รายงานวิจัยฉบับสมบูรณ์

ขั้นตอนวิธีการเข้ารหัสและถอดรหัสที่ขึ้นอยู่กับจำนวนจาคอบส์ทัล

An Encoding-Decoding Algorithm based on Jacobsthal Numbers

โดย

นายสมคิด อินเทพ

นายบุญยงค์ ศรีพลแผ้ว

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์

โครงการวิจัยประเภทงบประมาณเงินรายได้ส่วนงาน

ประจำปีงบประมาณ พ.ศ. ๒๕๖๓

คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา

รหัสโครงการ.....

สัญญาเลขที่ sc02/2563

รายงานวิจัยฉบับสมบูรณ์

ขั้นตอนวิธีการเข้ารหัสและถอดรหัสที่ขึ้นอยู่กับจำนวนจาคอบส์ทัล

An Encoding-Decoding Algorithm based on Jacobsthal Numbers

โดย

นายสมคิด อินเทพ

นายบุญยงค์ ศรีพลแผ้ว

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนสนับสนุนการวิจัยจากงบประมาณเงินรายได้ส่วนงาน ประจำปีงบประมาณ พ.ศ. 2563 คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา เลขที่สัญญา sc02/2563

นายสมคิด อินเทพ

นายบุญยงค์ ศรีพลแผ้ว

ผู้วิจัย

บทคัดย่อ

ชื่อโครงการ ขั้นตอนวิธีการเข้ารหัสและถอดรหัสที่ขึ้นอยู่กับจำนวนจาคอบส์ทัล

ชื่อผู้วิจัย นายสมคิด อินเทพ และนายบุญยงค์ ศรีพลแผ้ว

เราแนะนำ Q-เมทริกซ์ จากจำนวน c-Jacobsthal และวิธีเข้ารหัสและถอดรหัสจาก Q-เมทริกซ์ นอกจากนั้น เราได้ทำการสร้างความสัมพันธ์ระหว่างสมาชิกของเมทริกซ์รหัส การตรวจจับและการแก้ไขข้อผิดพลาดสำหรับทฤษฎีรหัสนี้ ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัส คือ 93.33%

Abstract

Project Title: An Encoding-Decoding algorithm based on Jacobsthal numbers

Investigators: Somkid Intep and Boonyong Sriponpeaw

We introduce Q-matrix from c-Jacobsthal numbers and a method for coding and decoding messages from this Q-matrix. In addition, we construct the relations between the code matrix elements, error detection and correction for this coding theory. Correction ability of this method is 93.33%.

สารบัญ

บทที่ 1
บทนำ

1.1 ความสำคัญและสรุปความเป็นมาของโครงการฯ

ทฤษฎีการถอดรหัส (Coding theory) เป็นการศึกษาคุณสมบัติของรหัสและนำไปปรับใช้อย่างเหมาะสม เพื่อให้เข้ากับสถานการณ์ต่าง ๆ ไม่ว่าจะเป็นการบีบอัดข้อมูล วิทยาการเข้ารหัสลับ การตรวจหาและแก้ไขข้อผิดพลาดการส่งและการเก็บข้อมูล รหัสจะถูกนำไปใช้ประโยชน์ในสาขาวิชาต่าง ๆ เช่น ทฤษฎีสารสนเทศ วิศวกรรมไฟฟ้า ภาษาศาสตร์ และวิทยาการคอมพิวเตอร์

ในทุกวันนี้ ความปลอดภัยของข้อมูลกลายเป็นสิ่งสำคัญมากขึ้น ในแง่การส่งข้อมูลผ่านทางช่องทางการสื่อสาร ขั้นตอนวิธีการเข้าและถอดรหัสเป็นสิ่งที่สำคัญมากที่จะช่วยในการเพิ่มความปลอดภัยของข้อมูล ซึ่งได้มีนักคณิตศาสตร์ได้เริ่มนำจำนวนสำคัญทางคณิตศาสตร์มาประยุกต์ในการสร้างทฤษฎีการเข้าและถอดรหัส ในปี 2006, Stakov (2006) ได้เสนอทฤษฎีรหัสตัวใหม่ที่สร้างจากเมทริกซ์ของฟิโบนักชี (Fibonacci matrix) ในปี 2009, Basu และ Prasad (2009) ได้เสนอความสัมพันธ์ทั่วไประหว่างสมาชิกของเมทริกซ์รหัสสำหรับทฤษฎีรหัสของฟิโบนักชี ต่อมามีนักคณิตศาสตร์หลายท่านได้พัฒนาทฤษฎีรหัสบนจำนวนอื่น ๆ ทางคณิตศาสตร์ซึ่งทำให้ขั้นตอนวิธีการเข้าและถอดรหัสมีความปลอดภัยมากขึ้น (อาทิเช่น (Basu & Das, 2014a; Basu & Das, 2014b; Tas, Ucar, & Ozgur, 2017; Prasad, 2016))

