ใบรับรองวิทยานิพนธ์
บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

ปริญญา

วิศวกรรมคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์

สาขา **ภาควิชา**

เรื่อง การเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทางปลายทางแบบหลายคู่

Linear Network Coding for the Multiple Source-Sink Pair Communication Problem

นามผู้วิจัย นายมุนินทร์ เอี่ยมโอภาส

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก .....

(ผู้ช่วยศาสตราจารย์จิตร์ทัศน์ ฝักเจริญผล, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม .....

(ผู้ช่วยศาสตราจารย์ชัยพร ใจแก้ว, Ph.D.)

หัวหน้าภาควิชา .....

(ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ, Ph.D.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

.....

(รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr.)

คณบดีบัณฑิตวิทยาลัย

วันที่ ..... **เดือน** ..... **พ.ศ.** .....

วิทยานิพนธ์

เรื่อง

การเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทางปลายทางแบบหลายคู่

Linear Network Coding for the Multiple Source-Sink Pair Communication Problem

โดย

นายมุนินทร์ เอี่ยมโอภาส

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์
เพื่อความสมบูรณ์แห่งปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)
พ.ศ. 2554

มุนินทร์ เอี่ยมโอภาส 2554: การเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทางปลายทางแบบหลายคู่ ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์จิตร์ทัศน์ ฝักเจริญผล, Ph.D. 28 หน้า

การเข้ารหัสเครือข่ายเป็นอีกวิธีที่สามารถใช้เพิ่มประสิทธิภาพในการส่งข้อมูลภายในเครือข่ายได้ งานวิจัยนี้มีจุดประสงค์เพื่อศึกษาและพัฒนาการเข้ารหัสเครือข่ายเพื่อให้ทำงานได้ดียิ่งขึ้น โดยสนใจในการเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทางปลายทางแบบหลายคู่

ไม่นานมานี้ Iwama *et al.* ได้เสนออัลกอริทึมสำหรับคำนวณการเข้ารหัสเครือข่ายในเครือข่ายที่มีคู่รับส่ง k คู่ ที่ทำงานในเวลาเป็นพหุนามในขนาดของเครือข่าย ในกรณีที่ k เป็นค่าคงที่ เวลาการทำงานของอัลกอริทึมนี้ขึ้นอยู่กับขีดจำกัดบนของจำนวนโหนดที่ทำการเข้ารหัสเครือข่ายในคำตอบ Iwama *et al.* ได้พิสูจน์ขีดจำกัดบนของจำนวนโหนดเข้ารหัสว่าจำเป็นต้องใช้ไม่เกิน $|\mathfrak{I}|^{3k}$ โหนด ถ้าการเข้ารหัสกระทำบนฟิลด์ $\mathfrak{I}$ งานวิจัยนี้เสนอว่าโหนดเข้ารหัสจำนวนไม่เกิน $k^2|\mathfrak{I}|^{2k}$ โหนดนั้นเพียงพอต่อการหาการเข้ารหัสเครือข่าย ในกรณีที่มีคู่รับส่ง k คู่ ขีดจำกัดบนที่แน่นขึ้นดังกล่าว ทำให้เวลาในการทำงานของอัลกอริทึมที่เสนอโดย Iwama *et al.* ลดลงอย่างมาก การพิสูจน์ขีดจำกัดบนใหม่นี้ใช้หลักทางพีชคณิตเชิงเส้นและทฤษฎีบทของ Dilworth

_____ _____ ___ / ___ / ___

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Munin Eamopas 2011: Linear Network Coding for the Multiple Source-Sink Pair Communication Problem. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Assistant Professor Jittat Fakcharoenphol, Ph.D. 28 pages.

Network coding is an another technique to improve efficiency of the network. This thesis has the objectives to study and to improve the network coding, and focus on the multiple source-sink pair communication problem

Recently, Iwama *et al.* present an algorithm for k source-sink pair network coding, when k is some fixed constant. The running time of the algorithm depends on the upper bound on number of vertices performing encoding operations. Iwama et al prove that $|\mathfrak{I}|^{3k}$ encoding vertices are sufficient to obtain the network coding whose operated on field $\mathfrak{I}$. In this work, we improve the bound to $k^2|\mathfrak{I}|^{2k}$ and this tighter bound, in turns, improves the running time of the algorithm proposed by Iwama *et al.* The techniques used are elementary linear algebra and Dilworth's theorem.

_____ _____ ___ / ___ / ___

Student's signature Thesis Advisor's signature

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณผู้ช่วยศาสตราจารย์จิตร์ทัศน์ ฝักเจริญผล ประธานกรรมการที่ปรึกษา และผู้ช่วยศาสตราจารย์ชัยพร ใจแก้ว กรรมการที่ปรึกษาร่วม ที่ช่วยให้คำปรึกษาและแนวทางในการวิจัย รวมถึงข้อเสนอแนะต่างๆ จนทำให้งานวิจัยนี้สำเร็จเป็นผลออกมาได้ด้วยดี

ขอขอบคุณพี่ๆเพื่อนๆนิสิตปริญญาโทและสมาชิกกลุ่มวิจัยเชิงทฤษฎีทุกคนที่ช่วยแลกเปลี่ยนความรู้และจุดประกายความคิดต่างๆ ขอบคุณเจ้าหน้าที่ภาควิชาวิศวกรรมคอมพิวเตอร์ที่ช่วยอำนวยความสะดวกและประสานงานต่างๆให้ สุดท้ายนี้ขอขอบคุณบิดามารดาที่คอยดูแลเอาใจใส่และให้กำลังใจอยู่เสมอมา

มุนินทร์ เอี่ยมโอภาส

พฤษภาคม 2554

สารบัญ

หน้า

สารบัญภาพ

การเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสาร ระหว่างต้นทางปลายทางแบบหลายคู่

