9 บล็อกดีไซน์และรหัสแก้ไขข้อผิดพลาด
Block Designs and Error-Correcting Codes

การศึกษาในเรื่องบล็อกดีไซน์นั้นมีกำเนิดมาจากการศึกษาปัญหาเกี่ยวกับการออกแบบการทดลองในเชิงสถิติ (statistical experiment) ในบทนี้เราจะพิจารณาถึงปัญหาหรือคำถามเชิงคอมบินาทอริคที่เกิดขึ้นจากความพยายามที่จะออกแบบการทดลองดังกล่าว รวมทั้งการวิเคราะห์เชิงคอมบินาทอริคในทฤษฎีบทต่าง ๆ ที่เกี่ยวข้องกับการออกแบบการทดลอง บล็อกดีไซน์แบ่งออกเป็น 2 แบบใหญ่ ๆ คือบล็อกดีไซน์แบบสมบูรณ์ (complete block design) และบล็อกดีไซน์แบบไม่สมบูรณ์ (incomplete block design) เราจะศึกษาดีไซน์ทั้งสองแบบ และในตอนสุดท้ายของบทนี้จะนำผลจากการศึกษาเรื่องบล็อกดีไซน์ไปใช้ในการออกแบบรหัสแก้ไขข้อผิดพลาด (error correcting code)

9.1 แบบการทดลอง

Experimental Designs

จะเริ่มต้นด้วยการศึกษาปัญหาการออกแบบการทดลองเพื่อเปรียบเทียบคุณภาพยางรถยนต์ 4 ยี่ห้อ เป็นที่แจ้งชัดว่ายางรถยนต์แต่ละเส้นนั้น ถึงแม้จะเป็นยี่ห้อเดียวกันก็ยังมีความแตกต่างกันอยู่ ดังนั้นเราจึงต้องใช้ยางแต่ละยี่ห้อมากกว่าหนึ่งเส้นในการทดลองเพื่อเปรียบเทียบคุณภาพของยาง สมมุติว่าเราทำการทดสอบโดยนำยางมาทดสอบใช้กับรถยนต์ประเภทรถนั่งส่วนบุคคล (คือมี 4 ล้อ) ในสภาพการขับจริงบนท้องถนน นั่นคือเราจะต้องจัดแบ่งยางเป็นกลุ่ม ๆ ละ 4 เส้น สำหรับใช้ในการทดสอบแต่ละครั้ง โดยธรรมชาติแล้ว เรามักต้องการให้ยางแต่ละยี่ห้อได้รับการนำไปทดลองหรือทดสอบเป็นจำนวนครั้งเท่า ๆ กัน เช่นสมมุติว่าต้องการให้ยางแต่ละยี่ห้อได้รับการนำไปทดสอบ r ครั้งเท่า ๆ กัน ดังนั้นจำนวนยางที่จะต้องใช้ในการทดลองทั้งหมดจะเท่ากับ 4r เพราะว่ามี 4 ยี่ห้อ ทดสอบยี่ห้อละ r ครั้ง ข้อสังเกตในตอนนี้คือจำนวนยางที่จะต้องใช้ในการทดสอบทั้งหมดจะต้องหารด้วย 4 ลงตัว ทั้งนี้เนื่องจากการทดลองแต่ละครั้งจะต้องใช้ยาง 4 เส้น ในกรณีนี้ r จะเป็นจำนวนเต็มบวกใด ๆ ก็ได้ เพราะ 4r หารด้วย 4 ลงตัวเสมอ ถ้ามียาง 5 ยี่ห้อ จำนวนยางที่จะใช้ทั้งหมดคือ 5r เส้น ในกรณีนี้ r จะต้องเป็นจำนวนซึ่งทำให้ 5r หารด้วย 4 ได้ลงตัว

ถ้า r = 4 แบบการทดลองที่ง่ายที่สุดคือใช้รถ 4 คัน สมมุติว่าคือรถ A, B, C และ D ใช้ยางยี่ห้อที่ 1 เป็นจำนวน 4 เส้นใส่กับรถ A ใช้ยางยี่ห้อที่2 เป็นจำนวน 4 เส้นใส่กับรถ B ใช้ยางยี่ห้อที่ 3 เป็นจำนวน 4 เส้นใส่กับรถ C และใช้ยางยี่ห้อที่ 4 เป็นจำนวน 4 เส้นใส่กับรถ D แบบการทดลองดังกล่าวนี้เขียนอธิบายได้ดังในตาราง 9.1.1

		รถยนต์			
		A	B	C	D
ตำแหน่งของยาง	หน้าซ้าย	1	2	3	4
	หน้าขวา	1	2	3	4
	หลังซ้าย	1	2	3	4
	หลังขวา	1	2	3	4

ตาราง 9.1.1

จะเห็นว่าการทดลองดังกล่าวนี้ไม่เป็นที่น่าพอใจ ทั้งนี้เนื่องจากปริมาณการใช้ยางของรถแต่ละคันไม่เหมือนกัน รถบางคันทำให้ยางสึกเร็วกว่ารถบางคันเป็นต้น ซึ่งอาจทำให้ข้อมูลหรือผลสรุปที่ได้จากการทดสอบผิดพลาดได้

ในหลักทฤษฎีเกี่ยวกับการออกแบบการทดลองนั้น โดยปกติเรามักต้องการให้ผลที่ได้จากการทดลองมีความเที่ยงตรงที่สุดที่จะทำได้ เราไม่ต้องการให้การใช้รถต่างคันกันเป็นผลกระทบต่อการทดลอง เราจึงมักขจัดหรือลดข้อไม่เที่ยงตรง (bias) นี้ด้วยการสุ่มเลือกยางทั้ง 4 ยี่ห้อ แล้วนำไปใส่กับรถยนต์ทั้ง 4 คัน ในตำแหน่งที่สุ่มเลือก ซึ่งอาจจะได้แบบการทดลองดังปรากฏในตาราง 9.1.2

		รถยนต์			
		A	B	C	D
ตำแหน่งของยาง	หน้าซ้าย	3	4	2	2
	หน้าขวา	1	1	4	4
	หลังซ้าย	3	4	1	3
	หลังขวา	2	3	2	1

ตาราง 9.1.2

ในแบบการทดลองนี้ เราอาจจะพบการทดลองซึ่งมียางบางยี่ห้อไม่ถูกใช้กับรถยนต์บางคันเลย เช่นยางยี่ห้อที่ 4 ไม่ถูกใช้กับรถยนต์ A เลย เป็นต้น ซึ่งผลที่ได้จากการทดลองอาจจะยังไม่เที่ยงตรงพอ เราอาจเลี่ยงเหตุการณ์เช่นนี้ได้โดยจำกัดให้ใช้ยางแต่ละยี่ห้อกับรถยนต์แต่ละคัน คำถามที่เกิดขึ้นคือ

> จะมีแบบการทดลอง ซึ่งใช้ยาง 4 ยี่ห้อ และรถ 4 คัน โดยที่ยางแต่ละยี่ห้อจะต้องได้รับการทดลองเป็นจำนวนครั้งเท่ากันคือ 4 ครั้ง และยางแต่ละยี่ห้อจะต้องถูกใช้อย่างน้อย 1 ครั้ง (ในที่นี้มีความหมายเท่ากับถูกใช้เพียงครั้งเดียว เพราะมีล้อแค่ 4 ล้อ ต่อรถหนึ่งคัน และมียาง 4 ยี่ห้อพอดี) กับรถยนต์แต่ละคันหรือไม่

คำตอบคือ "มี" และแบบการทดลองในตาราง 9.1.3 เป็นเพียงการทดลองแบบหนึ่งซึ่งสอดคล้องกับเงื่อนไขดังกล่าว

ตำแหน่งของยาง	รถยนต์ A	B	C	D
หน้าซ้าย	1	1	3	4
หน้าขวา	2	3	4	2
หลังซ้าย	3	2	1	1
หลังขวา	4	4	2	3

ตาราง 9.1.3

ตาราง 9.1.3 ยังมีข้อไม่เที่ยงตรง เนื่องจากตำแหน่งของล้ออาจเป็นผลต่อปริมาณการใช้ยาง เช่นล้อหน้าอาจทำให้ยางสึกมากกว่าล้อหลัง หรือล้อขวาอาจทำให้ยางสึกมากกว่าล้อซ้าย เหล่านี้เป็นต้น ถ้าเราต้องการขจัดข้อไม่เที่ยงตรงนี้ เราอาจเพิ่มข้อจำกัดว่ายางแต่ละยี่ห้อจะต้องถูกใช้อย่างน้อยหนึ่งครั้งกับรถยนต์แต่ละคันและจะต้องถูกใช้หนึ่งครั้งใน

ตำแหน่งแต่ละตำแหน่งของล้อรถยนต์ นั่นคือเรากำลังมองหาแบบการทดลองซึ่งอธิบายได้ด้วยตารางขนาด 4 x 4 ซึ่งประกอบด้วยตัวเลข 1, 2, 3, 4 ซึ่งใช้แทนยี่ห้อของยางทั้งสี่ยี่ห้อ โดยที่ตัวเลขแต่ละตัวจะต้องปรากฏในแต่ละแถวเพียงครั้งเดียวและปรากฏในแต่ละคอลัมน์เพียงครั้งเดียวเช่นกัน แบบการทดลองซึ่งสอดคล้องกับเงื่อนไขดังกล่าวแบบหนึ่งได้แก่แบบการทดลองที่ปรากฏในตาราง 9.1.4

		รถยนต์			
		A	B	C	D
ตำแหน่งของยาง	หน้าซ้าย	1	2	3	4
	หน้าขวา	2	3	4	1
	หลังซ้าย	3	4	1	2
	หลังขวา	4	1	2	3

ตาราง 9.1.4

เราเรียกแบบการทดลองซึ่งมีลักษณะดังในตาราง 9.1.4 ว่า **จัตุรัสละติน** (Latin Square) จัตุรัสละตินเป็นตัวอย่างของ **บล็อกดีไซน์แบบสมบูรณ์** ซึ่งจะได้กล่าวถึงในรายละเอียดในหัวข้อต่อไป

สมมุติว่าเรามียาง 5 ยี่ห้อที่จะต้องทำการทดลองโดยกำหนดให้ยางแต่ละยี่ห้อได้รับการนำไปทดลองเป็นจำนวนเท่ากัน คือเท่ากับ 5 เราจะต้องใช้ยางทั้งหมด 5r เส้น ดังนั้น 5r จะต้องหารด้วย 4 ลงตัวเช่น r อาจจะต้องเป็น 4, 8, หรือ 12 เป็นต้น ข้อสังเกตคือ เราไม่สามารถทำการทดลองโดยใช้รถ 6 คันได้ นั่นคือจะไม่มีแบบการทดลองซึ่งใช้ยาง 5 ยี่ห้อ รถ 6 คัน โดยที่ยางแต่ละยี่ห้อถูกใช้เป็นจำนวนครั้งเท่ากัน ทั้งนี้