ในงานวิจัยนี้ เราจะประยุกต์ใช้จำนวนจาคอบส์ทัลอันดับ k ((k,c)-Jacobsthal number) มาเป็นตัวสร้างทฤษฎีการเข้าและการถอดรหัสตัวใหม่ พร้อมทั้งแสดงถึงการคำนวณการตรวจสอบข้อผิดพลาดและแสดงถึงค่าความถูกต้องของการใช้รหัสด้วย

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อสร้างทฤษฎีรหัสจากจำนวนจาคอบส์ทัลอันดับ k
2. เพื่อตรวจสอบข้อผิดพลาดและแสดงถึงค่าความถูกต้องของการเข้าและถอดรหัสที่เกิดจากจำนวนจาคอบส์ทัลอันดับ k

1.3 ขอบเขตของการวิจัย

ในการทำวิจัยนี้ เราจะสร้างทฤษฎีรหัสจากจำนวนจาคอบส์ทัลอันดับ k โดยใช้การแบ่งข้อความออกเป็นรูปแบบของเมทริกซ์อันดับ k และใช้เมทริกซ์สร้างรหัสจากการยกกำลังที่เหมาะสมของเมทริกซ์ที่เกิดจากจำนวนจาคอบส์ทัลอันดับ k และใช้เมทริกซ์อินเวอร์สของเมทริกซ์ดังกล่าวเป็นตัวดำเนินการในการถอดรหัส ทำการตรวจสอบข้อผิดพลาดโดยใช้สมการพีชคณิตที่เกิดจากค่าดีเทอร์มิแนนต์ของเมทริกซ์และคำนวณค่าความน่าจะเป็นของความถูกต้องของการเข้าและถอดรหัสที่เกิดจากจำนวนจาคอบส์ทัลอันดับ k

บทที่ 2

วิธีการดำเนินการวิจัย

ในโครงการวิจัย เรื่อง ขั้นตอนวิธีการเข้ารหัสและถอดรหัสที่ขึ้นอยู่กับจำนวนจาคอบส์ทัล นี้ ผู้วิจัยมีขั้นตอนวิธีการดำเนินการวิจัย ดังนี้

1. ทำการศึกษาทฤษฎีการสร้างรหัสโดยใช้จำนวนต่าง ๆ อาทิเช่น ฟิโบนักชี ไตรโบนักชี พาร์โดแวน เป็นต้น

2. ศึกษาความสัมพันธ์เวียนเกิดของจำนวนจาคอบส์ทัลอันดับ k พร้อมทั้งศึกษา Q-matrix และคุณสมบัติของ Q-matrix ที่เกิดจากจำนวนจาคอบส์ทัลอันดับ k

3. ทดลองสร้างทฤษฎีถอดรหัสของจำนวนจาคอบส์ทัลอันดับ k และทดลองหาค่าความผิดพลาด

บทที่ 3

ผลการวิจัย

จากความสัมพันธ์เวียนเกิดของลำดับ c-Jacobsthal อันดับ k (Marques & Trojovsky, 2019)

$$J_n = J_{n-1} + J_{n-2} + \cdots + c \cdot J_{n-k} \quad \text{สำหรับ } n \geq 2 \text{ และ } c > 0 \tag{1}$$

และมีค่าเริ่มต้นเป็น $J_{2-k} = J_{3-k} = \cdots = J_0 = 0,\ J_1 = 1$

เราสามารถนิยาม Q-เมทริกซ์ ได้ดังนี้

$$Q = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & c \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

ซึ่งเราสามารถเขียน Q-เมทริกซ์ ในรูปของจำนวน c-Jacobsthal ดังนี้

$$Q = \begin{bmatrix} J_k & J_{k-1} + J_{k-2} + \cdots + cJ_1 & J_{k-1} + J_{k-2} + \cdots + cJ_2 & \cdots & cJ_{k-1} \\ J_{k-1} & J_{k-2} + J_{k-3} + \cdots + cJ_0 & J_{k-2} + J_{k-3} + \cdots + cJ_1 & \cdots & cJ_{k-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ J_2 & J_1 + J_0 + \cdots + cJ_{3-k} & J_1 + J_0 + \cdots + cJ_{2-k} & \cdots & cJ_1 \\ J_1 & J_0 + J_{-1} + \cdots + cJ_{2-k} & J_0 + J_{-1} + \cdots + cJ_{1-k} & \cdots & cJ_0 \end{bmatrix}$$

โดยที่ $\det(Q) = (-1)^{k+1} c$

และกำลัง n ของเมทริกซ์ Q คือ

$$Q^n = \begin{bmatrix} J_{n+k-1} & J_{n+k-2} + J_{n+k-3} + \cdots + cJ_n & J_{n+k-2} + J_{n+k-3} + \cdots + cJ_{n+1} & \cdots & cJ_{n+k-2} \\ J_{n+k-2} & J_{n+k-3} + J_{n+k-4} + \cdots + cJ_{n-1} & J_{n+k-3} + J_{n+k-4} + \cdots + cJ_n & \cdots & cJ_{n+k-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ J_{n+1} & J_n + J_{n-1} + \cdots + cJ_{n-k+2} & J_n + J_{n-1} + \cdots + cJ_{n-k+1} & \cdots & cJ_n \\ J_n & J_{n-1} + J_{n-2} + \cdots + cJ_{n-k+1} & J_{n-1} + J_{n-2} + \cdots + cJ_{n-k} & \cdots & cJ_{n-1} \end{bmatrix}$$

