2 = 1 + x^3 + x^5 + x^6$$

ซึ่งสมนัยกับเวกเตอร์ 1001011

ถ้าเราคำนวณหาซินโดรมของ **w** ตามวิธีที่เราใช้ในบทที่ 3 นั่นคือ คูณเวกเตอร์ที่ได้รับด้วยเมทริกซ์สลับเปลี่ยนของ H เราได้

$$\mathbf{s} = \mathbf{w}H^T = 001$$

จะเห็นว่า $\mathbf{s}^T$ ตรงกับหลักที่สามของเมทริกซ์ H แสดงว่าเวกเตอร์ **w** ที่ได้รับมีข้อผิดพลาดในตำแหน่งที่ 3 ซึ่งตรงกับวิธีที่ใช้พหุนามข้างบนนี้

นอกจากนี้ จะเห็นว่าซินโดรมของ **w** และซินโดรมของ $\mathbf{w}^1$ ซึ่งเป็นเวกเตอร์เลื่อนวนของ **w** มีความสัมพันธ์กัน ดังในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 5.7.2

ถ้า C เป็นรหัสวัฏจักรก่อกำเนิดโดย $g(x)$ ที่มีดีกรี $n-k$ มีเมทริกซ์ก่อกำเนิด G และเมทริกซ์ตรวจสอบภาวะเสมอ H อยู่ในรูปที่เป็นระบบ ถ้าซินโดรม $s(w) = s$ แล้วซินโดรมของเวกเตอร์เลื่อนวน $S(w^1)$ ในรูปของพหุนามจะเท่า $xs(x) - s_{n-k-1}g(x)$

พิสูจน์ จากทฤษฎีบท 5.7.1 เรามี

$$w(x) = q(x)g(x) + s(x)$$

เมื่อ $\deg s(x) < n-k$ นั่นคือ $s(x)$ เป็นซินโดรมของ $w(x)$ เมื่อคูณด้วย x ทั้งสองข้าง เราได้

$$\begin{aligned} xw(x) &= xq(x)g(x) + xs(x) \\ &= xq(x)g(x) + Q(x)g(x) + t(x) \end{aligned}$$

เมื่อ $Q(x)$ และ $t(x)$ เป็นผลหารและเศษที่ได้จากการหาร $xs(x)$ ด้วย $g(x)$

เนื่องจาก $\deg s(x) \leq n-k-1$ และ $g(x)$ เป็นพหุนามโมนิกที่มีดีกรี $n-k$ ดังนั้น ถ้า $\deg s(x) < n-k-1$ เราได้ $\deg xs(x) < n-k$ แสดงว่า $Q(x) = 0$ และ $t(x) = xs(x)$ แต่ถ้า $\deg s(x) = n-k-1$ แล้ว $Q(x)$ จะเท่ากับค่าคงตัว s_{n-k-1} และ $t(x) = xs(x) - s_{n-k-1}g(x)$ นั่นคือ $t(x)$ เป็นพหุนามซึ่งสมนัยกับซินโดรม $xw(x)$ ∎

ต่อไป เราจะแสดงวิธีถอดรหัสโดยใช้ซินโดรมในรูปของพหุนาม สมมุติว่า C เป็นรหัสเชิงเส้น-[n, k] (ไม่จำเป็นต้องเป็นรหัสวัฏจักร) ซึ่งมี $d(C) = 2t + 1$ แสดงว่ารหัส C สามารถแก้ไขข้อผิดพลาดได้ถึง t ตำแหน่ง และสมมุติว่า $H = [I_{n-k} \mid A]$ เป็นเมทริกซ์ตรวจสอบภาวะเสมอของ C ให้ **e** เป็นรูปแบบของข้อผิดพลาดซึ่ง $wt(e) \leq t$ และมีซินโดรม $\mathbf{s} = S(e)$ ซึ่ง $wt(s) \leq t$ เช่นกัน เราให้ s' เป็นเวกเตอร์ที่ยาว

n โดยมี $s_0 s_1 \ldots s_{n-k-1}$ เป็น n – k ตำแหน่งแรกของ s^* และมี 0 ในตำแหน่งที่เหลือ ในกรณีนี้ เราเขียน $s^* = s \mid 0$ ดังนั้น

$$eH^T = s = s^*H^T$$

นั่นคือ e และ s^* มีซินโดรมเหมือนกัน ซึ่งแสดงว่า e และ s^* อยู่ในแถว (โคเซต) เดียวกันของแถวลำดับมาตรฐานที่ศึกษาแล้วในหัวข้อ 3.6 และเนื่องจาก

$$wt(e) = wt(s^*) \leq t$$

ทั้ง e และ s^* เป็นโคเซตนำของแถวนั้น นั่นคือ $e = s^*$ ทั้งหมดนี้ชี้ให้เห็นว่า เราสามารถหาเวกเตอร์ข้อผิดพลาดได้ทันทีจากซินโดรม s ของ w โดยไม่ต้องเสียเวลาในการค้นหาโคเซตนำในแถวลำดับมาตรฐาน ซึ่งจะช่วยประหยัดเวลาได้มาก ปัญหาคือ ในกรณีทั่วไป อาจเป็นไปได้ว่า $wt(s) > t$