เพราะว่า ถ้าใช้รถ 6 คัน ตำแหน่งของยางทั้งหมดจะเท่ากับ 6 x 4 = 24 ตำแหน่ง ดังนั้น 5r = 24 ซึ่งเป็นไปไม่ได้เพราะ r จะต้องเป็นจำนวนเต็ม

ถ้า r = 4 แล้ว 5r = 20 จะเป็นจำนวนยางทั้งหมดที่ต้องใช้ นั่นคือ ตำแหน่งของล้อทั้งหมดจะต้องเท่ากับ 20 ถ้าให้ s เป็นจำนวนรถยนต์ที่ต้องใช้ จะได้ 4s=20 นั่นคือ s จะต้องเท่ากับ 5 การทดลองจึงจะเป็นไปได้ เช่นแบบการทดลองในตาราง 9.1.5

		รถยนต์				
		A	B	C	D	E
ตำแหน่งของยาง	หน้าซ้าย	1	2	3	4	5
	หน้าขวา	2	3	4	5	1
	หลังซ้าย	3	4	5	1	2
	หลังขวา	4	5	1	2	3

ตาราง 9.1.5

แบบการทดลองในตาราง 9.1.5 เป็นตัวอย่างหนึ่งของ **บล็อกดีไซน์แบบไม่สมบูรณ์** เนื่องจากการทดลองแต่ละครั้งเราใช้ยางเพียง 4 ยี่ห้อ จากทั้งหมด 5 ยี่ห้อ

9.2 จัตุรัสละติน
Latin Squares

จัตุรัสละตินขนาด n ได้แก่ แถวลำดับ (array) ของตัวเลข 1, 2, ..., n ซึ่งมี n แถวและ n คอลัมน์ โดยมีตัวเลขแต่ละตัวปรากฏในแต่ละแถวเพียงครั้งเดียวและปรากฏในแต่ละคอลัมน์เพียงครั้งเดียว ข้างล่างนี้เป็นตัวอย่างของจัตุรัสละตินขนาด 2, 3, และ 4 ตามลำดับ

1	2
2	1

3	2	1
2	1	3
1	3	2

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

ตาราง 9.2.1

ให้ A เป็นจัตุรัสละตินขนาด n ให้ a_{ij} แทนสมาชิกในแถวที่ i คอลัมน์ที่ j ของจัตุรัสละติน A ให้ B เป็นจัตุรัสละตินขนาด n อีกจัตุรัสหนึ่ง ซึ่งมี b_{ij} เป็นสมาชิกในแถวที่ i คอลัมน์ที่ j คู่ลำดับ (a_{ij}, b_{ij}) คือคู่ลำดับซึ่งเกิดจากการประกบกันของจัตุรัสละติน A และ B นั่นคือนำเอาสมาชิก a_{ij} ของจัตุรัสละติน A และสมาชิก b_{ij} ของจัตุรัสละติน B ซึ่งอยู่ในตำแหน่งเดียวกันมาเขียนเรียงกันแบบคู่อันดับซึ่งมีทั้งหมด n^2 คู่ จะกล่าวว่าจัตุรัสละติน A ตั้งฉาก (orthogonal) กับจัตุรัสละติน B ถ้าคู่ลำดับ (a_{ij}, b_{ij}) แต่ละคู่แตกต่างกัน เมื่อ i = 1, 2, ..., n และ j = 1, 2, ..., n

ตัวอย่าง 9.2.1 ให้ A และ B เป็นจัตุรัสละตินขนาด 3 ซึ่งอยู่ทางซ้ายมือ

3	2	1
2	1	3
1	3	2

2	3	1
1	2	3
3	1	2

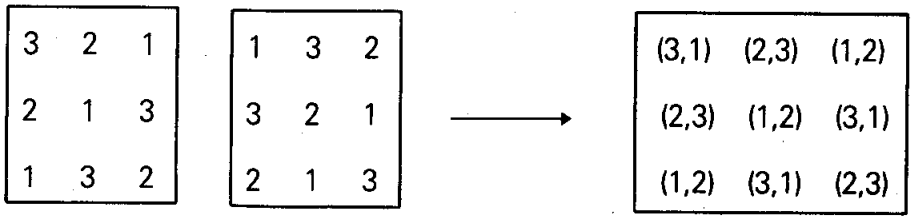
⟶

(3,2)	(2,3)	(1,1)
(2,1)	(1,2)	(3,3)
(1,3)	(3,1)	(2,2)

ตาราง 9.2.2

เนื่องจากคู่ลำดับทั้งหมดที่ได้ในตารางที่อยู่ขวาสุดแตกต่างกัน จึงกล่าวได้ว่าจัตุรัสละติน A ตั้งฉากกับจัตุรัสละติน B หรือกล่าวว่าจัตุรัสละติน A และ B ตั้งฉากกัน

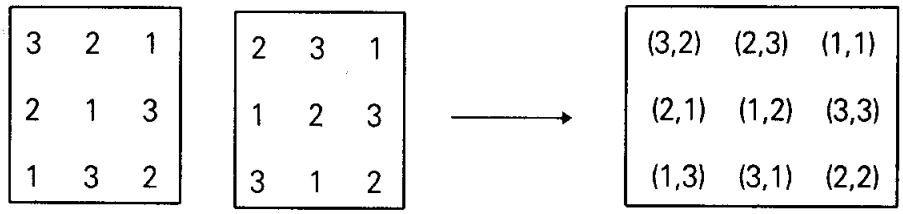
ตัวอย่าง 9.2.2 จัตุรัสละติน A และ B ซึ่งมีขนาด 3 ข้างล่างนี้ไม่ตั้งฉากกัน เนื่องจากมีคู่ลำดับบางคู่ซ้ำกัน เช่นมี (1,2) , (2,3) และ (3,1) ซ้ำกัน



ตาราง 9.2.3

การตั้งฉากของจัตุรัสละติน สามารถนำไปประยุกต์ใช้กับการออกแบบการทดลองได้ เช่นสมมุติว่าเราต้องการทดสอบผลกระทบจากการใช้ปริมาณน้ำและปริมาณปุ๋ยขนาดต่าง ๆ กันในแปลงข้าวสาลีบนผืนดินแห่งหนึ่ง สมมุติว่าปริมาณน้ำที่ใช้มี n ขนาดต่าง ๆ กัน และปริมาณปุ๋ยที่ใช้มี n ขนาดต่าง ๆ กัน สมมุติว่าเราต้องการทดสอบหาความเหมาะสมของปริมาณน้ำและปริมาณปุ๋ยที่จะทำให้ได้ผลผลิตข้าวสาลีมากที่สุด เราจะต้องทำการทดลองทั้งหมด n^2 การทดลองแตกต่างกันตามปริมาณน้ำและปริมาณปุ๋ยทั้งหมด แบ่งแปลงทดลองออกเป็น n^2 แปลงย่อย ๆ ใช้ปริมาณน้ำและปริมาณปุ๋ยที่แตกต่างกันในแต่ละแปลงย่อย โดยธรรมชาติแล้วแปลงย่อยในแต่ละแถวย่อมมีความอุดมสมบูรณ์ไม่เท่ากัน เช่นแปลงย่อยที่อยู่ในแถวหน้าอาจจะอุดมสมบูรณ์กว่าแปลงย่อยที่อยู่แถวหลัง ซึ่งจะเป็นผลทำให้เกิดความไม่เที่ยงตรงของผลการทดลองได้ เพื่อลดความไม่เที่ยงตรงที่จะเกิดขึ้น อาจมีข้อจำกัดว่าปุ๋ยแต่ละขนาดจะต้องไม่ปรากฏมากกว่าหนึ่งครั้งในแปลงย่อยที่อยู่ในแต่ละแถวและแต่ละคอลัมน์ และอาจมีข้อจำกัดทำนองเดียวกันกับปริมาณน้ำ นั่นคือเราต้องการจัตุรัสละติน A และจัตุรัสละติน B ขนาด n ซึ่งตั้งฉาก

กัน ตัวอย่างเช่น สมมุติว่ามีปุ๋ย 3 ขนาดให้หมายเลข 1 , 2 , 3 และปริมาณน้ำ 3 ขนาด ให้หมายเลข 1, 2, 3 เช่นกัน จะพบว่าแบบการทดลองที่เหมาะสมแบบหนึ่งคือ



ตาราง 9.2.4

ทฤษฎีบท 9.2.1

ให้ $A^{(1)}, A^{(2)}, \ldots, A^{(k)}$ เป็นจัตุรัสละตินขนาด n ถ้าแต่ละคู่ของจัตุรัสละตินนี้ตั้งฉากกันแล้ว $k \leq n-1$

พิสูจน์ ให้ $a_{ij}^{(p)}$ แทนสมาชิกซึ่งอยู่ในตำแหน่ง (i,j) ของจัตุรัสละติน $A^{(p)}$ จัดเรียงสมาชิกใน $A^{(1)}$ ใหม่โดยไม่ทำให้สมบัติของการเป็นจัตุรัสละตินและสมบัติของการตั้งฉากกันสูญหายไป เราดำเนินการสลับเปลี่ยนที่ของสมาชิกใน $A^{(1)}$ ดังนี้

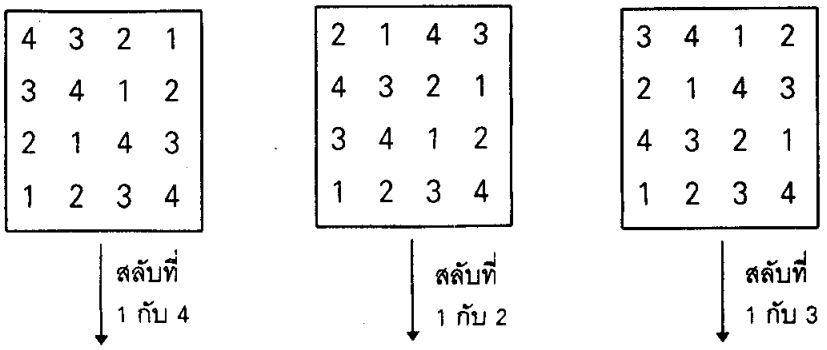
ถ้า $a_{11}^{(1)}$ เท่ากับ m ($\neq 1$) สลับที่ระหว่าง 1 และ m เห็นได้ชัดเจนว่าการสลับที่ดังกล่าวนี้ไม่ทำให้ $A^{(1)}$ สูญเสียความเป็นจัตุรัสละตินไป นอกจากนี้สมบัติของการตั้งฉากกันก็ยังคงอยู่ ถ้าคู่ลำดับ $(a_{ij}^{(1)}, a_{ij}^{(p)})$ อยู่ในรูป (m,t) คู่ลำดับใหม่ที่ได้หลังจากการสลับที่ระหว่าง 1 และ m แล้วจะเป็น (1,t) และถ้าคู่ลำดับเดิมคือ (1,t) ก็จะถูกเปลี่ยนเป็น (m,t) ด้วยเหตุผลทำนองเดียวกันนี้ เราสามารถทำการสลับที่ให้สมาชิกของจัสตุรัสละตินมีลักษณะดังนี้