Linear Network Coding for the Multiple Source-Sink Pair Communication Problem

คำนำ

ในปัจจุบันความสามารถในการส่งข้อมูลในเครือข่ายเป็นสิ่งที่มีความสำคัญ การเข้ารหัสเครือข่าย (Network Coding) นับเป็นอีกวิธีการหนึ่งที่น่าสนใจและช่วยเพิ่มความสามารถในการส่งข้อมูลที่มีเป้าหมายในการส่งหลายเป้าหมายในเครือข่ายได้ โดยทั่วไปแล้วการส่งข้อมูลที่มีหลายเป้าหมาย มักมีบางการเชื่อมต่อที่ต้องใช้ร่วมกัน เนื่องจากการส่งข้อมูลตามปกตินั้นไม่สามารถนำข้อมูลจากหลายเป้าหมายมาประมวลผลรวมกันได้ จึงทำให้ต้องมีการแยกส่งเป็นหลายรอบ (ดังจะแสดงในตัวอย่างต่อไป) ซึ่งทำให้ประสิทธิภาพลดลง

ในเครือข่ายที่ใช้การส่งข้อมูลแบบการเข้ารหัสเครือข่าย อุปกรณ์และตัวกลางรับส่งข้อมูลสามารถนำข้อมูลที่ต้องการส่งจากหลายต้นทางไปยังหลายปลายทางมาประมวลผลร่วมกันได้ ซึ่งในหลาย ๆ กรณี ทำให้สามารถส่งข้อมูลได้โดยไม่ต้องรอส่งข้อมูลทีละครั้ง และเพิ่มประสิทธิภาพการส่งข้อมูล

รูปแบบการสื่อสารที่เป็นจุดเริ่มต้นของการศึกษาการเข้ารหัสเครือข่าย คือการสื่อสารแบบมัลติคาสต์ (multicast) ที่เป็นการสื่อสารที่โหนดต้นทางเพียงหนึ่งโหนด ต้องการส่งข้อมูลไปยังโหนดปลายทางหลาย ๆ โหนด การเข้ารหัสเครือข่ายสามารถรองรับปัญหานี้ได้เป็นอย่างดี นอกจากนี้ยังมีงานวิจัยที่ศึกษาปัญหานี้เป็นจำนวนมากและครอบคลุมในแทบจะทุกด้าน

ในงานวิจัยนี้เราสนใจในปัญหาที่กว้างขึ้น กล่าวคือเราสนใจปัญหาในการเข้ารหัสเครือข่ายสำหรับการสื่อสารระหว่างต้นทางปลายทางหลายคู่ ในปัญหาดังกล่าว มีคู่โหนด k คู่ ที่ต้องการส่งข้อมูลถึงกัน การส่งข้อมูลผ่านทางการเข้ารหัสเครือข่ายจะสำเร็จถ้าข้อมูลจากแต่ละต้นทางสามารถส่งไปถึงปลายทางที่คู่กันได้อย่างถูกต้อง

สำหรับปัญหานี้ในปี 2003 Lehman and Lehman ได้พิสูจน์ว่าในกรณีที่ไม่จำกัดจำนวนคู่รับส่ง การคำนวณการเข้ารหัสเครือข่ายในเครือข่ายนี้เป็นปัญหา NP-Hard ต่อมาในปี 2007 Wang and Shroff ได้พิสูจน์ว่าสามารถคำนวณการเข้ารหัสเครือข่ายในเครือข่ายที่มีคู่รับส่ง 2 คู่ได้ แต่วิธีการดังกล่าวไม่สามารถใช้ได้กับเครือข่ายที่มีคู่รับส่งมากกว่า 2 คู่

งานวิจัยนี้พัฒนาต่อจากงานของ Iwama *et al.* (2008) งานดังกล่าวเสนออัลกอริทึมสำหรับคำนวณการเข้ารหัสเครือข่ายในเครือข่ายที่มีคู่รับส่ง k คู่ ที่ทำงานในเวลาเป็นพหุนามในขนาดของเครือข่าย ในกรณีที่ k เป็นค่าคงที่ เวลาการทำงานของอัลกอริทึมนี้ขึ้นอยู่กับขีดจำกัดบนของจำนวนโหนดที่ทำการเข้ารหัสเครือข่ายในคำตอบ

Iwama *et al.* ได้พิสูจน์ขีดจำกัดบนของจำนวนโหนดเข้ารหัสว่าจำเป็นต้องใช้ไม่เกิน $|\mathfrak{I}|^{3k}$ โหนด ถ้าการเข้ารหัสกระทำบนฟิลด์ $\mathfrak{I}$ งานวิจัยนี้เสนอว่าโหนดเข้ารหัสจำนวนไม่เกิน $k^2|\mathfrak{I}|^{2k}$ โหนดนั้นเพียงพอต่อการหาการเข้ารหัสเครือข่าย ในกรณีที่มีคู่รับส่ง k คู่

ขีดจำกัดบนที่แน่นขึ้นดังกล่าว ทำให้เวลาในการทำงานของอัลกอริทึมที่เสนอโดย Iwama *et al.* ลดลงอย่างมาก การพิสูจน์ขีดจำกัดบนใหม่นี้ใช้หลักทางพีชคณิตเชิงเส้นและทฤษฎีบทของ Dilworth

วัตถุประสงค์

1. พัฒนาและปรับปรุงอัลกอริทึมสำหรับการเข้ารหัสเครือข่ายสำหรับปัญหาการสื่อสารระหว่างต้นทางและปลายทางหลายคู่