อย่างไรก็ตาม ถ้าเราเน้นเฉพาะรหัสวัฏจักรแล้ว เราสามารถพัฒนาความรู้ข้างบนนี้ ไปสู่การสร้างเทคนิคการถอดรหัสที่เรียกว่า error – trapping ดังรายละเอียดที่อธิบายต่อไปนี้

ให้ C เป็นรหัสวัฏจักร – [n, k] ซึ่ง d(C) = 2t + 1 และมีเมทริกซ์ตรวจสอบภาวะเสมออยู่ในรูป $H = [\, I_{n-k} \mid A]$ สมมุติให้ e เป็นรูปแบบของข้อผิดพลาดซึ่ง $wt(e) \leq t$ และสมมุติว่ามี 0 ใน e ในตำแหน่งที่ติดกันหรือในตำแหน่งที่วนติดกันอย่างน้อย k ตัว (ตัวอย่างเช่น 11<u>0000</u>1010 มี 0 ในตำแหน่งที่ติดกัน 4 ตำแหน่ง หรือ <u>00</u>101101<u>00</u> มี 0 ในตำแหน่งที่วนติดกันอย่างน้อย 4 ตำแหน่ง เรากล่าวว่า ทั้งสองเวกเตอร์นี้มี cyclic run เท่ากับ 4) สมมุติว่า c เป็นคำรหัสที่ส่ง และ w เป็นเวกเตอร์ที่ได้รับ จะมีจำนวนเต็มบวก i ที่ทำให้ e^i มี 0 อยู่ใน k ตำแหน่งสุดท้าย และ $wt(e^i) \leq t$ ดังนั้น $e^i = f \mid 0$ เมื่อ 0 แทนเวกเตอร์ศูนย์ที่ยาว k และ $S(e^i) = f$, $wt(f) \leq t$ ดังนั้น เราได้ขั้นตอนการถอดรหัสดังนี้

เมื่อได้รับเวกเตอร์ **w** เราคำนวณหาซินโดรม S(**w**) แต่เนื่องจาก S(**w**) = S(**e**) นั่นคือเรารู้ S(**e**) ต่อไปเราใช้ทฤษฎีบท 5.7.2 ในการคำนวณหา i ที่เล็กที่สุดที่ทำให้ $S(\mathbf{e}^i)$ มีน้ำหนักน้อยกว่าหรือเท่ากับ t ดังนั้น เราจะได้ $\mathbf{e}^i = S(\mathbf{e}^i) \mid \mathbf{0}$ ซึ่งเมื่อเราเลื่อนวน $\mathbf{e}^i$ ถอยหลังกลับไป i ตำแหน่ง เราได้เวกเตอร์ **e** ซึ่งเป็นรูปแบบของข้อผิดพลาด นำ **e** ไปหักออกจาก **w** เราจะได้คำรหัส นั่นคือ เราสามารถแก้ไขข้อผิดพลาดได้

ตัวอย่าง 5.7.2 : ให้ C เป็นรหัสวัฏจักร – [7, 4] บนฟิลด์ F_2 ซึ่งก่อกำเนิดโดยพหุนาม $g(x) = 1 + x + x^3$ จากแบบฝึกหัด 5 ข้อ 18 เรามี d(C) = 3 ดังนั้น C เป็นรหัสที่สามารถแก้ไขข้อผิดพลาดได้ถึง t = 1 ตำแหน่ง สมมุติว่า **w** = 1011101 เป็นเวกเตอร์ที่ได้รับ ซึ่งสมนัยกับพหุนาม

$$w(x) = 1 + x^2 + x^3 + x^4 + x^6$$

คำนวณหาซินโดรมของ **w** โดยใช้ทฤษฎีบท 5.7.1 นั่นคือหาร w(x) ด้วย g(x) เราได้เศษ

$$s(x) = 1 + x^2$$

เป็นซินโดรมของ **w** ซึ่งเท่ากับ S(**e**) นั่นคือ

$$S(\mathbf{e}) = \mathbf{s} = s_0s_1s_2 = 101$$

ขณะนี้เรารู้ S(**e**) = **s** แต่ยังไม่รู้ **e** จุดประสงค์ของเราคือ หารูปแบบข้อผิดพลาด **e** ซึ่งสามารถหาได้โดยใช้ S(**e**) ที่มีอยู่และทฤษฎีบท 5.7.2 หา $S(\mathbf{e}^i)$ ดังนี้ ให้ $S(\mathbf{e}^i) = \mathbf{s}^1$ เราได้