และจะได้ $\det(Q^n) = (-1)^{n(k+1)} c^n$

ถ้าเราแทนค่าข้อความเริ่มต้นในรูปเมทริกซ์ไม่เอกฐานขนาด $k \times k$ ดังนี้

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1k} \\ m_{21} & m_{22} & \cdots & m_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ m_{k1} & m_{k2} & \cdots & m_{kk} \end{bmatrix}$$

โดยที่ m_{ij} เป็นจำนวนเต็มที่ไม่ติดลบ

และสำหรับจำนวนเต็มบวก n ใด ๆ เราสามารถทำการเข้ารหัส โดยการคูณด้วยเมทริกซ์ Q^n จากด้านขวา

$$M \times Q^n = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ e_{k1} & e_{k2} & \cdots & e_{kk} \end{bmatrix} = E$$

และส่งข้อความที่เป็นรหัสผ่านช่องทางการสื่อสาร และทำการถอดรหัส โดยการคูณเมทริกซ์ E ด้วย Q^{-n} ดังนี้

$$E \times Q^{-n} = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ e_{k1} & e_{k2} & \cdots & e_{kk} \end{bmatrix} \times Q^{-n} = M$$

ผลการวิจัย

เพื่อความสะดวกในการพิสูจน์เราทำการแสดงการพิสูจน์สมบัติพื้นฐานของค่า Q-เมทริกซ์ และค่าของลิมิตของสัดส่วน J_{n+1} และ J_n ดังนี้

ทฤษฎีบทที่ 1 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ และ $Q = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & c \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$ จะได้ว่า

$$Q^n = \begin{bmatrix} J_{n+k-1} & J_{n+k-2} + J_{n+k-3} + \cdots + cJ_n & J_{n+k-2} + J_{n+k-3} + \cdots + cJ_{n+1} & \cdots & cJ_{n+k-2} \\ J_{n+k-2} & J_{n+k-3} + J_{n+k-4} + \cdots + cJ_{n-1} & J_{n+k-3} + J_{n+k-4} + \cdots + cJ_n & \cdots & cJ_{n+k-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ J_{n+1} & J_n + J_{n-1} + \cdots + cJ_{n-k+2} & J_n + J_{n-1} + \cdots + cJ_{n-k+1} & \cdots & cJ_n \\ J_n & J_{n-1} + J_{n-2} + \cdots + cJ_{n-k+1} & J_{n-1} + J_{n-2} + \cdots + cJ_{n-k} & \cdots & cJ_{n-1} \end{bmatrix}$$

พิสูจน์ เราจะใช้วิธีการอุปนัยทางคณิตศาสตร์

<u>ขั้นฐาน</u>

$$Q = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & c \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} J_k & J_{k-1} + J_{k-2} + \cdots + cJ_1 & J_{k-1} + J_{k-2} + \cdots + cJ_2 & \cdots & cJ_{k-1} \\ J_{k-1} & J_{k-2} + J_{k-3} + \cdots + cJ_0 & J_{k-2} + J_{k-3} + \cdots + cJ_1 & \cdots & cJ_{k-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ J_2 & J_1 + J_0 + \cdots + cJ_{3-k} & J_1 + J_0 + \cdots + cJ_{2-k} & \cdots & cJ_1 \\ J_1 & J_0 + J_{-1} + \cdots + cJ_{2-k} & J_0 + J_{-1} + \cdots + cJ_{1-k} & \cdots & cJ_0 \end{bmatrix}$$

ดังนั้น ขั้นฐานเป็นจริง

<u>ขั้นอุปนัย</u> สมมติว่า

$$Q^j=\begin{bmatrix} J_{j+k-1} & J_{j+k-2}+J_{j+k-3}+\cdots+cJ_j & J_{j+k-2}+J_{j+k-3}+\cdots+cJ_{j+1} & \dots & cJ_{j+k-2} \\ J_{j+k-2} & J_{j+k-3}+J_{j+k-4}+\cdots+cJ_{j-1} & J_{j+k-3}+J_{j+k-4}+\cdots+cJ_j & \dots & cJ_{j+k-3} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ J_{j+1} & J_j+J_{j-1}+\cdots+cJ_{j-k+2} & J_j+J_{j-1}+\cdots+cJ_{j-k+1} & \dots & cJ_j \\ J_j & J_{j-1}+J_{j-2}+\cdots+cJ_{j-k+1} & J_{j-1}+J_{j-2}+\cdots+cJ_{j-k} & \dots & cJ_{j-1} \end{bmatrix}$$