การตรวจเอกสาร

การเข้ารหัสเครือข่ายเป็นเทคนิคหนึ่งในการส่งข้อมูลที่ช่วยเพิ่มความสามารถในการส่งข้อมูลให้เครือข่ายในกรณีที่มีการส่งไปยังเป้าหมายจำนวนหลายเป้าหมาย โดยก่อนที่จะกล่าวถึงการเข้ารหัสเครือข่ายนั้นจะขอกล่าวถึงนิยามและพื้นฐานที่จำเป็นต้องใช้ก่อน

พื้นฐานด้านพีชคณิตเชิงเส้น

ฟิลด์ $\mathfrak{F}$ คือเซตที่มีเครื่องหมาย บวก ”+” และ คูณ “ · ” โดยเครื่องหมายทั้งสองนี้นิยามบนฟิลด์ และทำให้ข้อกำหนดเหล่านี้เป็นจริง

1. มีสมบัติปิด :

กล่าวคือผลบวกและ ผลคูณ ของสมาชิกในฟิลด์จะต้องอยู่ภายในฟิลด์

2. มีสมบัติการสลับที่ :

สำหรับสมาชิก a และ b ใดๆที่อยู่ในฟิลด์ $a + b = b + a$ และ $a \cdot b = b \cdot a$

3. มีสมบัติการจัดหมู่ :

สำหรับสมาชิก a, b และ c ใดๆที่อยู่ในฟิลด์ $a + (b+c) = (a+b) + c$ และ $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

4. การคูณมีสมบัติการกระจาย :

สำหรับสมาชิก a, b และ c ใดๆที่อยู่ในฟิลด์ $a\cdot(b+c) = (a\cdot b) + (a\cdot c)$

5. มีเอกลักษณ์การบวก 0 และ เอกลักษณ์การคูณ 1 :

สำหรับสมาชิก a ใดๆในฟิลด์ $a + 0 = a$ และ $a\cdot 1 = a$

6. มีตัวผกผันการบวก :

สำหรับสมาชิก a ในฟิลด์ สามารถหาค่าตัวผกผันการบวก b ในฟิลด์ที่ทำให้ $a + b = 0$

7. มีตัวผกผันการคูณ :

สำหรับสมาชิก a ในฟิลด์ ที่ไม่เท่ากับ 0 สามารถหาตัวผกผันการคูณ b ในฟิลด์ที่ทำให้ $a\cdot b = 1$

ตัวอย่างฟิลด์ที่ใช้กันบ่อยได้แก่ ฟิลด์จำนวนจริง, ฟิลด์จำนวนเชิงซ้อน

ฟิลด์จำกัด (Finite field) หมายถึงฟิลด์ที่มีสมาชิกในฟิลด์มีจำนวนจำกัด ขนาดของฟิลด์จำกัดมีขนาดเล็กที่สุดที่เป็นได้คือ 2 มีสมาชิกคือ (0,1) เรียกว่า Binary field

หลังจากนี้เราจะนำสมาชิกในฟิลด์มาใช้ในการระบุขนาดของจำนวนโดย *สเกลาร์* (Scalar) คือจำนวนที่มีแต่ขนาดเพียงอย่างเดียว และ *เวกเตอร์* (Vector) คือจำนวนที่มีทั้งขนาดและทิศทาง

ปริภูมิเวกเตอร์ V บนฟิลด์ ประกอบด้วยส่วนประกอบสองส่วนคือเวกเตอร์และฟิลด์ และมีการดำเนินการสองอย่างคือ การบวกเวกเตอร์ (Vector addition) และ การคูณด้วยสเกลาร์ (Scalar multiplication) กระบวนการทั้ง 2 จะต้องเป็นไปตามข้อกำหนดดังนี้

1. การบวกเวกเตอร์มีสมบัติปิด :

สำหรับทุกๆค่าของเวกเตอร์ x และ y ใน V เวกเตอร์ $x + y$ นั้นอยู่ใน V

2. การบวกเวกเตอร์มีสมบัติการสลับที่ :

สำหรับค่า x และ y ใดใน V , $x + y = y + x$

3. การบวกเวกเตอร์มีสมบัติการจัดลำดับ :

ได้สำหรับค่า x y และ z ใดใน V , $(x+y)+z = x+(y+z)$

4. มีเอกลักษณ์การบวก :

มี 0 ในเซต V ที่ทำให้ $0 + x = x$ สำหรับค่า x ใดๆใน V

5. มีค่าผกผันการบวก :

สำหรับค่า x ที่อยู่ใน V จะมีเวกเตอร์ y ที่ทำให้ $x + y = 0$

6. การคูณสเกลาร์มีสมบัติปิด :

สำหรับทุกค่าของ a ในฟิลด์ และทุกๆค่าของ x ใน V ค่า ax จะอยู่ใน V โดยค่า ax นี้เรียกว่าเป็นผลคูณเชิงสเกลาร์ (scalar product)

7. การคูณด้วยสเกลาร์มีสมบัติการจัดลำดับ :

สำหรับค่า a และ b ใดๆในฟิลด์ และค่า x ใน V เราได้ว่า $a(bx) = (ab)\,x$

8. การคูณด้วยสเกลาร์สามารถกระจายได้เมื่อเทียบกับการบวกเวกเตอร์ :

สำหรับค่า a ในฟิลด์ และ x, y ใน V, $a(x + y) = ax + ay$

9. การคูณด้วยสเกลาร์สามารถกระจายได้เมื่อเทียบกับการบวกสเกลาร์ :

สำหรับค่า a,b ในฟิลด์ และ x ใน V, $(a+b)x = ax + bx$

10.มีเอกลักษณ์การคูณ 1 อยู่ในฟิลด์ :

