บทที่ 4

รูปแบบทั่วไปของการแปลงให้อยู่ในรูปน้ำหนักต่ำสุดแบบเชื่อมตรง

ในบทนี้จะกล่าวถึงรูปแบบทั่วไปของการแปลงให้อยู่ในรูปน้ำหนักต่ำสุดแบบเชื่อมตรงภายใต้ระบบจำนวนฐาน β โดยที่ β เป็นจำนวนเต็มที่มีค่ามากกว่าหรือเท่ากับสอง โดยได้เสนออัลกอริทึมที่ 4.1 ซึ่งมีความหน่วงในการทำงานเป็นสอง และอัลกอริทึมที่ 4.2 สำหรับการคูณสเกลาร์ในระบบจำนวนฐาน β ภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยตัวดำเนินการที่ใช้ในการคูณสเกลาร์จะเปลี่ยนไปตามระบบฐาน β ที่ใช้ และมีจำนวนของตัวดำเนินการเท่ากับ $\beta+2$

4.1 การแปลงให้อยู่ในรูปน้ำหนักต่ำสุดภายใต้ระบบจำนวนฐาน β

ในการแปลงให้อยู่ในรูปน้ำหนักต่ำสุด จะต้องใช้ค่านำเข้าที่มีความกำกวมเพื่อให้สามารถแปลงให้อยู่ในรูปอื่นที่อาจให้ค่าน้ำหนักที่ต่ำกว่าได้ ซึ่งในที่นี้จะกำหนดให้เป็นเซตตัวเลข $\{\bar{1},0,\ldots,(\beta-1)\}$ แล้วผลลัพธ์ที่ได้จะอยู่ในรูปน้ำหนักต่ำภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ ซึ่งจะกำหนดให้มีความหน่วงคงที่เป็นสอง และดำเนินการภายใต้ระบบจำนวนฐาน β

จุดมุ่งหมายหลักของการแปลงนั้นคือลดค่าน้ำหนักของระบบจำนวนฐาน β กล่าวคือลดจำนวนบิตที่ไม่ใช่ศูนย์โดยการแปลงให้อยู่ในรูปอื่นที่มีค่าน้ำหนักน้อยกว่า แต่ต้องมีค่าคงเหลือเชิงตัวเลขเท่าเดิม โดยมีรูปแบบทั่วไปที่ใช้ในการแปลงค่าดังนี้

กำหนดให้เครื่องหมาย $\rightarrow$ แทนทิศทางการแปลงรูปจากทางด้านซ้ายไปด้านขวา และ β เป็นจำนวนเต็มที่มีค่ามากกว่าหรือเท่ากับสอง

$\bar{1}(\beta-1)\rightarrow 0\bar{1}$	มีค่าคงเหลือเชิงตัวเลขเป็น $\bar{1}$
$1\bar{1}\rightarrow 0(\beta-1)$	มีค่าคงเหลือเชิงตัวเลขเป็น $\beta-1$
$\bar{1}(\beta-1)\bar{1}\rightarrow 00(\overline{\beta+1})$	มีค่าคงเหลือเชิงตัวเลขเป็น $(\overline{\beta+1})$
$\bar{1}(\beta-2)(\beta-1)\rightarrow 00(\overline{\beta+1})$	มีค่าคงเหลือเชิงตัวเลขเป็น $(\overline{\beta+1})$

การทำงานจะเริ่มต้นจากบิตแรกซ้ายสุด โดยทำการแปลงค่าตัวเลขตามกฎ ถ้าไม่เข้าตามกฎก็จัดเก็บบิตซ้ายสุดตามค่าเดิม แล้วอ่านบิตเพิ่มทางขวาเพื่อเปรียบเทียบตามกฎทำซ้ำจนครบทุกบิตนำเข้า

ทฤษฎีบทที่ 4.1 *การแปลงจำนวนให้มีน้ำหนักต่ำสุดในระบบจำนวนฐาน* β *เมื่อ* $\beta \geq 2$ *สามารถทำได้แบบเชื่อมตรงภายใต้เซตตัวเลข* $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ *ด้วยความหน่วงเป็นสอง*

บทพิสูจน์ จะพิสูจน์โดยการเสนออัลกอริทึมการแปลงจำนวน อัลกอริทึมที่ 4.1

อัลกอริทึมที่ 4.1 อัลกอริทึมการแปลงจำนวนให้อยู่ในระบบจำนวนฐาน β ที่มีน้ำหนักต่ำสุด