ดังนั้น

$$Q^{j+1}=Q^jQ$$

$$=\begin{bmatrix} J_{j+k-1} & J_{j+k-2}+J_{j+k-3}+\cdots+cJ_j & \dots & cJ_{j+k-2} \\ J_{j+k-2} & J_{j+k-3}+J_{j+k-4}+\cdots+cJ_{j-1} & \dots & cJ_{j+k-3} \\ \vdots & \vdots & \vdots & \vdots \\ J_j & J_{j-1}+J_{j-2}+\cdots+cJ_{j-k+1} & \dots & cJ_{j-1} \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & c \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

$$=\begin{bmatrix} J_{j+k} & J_{j+k-1}+J_{j+k-2}+\cdots+cJ_{j+1} & J_{j+k-1}+J_{j+k-2}+\cdots+cJ_{j+2} & \dots & cJ_{j+k-1} \\ J_{j+k-1} & J_{j+k-2}+J_{j+k-3}+\cdots+cJ_j & J_{j+k-2}+J_{j+k-3}+\cdots+cJ_{j+1} & \dots & cJ_{j+k-2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ J_{j+2} & J_{j+1}+J_j+\cdots+cJ_{j-k+3} & J_{j+1}+J_j+\cdots+cJ_{j-k+2} & \dots & cJ_{j+1} \\ J_{j+1} & J_j+J_{j-1}+\cdots+cJ_{j-k+2} & J_j+J_{j-1}+\cdots+cJ_{j-k+1} & \dots & cJ_j \end{bmatrix}$$

ดังนั้น ทฤษฎีบทเป็นจริง

บทแทรกที่ 2 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ จะได้ว่า $\det(Q^n)=(-1)^{n(k+1)}c^n$

พิสูจน์ สังเกตได้ว่า $\det Q=(-1)^{k+1}c$

ดังนั้น $\det(Q^n)=(\det Q)^n=((-1)^{k+1}c)^n=(-1)^{n(k+1)}c^n$

ทฤษฎีบทที่ 3 สำหรับ n เป็นจำนวนเต็มบวกใด ๆ และ $k=2$ จะได้ว่า พจน์ที่ n ของสมการ (1) คือ

$$J_n=\frac{(\sqrt{4c+1}+1)^n-(-\sqrt{4c+1}+1)^n}{2^n\sqrt{4c+1}} \quad \text{และ} \quad \lim_{n\to\infty}\frac{J_{n+1}}{J_n}=\frac{\sqrt{4c+1}+1}{2}$$

พิสูจน์ เราสามารถหาค่าลักษณะเฉพาะและเวกเตอร์ลักษณะเฉพาะของ Q-เมทริกซ์ ของสมการสมการเวียนเกิดจาคอบส์ทัลอันดับ 2

$$J_n=J_{n-1}+c\cdot J_{n-2},\ n\geq 2 \quad \text{โดยที่ } J_0=0,\ J_1=1$$

ได้ดังนี้

$\lambda_1=\frac{1+\sqrt{4c+1}}{2}$ ซึ่งสอดคล้องกับเวกเตอร์ $v_1=\begin{bmatrix}\frac{1+\sqrt{4c+1}}{2}\\ 1\end{bmatrix}$

และ $\lambda_2 = \dfrac{1-\sqrt{4c+1}}{2}$ ซึ่งสอดคล้องกับเวกเตอร์ $v_2 = \begin{bmatrix} \dfrac{1-\sqrt{4c+1}}{2} \\ 1 \end{bmatrix}$

ดังนั้นเราสามารถเขียน Q ในรูปของเมทริกซ์ทะแยงมุมได้ดังนี้

$$D = P^{-1}QP$$

โดยที่ $D = \begin{bmatrix} \dfrac{1+\sqrt{4c+1}}{2} & 0 \\ 0 & \dfrac{1-\sqrt{4c+1}}{2} \end{bmatrix}$ และ $P = \begin{bmatrix} \dfrac{1+\sqrt{4c+1}}{2} & \dfrac{1-\sqrt{4c+1}}{2} \\ 1 & 1 \end{bmatrix}$

จะได้ว่า $D^n = P^{-1}Q^nP$

ดังนั้น $Q^n = PD^nP^{-1}$

โดยที่ $D^n = \begin{bmatrix} \left(\dfrac{1+\sqrt{4c+1}}{2}\right)^n & 0 \\ 0 & \left(\dfrac{1-\sqrt{4c+1}}{2}\right)^n \end{bmatrix}$

จากการคำนวณ สามารถแสดงได้ว่า

$$\begin{bmatrix} J_{n+1} & cJ_n \\ J_n & cJ_{n-1} \end{bmatrix} = \begin{bmatrix} \dfrac{\left(1+\sqrt{4c+1}\right)^{n+1} - \left(1-\sqrt{4c+1}\right)^{n+1}}{2^{n+1}\sqrt{4c+1}} & \alpha \\ \dfrac{\left(1+\sqrt{4c+1}\right)^{n} - \left(1-\sqrt{4c+1}\right)^{n}}{2^{n}\sqrt{4c+1}} & \beta \end{bmatrix}$$