สำหรับทุกค่า x ใน V , $1x = \mathrm{x}$

ให้ $v_1, v_2, \ldots, v_n$ เป็นเวกเตอร์ใดๆ ในปริภูมิเวกเตอร์ ค่าผลรวมในรูป $a_1v_1+a_2v_2+\ldots + a_iv_i$ เมื่อ $a_1,a_2,\ldots, a_i$ เป็นค่าสเกลาร์ เรียกว่าค่าผลรวมเชิงเส้น (linear combination) เซตของผลรวมเชิงเส้นทุกๆค่าเป็นผลของการ *แผ่ทั่ว* ของ $v_1, v_2, \ldots , v_n$ โดยจะย่อด้วย Span$(v_1, v_2, \ldots , v_n)$

เซตอันดับ (Ordered Set) คือเซตที่มีการกำหนดความสัมพันธ์หรืออันดับระหว่างสมาชิกในเซต โดยเราเรียกความสัมพันธ์ $\leq$ ว่าอันดับบนเซต P เมื่อ $\leq$ มีสมบัติ 3 ข้อดังนี้

1. สมบัติการสะท้อน (reflexive) :

$a \leq a$ เมื่อ a เป็นสมาชิกใดๆใน P

2. สมบัติการปฏิสมมาตร (antisymmetric) :

ถ้า $a \leq b$ และ $b \leq a$ แล้ว $a = b$ เมื่อ a,b เป็นสมาชิกใดๆใน P

3. สมบัติการถ่ายทอด (transitive) :

ถ้า $a \leq b$ และ $b \leq c$ แล้ว $a \leq c$ เมื่อ a,b,c เป็นสมาชิกใดๆใน P

สำหรับคู่สมาชิกใดๆ a และ b ใน P จะเรียกว่าเปรียบเทียบกันได้ (comparable) ถ้า $a \leq b$ หรือ $b \leq a$ หากเงื่อนไขทั้งสองไม่เป็นจริงจะเรียกว่าเปรียบเทียบกันไม่ได้ (incomparable) และเราจะเรียกเซตอันดับว่า *โซ่* (chain) ถ้าหากสมาชิกทุกคู่ในเซตสามารถเปรียบเทียบกันได้ และเรียกว่า *ปฏิโซ่* (antichain) หากสมาชิกทุกๆคู่ในเซตเปรียบเทียบกันไม่ได้ และเรียกเซตอันดับที่เปรียบเทียบกันได้เพียงบางคู่ในเซตว่า*เซตอันดับบางส่วน* (Partially Ordered Set)

รูปแบบการส่งข้อมูล

รูปแบบการส่งข้อมูลในเครือข่ายแบ่งออกได้เป็น 3 ประเภทใหญ่ตามเป้าหมายที่ต้องการส่ง

1. การส่งข้อมูลแบบยูนิคาสต์ (Unicast) ยูนิคาสต์เป็นการส่งข้อมูลที่มีลักษณะการส่งแบบหนึ่งต่อหนึ่ง คือมีต้นทางหนึ่งตัวต้องการส่งไปยังปลายทางหนึ่งตัว ยูนิคาสต์เป็นรูปแบบการส่งข้อมูลที่พบได้ทั่วไปและมีการใช้งานเยอะ

2. การส่งข้อมูลแบบมัลติคาสต์ (Multicast) เป็นการส่งข้อมูลที่มีลักษณะการส่งแบบหนึ่งต่อหลาย คือมีต้นทางหนึ่งตัวต้องการส่งไปยังปลายทางหลายตัว โดยปลายทางเป็นสมาชิกที่เจาะจงกลุ่มหนึ่งซึ่งอยู่ในเครือข่าย แต่ไม่ใช่สมาชิกทั้งหมดในเครือข่าย

3. การส่งข้อมูลแบบบรอดคาสต์ (Broadcast) เป็นการส่งข้อมูลที่มีลักษณะการส่งแบบหนึ่งต่อหลายเช่นเดียวกับมัลติคาสต์ แต่ปลายทางของการส่งแบบบรอดคาสต์นั้นคือสมาชิกทั้งหมดที่อยู่ในเครือข่าย ต่างจากมัลติคาสต์ที่ส่งไปยังกลุ่มสมาชิกเพียงบางส่วนในเครือข่าย

การส่งข้อมูลระหว่างต้นทางปลายทางหลายคู่

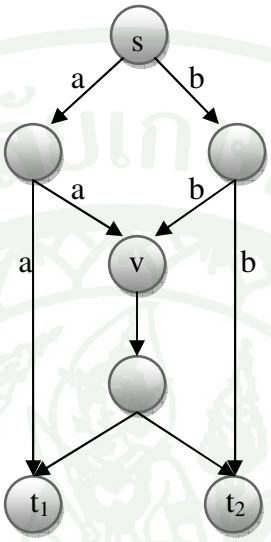
การส่งข้อมูลระหว่างต้นทางปลายทางหลายคู่เป็นการส่งข้อมูลที่มีจำนวนต้นทางเท่ากับจำนวนปลายทาง โดยต้นทางแต่ละตัวจะมีปลายทางที่เป็นคู่อยู่กับต้นทางนั้นๆ ในการส่งข้อมูลแบบนี้ต้นทางจะต้องการส่งข้อมูลไปยังปลายทางเพียงตัวเดียวที่เป็นคู่กับตัวมัน หรืออาจมองได้ว่าเป็นการส่งข้อมูลที่รวมการส่งแบบหนึ่งต่อหนึ่งจำนวนหลายการส่งไว้ด้วยกัน

การเข้ารหัสเครือข่าย (Network Coding)