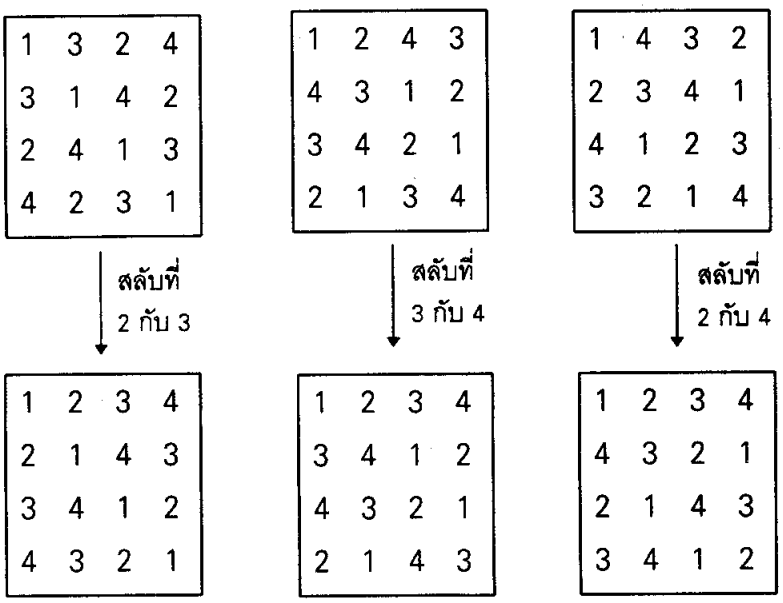
$$a_{11}^{(1)} = a_{11}^{(2)} = \cdots = a_{11}^{(p)} = 1$$
$$a_{12}^{(1)} = a_{12}^{(2)} = \cdots = a_{12}^{(p)} = 2$$
$$a_{13}^{(1)} = a_{13}^{(2)} = \cdots = a_{13}^{(p)} = 3$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_{1n}^{(1)} = a_{1n}^{(2)} = \cdots = a_{1n}^{(p)} = n$$

นั่นคือทำการสลับที่ให้แถวที่ 1 ของจัตุรัสละตินทุกรูปเรียงลำดับในลักษณะธรรมชาติ คือ 1 2 3 ... n โดยไม่ทำให้สมบัติของการเป็นจัตุรัสละตินและสมบัติของการตั้งฉากกันสูญหายไป

ต่อไป พิจารณาสมาชิกในตำแหน่ง (2,1) ของจัตุรัสละตินแต่ละรูป เราทราบว่า $a_{21}^{(p)} \neq 1$ และจากสมบัติของการตั้งฉาก เราทราบว่า $a_{21}^{(p)}$ จะต้องไม่เหมือนกับ $a_{21}^{(q)}$ สำหรับ $p \neq q$ เพราะถ้าเหมือนกันแล้วจะทำให้ $(a_{21}^{(p)}, a_{21}^{(q)}) = (i,i)$ สำหรับค่า i บางค่า ซึ่งเป็นผลให้ $(a_{21}^{(p)}, a_{21}^{(q)})$ ต้องเท่ากับ $(a_{1i}^{(p)}, a_{1j}^{(q)})$ ซึ่งขัดแย้งกับสมบัติของการตั้งฉากกัน ดังนั้น $a_{21}^{(1)}$, $a_{21}^{(2)}$, ...และ $a_{21}^{(k)}$ จะต้องแตกต่างกัน แสดงว่าเซตของจัตุรัสละตินซึ่งทุกคู่ตั้งฉากกันจะมีได้ไม่เกิน n-1 รูป นั่นคือ $k \leq n-1$ ดังข้อสรุปในทฤษฎีบท ■

เพื่อขยายความในข้อพิสูจน์ของทฤษฎีบท 9.2.1 เราจะแสดงวิธีสลับเปลี่ยนสมาชิกของจัตุรัสละตินขนาด 4 ให้ดูเป็นตัวอย่างดังนี้





ตาราง 9.2.5

เราสามารถสร้างจัตุรัสละตินขนาดต่าง ๆ ได้ไม่ยากนัก ข้างล่างนี้เป็นตัวอย่างแสดงวิธีสร้างจัตุรัสละตินขนาด 6 สำหรับจัตุรัสละตินขนาดอื่น ๆ ก็ทำได้ในทำนองเดียวกัน

ตัวอย่าง 9.2.3 จงสร้างจัตุรัสละตินขนาด 6

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
4	5	6	1	2	3
3	4	5	6	1	2
2	3	4	5	6	1

ตาราง 9.2.6

วิธีทำ เราเริ่มด้วยการให้ 1, 2, 3, 4, 5, 6 เป็นสมาชิกในแถวแรก เราสร้างแถวที่สองได้โดยการเลื่อนสมาชิกแต่ละตัวในแถวที่หนึ่งไปทางขวามือหนึ่งตำแหน่ง สมาชิกตัวสุดท้ายในแถวที่หนึ่ง ซึ่งในที่นี้คือ 6 ให้นำไป

ใส่ไว้ในตำแหน่งแรก ส่วนแถวอื่น ๆ ก็ทำได้ในทำนองเดียวกัน คือเลื่อนสมาชิกแต่ละตัวในแถวก่อนหน้านั้นไปทางขวามือหนึ่งตำแหน่ง และนำสมาชิกตัวสุดท้ายมาใส่ไว้ในตำแหน่งแรก เราจะได้จัตุรัสละตินดังในตาราง 9.2.6

จัตุรัสละตินที่ได้โดยวิธีดังกล่าวนี้ เป็นเพียงแบบหนึ่งของจัตุรัสละตินเท่านั้น ยังมีจัตุรัสละตินรูปอื่น ๆ อีกมากมาย ที่กล่าวมานี้แสดงว่าเราสามารถหาจัตุรัสละตินขนาด n เมื่อ n เป็นจำนวนเต็มบวกใด ๆ ได้เสมอ คำถามที่น่าสนใจคือ **เมื่อกำหนด n ให้ จะมีจัตุรัสละตินขนาด n ซึ่งตั้งฉากกันหรือไม่** ถ้ามีจะสร้างได้อย่างไร การสร้างจัตุรัสละตินซึ่งตั้งฉากกันนั้น จะต้องอาศัยความรู้ในเรื่องฟีลด์จำกัด (finite field) และเลขาคณิตจำกัด (finite geometry) ซึ่งอยู่นอกเหนือขอบเขตของวิชานี้ ผู้อ่านที่สนใจในเรื่องนี้สามารถศึกษาเพิ่มเติมได้จากหนังสือ Introductory Combinatorics ซึ่งเขียนโดย Richard A. Brualdi

เราได้เห็นในบทที่หนึ่งแล้วว่า จัตุรัสละตินขนาดสอง มีเพียงสองรูปเท่านั้นที่แตกต่างกัน คือ

1	2
2	1

และ

2	1
1	2

จัตุรัสทั้งสองนี้ไม่ตั้งฉากกัน ส่วนในตาราง 9.2.2 แสดงให้เห็นว่ามีจัตุรัสละตินขนาด 3 ซึ่งตั้งฉากกัน

ทฤษฎีบทที่จะศึกษาต่อไปนี้ จะช่วยวิเคราะห์ว่าเมื่อใดจะมีจัตุรัสละตินตั้งฉากและเมื่อใดไม่มีจัตุรัสละตินตั้งฉาก

ทฤษฎีบท 9.2.2

ถ้า n > 1 และ $n = p^k$ เมื่อ p เป็นจำนวนเฉพาะ และ k เป็นจำนวนเต็มบวกแล้ว จะต้องมีจัตุรัสละตินขนาด n เป็นจำนวน n-1 รูป ซึ่งแต่ละคู่ตั้งฉากซึ่งกันและกัน

ทฤษฎีบทนี้กล่าวว่า ถ้า n เป็นจำนวนเฉพาะยกกำลัง(prime power) แล้วจะต้องมีจัตุรัสละตินขนาด n เป็นจำนวน n-1 รูป ซึ่งแต่ละคู่ตั้งแากกัน เราจะเว้นไม่พิสูจน์ทฤษฎีบทนี้

ทฤษฎีบท 9.2.2 รับประกันว่าจะต้องมีจัตุรัสละตินขนาด 3 อย่างน้อยหนึ่งคู่ที่ตั้งฉากกันและจะต้องมีจัตุรัสละตินขนาด 4 จำนวน 3 รูป ซึ่งแต่ละคู่ตั้งฉากกัน ทั้งนี้เนื่องจาก $3 = 3^1$ และ $4 = 2^2$ ตามลำดับ และจะต้องมีจัตุรัสละตินขนาด 5 เป็นจำนวน 4 รูป ซึ่งแต่ละคู่ตั้งฉากกัน แต่สำหรับกรณี n = 6 นั้น เราสรุปอะไรไม่ได้ เพราะ 6 ไม่ใช่จำนวนเฉพาะและไม่สามารถเขียนให้อยู่ในรูปของจำนวนเฉพาะยกกำลังได้ ดังนั้น เราไม่มีข้อยืนยันว่าจะมีจัตุรัสละตินขนาด 6 คู่ใดหรือไม่ที่ตั้งฉากกัน

จากทฤษฎีจำนวน เราทราบว่า ถ้า n > 1 เป็นจำนวนเต็มบวกใด ๆ แล้ว เราจะเขียน n ให้อยู่ในรูป $p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ ได้เพียงแบบเดียวเท่านั้น (unique) ถ้าไม่คำนึงถึงลำดับของ $p_1, p_2, \dots,$ และ p_k เช่น

$$6 = 2^1 \times 3^1$$

$$12 = 3 \times 4 = 3^1 \times 2^2$$

$$60 = 4 \times 15 = 2^2 \times 3^1 \times 5^1$$

เป็นต้น

ทฤษฎีบท 9.2.3

สมมุติให้ $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ เมื่อ $n > 1$ และให้ r เป็นจำนวนเต็มที่เล็กที่สุดในจำนวนต่อไปนี้ $p_1^{t_1} - 1, p_2^{t_2} - 1, \dots, p_k^{t_k} - 1$ จะต้องมีจัตุรัสละตินขนาด n จำนวน r รูป ซึ่งแต่ละคู่ตั้งฉากกันและกัน

ตัวอย่าง 9.2.4 เนื่องจาก $12 = 2^2 \times 3^1$ ดังนั้น $r = 2$ (จำนวนที่เล็กที่สุด) ทฤษฎีบท 9.2.3 รับประกันว่าจะต้องมีจัตุรัสละตินขนาด 12 จำนวน $r = 2$ รูปซึ่งตั้งฉากกันและกัน ■