$$s(x) = 1 + x^2$$

$$s^1(x) = x + x^3 + s_2g(x) = x + x^3 + 1g(x) = 1$$

ดังนั้น $\mathbf{s}^1 = 100$ จะเห็นว่า $wt(S(\mathbf{e}^1)) = wt(\mathbf{s}^1) = 1 = t$ ดังนั้น

$$\mathbf{e}^1 = \mathbf{f} \mid \mathbf{0} = \mathbf{s}^1 \mid \mathbf{0} = 1000000$$

เลื่อนวนเวกเตอร์ $\mathbf{e}^1$ ถอยไปทางซ้าย 1 ตำแหน่ง เราได้ **e** = 0000001 ดังนั้น เราถอดรหัส **w** ให้เป็นคำรหัส

$$c = w - e = 1011101 - 0000001 = 1011100$$

แสดงว่า $c(x) = 1 + x^2 + x^3 + x^4$ ถ้าเราหาร $c(x)$ ด้วย $g(x)$ จะเห็นว่าเศาเป็น 0 นั่นคือ $c(x)$ เป็นคำรหัสจริง

ตัวอย่าง 5.7.3 : ให้ C เป็นรหัสวัฏจักร – [15, 7] บนฟีลด์ F_2 ซึ่งก่อกำเนิดโดยพหุนาม $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ เราสามารถตรวจสอบได้ว่า $d(C) = 5$ ดังนั้น C เป็นรหัสที่สามารถแก้ไขข้อผิดพลาดได้ถึง $t = 2$ ตำแหน่ง สมมุติว่า **w** = 111101010010010 เป็นเวกเตอร์ที่ได้รับ ซึ่งสมนัยกับพหุนาม

$$w(x) = 1 + x + x^2 + x^3 + x^5 + x^7 + x^{10} + x^{13}$$

คำนวณหาซินโดรมของ **w** โดยใช้ทฤษฎีบท 5.7.1 นั่นคือหาร $w(x)$ ด้วย $g(x)$ เราได้เศษ

$$s(x) = 1 + x^2 + x^3 + x^4 + x^5$$

เป็นซินโดรมของ **w** ซึ่งเท่ากับ $S(\mathbf{e})$ นั่นคือ

$$S(\mathbf{e}) = \mathbf{s} = 1011110$$

ขณะนี้เรารู้ $S(\mathbf{e})$ แต่ยังไม่รู้ **e** จุดประสงค์ของเราคือ หารูปแบบข้อผิดพลาด **e** ซึ่งสามารถหาได้โดยใช้ $S(\mathbf{e})$ ที่มีอยู่และทฤษฎีบท 5.7.2 หา $S(\mathbf{e}^i)$ ดังนี้ ให้ $S(\mathbf{e}^i) = \mathbf{s}^i$ เราได้

$$s(x) = 1 + x^2 + x^3 + x^4 + x^5$$
$$s^1(x) = x + x^3 + x^4 + x^5 + x^6$$
$$s^2(x) = x^2 + x^4 + x^5 + x^6 + x^7$$
$$s^3(x) = x^3 + x^5 + x^6 + x^7 + x^8 + g(x) = 1 + x^3 + x^4 + x^5$$
$$s^4(x) = x + x^4 + x^5 + x^6$$
$$s^5(x) = x^2 + x^5 + x^6 + x^7$$
$$s^6(x) = x^3 + x^6 + x^7 + x^8 + g(x) = 1 + x^3 + x^4$$
$$s^7(x) = x + x^4 + x^5$$
$$s^8(x) = x^2 + x^5 + x^6$$

$s^9(x) = x^3 + x^6 + x^7$

$s^{10}(x) = x^4 + x^7 + x^8 + g(x) = 1 + x^6 = 10000010$

จะเห็นว่า $wt(S(e^{10}) = wt(s^{10}) = 2 = t$ ดังนั้น

$$e^{10} = f \mid 0 = S(e^{10}) \mid 0 = 100000100000000$$

เนื่องจาก $e^{15} = e$ แสดงว่าถ้าเราเลื่อนวน e^{10} ไปทางขวา 5 ตำแหน่ง (เท่ากับเลื่อนวน e^{10} ถอยหลังไปทางซ้าย 10 ตำแหน่ง) จะได้เวกเตอร์ข้อผิดพลาด e = 000001000001000 แสดงว่าคำรหัสที่ส่งคือ

$$c = w - e = 111100010011010$$

เราสามารถตรวจสอบว่า c เป็นคำรหัสจริง โดยการหารพหุนาม c(x) ด้วย g(x) แล้วดูว่าเศษเป็น 0 จริงหรือไม่