ดังนั้น $J_n = \dfrac{\left(1+\sqrt{4c+1}\right)^n - \left(1-\sqrt{4c+1}\right)^n}{2^n\sqrt{4c+1}}$

และ

$$\lim_{n\to\infty}\frac{J_{n+1}}{J_n} = \lim_{n\to\infty}\frac{\left(1+\sqrt{4c+1}\right)^{n+1} - \left(1-\sqrt{4c+1}\right)^{n+1}}{2^{n+1}\sqrt{4c+1}} \cdot \frac{2^n\sqrt{4c+1}}{\left(1+\sqrt{4c+1}\right)^n - \left(1-\sqrt{4c+1}\right)^n}$$

$$= \frac{1+\sqrt{4c+1}}{2}$$

สำหรับ $k > 2$ และ c เป็นจำนวนเต็มบวกใด ๆ จะได้ว่าสมการลักษณะเฉพาะของสมการเวียนเกิด (1)

$$x^k - x^{k-1} - \cdots - x - c = 0$$

มีค่าราก $\lambda_1, \lambda_2, ..., \lambda_k$ ที่แตกต่างกัน (Marques & Trojovsky, 2019)

ให้ V เป็นเมทริกซ์ของวานเดอร์มอนด์ (Vandermonde matrix) ของ Q-เมทริกซ์ จะได้

$$V=\begin{bmatrix} \lambda_1^{k-1} & \lambda_1^{k-2} & \dots & \lambda_1 & 1 \\ \lambda_2^{k-1} & \lambda_2^{k-2} & \dots & \lambda_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda_k^{k-1} & \lambda_k^{k-2} & \dots & \lambda_k & 1 \end{bmatrix}$$

และกำหนดให้ a_k เป็นเวกเตอร์คอลัมน์

$$a_k=\begin{bmatrix} \lambda_1^{n+k-1} \\ \lambda_2^{n+k-1} \\ \vdots \\ \lambda_k^{n+k-1} \end{bmatrix}$$

และ V_1 เป็นเมทริกซ์จัตุรัสที่เกิดจากการแทนที่คอลัมน์ที่ 1 ของเมทริกซ์ V ด้วย a_k โดย (Yilmaz & Bozkurt, 2009) จะได้ว่า

$$J_n=\frac{\det(V_1)}{\det(V)}$$

และสามารถแสดงได้ว่า

$$\lim_{n\to\infty}\frac{J_{n+1}}{J_n}=r$$

เมื่อ r เป็นค่าคงที่

ความสัมพันธ์ระหว่างสมาชิกของเมทริกซ์รหัส

กรณี $k=2$

จาก $E=M\times Q^n=\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}\begin{bmatrix} J_{n+1} & cJ_n \\ J_n & cJ_{n-1} \end{bmatrix}=\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}$

และ $Q^{-n}=\frac{1}{(-1)^{3n}c^n}\begin{bmatrix} cJ_{n-1} & -cJ_n \\ -J_n & J_{n+1} \end{bmatrix}=\frac{1}{(-1)^n c^n}\begin{bmatrix} cJ_{n-1} & -cJ_n \\ -J_n & J_{n+1} \end{bmatrix}$

โดยไม่เสียนัยทั่วไป สมมติ n เป็นจำนวนคู่ จะได้ว่า

$$M=E\times Q^{-n}=\frac{1}{c^n}\begin{bmatrix} ce_{11}J_{n-1}-e_{12}J_n & -ce_{11}J_n+e_{12}J_{n+1} \\ ce_{21}J_{n-1}-e_{22}J_n & -ce_{21}J_n+e_{22}J_{n+1} \end{bmatrix}$$

ดังนั้น จะได้ว่า

$$ce_{11}J_{n-1}-e_{12}J_n>0 \quad (2)$$

$$-ce_{11}J_n+e_{12}J_{n+1}>0 \quad (3)$$

$$ce_{21}J_{n-1}-e_{22}J_n>0 \quad (4)$$

$$-ce_{21}J_n+e_{22}J_{n+1}>0 \quad (5)$$

จาก (2) และ (3) เราสามารถแสดงได้ว่า

$$\frac{J_{n+1}}{cJ_n}>\frac{e_{11}}{e_{12}}>\frac{J_n}{cJ_{n-1}}$$

เมื่อ n มีค่ามาก จะได้ว่า

$$\frac{e_{11}}{e_{12}} \approx R$$

โดยที่ $R = \dfrac{1+\sqrt{4c+1}}{2c}$

ในทำนองเดียวกัน จาก (4) และ (5) เราสามารถสรุปได้ว่า สำหรับ n มีค่ามาก

$$\frac{e_{21}}{e_{22}} \approx R$$

กรณี $k > 2$

จาก $M \times Q^n = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1k} \\ m_{21} & m_{22} & \cdots & m_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ m_{k1} & m_{k2} & \cdots & m_{kk} \end{bmatrix} \times Q^n = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ e_{k1} & e_{k2} & \cdots & e_{kk} \end{bmatrix} = E$