นำเข้า: ระบบจำนวนฐาน β : $\mu_J,...,\mu_0$ เมื่อ $\mu \in \{\bar{1},0,\ldots,(\beta-1)\}$ โดยที่ $\beta \geq 2$

นำออก: ระบบจำนวนฐาน β : $\omega_J,...,\omega_0$ เมื่อ $\omega \in \{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยที่ $\beta \geq 2$

$\mu_{-1},\mu_{-2} \leftarrow 0$

$I \leftarrow J-2$

$C_1 \leftarrow \mu_J$

$C_2 \leftarrow \mu_{J-1}$

while $J \geq 0$ do

    $T \leftarrow (C_1 \times \beta)+C_2$

    if $T=\bar{1}$ or $T=\beta-1$ then

        $C_1 \leftarrow 0$

        $C_2 \leftarrow T$

    end if

    $C_3 \leftarrow \mu_I$

    $S \leftarrow (T \times \beta)+C_3$

    if $S=(\overline{\beta+1})$ then

        $\omega_J \leftarrow 0$

        $C_1 \leftarrow 0$

        $C_2 \leftarrow S$

    else if $S=\bar{1}$ or $S=\beta-1$ then

        $\omega_J \leftarrow C_1$

        $C_1 \leftarrow 0$

        $C_2 \leftarrow S$

    else

        $\omega_J \leftarrow C_1$

        $C_1 \leftarrow C_2$

        $C_2 \leftarrow C_3$

    end if

    $J \leftarrow J-1$

    $I \leftarrow I-1$

end while

พิสูจน์อัลกอริทึม อัลกอริทึมที่ 4.1 ให้ค่าผลลัพธ์ที่ถูกต้อง และผลลัพธ์มีค่าน้ำหนักต่ำสุด สำหรับทุกค่านำเข้า $(\mu_J,...,\mu_0)_\beta$ เมื่อ $\mu \in \{\bar{1},0,\ldots,(\beta-1)\}$ และได้ค่านำออกเป็น $(\omega_J,...,\omega_0)_\beta$ $\omega \in \{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ ภายใต้ความหน่วงของการทำงานเป็นสอง

จาก $S \leftarrow (T \times \beta)+C_3$ โดยที่ $T \leftarrow (C_1 \times \beta)+C_2$ ค่า C_1 คือบิตทางซ้ายสุด และ C_2 คือบิตถัดมา ซึ่งทั้งสองบิตดังกล่าวถูกอ่านค่าเก็บไว้ตามความหน่วงสอง และ $C_3 \leftarrow \mu_I$ ซึ่งเป็นค่านำเข้าปัจจุบัน จะได้ว่าค่า S คือค่าเชิงตัวเลขคงเหลือในปัจจุบัน ซึ่งเป็นตัวกำหนดค่านำออก ω ที่มีค่าเชิงตัวเลขโดยรวมเท่ากันกับ μ ตามเงื่อนไขดังต่อไปนี้

1) $\bar{1}(\beta-1) \rightarrow 0\bar{1}$ มีค่าคงเหลือเชิงตัวเลขเป็น $\bar{1}$
2) $1\bar{1} \rightarrow 0(\beta-1)$ มีค่าคงเหลือเชิงตัวเลขเป็น $\beta-1$
3) $\bar{1}(\beta-1)\bar{1} \rightarrow 00(\overline{\beta+1})$ มีค่าคงเหลือเชิงตัวเลขเป็น $(\overline{\beta+1})$
4) $\bar{1}(\beta-2)(\beta-1) \rightarrow 00(\overline{\beta+1})$ มีค่าคงเหลือเชิงตัวเลขเป็น $(\overline{\beta+1})$
5) หากไม่สามารถแปลงได้ตามกฎก็ให้นำออกบิตซ้ายสุดตามค่าเดิมแล้วอ่านบิตใหม่เพิ่มทางขวาเข้ามาเพื่อเทียบ

นั่นคือ ผลลัพธ์ที่ได้หลังการแปลงจะมีค่าเชิงตัวเลขเท่ากันกับค่าตั้งต้น และมีค่าน้ำหนักต่ำสุด ภายใต้ระบบจำนวนฐาน β ด้วยเซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ เมื่อกำหนดความหน่วงของการทำงานคงที่คือสอง ■