ในการส่งข้อมูลตามปกติข้อมูลจะถูกส่งอยู่ภายในแพคเกต (Packet) โดยอุปกรณ์จะรู้แค่เพียงว่าแพคเกตนั้นมีเป้าหมายไปที่ใดแต่ไม่สามารถรู้ถึงข้อมูลที่อยู่ภายในแพคเกตได้ การเข้ารหัสเครือข่ายอุปกรณ์จะสามารถดูข้อมูลในแพคเกตจากหลายๆแพคเกตและนำข้อมูลเหล่านั้นมารวมกันด้วยวิธีการบางอย่างได้ ซึ่งในที่นี้เราจะเรียกว่าเป็นการเข้ารหัส จากนั้นอุปกรณ์จะนำข้อมูลที่ได้จากการเข้ารหัสไปส่งโดยใช้แพคเกตใหม่ และปลายทางจะสามารถถอดรหัสได้ถ้าหากได้รับข้อมูลที่มีการเข้ารหัสเป็นจำนวนมากเพียงพอ

Ahlswede *et al.* (2000) ได้แสดงว่าในการส่งแบบมัลติคาสต์นั้นจะมีปัญหาในการส่งข้อมูลเนื่องจากมีการใช้การเชื่อมต่อร่วมกันทำให้ไม่สามารถส่งข้อมูลไปได้เต็มประสิทธิภาพ และการเข้ารหัสเครือข่ายสามารถทำให้การส่งข้อมูลในเครือข่ายมีประสิทธิภาพมากขึ้นได้

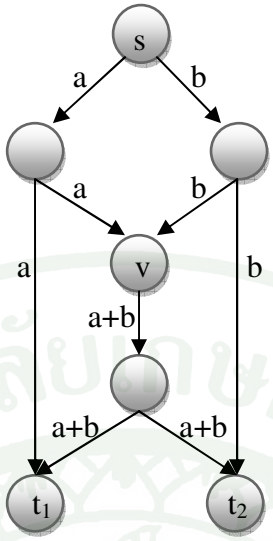
เราจะแสดงตัวอย่างการส่งข้อมูลที่หากเรายอมให้มีการประมวลผลข้อมูลที่โหนดกลางทางก่อนทำการส่งต่อจะสามารถส่งข้อมูลได้อย่างมีประสิทธิภาพมากขึ้น โดยเราจะใช้กราฟแบบมีทิศทางในการแสดงลักษณะของเครือข่าย



ภาพที่ 1 ตัวอย่างเครือข่ายที่มีการส่งแบบมัลติคาสต์

สมมติให้เครือข่ายมีต้นทางคือ s และต้องการส่งข้อมูลสองตัว a และ b ไปยังปลายทางสองตัว t_1 และ t_2 ดังภาพที่ 1 โดยแต่ละเส้นเชื่อมแทนการเชื่อมต่อที่มีความสามารถในการส่งเท่ากับ 1 หน่วยข้อมูล จะเห็นว่าโหนด v ต้องการส่งข้อมูลมากกว่าความสามารถในการส่ง หากทำการส่งข้อมูลตามปกติ โหนด v จำเป็นต้องเลือกส่งข้อมูล a หรือ b ไปทีละครั้ง เนื่องจากสามารถส่งข้อมูลได้เพียงหนึ่งหน่วยข้อมูล การส่งข้อมูลไปยังปลายทางทั้งสองโหนด v จึงต้องส่งข้อมูลสองครั้ง

หากมีการเข้ารหัสเครือข่ายโหนด v สามารถนำข้อมูล a และ b มาสร้างเป็นข้อมูลใหม่ได้ โดยให้ข้อมูลใหม่คือ a+b ข้อมูลนี้เมื่อส่งไปยังปลายทางแล้ว ปลายทางสามารถแปลงข้อมูลกลับมาเป็นข้อมูลที่ต้องการได้ กล่าวคือ t_1 สามารถนำข้อมูลที่ได้รับมาลบกันเพื่อหาข้อมูล b ได้ ในทำนองเดียวกัน t_2 สามารถนำข้อมูลที่ได้รับมาหาข้อมูล a ได้



ภาพที่ 2 เครือข่ายที่มีการเข้ารหัสเครือข่าย

การเข้ารหัสเครือข่ายเชิงเส้น (Linear Network Coding)

เนื่องจากวิธีการเข้ารหัสเครือข่ายในตอนแรกนั้นยังมีความยุ่งยากและค่อนข้างซับซ้อนอยู่ Li *et al.* (2003) จึงได้แสดงว่าการเข้ารหัสเครือข่ายสำหรับการส่งข้อมูลแบบมัลติคาสต์นั้นสามารถทำได้โดยให้ข้อมูลที่เข้ารหัสเป็นผลรวมเชิงเส้นของข้อมูลที่ได้รับ และแสดงว่ามีอัลกอริทึมเชิงละโมบที่ใช้สร้างการเข้ารหัสได้แต่ยังไม่ใช่วิธีที่ดีสุดในการสร้างการเข้ารหัสเครือข่าย การเข้ารหัสเครือข่ายที่ใช้ผลรวมเชิงเส้นของข้อมูลในการเข้ารหัสนี้เราจะเรียกว่า*การเข้ารหัสเครือข่ายเชิงเส้น*

หลังจากมีการแสดงว่าการเข้ารหัสเชิงเส้นนั้นเพียงพอที่จะนำไปใช้ได้ (Li *et al.*, 2003) แต่ยังไม่มีขั้นตอนวิธีที่ดีในการหาวิธีเข้ารหัสเครือข่าย Jaggi *et al.* (2005) จึงได้การนำเสนอวิธีการสร้างการเข้ารหัสเครือข่ายเชิงเส้นสำหรับการส่งข้อมูลแบบมัลติคาสต์ภายในเวลาที่เป็นฟังก์ชันพหุนาม โดยวิธีการคือหาเส้นทางของการส่งข้อมูลในเครือข่ายและนำมาหาการเข้ารหัสตามลำดับของเส้นเชื่อมที่ปรากฏในเส้นทางในเครือข่ายเริ่มจากต้นทางไปยังปลายทาง ในแต่ละเส้นเชื่อมการเข้ารหัสจะสุ่มค่าสัมประสิทธิ์ที่ใช้ในผลรวมเชิงเส้น ซึ่งผลรวมเชิงเส้นจากการเข้ารหัสที่สร้างขึ้นมานี้จะต้องเป็นอิสระเชิงเส้นต่อกันกับผลรวมในทุกๆเส้นทางที่ส่งไปยังเป้าหมายเดียวกัน เพื่อให้สุดท้ายเมื่อส่งถึงเป้าหมายแล้วจะสามารถถอดรหัสได้ หากตรวจสอบแล้วไม่เป็นอิสระเชิงเส้นต่อกันจะทำการหาการเข้ารหัสใหม่ โดยเลือกใช้ค่าสัมประสิทธิ์อื่น