โดยเราสามารถแสดงได้ว่า เมื่อ n มีค่ามาก จะได้ว่า

$$\frac{e_{i1}}{e_{i2}} \approx \frac{r^{k-1}}{1+r+r^2+\cdots+r^{k-2}},\ \frac{e_{i1}}{e_{i3}} \approx \frac{r^{k-2}}{1+r+r^2+\cdots+r^{k-3}},\ldots,\ \frac{e_{i1}}{e_{ik}} \approx r,$$

$$\frac{e_{i2}}{e_{i3}} \approx \frac{1+r+r^2+\cdots+r^{k-2}}{r+r^2+\cdots+r^{k-2}},\ \frac{e_{i2}}{e_{i4}} \approx \frac{1+r+r^2+\cdots+r^{k-2}}{r^2+r^3+\cdots+r^{k-2}},\ldots,\ \frac{e_{i2}}{e_{ik}} \approx \frac{1+r+r^2+\cdots+r^{k-2}}{r^{k-2}},$$

$$\frac{e_{i3}}{e_{i4}} \approx \frac{1+r+r^2+\cdots+r^{k-3}}{r+r^2+\cdots+r^{k-3}},\ \frac{e_{i3}}{e_{i5}} \approx \frac{1+r+r^2+\cdots+r^{k-3}}{r^2+r^3+\cdots+r^{k-3}},\ldots,\ \frac{e_{i3}}{e_{ik}} \approx \frac{1+r+r^2+\cdots+r^{k-3}}{r^{k-3}},$$

$$\vdots$$

$$\frac{e_{i(k-1)}}{e_{ik}} \approx \frac{1+r}{r}, \quad \text{for} \quad i = 1,2,3,\ldots,k$$

การตรวจข้อผิดพลาดของรหัส

ในทฤษฎีรหัส การตรวจสอบและแก้ไขข้อผิดพลาดของรหัสเป็นเรื่องสำคัญที่ต้องพิจารณาเพราะในช่องทางการสื่อสารอาจจะมีการรบกวนเกิดขึ้น ซึ่งสิ่งที่ช่วยในการตรวจสอบ คือ ค่าดีเทอร์มิแนนท์ของเมทริกซ์ จากสมการ $M \times Q^n = E$

จะได้ว่า

$$\det E = (\det M) \times (-1)^{n(k+1)} c^n \qquad (6)$$

ดังนั้น ถ้าค่าดีเทอร์มิแนนท์ของ E และ M ไม่สอดคล้องสมการ (6) เราสามารถสรุปได้ว่ารหัสเกิดข้อผิดพลาดขึ้น

การแก้ไขข้อผิดพลาดของรหัส

ในความเป็นจริงเราไม่สามารถพิจารณาว่าตำแหน่งไหนที่เกิดข้อผิดพลาดของรหัส เราทำได้แค่พิจารณาตามกรณีที่สมมติตามจำนวนตำแหน่งของข้อผิดพลาดของข้อมูล โดยในที่นี้เราจะแสดงเฉพาะกรณี $k=2$ ดังนี้

<u>กรณีที่ 1</u> มีข้อผิดพลาดของรหัสแค่ 1 ตำแหน่ง

โดยไม่เสียนัยทั่วไป ให้สมาชิกตัวแรกของเมทริกซ์ E เป็นตัวที่มีข้อผิดพลาด ดังนั้น เมทริกซ์ที่ผิดพลาดคือ

$$E' = \begin{bmatrix} u & e_{12} \\ e_{21} & e_{22} \end{bmatrix}$$

โดยที่ u คือ รหัสที่ถูกเปลี่ยนแปลงไป และสมาชิกที่เหลือมีความถูกต้องของรหัส

จากสมการ $M \times Q^n = E$ จะได้ว่า ค่าดีเทอร์มิแนนท์ของทั้งสองข้างของสมการเท่ากัน

$$\det(M) \times (-1)^n c^n = ue_{22} - e_{12}e_{21}$$

ซึ่งเราสามารถแก้สมการหาค่า u ที่ถูกต้องได้ในรูป

$$u = \frac{\det(M) \times (-c)^n + e_{12}e_{21}}{e_{22}}$$

โดยการใช้ค่า u ที่ถูกต้องนี้ เราสามารถแก้ไขข้อผิดพลาดของรหัสใน 1 ตำแหน่งได้

<u>กรณีที่ 2</u> มีข้อผิดพลาดของรหัส 2 ตำแหน่ง

สมมติตัวที่มีข้อผิดพลาดเป็นสมาชิกในแถวที่ 1 ของเมทริกซ์ E ดังนั้น เมทริกซ์ที่ผิดพลาด คือ