หมายเหตุ : เราจะใช้การถอดรหัสด้วยวิธี error – trapping ได้เวกเตอร์ข้อผิดพลาด e จะต้องมี cyclic run อย่างน้อย k ในตัวอย่าง 5.7.3 เรามี n = 15, k = 7 ดังนั้นเวกเตอร์ข้อผิดพลาด e ทั้งหลายที่มี $wt(e) \leq 2$ จะสอดคล้องกับเงื่อนไขที่ต้องการ

แบบฝึกหัด 5

1. จงพิจารณาว่ารหัสในแต่ละข้อต่อไปนี้ เป็นรหัสวัฏจักรหรือไม่
   - 1.1 รหัสไบนารี { 000, 100, 011, 111}
   - 1.2 รหัสเทอร์นารี {0000, 1122, 2211}
   - 1.3 รหัสเทอร์นารี {0112, 2011, 1201, 1120}
   - 1.4 รหัสแบบซ้ำฐาน q ที่มีความยาว n
   - 1.5 รหัสไบนารีที่มีความยาว n ซึ่งคำรหัสทุกคำมีน้ำหนักเป็นจำนวนคู่

1.6 รหัสเทอร์นารีที่มีความยาว n ซึ่งคำรหัสทุกคำมีน้ำหนักเป็นจำนวนซึ่ง $\equiv 0 \pmod 3$

2 พหุนาม f(x) และ g(x) ใน $F_q[x]$ ที่กำหนดให้ในแต่ละข้อต่อไปนี้ จงหาผลหาร q(x) และเศษ r(x) ซึ่งทำให้ $f(x) = q(x)g(x) + r(x)$ เมื่อ $r(x) = 0$ หรือ $\deg r(x) < \deg g(x)$ พร้อมทั้งพิจารณาว่า $g(x) \mid f(x)$ หรือไม่ ถ้า $g(x) \mid f(x)$ จงเขียน f(x) ในรูปพหุคูณของ g(x)

2.1 $f(x) = x + x^4 + x^5$, $g(x) = 1 + x + x^3$ ใน $F_2[x]$

2.2 $f(x) = x + x^7$, $g(x) = 1 + x + x^3 + x^4 + x^5$ ใน $F_2[x]$

2.3 $f(x) = 3 + 4x + x^4 + 2x^5$, $g(x) = 1 + 3x^2$ ใน $F_5[x]$

3. จงพิสูจน์ทฤษฎีบท 5.2.2

4. จงหาผลคูณ $(1 + x + 2x^3)(2 + 2x + x^2 + x^4)$ ใน $F_3[x]$

5. จงหาผลคูณ $(1 + x + 2x^3)(2 + 2x + x^2 + x^4)$ ใน $F_3[x]/(1+2x^2+ x^3)$

6. จงพิสูจน์ทฤษฎีบท 5.3.1

7. จงสร้างตารางการบวกและตารางการคูณของริง $F_3[x]/(x^2 + 1)$

8. จงแสดงว่า $\langle 1 + x\rangle = \langle x + x^2\rangle$ ใน $F_2[x] / (x^3 - 1)$

9. พหุนามต่อไปนี้ เป็นพหุนามลดทอนได้ในฟิลด์ที่กำหนดให้หรือไม่ ถ้าลดทอนได้ จงแยกตัวประกอบของพหุนามนั้นออกเป็นผลคูณของพหุนามลดทอนไม่ได้ ถ้าลดทอนไม่ได้ จงให้เหตุผล

9.1 $1 + x^5$ ใน $F_2[x]$

9.2 $1 + x + x^3$ ใน $F_2[x]$

9.3 $1 + x + x^2 + x^3 + x^4$ ใน $F_2[x]$

9.4 $1 + x^2 + x^3 + x^4$ ใน $F_3[x]$

10. จงหาพหุนามที่ลดทอนไม่ได้ทั้งหมดใน $F_2[x]$ ที่มีดีกรี 3

11. จงหาพหุนามที่ลดทอนไม่ได้ทั้งหมดใน $F_3[x]$ ที่มีดีกรี 3

12. ให้ C = {0000, 1011, 0101, 1110} เป็นรหัสวัฏจักรบนฟีลด์ F_2 จงเขียน C ในรูปเซตของพหุนาม