ค่าสัมประสิทธิ์ที่ใช้นี้จะสุ่มจากฟิลด์จำกัด $\mathfrak{I}$ โดยความน่าจะเป็นที่ผลรวมเชิงเส้นจากการเข้ารหัสจะไม่เป็นอิสระเชิงเส้นต่อกันจะแปรผกผันกับขนาดของฟิลด์นี้ นั่นคือหากสัมประสิทธิ์มีค่าที่เป็นไปได้มากผลรวมเชิงเส้นจะมีโอกาสไม่เป็นอิสระเชิงเส้นต่อกันน้อยลง ซึ่งมีผลต่อจำนวนครั้งที่ต้องทำการหาการเข้ารหัส และเวลาในการทำงานทั้งหมดจะอยู่ภายใน $O\left(E \cdot T \cdot H^2\right)$ เมื่อ

E คือจำนวนการเส้นเชื่อมทั้งหมด

T คือจำนวนของเป้าหมาย

H คือความสามารถในการส่งข้อมูลแบบมัลติคาสต์

การเข้ารหัสเครือข่ายสำหรับการสื่อสารระหว่างต้นทางปลายทางหลายคู่

การเข้ารหัสเครือข่ายสำหรับการสื่อสารระหว่างต้นทางปลายทางหลายคู่นั้นเป็นอีกปัญหาที่น่าสนใจ โดยมีลักษณะคล้ายกับการสื่อสารแบบมัลติคาสต์ที่มีหลายปลายทาง แต่การสื่อสารระหว่างต้นทางปลายทางหลายคู่นั้นแต่ละปลายทางจะต้องการเพียงข้อมูลจากต้นทางที่เป็นคู่กับปลายทางนั้นเท่านั้น

ในปี 2003 Lehman and Lehman ได้แสดงให้เห็นว่าในการส่งข้อมูลที่ไม่ใช่มัลติคาสต์นั้น การเข้ารหัสเครือข่ายแบบเชิงเส้นไม่เพียงพอต่อการส่งข้อมูลในเครือข่ายบางรูปแบบ และในกรณีที่เครือข่ายมีการส่งข้อมูลในลักษณะที่เป็นการส่งข้อมูลระหว่างต้นทางปลายทางหลายคู่นั้น หากไม่จำกัดจำนวนคู่ต้นทางปลายทางจะเป็นปัญหา NP-Hard

Wang and Shroff (2007) ได้พิจารณาการเข้ารหัสเครือข่ายเชิงเส้นในเครือข่ายที่มีเพียง 2 คู่ต้นทางปลายทางซึ่งเป็นจำนวนคู่น้อยสุดที่เป็นไปได้ และแสดงว่าในกรณีนี้สามารถทำการเข้ารหัสเครือข่ายได้โดยใช้การเข้ารหัสเครือข่ายแบบเชิงเส้นและหาได้ภายในเวลาที่เป็นฟังก์ชันพหุนาม แต่วิธีการดังกล่าวไม่สามารถใช้ได้กับเครือข่ายที่มีจำนวนคู่ต้นทางปลายทางมากกว่า 2 ได้

ต่อมาในปี 2008 Iwama *et al.* ได้เสนออัลกอริทึมเพื่อหาการเข้ารหัสเครือข่ายเชิงเส้นในเครือข่ายที่มีจำนวนคู่ต้นทางปลายทางมากกว่า 2 คู่ภายในเวลาที่เป็นฟังก์ชันพหุนาม เมื่อกำหนดให้จำนวนคู่ต้นทางปลายทางนั้นเป็นค่าคงที่ k โดยในงานนี้ Iwama *et al.* ได้แสดงว่าจำเป็นต้องใช้

โหนดเข้ารหัสเพียงไม่เกินจำนวนหนึ่ง จำนวนนี้ขึ้นอยู่กับจำนวนของคู่ต้นทางปลายทางและขนาดของฟิลด์จำกัดที่ใช้ในการเข้ารหัสเครือข่าย โดยจะอธิบายรายละเอียดในหัวข้อถัดไป

อัลกอริทึมของ Iwama *et al.*

ในหัวข้อนี้จะนิยามปัญหาและกล่าวถึงอัลกอริทึมเพื่อหาการเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทางปลายทางจำนวน k คู่ของ Iwama *et al.* และจำนวนของโหนดเข้ารหัสที่พวกเขาได้แสดงไว้

นิยาม สมมติให้โหนด v ได้รับข้อมูลเข้ามาเป็น x และ y ตามลำดับ *การเข้ารหัสของโหนด v* เขียนแทนด้วย $\sigma(v)$ เป็นเวกเตอร์แสดงถึงการเข้ารหัสเครือข่ายเชิงเส้นของโหนด v โดยกำหนดให้ $\sigma(v)=(a,b)$ เมื่อข้อมูลที่จะส่งต่อไปนั้นเท่ากับ $ax+by$ เมื่อ a และ b อยู่ในฟิลด์จำกัด $\mathfrak{I}$ ที่ใช้ในการเข้ารหัสเครือข่าย โดยหากทั้ง a และ b ไม่เท่ากับ 0 จะเรียกโหนด v นี้ว่าเป็น *โหนดเข้ารหัส* (coding vertex)