$$E' = \begin{bmatrix} u & v \\ e_{21} & e_{22} \end{bmatrix}$$

จากการเท่ากันของค่าดีเทอร์มิแนนท์ จะได้

$$ue_{22} - ve_{21} = (-c)^n \det(M) \qquad (7)$$

เรารู้จากการพิสูจน์ว่า

$$\frac{u}{v} \approx R \qquad (8)$$

เราสามารถเห็นได้ชัดเจนว่า สมการ (7) เป็นสมการไดโอแฟนไทน์ ซึ่งมีคำตอบจำนวนมาก เราสามารถหาคำตอบที่สอดคล้องกับสมการ (8) โดยการใช้ค่า u และ v ที่ถูกต้องนี้ เราสามารถแก้ไขข้อผิดพลาดของรหัสใน 2 ตำแหน่งได้

<u>กรณีที่ 3</u> มีข้อผิดพลาดของรหัส 3 ตำแหน่ง

$$\begin{bmatrix} u & v \\ w & e_{22} \end{bmatrix}$$

โดยการเท่ากันของดีเทอร์มิแนนท์ จะได้ว่า

$$ue_{22} - vw = (-c)^n \det(M)$$

จาก $\frac{w}{e_{22}} \approx R$ เราสามารถลดรูปสมการดังกล่าวให้เหลือสมการไดโอแฟนไทน์สองตัวแปร และเนื่องจาก $\frac{u}{v} \approx R$ โดยกระบวนการที่เหมือนกันกับกรณีที่ 2 เราสามารถแก้สมการในกรณีที่มีข้อผิดพลาด 3 ตำแหน่งได้

ส่วนในกรณีที่มีข้อผิดพลาด 4 ตำแหน่ง นั่นคือ E เป็นรหัสที่ผิดพลาดทุกตำแหน่งและไม่สามารถที่จะแก้ไขข้อผิดพลาดได้

เนื่องจากรหัสอาจเกิดข้อผิดพลาดขึ้นได้ ตั้งแต่การเกิดข้อผิดพลาด 1 ตำแหน่ง จนถึงเกิดข้อผิดพลาด 4 ตำแหน่ง ดังนั้น จำนวนวิธีการเกิดข้อผิดพลาดทั้งหมด เท่ากับ
${}^4C_1 + {}^4C_2 + {}^4C_3 + {}^4C_4 = 15$ วิธี โดยที่เราสามารถแก้ไขรหัสให้ถูกต้องได้ทุกวิธี ยกเว้นวิธีเดียวคือกรณีที่เกิดข้อผิดพลาดทั้ง 4 ตำแหน่ง $\left({}^4C_4 = 1\right)$ ดังนั้น ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัสจึงมีค่า เท่ากับ
$\frac{14}{15} = 0.9333 = 93.33\%$

ตัวอย่างการเข้าและถอดรหัส

สำหรับการเข้าและถอดรหัสของการส่งข้อความ เริ่มแรกเราจะทำการใส่ข้อความที่ต้องการส่งลงในเมทริกซ์ขนาดเป็นเลขคู่ โดยเติม 0 ลงระหว่างคำ และเติม 0 ที่ท้ายประโยคจนกว่าเต็มเมทริกซ์
หลังจากนั้น ทำการแบ่งเมทริกซ์เป็นเมทริกซ์บล็อคขนาด 2×2 โดยกำหนดการแปลงตัวอักษรให้เป็นตัวเลขดังนี้

ตารางที่ 1 การแปลงตัวอักษร

ตัวอักษร	A	B	C	D	E	F	G	H	I	J	K	L	M	
ตัวเลข	1	2	3	4	5	6	7	8	9	10	11	12	13	
ตัวอักษร	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
ตัวเลข	14	15	16	17	18	19	20	21	22	23	24	25	26	0

สมมติว่า เราต้องการส่งข้อความคำว่า “NAKHON SAWAN MAP” ซึ่งเราสามารถกำหนดเมทริกซ์ข้อความได้ดังนี้

$$B = \begin{bmatrix} N & A & K & H \\ O & N & 0 & S \\ A & W & A & N \\ 0 & M & A & P \end{bmatrix}$$

ทำการแบ่งเมทริกซ์ให้เป็นเมทริกซ์บล็อคขนาด 2x2 และแปลงตัวอักษรให้เป็นตัวเลข ได้เป็น

$$B = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}$$

โดยที่ $M_1 = \begin{bmatrix} 14 & 1 \\ 15 & 14 \end{bmatrix}, M_2 = \begin{bmatrix} 11 & 8 \\ 0 & 19 \end{bmatrix}, M_3 = \begin{bmatrix} 1 & 23 \\ 0 & 13 \end{bmatrix}, M_4 = \begin{bmatrix} 1 & 14 \\ 1 & 16 \end{bmatrix}$

หลังจากนั้น ทำการเข้ารหัส โดยในที่นี้เรากำหนดให้ $c = 3$ และ $n = 2$ จะได้

$$M_i \times Q^n = \begin{bmatrix} e_{i1} & e_{i2} \\ e_{i3} & e_{i4} \end{bmatrix} = E_i, \quad i = 1,2,3,4$$