13. จากข้อ 12 จงหาพหุนามก่อกำเนิด g(x) ของรหัส C และเขียนสมาชิกอื่น ๆ ใน C ในรูปพหุคูณของ g(x)

14. กำหนดให้ $x^7 - 1 = (1 + x)(1 + x + x^3)(1+ x^2 + x^3)$ จงหารหัสวัฏจักรบนฟีลด์ F_2 ทั้งหลายที่มีความยาว 7

15. จงหาเมทริกซ์ตรวจสอบภาวะเสมอของรหัสทั้งหลายในข้อ 15

16. จงหาพหุนามก่อกำเนิดของรหัสวัฏจักรบนฟีลด์ F_2 ทั้งหลายที่มีความยาว 21 และมีมิติเท่ากับ 9

17. จงตรวจสอบว่าเมทริกซ์ H ในตัวอย่าง 5.5.5 เป็นเมทริกซ์ตรวจสอบภาวะเสมอของรหัส $C = <1 + x + x^3>$

18. จงแสดงว่า dim(C) = 3 เมื่อรหัส $C = <1 + x + x^3>$ ในตัวอย่าง 5.5.5

19. ให้ C เป็นรหัสวัฏจักรบนฟีลด์ F_2 ที่มีความยาว 8 และมีมิติ 4 จงหาเมทริกซ์ก่อกำเนิดและเมทริกซ์ตรวจสอบภาวะเสมอของ C และ $C^\perp$

20. ให้ $C = <g(x)>$ เป็นรหัสวัฏจักรใน R_n ถ้า g(x) เป็นพหุนามใน C ที่หาร $x^n - 1$ ได้ลงตัว จงแสดงว่า g(x) เป็นพหุนามที่มีดีกรีต่ำที่สุดใน C

21. พิจารณาริง $R_7 = F_2/(x^7 - 1)$ และตอบคำถามต่อไปนี้

    21.1 จงหาขนาดของ R_7

    21.2 จงหาจำนวนรหัสวัฏจักรที่มีความยาว 7 ทั้งหมด

    21.3 ให้ $C =<g(x)>$ เมื่อ $g(x) = 1 + x + x^3$ เป็นตัวประกอบของ $x^7 - 1$ จงหา dim(C)

21.4 ถ้า $h(x)$ เป็นพหุนามตรวจสอบาวะเสมอของ C จงหาดีกรีของ $h(x)$

21.5 ให้ C' เป็นรหัสที่ก่อกำเนิดโดย $h(x)$ จงหา $\dim(C)$

21.6 จงหาคำรหัส $xg(x)$ ในรูปของพหุนามและในรูปของ 7–สิ่งอันดับที่สมนัยกัน

21.7 จงแสดงว่าผลคูณของ $c(x) = xg(x)$ และ $h(x)$ เป็น 0 ใน R_7

21.8 จงแสดงว่า $\mathbf{c.h \neq 0}$ ดังนั้น $C' \neq C^{\perp}$

22. ให้ C เป็นรหัสวัฏจักรที่มีความยาว 7 บนฟีลด์ F_2 ที่ก่อกำเนิดโดย $g(x) = 1 + x^2 + x^3$ จงหาเมทริกซ์ก่อกำเนิดของรหัส C ที่อยู่ในรูป $G = [\, R \mid I \,]$ พร้อมทั้งหาเมทริกซ์ตรวจสอบภาวะเสมอของ C ที่สมนัยกัน

23. พิจารณารหัสในข้อ 22 ถ้า $\mathbf{w}$ = 1101111 เป็นคำที่ได้รับ จงถอดรหัส $\mathbf{w}$

24. ให้ C เป็นรหัสวัฏจักรในตัวอย่าง 5.7.3 จงแสดงวิธีถอดรหัสของเวกเตอร์ต่อไปนี้

24.1 $\mathbf{w}$ = 010011000111010

24.2 $\mathbf{w}$ = 111110000000000

25. บนฟีลด์ F_3 จงแสดงว่า $g(x) = x^5 + x^4 + 2x^3 + x^2 + 2$ หาร $x^{11}-1$ ได้ลงตัว

26. จากข้อ 25 ถ้าให้ C เป็นรหัสวัฏจักร – [11, 6] บนฟีลด์ F_3 ซึ่งก่อกำเนิดโดย $g(x)$ และกำหนดให้ $d(C) = 5$ จงใช้วิธี error – trapping ถอดรหัสคำ 20121020112 ที่ได้รับ

27. จงพิสูจน์ทฤษฎีบท 5.3.2