นิยาม การเข้ารหัสเครือข่าย σ หมายถึงเซตของการเข้ารหัสเครือข่ายของโหนดเข้ารหัสทั้งหมดที่มี เมื่อการเข้ารหัสเครือข่ายของโหนดเข้ารหัส v ใดๆคือ $\sigma(v)$

นิยาม *ปัญหาการเข้ารหัสเครือข่ายเชิงเส้นสำหรับการสื่อสารระหว่างต้นทางปลายทางหลายคู่* คือปัญหาที่ได้รับกราฟอวัฏจักรระบุทิศทางและคู่ต้นทางกับปลายทางจำนวน k คู่ และมีเป้าหมายคือการหาการเข้ารหัสเครือข่ายเชิงเส้นให้กับโหนดเข้ารหัสทั้งหมดที่มีในกราฟ โดยปลายทางแต่ละตัวได้รับเฉพาะข้อมูลที่มาจากต้นทางที่เป็นคู่กับตัวมันเท่านั้น และเรากล่าวว่าการเข้ารหัสเครือข่าย σ *ใช้งานได้* หากการเข้ารหัสเครือข่าย σ อยู่ในคำตอบที่เป็นไปได้ของปัญหานี้

Iwama *et al.* สมมติว่ากราฟที่ได้รับมีลักษณะเป็น *2/1 Restricted Graph* ซึ่งเป็นกราฟที่มีข้อจำกัดเพิ่มขึ้นมาคือสำหรับโหนดใดๆที่ไม่ใช่ต้นทางและปลายทางจะมีคู่ (indegree,outdegree) เป็น (2,1) หรือ (1,2) ได้เท่านั้น และสมมติว่าแหล่งต้นทางทั้งหมดมีคู่ (indegree,outdegree) เป็น (0,1) และปลายทางมีคู่ (indegree, outdegree) เป็น (1,0) ทั้งหมด

กราฟอวัฏจักรระบุทิศทางใดๆสามารถแปลงเป็น 2/1 Restricted Graph ได้โดยเพิ่มจำนวนโหนดและเส้นเชื่อมไปในตำแหน่งโหนดที่ไม่ตรงเงื่อนไข การเข้ารหัสเครือข่ายนั้นจะพิจารณาโหนดเข้ารหัสจากโหนดที่มีคู่ (indegree, outdegree) เป็น (2,1) เท่านั้น กำหนดให้เส้นเชื่อมเข้าโหนด v เส้นหนึ่งเป็น *เส้นเชื่อมซ้าย* และอีกเส้นหนึ่งเป็น *เส้นเชื่อมขวา* ข้อมูลที่ส่งต่อไปจะมาจากผลรวมเชิงเส้นของข้อมูลที่ได้รับจากเส้นเชื่อมเข้าทั้งสอง และเราจะเรียกโหนดที่มีคู่ (indegree, outdegree) เป็น (1,2) ว่า*โหนดทางแยก* (Fork vertex)

อัลกอริทึมจะต้องหาการเข้ารหัสให้กับโหนดเข้ารหัสทั้งหมด ดังนั้นหากมีจำนวนโหนดเข้ารหัสเป็นจำนวนมากเวลาที่ใช้ในการทำงานก็จะมากตามไปด้วย Iwama *et al.* จึงได้แสดงว่าจำนวนโหนดเข้ารหัสที่ต้องใช้นั้นไม่จำเป็นต้องมากเกินจำนวนหนึ่ง โดยหากมีการเข้ารหัสเครือข่ายที่ใช้โหนดเข้ารหัสมากกว่าจำนวนดังกล่าวแล้ว จะสามารถแปลงการเข้ารหัสเพื่อให้จำนวนโหนดเข้ารหัสลดลงโดยผลของการเข้ารหัสเครือข่ายยังคงเดิมอยู่ได้

การแปลงการเข้ารหัสนี้ทำได้โดยการเปลี่ยนการเข้ารหัสเครือข่ายให้บางเส้นเชื่อมมีค่าของข้อมูลที่ส่งเป็น 0 แทน จากนั้นพิจารณาเสมือนว่าไม่มีเส้นเชื่อมนั้นอยู่ และมองว่าโหนดมีคู่ (indegree,outdegree) เป็น (1,1) ซึ่งแทนด้วยเส้นเชื่อมธรรมดาได้ โดยเราจะนิยามวิธีการเปลี่ยนการเข้ารหัสดังนี้

นิยาม สมมติให้โหนด v มีการเข้ารหัส $\sigma(v)=(a,b)$ *การเปลี่ยนทางซ้ายไป* α หมายถึงการเปลี่ยนการเข้ารหัสของโหนดให้เป็น $(a+\alpha,b)$ และเรียกว่า *การตัดทางซ้าย* ถ้าหาก $\alpha=-a$ ในทำนองเดียวกัน *การเปลี่ยนทางขวาไป* β คือการเปลี่ยนให้การเข้ารหัสของโหนดเป็น $(a,b+\beta)$ และ *การตัดทางขวา* ถ้า $\beta=-b$

จากนี้เราจะแสดงว่าเราสามารถใช้การเปลี่ยนนี้แปลงการเข้ารหัสให้มีจำนวนโหนดเข้ารหัสลดลงโดยให้ผลของการเข้ารหัสเครือข่ายยังคงเดิมได้ โดยทำการตัดทางซ้ายหรือทางขวาที่โหนดเข้ารหัสหนึ่งและทำการเปลี่ยนการเข้ารหัสที่อีกโหนดเข้ารหัสเพื่อชดเชยผลที่เปลี่ยนไปจากการตัด โดยจำเป็นต้องใช้นิยามเพิ่มดังนี้