จะเห็นว่าทฤษฎีบท 9.2.3 ไม่ได้จำกัดว่าจำนวนจัตุรัสละตินซึ่งตั้งฉากกันนั้นจะมีจำนวนมากกว่า 2 ไม่ได้ ถ้าลองพยายามใช้ทฤษฎีบท 9.2.3 กับกรณี $n = 6 = 2^1 \times 3^1$ จะพบว่า $2^1 - 1 = 1$ และ $3^1 - 1 = 2$ ดังนั้น $r = 1$ ซึ่งไม่เป็นประโยชน์ต่อข้อมูลเกี่ยวกับการมีหรือไม่มีของจัตุรัสละตินขนาด 6 ซึ่งตั้งฉากกันเลย

ในปี 1782 นักคณิตศาสตร์ชื่อ ออยเลอร์ ได้คาดเดาว่า ไม่มีจัตุรัสละตินขนาด 6 คู่ใดตั้งฉากกัน เวลาล่วงเลยมาจนกระทั่งในราวปี ค.ศ.1900 แทร์รี่ (Tarry) ได้พิสูจน์ให้เห็นว่าข้อคาดเดาของออยเลอร์นั้นเป็นจริง นั่นคือพิสูจน์ได้ว่าไม่มีจัตุรัสละตินขนาด 6 คู่ใดที่ตั้งฉากกัน ข้างล่างนี้เป็นบทแทรกของทฤษฎีบท 9.2.3

บทแทรก 9.2.1

สมมุติให้ $n > 1$ เป็นจำนวนเต็มบวก ซึ่งหารด้วย 2 ไม่ลงตัว หรือ $n = 2^{t_1} p_2^{t_2} \dots p_k^{t_k}$ เมื่อ $t_1 > 1$ แล้วจะต้องมีจัตุรัสละตินคู่หนึ่งที่ตั้งฉากกัน

พิสูจน์ เมื่อ $t_1 > 1$ เราได้ $2^{t_1} - 1 \geq 3$

สำหรับ p_i ตัวอื่น ๆ เราได้ $p_i^{r} - 1 \geq 2$ ดังนั้น $r \geq 2$ ■

จะเห็นว่าบทแทรก 9.2.1 นี้ ไม่คลุมถึงกรณี $n = 2k$ เมื่อ k หารด้วย 2 ไม่ลงตัว เช่น $n = 6 = 2 \times 3$ ในปี ค.ศ.1782 เช่นกัน ออยเลอร์ได้คาดเดาว่าไม่มีจัตุรัสละตินขนาด $n = 2k$ คู่ใดตั้งฉากกัน เมื่อ 2 หาร k ไม่ลงตัว ข้อคาดเดาของออยเลอร์ถูกต้องเฉพาะในกรณี $n = 2$ และ $n = 6$ แต่สำหรับกรณีอื่น ๆ นั้น ข้อคาดเดาของเขาถูกพิสูจน์ในราวปี ค.ศ.1960 ว่าไม่ถูกต้อง ดังปรากฏในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 9.2.4 (Bose, Shrikhande และ Parker)

ถ้า $n > 6$ และ $n = 2k$ เมื่อ 2 หาร k ไม่ลงตัวแล้วจะต้องมีจัตุรัสละตินขนาด n คู่หนึ่งซึ่งตั้งฉากกัน

ที่กล่าวมาแล้วสรุปได้ว่า ถ้า $n > 1$ แล้ว จะต้องมีจัตุรัสละตินขนาด n คู่หนึ่งซึ่งตั้งฉากกัน ยกเว้นกรณีที่ $n = 2$ หรือ $n = 6$

จากปัญหานายทหาร 36 นายที่กล่าวถึงในบทที่หนึ่งนั้น ผู้อ่านคงจะนำผลที่ได้จากบทนี้ตอบปัญหาดังกล่าวได้

แบบฝึกหัด

1. จงพิจารณาจัตุรัสละตินแต่ละคู่ต่อไปนี้ว่า คู่ใดตั้งฉากกันและคู่ใดไม่ตั้งฉากกัน

   ก.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

ข.

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

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

ค.

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

1	2	3	4	5
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1
1	2	3	4	5

2. จากค่าของ n ที่กำหนดให้ต่อไปนี้ จงพิจารณาว่าข้อใดมีวงศ์ (family) ของจัตุรัสละตินตั้งฉากซึ่งประกอบด้วยจัตุรัสละติน 3 จัตุรัส เพราะเหตุใด

   ก. n = 12 ข. n = 13 ค. n = 21

   ง. n = 25 จ. n = 35 ช. n = 36

3. ถ้า n = 275 จงแสดงให้เห็นว่า มีเซตของจัตุรัสละตินขนาด 275 เป็นจำนวน 10 จัตุรัส ซึ่งแต่ละคู่ตั้งฉากกัน

4. ถ้า n = 54 อยากทราบว่าจะมีจัตุรัสละตินขนาด 54 ซึ่งตั้งฉากกันหรือไม่ เพราะเหตุใด

5. จากวงศ์สมบูรณ์ของจัตุรัสละตินขนาด 5 ที่กำหนดให้ต่อไปนี้ จงใช้วิธีสลับที่เพื่อแปลงให้แถวแรกของแต่ละจัตุรัสเขียนเรียงกันใน

ลักษณะ 1 2 3 4 5 โดยไม่ทำให้สมบัติของการเป็นจัตุรัสละตินและสมบัติของการตั้งฉากสูญหายไป

5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1
1	2	3	4	5

4	5	1	2	3
2	3	4	5	1
5	1	2	3	4
3	4	5	1	2
1	2	3	4	5

3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3
1	2	3	4	5

2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4
1	2	3	4	5

9.3 บล็อกดีไซน์แบบไม่สมบูรณ์
Incomplete Block Designs

จัตุรัสละตินเป็นตัวอย่างหนึ่งของบล็อกดีไซน์แบบสมบูรณ์ ส่วนแบบการทดลองในตาราง 9.1.5 เป็นตัวอย่างของบล็อกดีไซน์แบบไม่สมบูรณ์ ข้อแตกต่างของทั้งสองแบบนี้คือจำนวนสมาชิก การทดลองในตาราง 9.1.4 นั้น เรามียางที่จะต้องเปรียบเทียบคุณภาพ 4 ยี่ห้อ ส่วนการทดลองในตาราง 9.1.5 เรามียางที่จะต้องทดสอบ 5 ยี่ห้อ แต่การทดลองแต่ละครั้งใช้เพียง 4 ยี่ห้อเท่านั้น ต่อไปนี้เราจะเรียกการทดลองแต่ละครั้งว่า **บล็อก** ถ้าแต่ละบล็อกประกอบด้วยสิ่งของทั้งหมดที่นำมาทดลอง เช่นยางยี่ห้อต่าง ๆ เราจะเรียกแบบการทดลองนั้นว่า **บล็อกดีไซน์แบบสมบูรณ์** และถ้าแต่ละบล็อกประกอบด้วยสมาชิกเพียงบางส่วน จะเรียกแบบการทดลองนั้นว่า**บล็อกดีไซน์แบบไม่สมบูรณ์** จะเห็นว่าในตาราง 9.1.5 มียางทั้งหมด 5 ยี่ห้อ แต่ว่าบล็อกแต่ละบล็อกมีสมาชิกเพียง 4 ตัวเท่านั้นจึงเป็นบล็อกดีไซน์แบบไม่สมบูรณ์

ในบทนี้จะศึกษาเฉพาะบล็อกดีไซแบบน์ไม่สมบูรณ์เท่านั้น ดังนั้นเพื่อความสะดวกบางครั้งจะละคำว่า **บล็อก** และคำว่า **ไม่สมบูรณ์**

ไว้ในฐานที่เข้าใจ เราจะเรียกสั้น ๆ ว่า **ดีไซน์** หรือบางครั้งเราจะใช้คำว่า **การออกแบบ** แทนคำว่าดีไซน์

เพื่อให้เข้าใจแนวความคิดกว้าง ๆ เกี่ยวกับเรื่องดีไซน์ ลองพิจารณาปัญหาในลักษณะต่อไปนี้

สมมุติว่ามีกาแฟยี่ห้อต่าง ๆ จำนวนหนึ่งซึ่งเราต้องการจะเปรียบเทียบว่ากาแฟยี่ห้อใดเป็นที่นิยมของประชาชน โดยนำไปแจกให้แม่บ้านกลุ่มหนึ่งได้ทดลองชิมเพื่อตัดสินว่าชอบยี่ห้อใด ในการทดลองนี้เราต้องการให้ผลการทดลองเที่ยงตรงมากที่สุดเท่าที่จะทำได้ ดังนั้นจึงอาจตั้งเงื่อนไขดังนี้

1. จำนวนยี่ห้อของกาแฟที่แม่บ้านแต่ละคนทดลองชิมต้องเท่ากัน
2. กาแฟยี่ห้อหนึ่ง ๆ จะต้องถูกชิมโดยแม่บ้านจำนวนเท่ากัน
3. จำนวนแม่บ้านที่ทดลองชิมยี่ห้อกาแฟแต่ละคู่จะต้องเท่ากัน

การทดลองแบบหนึ่งที่สอดคล้องกับเงื่อนไขดังกล่าวคือ ให้แม่บ้านแต่ละคน (ทุกคน) ทดลองชิมกาแฟทุกยี่ห้อ วิธีนี้เป็นวิธีที่ง่ายแต่เสียเวลาและสิ้นเปลือง ดังนั้นจุดประสงค์อีกข้อหนึ่งของการทดลองคือต้องการผลด้วยวิธีที่ประหยัด

ถ้าให้ S เป็นเซตของกาแฟยี่ห้อต่าง ๆ ที่ต้องการทำการเปรียบเทียบความนิยม ยี่ห้อกาแฟที่ถูกทดลองชิมโดยแม่บ้านแต่ละคนก็คือเซตย่อยของ S จากเงื่อนไขข้อแรกจะพบว่าเซตย่อยเหล่านั้นต้องประกอบด้วยสมาชิกเป็นจำนวนเท่ากัน จากเงื่อนไขข้อที่สองแสดงว่ากาแฟยี่ห้อหนึ่ง ๆ จะต้องปรากฏอยู่ในเซตย่อยเป็นจำนวนครั้งเท่ากัน และจากเงื่อนไขข้อสุดท้าย แสดงว่าสมาชิกแต่ละคู่ของเซต S จะต้องปรากฏในเซตย่อยเหล่านั้นเป็นจำนวนครั้งเท่ากัน เรียกการจัดสิ่งของ (ในที่นี้คือกาแฟยี่ห้อต่าง ๆ) เป็นกลุ่มย่อย ๆ ซึ่งสอดคล้องกับเงื่อนไขที่กล่าวมา

แล้วข้างต้นนี้ว่า **บล็อกดีไซน์** ดังนั้นเราให้คำจำกัดความของบล็อกดีไซน์ทั่ว ๆ ไปดังต่อไปนี้

นิยาม 9.3.1

บล็อกดีไซน์ ประกอบด้วยเซต S และกลุ่มของเซตย่อยของ S ซึ่งจะเรียกว่า **บล็อก** และสอดคล้องกับเงื่อนไขต่อไปนี้