ตัวอย่างที่ 4.1 *การแปลงจำนวนด้วยอัลกอริทึมที่ 4.1 เมื่อกำหนด* $\beta=3$
จาก $\beta=3$ จะได้ว่า $\mu \in \{\bar{1},0,1,2\}$ และ $\omega \in \{\bar{4},\bar{1},0,1,2\}$ กำหนด $k=293$ จะได้ $k=(11\bar{1}\bar{1}12)_3$ ขั้นตอนการทำงานตามอัลกอริทึมที่ 4.1 ได้แสดงไว้ดังตารางที่ 4.1

ตารางที่ 4.1 ตารางการแปลง $k=293$ ด้วยอัลกอริทึมที่ 4.1

J	I	C_1	C_2	$T \leftarrow (C_1 \times \beta)+C_2$	$C_3 \leftarrow \mu_I$	$S \leftarrow (T \times \beta)+C_3$	ω_J
5	3	1	1	4	$\bar{1}$	11	1
4	2	0	2	2	$\bar{1}$	5	0
3	1	2	$\bar{1}$	5	1	16	2
2	0	$\bar{1}$	1	$\bar{2}$	2	$\bar{4}$	0
1	$\bar{1}$	0	$\bar{4}$	$\bar{4}$	0	$\bar{1}\bar{2}$	0
0	$\bar{2}$	$\bar{4}$	0	$\bar{1}\bar{2}$	0	$\bar{3}\bar{6}$	$\bar{4}$

ดังนั้นจะได้จำนวนฐานสาม $\omega_J,...,\omega_0$ เมื่อ $\omega \in \{\bar{4},\bar{1},0,1,2\}$ คือ $(10200\bar{4})_3$ □

4.2 การคูณสเกลาร์ด้วยวิธีการของชามีร์ภายใต้ระบบจำนวนฐาน β

การคูณสเกลาร์ในระบบจำนวนฐาน β สามารถกระทำได้อย่างเป็นลำดับต่อเนื่องจากซ้ายไปขวา ภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยตัวดำเนินการที่ใช้ในการคูณสเกลาร์จะเปลี่ยนไปตามระบบฐาน β ที่ใช้ และมีจำนวนของตัวดำเนินการเท่ากับ $\beta+2$

ทฤษฎีบทที่ 4.2 *การคูณสเกลาร์สามารถทำได้อย่างเป็นลำดับต่อเนื่องจากซ้ายไปขวาด้วยเซตตัวเลข* $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ *ในระบบจำนวนฐาน* β *เมื่อ* $\beta\geq 2$

บทพิสูจน์ จะพิสูจน์โดยการเสนออัลกอริทึมการคูณสเกลาร์ อัลกอริทึมที่ 4.2

อัลกอริทึมที่ 4.2 อัลกอริทึมการคูณสเกลาร์ภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ ฐาน β

นำเข้า: ระบบจำนวนฐาน β : $\omega_J,\ldots,\omega_0$ เมื่อ $\omega\in\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยที่ $\beta\geq 2$

นำออก: ผลการคูณสเกลาร์ $G=kP$

$G\leftarrow 0$
while $J\geq 0$ do
    $G\leftarrow \beta\times G$
    $k\leftarrow \omega_J$
    if $k=0$ then
        $G\leftarrow G$
    else /* $k\in\{(\overline{\beta+1}),\bar{1},1,\ldots,(\beta-1)\}$ */
        $G\leftarrow G+kP$
    end if
    $J\leftarrow J-1$
end while

พิสูจน์อัลกอริทึม อัลกอริทึมที่ 4.2 ให้ค่าผลลัพธ์ที่ถูกต้องเสมอ โดยจะแสดงรูปแบบทั่วไปของทุกตัวดำเนินการ ดังในตารางที่ 4.2 (หมายเหตุ x จะปรากฏได้เพียงหนึ่งครั้งในแต่ละค่า J)

ตารางที่ 4.2 ตารางทั่วไปในการคูณสเกลาร์สำหรับระบบจำนวนฐาน β

J	$k\leftarrow\omega_J$	$G\leftarrow operator$					
		β	$(\beta-1)P$	.....	$+P$	$-P$	$(\overline{\beta+1})P$
J	ω_J	0	x	.....	x	x	x
$\vdots$	$\vdots$	$\vdots$	x	.....	x	x	x
0	ω_0	x	x	.....	x	x	x