ดังนั้น $E_1 = \begin{bmatrix} 57 & 45 \\ 74 & 87 \end{bmatrix}$, $E_2 = \begin{bmatrix} 52 & 57 \\ 19 & 57 \end{bmatrix}$, $E_3 = \begin{bmatrix} 27 & 72 \\ 13 & 39 \end{bmatrix}$, $E_4 = \begin{bmatrix} 18 & 45 \\ 20 & 51 \end{bmatrix}$

และเมื่อข้อความที่เป็นรหัสถูกส่งถึงปลายทาง จะสามารถถูกถอดรหัส ได้เป็น

$$E_i \times Q^{-n} = \begin{bmatrix} e_{i1} & e_{i2} \\ e_{i3} & e_{i4} \end{bmatrix} \times Q^{-n} = M_i, \quad i = 1,2,3,4$$

ซึ่งจะได้เมทริกซ์รหัส M_i

และได้เมทริกซ์ข้อความ คือ

$$B = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} = \begin{bmatrix} 14 & 1 & 11 & 8 \\ 15 & 14 & 0 & 19 \\ 1 & 23 & 1 & 14 \\ 0 & 13 & 1 & 16 \end{bmatrix}$$

และเมื่อทำการแปลงตัวเลขให้เป็นตัวอักษรตามตารางการแปลงข้างต้น จะได้ข้อความที่ถูกส่งไปนั่นเอง

จากตัวอย่างข้างต้น เมื่อเราพิจารณา E_1 จะพบว่าอัตราส่วนของสมาชิกในแต่ละแถว เป็นดังนี้

ตารางที่ 2 อัตราส่วนของสมาชิกในแต่ละแถวของ E_1

n	e_{11}/e_{12}	e_{21}/e_{22}
2	1.2667	0.8506
5	0.7070	0.7537
6	0.8048	0.7756
10	0.7756	0.7684
15	0.7674	0.7675
20	0.7676	0.7676

จากตารางจะเห็นว่า เมื่อ *n* มีค่ามากขึ้น ค่าของอัตราส่วนของสมาชิกในแต่ละแถวจะมีค่าเข้าใกล้ 0.7676 มากขึ้น สำหรับเมทริกซ์ *E* อื่น ๆ ค่าของอัตราส่วนของสมาชิกในแต่ละแถวมีค่าเข้าใกล้ 0.7676 เมื่อ *n* มีค่ามากขึ้นเช่นเดียวกัน

บทที่ 4
สรุปผลการวิจัย

กระบวนการเข้ารหัสโดยใช้ Q-เมทริกซ์เป็นกระบวนการเข้ารหัสที่อยู่ในรูปของการคูณเมทริกซ์ ซึ่งสามารถไปประยุกต์ใช้ได้ง่ายกับการเขียนโปรแกรมสมัยใหม่ ในกรณีที่มีข้อมูลเป็นจำนวนมาก เราสามารถจัดการข้อความโดยแบ่งข้อความเป็นส่วน ๆ และรับข้อมูลได้ไม่จำกัด

ค่าความสามารถในการแก้ไขข้อผิดพลาดของรหัสของกระบวนการนี้ เท่ากับ 93.33% โดยที่สามารถแก้ไขข้อผิดพลาดของรหัสได้ถึง 3 ตำแหน่งจากทั้งหมด 4 ตำแหน่ง

บรรณานุกรม

Basu, M., & Das, M. (2014a). Coding theory on Fibonacci n-step numbers. *Discrete Mathematics Algorithms and Applications. 6*(2), 1450017(1-32).

Basu, M., & Das, M. (2014b). Tribonacci matrices and a new coding theory. *Discrete Mathematics Algorithms and Applications. 6*(1), 1450008(1-17).

Basu, M., & Prasad, B. (2009). The generalized relations among the code elements for Fibonacci coding theory, *Chaos Solitons and Fractals. 41*(5), 2517-2525.

Marques, D., & Trojovsky, P. (2019). On characteristic polynomial of higher order generalized Jacobsthal numbers. *Advances in Difference Equations*. 2019:392. https://doi.org/10.1186/s13662-019-2327-6

Prasad, B. (2016). Coding theory on Lucas p numbers. *Discrete Mathematics Algorithms and Applications. 8*(4), 1650074.

Stakhov, A., P. (2006). Fibonacci matrices, a generalization of “Cassini formula” and a new coding theory. *Chaos Solitons and Fractals. 30*(1), 56-66.

Tas, N., Ucar, S., & Ozgur, N. Y. (2017). Pell coding and Pell decoding methods with some applications. https://arxiv.org/pdf/1706.04377.

Yilmaz, F., & Bozkurt, D. (2009). The generalized order-k Jacobsthal numbers. *Int. J. contemp. Math. Sciences, 4*(34), 1685-1694.