1. จำนวนสมาชิกในแต่ละบล็อกมีจำนวนเท่ากัน
2. สมาชิกแต่ละตัวใน S ปรากฏในบล็อกเป็นจำนวนครั้งเท่ากัน
3. สมาชิกแต่ละคู่ใน S ปรากฏในบล็อกเป็นจำนวนครั้งเท่ากัน

ถ้า $v \geq 2$ เป็นจำนวนสมาชิกใน S

b เป็นจำนวนบล็อกทั้งหมด

r เป็นจำนวนครั้งที่สมาชิกตัวหนึ่ง ๆ ปรากฏ

k เป็นจำนวนสมาชิกในแต่ละบล็อก

λ เป็นจำนวนครั้งที่สมาชิกแต่ละคู่ของ S ปรากฏ

จะเรียกบล็อกดีไซน์ดังกล่าวนี้ว่า (v, b, r, k, λ)-ดีไซน์

ตัวอย่าง 9.3.1 ให้ $S = \{1,2,...,7\}$ เราพิจารณาเซตย่อยของ S ต่อไปนี้

{1,2,4}, {2,3,5}, {3,4,6}, {4,5,7}, {5,6,1}, {6,7,2} และ {7,1,3}

เรียกแต่ละเซตว่าบล็อก เพื่อความสะดวกบางครั้งเราจะเขียนในลักษณะเป็นแถวลำดับ ดังนี้

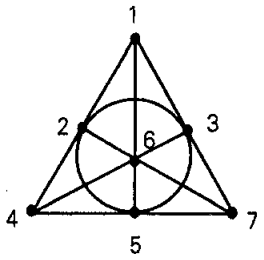
1	2	4
2	3	5
3	4	6
4	5	7
5	6	1
6	7	2
7	1	3

ในที่นี้ $v = 7, b = 7, r = 3, k = 3, \lambda = 1$ เพื่อแสดงให้เป็นว่า $\lambda = 1$ เราพิจารณาสมาชิกแต่ละคู่ของ S เช่น 4 และ 6 เราจะพบว่าสมาชิกคู่นี้ปรากฏเพียงครั้งเดียวในบล็อกที่ 3 คือบล็อกที่ประกอบด้วย 3, 4 และ 6 สำหรับสมาชิกคู่อื่น ๆ ก็พิจารณาได้ในทำนองเดียวกัน บล็อกดีไซน์นี้คือ (7,7,3,3,1) -ดีไซน์

บล็อกดีไซน์ในตัวอย่าง 9.3.1 ข้างบนนี้ สามารถนำไปใช้กับการทดลองซึ่งมีกาแฟ 7 ยี่ห้อ โดยใช้แม่บ้าน 7 คน แต่ละคนทดลองชิมกาแฟคนละ 3 ยี่ห้อ และยี่ห้อกาแฟแต่ละคู่จะต้องถูกเปรียบเทียบโดยแม่บ้านเพียงคนเดียว

เราสามารถแทนบล็อกดีไซน์ในตัวอย่าง 9.3.1 ด้วยรูปเชิงเรขาคณิต โดยแทนสมาชิก 1,2,...,7 ด้วยจุดเจ็ดจุดบนระนาบและแทนบล็อกด้วยเส้นดังรูป 9.3.1 ซึ่งเป็นตัวอย่างหนึ่งของ finite projective plane ตัวอย่างนี้เป็นที่รู้จักกันในนามของ **ระนาบเจ็ดจุด** (seven point plane)

รูป 9.3.1



ทุกเส้นเป็นเส้นตรง ยกเว้นเส้นที่ผ่านจุด 2,3 และ 5

นอกจากนี้เรายังสามารถแทนบล็อกดีไซน์ได้อีกวิธีหนึ่งคือแทนด้วยเมทริกซ์ ซึ่งสมาชิกแต่ละตัวเป็น 0 หรือ 1 และเราจะเรียกเมทริกซ์นี้ว่า **เมทริกซ์บังเกิด** ดังจะได้ศึกษารายละเอียดในหัวข้อต่อไปนี้

9.4 เมทริกซ์บังเกิดของบล็อกดีไซน์
Incidence Matrix of a Block Design

เราจะกล่าวว่าเมทริกซ์ $A = (a_{ij})$ เป็นเมทริกซ์บังเกิดของ (v,b,r,k,λ) - ดีไซน์ ถ้าเมทริกซ์ A มีขนาด $v \times b$ และ a_{ij} เป็นสมาชิกที่อยู่ในแถวที่ i คอลัมน์ที่ j ของ A ซึ่งจะเป็น 1 หรือ 0 เท่านั้น $a_{ij} = 1$ ก็ต่อเมื่อสมาชิกตัวที่ i ของเซต S ปรากฏในบล็อกที่ j ของ (v,b,r,k,λ) - ดีไซน์ นอกเหนือจากนี้แล้ว $a_{ij} = 0$ เราจะใช้สัญญลักษณ์ B_i แทนบล็อกที่ i ดังในตัวอย่างต่อไปนี้

ตัวอย่าง 9.4.1 เมทริกซ์บังเกิดของ (7,7,3,3,1) - ดีไซน์ในตัวอย่าง 9.3.1 คือ

$$A = \begin{array}{c} \begin{matrix} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

จากการสังเกตเมทริกซ์บังเกิด A จะพบว่าแต่ละคอลัมน์ของ A แทนแต่ละบล็อกของดีไซน์และแต่ละแถวของ A ให้ข้อมูลเกี่ยวกับสมาชิกตัวหนึ่ง ๆ ของ S เช่นแถวที่หนึ่งบ่งชี้ให้ทราบว่า สมาชิกตัวที่หนึ่งของเซต S ปรากฏอยู่ในบล็อกที่ 1, 5 และ 7 เป็นต้น

เนื่องจากสมาชิกแต่ละตัวใน S จะต้องปรากฏเป็นจำนวน $r = 3$ ครั้งเท่า ๆ กัน (นั่นคือปรากฏใน 3 บล็อก) ดังนั้นจำนวนเลข 1 ในแต่ละแถวของ A จึงเท่ากับ 3 หรือเท่ากับ r ในกรณีทั่วไป

เงื่อนไขซึ่งจำกัดให้สมาชิกแต่ละคู่ปรากฏในบล็อกเดียวกันได้เพียงครั้งเดียวนั้น เราสามารถตรวจสอบได้จากเมทริกซ์ โดยพิจารณาแถวสองแถวของเมทริกซ์ แถวแต่ละคู่เหล่านั้นจะต้องมี 1 ปรากฏอยู่ในคอลัมน์เดียวกันได้เพียงครั้งเดียวเท่านั้น ตัวอย่างเช่น พิจารณาแถวที่ 4 และ 6 ซึ่งเป็นแถวที่ให้ข้อมูลเกี่ยวกับสมาชิก 4 และ 6 จะพบว่า 4 และ 6 ปรากฏอยู่ในบล็อกที่ 3 ดังนั้นจะมี 1 ในแถวที่ 4 และแถวที่ 6 ปรากฏคู่กันในคอลัมน์ที่ 3 เมื่อตรวจสอบสมาชิก 1 ในแถวที่ 4 และ 1 ในแถวที่ 6 จะพบว่ามี 1 ตรงกันเพียงคู่เดียวเท่านั้นคือคู่ที่อยู่ในคอลัมน์ที่ 3

ข้อดีที่แทนดีไซน์ด้วยเมทริกซ์บังเกิดคือ ไม่ต้องแจกแจงสมาชิกของแต่ละบล็อกและสามารถมองเห็นโครงสร้างของดีไซน์ได้จากเมทริกซ์โดยไม่ต้องเรียกชื่อสมาชิกให้สับสน นอกจากนี้ เรายังตรวจสอบจากเมทริกซ์ได้โดยง่ายว่าสมาชิกตัวหนึ่ง ๆ อยู่ในบล็อกใดบ้าง แทนที่จะตรวจดูจากบล็อกทั้งหลายของดีไซน์

ตัวแปรทั้งห้าตัว คือ v,b,r,k และ λ ไม่เป็นอิสระต่อกัน ดังจะเห็นได้จากทฤษฎีบทต่อไปนี้

ทฤษฎีบท 9.4.1

ใน (v,b,r,k,λ)-ดีไซน์ เราได้

$$bk = vr \quad \text{และ} \quad r(k-1) = \lambda(v-1) \qquad \text{.....(9.4.1)}$$

พิสูจน์ จำนวนบล็อกทั้งหมดเท่ากับ b แต่ละบล็อกประกอบด้วยสมาชิก k ตัว ดังนั้นจำนวนสมาชิกที่ปรากฏทั้งหมดจะเท่ากับ bk และเนื่องจากจำนวนสมาชิกทั้งหมดเท่ากับ v โดยที่สมาชิกแต่ละตัวปรากฏ

เป็นจำนวน r ครั้ง ดังนั้นจำนวนสมาชิกที่ปรากฏทั้งหมดจะเท่ากับ vr นั่นคือ bk = vr

สมมุติว่า x เป็นสมาชิกตัวหนึ่งในเซต S ซึ่งปรากฏอยู่ใน r บล็อก ในแต่ละบล็อกเหล่านี้ยังประกอบด้วยสมาชิกอื่น ๆ อีก k-1 ตัว จับกลุ่มสมาชิกในแต่ละบล็อกเป็นคู่ ๆ จะเห็นว่าคู่ที่มี x อยู่ด้วยจะมีจำนวน k - 1 คู่ ใน r บล็อกที่มี x อยู่ เรานับจำนวนคู่ที่มี x รวมกันทั้งหมด จะได้ r(k-1) คู่

ในอีกแง่มุมหนึ่ง เราทราบว่าสมาชิกใน S มีทั้งหมด v ตัว ดังนั้นคู่ที่มี x อยู่ด้วยจะมีทั้งหมด v - 1 คู่ แต่ละคู่ปรากฏ λ ครั้ง แสดงว่าจำนวนคู่ที่มี x จะมีทั้งหมดเท่ากับ λ(v - 1) คู่ นั่นคือ r(k - 1) = λ(v - 1) ■

ทฤษฎีบท 9.4.1 กล่าวว่า ถ้าเรามี (v,b,r,k,λ) - ดีไซน์แล้ว ตัวแปรทั้งห้าตัวเหล่านี้จะสอดคล้องกับ (9.4.1) แต่ถ้าตัวแปรทั้งห้าตัวนั้นสอดคล้องกับ (9.4.1) แล้วทฤษฎีบท 9.4.1 ไม่ได้รับประกันว่า (v, b, r, k,λ) - ดีไซน์จะมีหรือไม่

ดีไซน์ซึ่งมีชื่อว่าระนาบเจ็ดจุดที่กล่าวถึงในตัวอย่าง 9.3.1 มีสมบัติพิเศษคือ b = v นั่นคือจำนวนสมาชิกในเซต S และจำนวนบล็อกเท่ากัน ซึ่งจะทำให้เมทริกซ์บังเกิดเป็นเมทริกซ์จัตุรัส เราจะเรียกดีไซน์ซึ่งมีลักษณะดังกล่าวนี้ว่า **ดีไซน์จัตุรัส** (square design) หรือ **ดีไซน์สมมาตร** (symmetric design) เมื่อ v = b เราจะได้ r = k ดังนั้นดีไซน์ดังกล่าวจึงขึ้นอยู่กับตัวแปรเพียงสามตัวเท่านั้น คือ v, k และ λ ในกรณีเช่นนี้เราจะเรียกดีไซน์นั้นว่า (v, k, λ) - ดีไซน์