จากอัลกอริทึมที่ 4.2 และตารางที่ 4.2 ได้แสดงให้เห็นถึงขั้นตอนการคูณสเกลาร์พร้อมทั้งแสดงตัวดำเนินการทั้งหมดของแต่ละฐาน β ที่จำเป็นต้องมี เพื่อใช้ในการคูณสเกลาร์ในแต่ละฐาน β ที่กำหนด โดยการทำงานจะเริ่มต้นจากรอบที่ J ลดลงที่ละหนึ่งจนถึงรอบที่ศูนย์เป็นรอบสุดท้าย ดังนี้

กำหนดให้ G มีค่าตั้งต้นเป็นศูนย์ จะมีการเรียกใช้ตัวดำเนินการในแต่ละรอบ ดังนี้

รอบที่ J อ่าน $k \leftarrow \omega_J$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$
รอบที่ $J-1$ อ่าน $k \leftarrow \omega_{J-1}$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$
รอบที่ $J-2$ อ่าน $k \leftarrow \omega_{J-2}$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$
$\vdots$ $\vdots$ $\vdots$
รอบที่ 2 อ่าน $k \leftarrow \omega_2$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$
รอบที่ 1 อ่าน $k \leftarrow \omega_1$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$
รอบที่ 0 อ่าน $k \leftarrow \omega_0$ มีการเรียกใช้ตัวดำเนินการคือ $G \leftarrow \beta \times G$ และ $G \leftarrow G + kP$

สามารถเขียนรูปการทำงานทั่วไปคือ $G = \left(\sum_{i=0}^{J} \omega_{J-i} \beta^{J-i} \right) P$ ซึ่งก็คือ $G = kP$ นั่นเอง ■

ตัวอย่างที่ 4.2 *การคูณสเกลาร์ด้วยอัลกอริทึมที่ 4.2 เมื่อกำหนด* $\beta = 3$

จาก $\beta = 3$ กำหนดให้ $\omega_J, ..., \omega_0 = (10200\bar{4})_3$ โดยที่ $\omega \in \{\bar{4}, \bar{1}, 0, 1, 2\}$ จะได้ขั้นตอนการทำงานตามอัลกอริทึมที่ 4.2 ได้แสดงไว้ดังตารางที่ 4.3

ตารางที่ 4.3 การคูณสเกลาร์ภายใต้ระบบจำนวนฐานสามเพื่อหา $293P$

J	$k \leftarrow \omega_J$	$G \leftarrow operator$				
		tripple	$+2P$	$+P$	$-P$	$-4P$
5	1	0	-	P	-	-
4	0	$3P$	-	-	-	-
3	2	$9P$	$11P$	-	-	-
2	0	$33P$	-	-	-	-
1	0	$99P$	-	-	-	-
0	$\bar{4}$	$297P$	-	-	-	$293P$

จากตารางที่ 4.3 มีการเรียกใช้ตัวดำเนินการ *tripple* ทั้งหมดหกครั้ง แต่เนื่องจากกำหนดค่าเริ่มต้นให้ G เป็นศูนย์จึงไม่นับรวมครั้งแรก คงเหลือทั้งหมดห้าครั้ง และเรียกใช้ตัวดำเนินการ $+2P$, $+P$ และ $-4P$ อย่างละหนึ่งครั้ง รวมทั้งสิ้นมีการเรียกใช้ตัวดำเนินการทั้งหมดแปดครั้ง □

4.3 สรุป

การแปลงให้อยู่ในรูปน้ำหนักต่ำสุดสำหรับระบบจำนวนฐาน β โดยที่ β เป็นจำนวนเต็มที่มากกว่าหรือเท่ากับสอง สามารถทำได้แบบเชื่อมตรงด้วยความหน่วงเป็นสอง ซึ่งผลลัพธ์ที่ได้จะมีเซตตัวเลขเป็น $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ และต้องมีตัวดำเนินการจำนวน $\beta+2$ ตัว เพื่อรองรับการคูณสเกลาร์ภายใต้เซตตัวเลขดังกล่าว โดยมีความซับซ้อนเชิงเวลาคือ $\Theta(n)$ เมื่อ n คือขนาดของจำนวนนำเข้า