ทฤษฎีบท 9.4.2

ถ้า $A = (a_{ij})$ เป็นเมทริกซ์ของ (v, b, r, k, λ) - ดีไซน์แล้ว

1. $\sum_{h=1}^{b} a_{ih}a_{jh} = \begin{cases} r & \text{ถ้า } i = j \\ \lambda & \text{ถ้า } i \neq j \end{cases}$
2. $AA' = (r - \lambda)I + \lambda J$

เมื่อ A' คือทรานสโพสของเมทริกซ์ A และ I เป็นเมทริกซ์เอกลักษณ์ขนาด v และ J เป็นเมทริกซ์จัตุรัสขนาด v ซึ่งสมาชิกทุกตัวเป็น 1

3. $\det(AA') = rk(r - \lambda)^{v-1}$

พิสูจน์ (1) ถ้า $i = j$ เราได้

$$\sum_{h=1}^{b} a_{ih}a_{jh} = \sum_{h=1}^{b} a_{ih}a_{ih} = \sum_{h=1}^{b} a_{ih}^2 = \sum_{h=1}^{b} a_{ih}$$

เหตุผลที่ $a_{ih}^2 = a_{ih}$ เนื่องมาจาก $a_{ih} = 0$ หรือ 1 นั่นเอง สมมุติว่าเราตรึงค่า i ให้คงที่ นั่นคือเราพิจารณาเฉพาะแถวที่ i ของเมทริกซ์ A เราทราบว่าสมาชิกตัวที่ i ปรากฏอยู่ใน r บล็อก แสดงว่าจะต้องมีค่า h เป็นจำนวน r ค่า ที่ทำให้ $a_{ih} = 1$ นอกนั้น $a_{ih} = 0$ ดังนั้น

$$\sum_{h=1}^{b} a_{ih}a_{jh} = \sum_{h=1}^{b} a_{ih} = r$$

ถ้า $i \neq j$ แล้ว $a_{ih}a_{jh} = 1$ ก็ต่อเมื่อ $a_{ih} = a_{jh} = 1$ นั่นคือสมาชิกในแถวที่ i และแถวที่ j ของเมทริกซ์ A ซึ่งอยู่ในคอลัมน์ที่ h จะต้องเป็น 1 ทั้งคู่ จากสมบัติของดีไซน์เราทราบว่าจะต้องมี λ บล็อก หรือ λ คอลัมน์ ซึ่งมีสมาชิกในแถวที่ i และสมาชิกในแถวที่ j เป็น 1 ทั้งคู่ ดังนั้น $\sum_{h=1}^{b} a_{ih}a_{jh} = \lambda$ ตามต้องการ

พิสูจน์ (2) ให้ b_{ij} เป็นสมาชิกในตำแหน่ง (i,j) ของเมทริกซ์ AA' ดังนั้น

$$b_{ij} = \sum_{h=1}^{b} a_{ih}a_{jh}$$

จากผลในข้อ (1) เราทราบว่า

$$b_{ii} = \sum_{h=1}^{b} a_{ih}a_{ih} = r \quad \text{และ} \quad b_{ij} = \sum_{h=1}^{b} a_{ih}a_{jh} = \lambda \quad \text{เมื่อ } i \neq j$$

ดังนั้น เราได้

$$AA' = \begin{bmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \dots & r \end{bmatrix}$$

$$= \begin{bmatrix} r-\lambda & 0 & 0 & \dots & 0 \\ 0 & r-\lambda & 0 & \dots & 0 \\ 0 & 0 & r-\lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & r-\lambda \end{bmatrix} + \begin{bmatrix} \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \dots & \lambda \end{bmatrix}$$

$$= (r-\lambda)I + \lambda J$$

พิสูจน์ (3)

$$\det(AA') = \begin{vmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \dots & r \end{vmatrix} = \{r+\lambda(v-1)\} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \dots & r \end{vmatrix}$$

เพื่อแสดงว่าจำนวนข้างบนนี้เท่ากันจริง เรานำ v - 1 แถวสุดท้ายไปบวกกับแถวแรก แล้วถอดตัวร่วม r + λ(v - 1) ออกจากแถวแรกจะได้ผลดังปรากฏในสมการข้างบนนี้ ถ้าเราคูณแถวแรกของดีเทอร์มิแนนต์ที่อยู่ขวามือสุดด้วย λ แล้วนำผลที่ได้ไปหักออกจากแถวอื่น ๆ เราได้

$$\det(AA') = \{r + \lambda(v-1)\}\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & r-\lambda & 0 & \dots & 0 \\ 0 & 0 & r-\lambda & \dots & 0 \\ & & \dots\dots\dots & & \\ 0 & 0 & 0 & \dots & r-\lambda \end{vmatrix}$$

$$= \{r + \lambda(v-1)\}(r-\lambda)^{v-1}$$

$$= \{r + r(k-1)\}(r-\lambda)^{v-1} \qquad \text{(จากทฤษฎีบท 9.4.1)}$$

$$= rk(r-\lambda)^{v-1}$$

ทฤษฎีบท 9.4.3

ใน (v, b, r, k, λ) - ดีไซน์ จะได้ $b \geq v$

พิสูจน์ ให้ A เป็นเมทริกซ์บังเกิดของ (v,b,r,k,λ) - ดีไซน์ เราจะพิสูจน์โดยวิธีหาข้อขัดแย้ง คือสมมุติให้ b < v แล้วพยายามหาข้อขัดแย้ง ถ้าพบข้อขัดแย้งแสดงว่า b น้อยกว่า v ไม่ได้ นั่นคือ b จะต้องมากกว่าหรือเท่ากับ v ให้ A_1 เป็นเมทริกซ์ขนาด v x v ซึ่งได้จากการเติมคอลัมน์ที่เป็น 0 ลงในเมทริกซ์ A นั่นคือ

$$A_1 = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1b} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2b} & 0 & \dots & 0 \\ & & \dots\dots\dots & & & & \\ a_{v1} & a_{v2} & \dots & a_{vb} & 0 & \dots & 0 \end{bmatrix}$$

ดังนั้น

$$\det(A_1A_1') = \det(AA') = rk(r-\lambda)^{v-1} \neq 0 \quad \text{เนื่องจาก } r > \lambda$$

แต่ $\det(A_1A_1') = (\det A_1)(\det A_1') = 0$

ทั้งนี้เพราะ A_1 มีคอลัมน์ที่เป็น 0 ทั้งคอลัมน์ ดังนั้นเราได้ข้อขัดแย้ง ซึ่งแสดงว่า $b < v$ ไม่ได้ นั่นคือ $b \geq v$ ■

ตัวอย่าง 9.4.2 ถ้า $v = 16$, $b = 8$, $r = 3$, $k = 6$, $\lambda = 1$ แล้ว เราไม่สามารถหา (16,8,3,6,1) - ดีไซน์ได้ ทั้งนี้เนื่องจาก $b < v$ ■

9.5 ระบบไตรภาคแบบสไตน์เนอร์
Steiner Triple Systems

ในปี ค.ศ.1850 บาทหลวงชื่อ ทอมัส พี เคริคแมน (Thomas P. Kirkman) ได้ยกปัญหาเกี่ยวกับการจัดนักเรียน 15 คน ให้เดินเข้าแถว ๆ ละ 3 คน อยากทราบว่าจะเป็นไปได้หรือไม่ที่จะจัดให้นักเรียนเดินในลักษณะดังกล่าวเป็นจำนวน 7 วัน โดยที่ไม่มีเด็กคู่ใดเดินด้วยกันในแถวเรียงสามนั้นมากกว่า 1 วัน

ถ้าแทนเด็กทั้ง 15 คน ด้วยตัวเลข 1, 2, 3, ... , 15 คำตอบของปัญหานี้ได้แก่การจัดดังต่อไปนี้

1 2 3	1 4 5	1 6 7	1 8 9
4 8 12	2 4 8	2 9 11	2 12 14
5 10 15	3 13 14	3 12 15	3 5 6
6 11 13	6 9 15	4 10 14	4 11 15
7 9 14	7 11 12	5 8 13	7 10 13

1 10 11	1 12 13	1 14 15
2 13 15	2 4 6	2 5 7
3 4 7	3 9 10	3 8 11
5 9 12	5 11 14	4 9 13
6 8 14	7 8 15	6 10 12

คำตอบจะประกอบด้วยนักเรียน 35 แถว ๆ ละ 3 คน ใน 35 แถวนี้ถูกแบ่งออกเป็น 7 กลุ่ม ๆ ละ 5 แถว และนักเรียน 2 คนใด ๆ จะเดินในแถวเดียวกันได้เพียงครั้งเดียวเท่านั้น เช่นเด็ก 1 และ 2 จะเดินคู่กันในวันแรกวันเดียวเท่านั้น จะเห็นว่าการจัดหรือการออกแบบข้างบนนี้ก็คือบล็อกดีไซน์ ซึ่งมี $k = 3$ และ $\lambda = 1$ นั่นเอง

นิยาม 9.5.1

เรียกบล็อกดีไซน์ซึ่งมี $k = 3$ และ $\lambda = 1$ ว่า **ระบบไตรภาคแบบสไตน์เนอร์**

จากทฤษฎีบท 9.4.1 เราได้

$$3b = vr \quad \text{และ} \quad v - 1 = 2r$$

ดังนั้น

$$r = \frac{v - 1}{2} \quad \text{และ} \quad b = \frac{v(v - 1)}{6} \qquad \text{.....(9.5.1)}$$

จะเห็นว่า b หรือจำนวนไตรภาคในระบบไตรภาคแบบสไตน์เนอร์ขึ้นอยู่กับค่าของ v นั่นคือขึ้นอยู่กับจำนวนสมาชิกในเซต S ดังนั้นเราจะกล่าวว่า v เป็นขนาดของระบบไตรภาค

เราทราบว่า v และ b เป็นจำนวนเต็ม ดังนั้นจาก (9.5.1) แสดงว่า v จะต้องเป็นจำนวนเต็มคี่ ซึ่ง $v \geq 3$ และจาก (9.5.1) อีกเช่นกันแสดงว่า 6 จะต้องหาร v หรือ v - 1 ลงตัว ดังนั้น 3 จะต้องหาร v หรือ v - 1 ได้ลงตัว สมมุติว่า 3 หาร v ได้ลงตัว นั่นคือ $v = 3m$ เมื่อ m เป็นจำนวนเต็มบวกบางจำนวน เราทราบว่า v เป็นจำนวนคี่ ดังนั้น m จะต้องเป็นจำนวนคี่ สมมุติว่า $m = 2n+1$ เมื่อ n เป็นจำนวนเต็มที่ไม่เป็นลบจำนวนหนึ่ง ดังนั้น

$$v = 3m = 3(2n+1) = 6n+3$$

ถ้า 3 หาร v - 1 ได้ลงตัวแล้ว v - 1 = 3m หรือ v = 3m+1 สำหรับ m ที่เป็นจำนวนเต็มบวกบางจำนวน เนื่องจาก v เป็นจำนวนคี่ ดังนั้น m จะต้องเป็นจำนวนคู่ สมมุติให้ m = 2n เมื่อ n เป็นจำนวนเต็มบวกจำนวนหนึ่ง จากการแทนค่า จะได้

$$v = 3m+1 = 3(2n)+1 = 6n+1$$

ที่กล่าวมาแล้วนั้น สรุปได้ดังนี้

ทฤษฎีบท 9.5.1

ถ้ามีระบบไตรภาคแบบสไตน์เนอร์ขนาด v แล้ว v = 6n+1 หรือ v = 6n+3 เมื่อ n เป็นจำนวนเต็มซึ่งไม่เป็นลบ

ตัวอย่าง 9.5.1 ให้ v = 3 และให้ S = {1,2,3} ดังนั้นระบบไตรภาคแบบสไตน์เนอร์ขนาด 3 จะมีจำนวนไตรภาคเท่ากับ

$$b = \frac{v(v-1)}{6} = \frac{3(3-1)}{6} = 1$$

ซึ่งได้แก่ไตรภาค {1,2,3} นั่นเอง ■

ตัวอย่าง 9.5.2 ให้ v = 7 และให้ S = {1,2,3,4,5,6,7}

ระบบไตรภาคแบบสไตน์เนอร์ขนาด 7 จะต้องมีจำนวนไตรภาคเท่ากับ

$$b = \frac{7(7-1)}{6} = 7$$

เช่น {1,2,4}, {2,3,5}, {3,4,7}, {4,5,7}, {5,6,1}, {6,7,2}, {7,1,3} ■

ปัญหาที่นิยมถามกันมากคือ ถ้า v = 6n +1 หรือ v = 6n+3 แล้วจะมีระบบไตรภาคแบบสไตน์เนอร์ขนาด v หรือไม่ ในปี ค.ศ.1847 เคริดแมน ได้พิสูจน์ทฤษฎีบทต่อไปนี้

ทฤษฎีบท 9.5.2

ระบบไตรภาคแบบสไตน์เนอร์จะมี ก็ต่อเมื่อ $v = 3$ หรือ $v = 6n+1$ หรือ $v = 6n+3$ เมื่อ n เป็นจำนวนเต็มบวกใด ๆ

แบบฝึกหัด

1. จงแสดงให้เห็นว่ากลุ่มของเซตย่อยข้างล่างนี้เป็นบล็อกดีไซน์ไม่สมบูรณ์ และจงหา v, b, r, k และ λ

1 2 3	1 4 7	1 5 9	1 6 8
4 5 6	2 5 8	2 6 7	2 4 9
7 8 9	3 6 9	3 4 8	3 5 7

2. ในบล็อกดีไซน์หนึ่งมี

   ก. $v = 15, k = 10, \lambda = 9$ จงหา b และ r

   ข. $v = 47, b = 47, r = 9$ จงหา k และ λ

   ค. $b = 14, k = 3, \lambda = 2$ จงหา v และ r

3. จงแสดงให้เห็นว่า ไม่มีบล็อกดีไซน์ซึ่งสอดคล้องกับตัวแปรต่อไปนี้

   ก. $v = 5, b = 7, r = 4, k = 3, \lambda = 2$

   ข. $v = 22, b = 22, r = 7, k = 7, \lambda = 1$

4. จงพิจารณาว่าจะมี (12,6,8,7,1) - ดีไซน์ได้หรือไม่

5. จงพิจารณาว่าจะมี (12,6,12,6,1) - ดีไซน์ได้หรือไม่

6. จงแสดงให้เห็นว่าเมทริกซ์ข้างล่างนี้เป็นเมทริกซ์บังเกิดของบล็อกดีไซน์ และจงหาตัวแปรเสริมต่าง ๆ ที่เกี่ยวข้อง

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

7. จงเขียนเมทริกซ์บังเกิดของ (v,b,r,k,λ) - ดีไซน์ ต่อไปนี้

1	2	3	4	5	6	7	8	9	1	4	7
2	5	8	3	6	9	1	5	9	2	6	7
3	4	8	1	6	8	2	4	9	3	5	7

และจงตรวจสอบว่า v = 9 , b = 12 , r = 4 , k = 3 , λ = 1

8. จงหา A'A และ AA' ของระนาบเจ็ดจุด

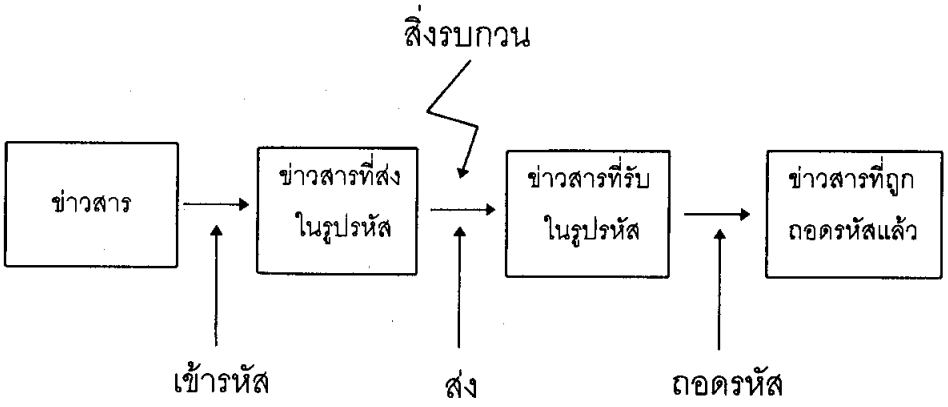
9. ในระบบไตรภาคแบบสไตน์เนอร์ซึ่งมีขนาด v = 9 จงหา b และ r

10. ถ้ามีระบบไตรภาคแบบสไตน์เนอร์ขนาด v = 63 อยากทราบว่า b จะมีขนาดเท่าใด

9.6 รหัสแก้ไขข้อผิดพลาด
Error-Correcting Codes

การส่งข่าวสาร (message) ในระยะทางไกล ๆ โดยผ่านช่องสื่อสาร (channel) ซึ่งอาจได้แก่ สายโทรศัพท์ คลื่นวิทยุ หรือผ่านดาวเทียม มักประสบกับสิ่งรบกวน (noise) อันอาจเป็นเหตุให้ข่าวสารที่ได้รับผิดไปจากข่าวสารที่ส่ง ตัวอย่างของสิ่งรบกวน ได้แก่ความผิดพลาดของมนุษย์ ความไม่สมบูรณ์ของเครื่องมือหรือสภาพดินฟ้าอากาศ เป็นต้น เราจึง

ควรมีวิธีสืบหาหรือตรวจจับ (detect) ว่าข่าวสารที่ได้รับนั้นมีข้อผิดพลาดหรือไม่ และถ้าเป็นไปได้เราควรแก้ไข (correct) ข่าวสารให้ถูกต้องได้ คำว่า **สืบหา** หรือ **ตรวจจับ** ในที่นี้หมายถึงสืบหรือบ่งบอกได้ว่ามีข้อผิดพลาดเกิดขึ้น แต่อาจจะบอกไม่ได้ว่าผิดที่ใด ระบบการสื่อสารโดยทั่วไปมีรูปแบบจำลองง่าย ๆ ดังนี้



โดยทั่วไปแล้วการสร้างรหัสมักจะเกิดจากการนำข่าวสารหรือข้อความที่จะส่งมาทำให้ยาวขึ้น เพื่อว่าเมื่อมีข้อผิดพลาดเกิดขึ้นผู้รับปลายทางสามารถรู้ได้ว่ามีข้อผิดพลาดเกิดขึ้น และถ้ารหัสที่สร้างสอดคล้องกับเงื่อนไขบางอย่างผู้รับปลายทางอาจแก้ไขข้อผิดพลาดได้ถ้าข่าวสารที่ได้รับนั้นมีข้อผิดพลาดไม่มากนัก จะเรียกขบวนการทำข่าวสารให้ยาวขึ้นนี้ว่าการเข้ารหัส (encoding) ซึ่งอาจทำโดยการส่งข่าวสารซ้ำ ๆ กันก็ได้

โดยปกติการส่งรหัส มักส่งในรูปรหัสทวิภาค (binary code) ซึ่งหมายถึงลำดับของเลข 0 และ 1 จะเรียกรหัสซึ่งคำรหัสแต่ละคำเป็นลำดับซึ่งมีความยาวเท่ากันว่า **รหัสแบบบล็อก** (block code) ในที่นี้เรา

จะกล่าวถึงเฉพาะรหัสแบบบล็อกเท่านั้น ดังนั้นจะละคำว่า **บล็อก** ไว้ ตัวอย่างของรหัสแบบบล็อก เช่น

001, 010, 011, 111

เป็นรหัสแบบบล็อกซึ่งมีคำรหัส 4 คำ แต่ละคำมีขนาด 3 นั่นคือมีความยาว 3 หลัก เป็นต้น

สมมุติว่ามีรหัสทวิภาคซึ่งประกอบด้วยคำรหัส 16 คำ แต่ละคำมีความยาว 4 หลัก นั่นคือมีรหัส

0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001,
0110, 0101, 0011, 1110, 1101, 1011, 0111, 1111

และสมมุติว่าข่าวสารที่ส่งคือ 1100 ซึ่งประกอบด้วย 4 หลัก สมมุติว่าผู้รับได้รับข่าวสารซึ่งประกอบด้วยเลข 4 หลักเช่นกัน ผู้รับจะไม่มีทางรู้เลยว่าเลขทั้ง 4 หลักที่ได้รับมานั้นมีข้อผิดพลาดหรือไม่ เช่น ถ้าผู้รับได้รับ 1000 ซึ่งเป็นคำรหัสด้วย ดังนั้นผู้รับจะคิดว่าข่าวสารที่ส่งมาคือ 1000 ไม่ตรงกับ 1100 ที่ส่ง แต่ถ้าเราส่งข่าวสารโดยส่งแต่ละคำรหัสซ้ำกันสองครั้ง คือแทนที่จะส่ง 1100 เราจะส่ง 1100 1100 ซึ่งมี 8 หลัก ในกรณีนี้ผู้รับข่าวสารสามารถสืบหาหรือตรวจจับได้ว่ารหัสที่ไดรับมีข้อผิดพลาดหรือไม่ เช่น ถ้าข่าวสารที่ได้รับเป็นดังนี้ 1100 0100 จะเห็นว่าเลข 4 หลักแรกแตกต่างไปจากเลข 4 หลักที่สอง ดังนั้นเราพอจะบอกได้ว่ามีข้อผิดพลาดเกิดขึ้น เพราะถ้าไม่มีข้อผิดพลาดแล้วเลขทั้งสองกลุ่มจะต้องเหมือนกัน แต่ไม่สามารถบอกได้ว่าผิดที่ใด อาจจะผิดทั้งสองกลุ่มเลยก็ได้ เช่น ส่ง 0011 0011 แต่ผู้รับได้รับ 0010 0010 เลข 4 หลักแรกเหมือนกับ 4 หลักสุดท้าย ดังนั้น ผู้รับอาจจะคิดว่าคำที่ส่งคือ 0010 0010 ในกรณีนี้เราไม่อาจรู้ว่ามีข้อผิดพลาดเกิดขึ้นหรือไม่ แต่ถ้าโอกาสที่เลข

แต่ละหลักจะผิดพลาดมีน้อย เหตุการณ์ที่จะผิดเหมือนกันทั้งสองกลุ่มจะเป็นไปได้น้อยมาก

ถ้าส่งข่าวสารแต่ละคำซ้ำกัน 3 ครั้ง เช่นถ้า 1100 ถูกส่งซ้ำกัน 3 ครั้งคำรหัสที่ส่งจะเป็น

1100 1100 1100

สมมุติว่าข่าวสารที่ได้รับคือ

0100 1100 1100

จะเห็นว่ากลุ่มแรกผิดไปจากกลุ่มที่สองและกลุ่มที่สาม แสดงว่ามีข้อผิดพลาดเกิดขึ้น นอกจากนี้เรายังสามารถแก้ไขให้ถูกต้องได้ โดยแก้กลุ่มแรกจาก 0100 เป็น 1100 ทั้งที่เนื่องจากเลขสองกลุ่มหลังเหมือนกันคือ 1100 โอกาสที่เลขสองกลุ่มจะผิดเหมือนกันจะมีโอกาสน้อยกว่าที่เลขกลุ่มหนึ่งจะผิด ด้วยเหตุนี้เราพอจะสรุปได้ว่าจำนวนครั้งที่จะส่งซ้ำกันนั้นควรจะเป็นจำนวนคี่ แต่ถ้าส่งซ้ำกันมากครั้งเกินไป รหัสที่ส่งจะยาว ทำให้เสียเวลาและสิ้นเปลืองค่าส่งมาก

การสร้างรหัสที่ดีจะต้องหลีกเลี่ยงการสร้างรหัสซึ่งมีคำรหัสใกล้เคียงกันมาก ๆ คำว่า **ใกล้เคียงกัน** ในที่นี้หมายถึงเมื่อมีข้อผิดพลาดเพียงเล็กน้อยเกิดขึ้น ทำให้ข่าวสารที่รับเหมือนกับคำรหัสหนึ่งซึ่งไม่ใช่คำรหัสที่ส่ง อาจทำให้ผู้รับเข้าใจผิดได้ เช่นในตัวอย่างของรหัสที่มีความยาวเท่ากับ 4 ข้างบนนี้ ดังนั้นในการสร้างรหัสเราควรสร้างให้คำรหัสแต่ละคำห่างกันพอสมควร เช่น สมมุติว่ามีคำรหัสอยู่ 4 คำ คือ

000000, 010101, 101010, 111111

สมมุติว่าคำแรกถูกส่ง แต่คำที่ได้รับคือ 000001 ซึ่งผิดไปหนึ่งตำแหน่ง เราสามารถบอกได้ว่ามีข้อผิดพลาดเกิดขึ้น นั่นคือ กรณีนี้เรากล่าวว่ารหัสนี้มีความสามารถในการตรวจจับข้อผิดพลาดได้ ทั้งนี้เนื่องจาก

000001 ไม่ใช่คำรหัสใดเลย ถ้าถามว่าคำรหัสที่ส่งควรเป็นคำรหัสใด คำตอบคือ คำรหัสที่ส่งน่าจะเป็น 000000 เพราะนั่นแสดงว่ามีข้อผิดพลาดเกิดขึ้นเพียงตำแหน่งเดียวเท่านั้น ผู้รับไม่น่าจะเดาว่าคำรหัสที่ส่งคือ 010101 เพราะนั่นแสดงว่าต้องมีข้อผิดพลาดถึงสองตำแหน่ง นั่นคือ ข่าวสาร 000001 ที่ได้รับจะใกล้กับคำรหัส 000000 มากกว่าคำรหัส 010101 ดังนั้นเราให้คำจำกัดความของระยะระหว่างคำว่า คือจำนวนตำแหน่งที่แตกต่างกัน เช่น ระยะระหว่างคำรหัส 000000 และ 010101 คือ 3 และจะเขียนแทนด้วย

$$d(000000, 010101) = 3$$

เรียกระยะดังกล่าวนี้ว่าระยะแฮมมิง (Hamming distance)

เราจะนำแนวความคิดเกี่ยวกับเมทริกซ์บังเกิดของ (v,k,λ) -ดีไซน์มาช่วยในการสร้างรหัส ถ้า A เป็นเมทริกซ์บังเกิดของ (v,k,λ) - ดีไซน์ เราจะพบว่าแต่ละแถวของเมทริกซ์ A มีความยาวเท่ากับ v และประกอบด้วยเลข 1 เป็นจำนวน k ตัว เพราะสมาชิกแต่ละตัวปรากฏ r ($r = k$) ครั้งเท่ากัน ที่เหลือนอกนั้นเป็นเลข 0 ถ้าพิจารณาแถวสองแถวใด ๆ ของเมทริกซ์ A จะพบว่ามีเลข 1 ปรากฏอยู่ในคอลัมน์เดียวกันเป็นจำนวน λ คอลัมน์ แสดงว่าจะต้องมี $2(k - \lambda)$ คอลัมน์ที่เลขในสองแถวนั้นแตกต่างกัน (ดูแผนผังข้างล่างนี้ประกอบ)

1 1 1	1 1 1	0 0 0	0 0 0
1 1 1	0 0 0	1 1 1	0 0 0
$\underbrace{\quad}_{\lambda}$	$\underbrace{\quad}_{k-\lambda}$	$\underbrace{\quad}_{k-\lambda}$	$\underbrace{\quad}_{v-2(k-\lambda)-\lambda}$

ดังนั้น ถ้าเราใช้แต่ละแถวของเมทริกซ์ A เป็นคำรหัส เราจะได้คำรหัสซึ่งมีความยาวเท่ากับ v และระยะห่างระหว่างคำรหัสเท่ากับ $2(k - \lambda)$

สมมุติว่ามีเซตของคำรหัส ซึ่งระยะห่างระหว่างคำรหัสที่น้อยที่สุดเท่ากับ d เราสามารถจะตรวจจับข้อผิดพลาดได้ถึง d-1 ตำแหน่ง หมายความว่าถ้าคำรหัสที่รับมีข้อผิดพลาด d-1 ตำแหน่งหรือน้อยกว่าแล้ว เราสามารถบอกได้ว่ามีข้อผิดพลาดเกิดขึ้น เพราะคำที่ได้รับนั้นจะไม่ตรงกับคำรหัสใดเลย นอกจากนี้เรายังสามารถแก้ไขข้อผิดพลาดได้ถ้าคำที่รับนั้นมีข้อผิดพลาดน้อยกว่า d/2 ตำแหน่ง ทั้งนี้เนื่องจากคำที่ได้รับนั้นจะใกล้กับคำรหัสใดคำหนึ่ง ดังนั้น ผู้รับสามารถเดาได้ว่าคำรหัสที่ส่งคือคำรหัสที่ใกล้เคียงที่สุดกับคำที่รับ เราจะเรียกรหัสซึ่งสามารถแก้ไขข้อผิดพลาดได้ถึง t ตำแหน่งว่า **รหัสแก้ไขข้อผิดพลาด** -t (t-error-correcting code) จากที่กล่าวมาทั้งหมดนี้พอจะสรุปได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 9.6.1

รหัสจะเป็นรหัสซึ่งสืบหาข้อผิดพลาดได้ถึง d-1 ตำแหน่ง ถ้าระยะระหว่างคำรหัสที่น้อยที่สุดเท่ากับ d

ทฤษฎีบท 9.6.2

รหัสจะเป็นรหัสแก้ไขข้อผิดพลาดได้ถึง t ตำแหน่ง ถ้าระยะระหว่างคำรหัสที่น้อยที่สุดเท่ากับ 2t+1

ทฤษฎีบท 9.6.3

ให้ A เป็นเมทริกซ์บังเกิดของ (v,k,λ) -ดีไซน์ ถ้าใช้แต่ละแถวของเมทริกซ์ A เป็นคำรหัส จะได้รหัสแก้ไขข้อผิดพลาด-t เมื่อ t = k-λ-1

พิสูจน์ เนื่องจากสองแถวใด ๆ ของเมทริกซ์ A แตกต่างกัน $2(k-\lambda)$ ตำแหน่ง ดังนั้น รหัสที่ได้จะแก้ไขข้อผิดพลาดได้ถึง

$$\frac{2(k-\lambda)}{2} - 1 = k - \lambda - 1$$

ตำแหน่ง นั่นคือรหัสที่ได้จะเป็นรหัสแก้ไขข้อผิดพลาด -t เมื่อ $t = k-\lambda-1$

ตัวอย่าง 9.6.1 พิจารณาระนาบ 7 จุดหรือ (7,3,1) - ดีไซน์ ในตัวอย่าง 9.3.1 เมทริกซ์บังเกิดของ (7,3,1) - ดีไซน์คือ

$$\begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}$$

ให้ A คือเมทริกซ์บังเกิดข้างบนนี้ ถ้าใช้แต่ละแถวของเมทริกซ์ A เป็นคำรหัส เราจะได้รหัสซึ่งประกอบด้วยคำรหัส 7 คำ สองแถวใด ๆ ของ A จะแตกต่างกัน

$$2(k - \lambda) = 2(3 - 1) = 4$$

ตำแหน่ง ดังนั้นรหัสที่ได้สามารถตรวจจับข้อผิดพลาดได้ถึง 3 ตำแหน่ง นอกจากนี้ $k - \lambda - 1 = 3 - 1 - 1 = 1$ ดังนั้น รหัสที่ได้จะเป็นรหัสที่มีความสามารถแก้ไขข้อผิดพลาดได้หนึ่งตำแหน่ง นั่นคือ เมื่อมีข้อผิดพลาดเพียงหนึ่งตำแหน่ง เราสามารถแก้ไขให้ถูกต้องได้

แบบฝึกหัด

1. จงหาระยะแฮมมิงระหว่างคำรหัส x และ y ในแต่ละข้อต่อไปนี้

ก. x = 110010, y = 0101010
ข. x = 1001000, y = 10100101
ค. x = 111111000, y = 001001001

2. จากรหัส C ที่กำหนดให้ต่อไปนี้ จงหาจำนวนข้อผิดพลาดที่รหัส C สามารถตรวจจับและแก้ไขได้
ก. C = { 0000000, 1111110, 1010100, 0101010 }
ข. C = { 0000000, 0001111, 1110000, 0000111 }
ค. C = { 000000, 000111, 010101, 101010, 111000, 111111 }