นิยาม *เวกเตอร์ข้อมูลบนเส้นเชื่อม* L คือเวกเตอร์ที่แสดงว่าข้อมูลที่ส่งในเส้นเชื่อม L มีค่าเท่าใดเมื่อเทียบกับข้อมูลต้นทาง โดยหากสมมติให้ต้นทาง s_i ส่งข้อมูลเป็น x_i ข้อมูลที่ส่งในเส้นเชื่อม L

จะต้องเป็นผลรวมเชิงเส้นของข้อมูลต้นทางทั้งหมดคือ $\sum_{i=1}^{k}(a_i x_i)$ เวกเตอร์ข้อมูลบนเส้นเชื่อม L คือ $(a_1, a_2, a_3, \ldots, a_k)$

นิยาม *ผลกระทบจากโหนด v ไปยังปลายทางตัวที่ i* หมายถึงค่าที่ส่งไปยังปลายทางตัวที่ i เมื่อต้นทางทั้งหมดส่งข้อมูลเป็น 0 และบังคับให้ข้อมูลที่ออกจากโหนด v เป็น 1 เขียนแทนด้วย $e_i(v)$

นิยาม *เวกเตอร์ผลกระทบจากโหนด v* แทนด้วย $E(v)$ คือเวกเตอร์ของผลกระทบจากโหนด v ไปยังปลายทางแต่ละตัว $E(v) = [e_1(v), e_2(v), \ldots, e_k(v)]$

สมมติโหนด v มีข้อมูลเข้ามาเป็น x และ y ทางเส้นเชื่อมซ้ายกับเส้นเชื่อมขวาตามลำดับ และมีผลกระทบจากโหนด v ไปยังปลายทางตัวที่ i เป็น e_i การเปลี่ยนทางซ้ายไป a จะทำให้ข้อมูลที่ส่งไปยังปลายทางตัวที่ i มีค่าเปลี่ยนไป $a \cdot x \cdot e_i$ ในทำนองเดียวกันการเปลี่ยนทางขวาไปb จะทำให้ข้อมูลที่ส่งไปยังปลายทางตัวที่ i มีค่าเปลี่ยนไป $b \cdot y \cdot e_i$

จะเห็นว่าถ้าเรามีโหนดที่มีผลกระทบไปยังปลายทางเหมือนกัน 2 โหนด หากว่าเราเปลี่ยนการเข้ารหัสเครือข่ายของโหนดทั้งสอง โดยให้โหนดแรกข้อมูลที่ส่งมีค่าเปลี่ยนไป a และจากโหนดที่สองมีค่าเปลี่ยนไป $-a$ การเข้ารหัสเครือข่ายจะเปลี่ยนไป โดยที่การส่งข้อมูลไปยังปลายทางยังคงเดิมอยู่

ทฤษฎีบทที่ 1 *หากมีการเข้ารหัสเครือข่ายที่ใช้งานได้โดยใช้โดยมีโหนดเข้ารหัสทั้งหมดมากกว่า $|\Im|^{3k}$ โหนดจะมีการเข้ารหัสเครือข่ายอีกแบบรูปหนึ่งที่ใช้งานได้โดยมีโหนดเข้ารหัสทั้งหมดไม่เกิน $|\Im|^{3k}$ โหนด*

พิสูจน์ สมมติให้มีโหนดเข้ารหัส 2 โหนดที่มีข้อมูลเข้าทั้งสองข้างเป็น u และ v และมีผลกระทบไปยังปลายทางเหมือนกันและการเข้ารหัสเครือข่ายเป็น (a_1,b_1) กับ (a_2,b_2) โดยโหนดแรกไม่เป็นผู้สืบเชื้อสาย (descendant) มาจากโหนดที่สอง ผลกระทบจากโหนดแรกไปจนถึงเส้นเชื่อมซ้ายของโหนดที่สองเป็น e_L และผลกระทบจากโหนดแรกไปจนถึงเส้นเชื่อมขวาของโหนดที่สองเป็น e_R เราจะแบ่งออกเป็น 3 กรณีดังนี้

กรณีแรก $a_1e_L \neq 1$ เราจะทำการตัดทางซ้ายที่โหนดแรก การตัดนี้ทำให้ข้อมูลที่ส่งของโหนดแรกเปลี่ยนไป $-a_1u$ และข้อมูลเข้าทางซ้ายของโหนดที่สองเปลี่ยนเป็น $(1-a_1e_L)u$ เราสามารถทำการเปลี่ยนทางซ้ายที่โหนดที่สองไป $a_1/(1-a_1e_L)$ เพื่อให้ข้อมูลของโหนดที่สองเปลี่ยนไป $-a_1u$ ได้

กรณีที่สอง $b_1e_R \neq 1$ ในทำนองเดียวกับกรณีแรก เราจะทำการตัดทางขวาที่โหนดแรกและทำการเปลี่ยนทางขวาไป $b_1/(1-b_1e_R)$ ที่โหนดที่สอง

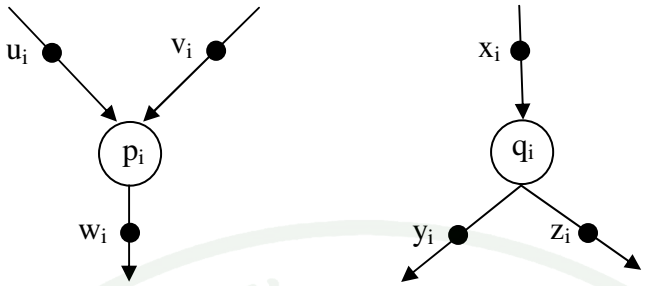
กรณีสุดท้าย $a_1e_L = b_1e_R = 1$ เราจะทำทั้งการตัดทางซ้ายและการตัดทางขวาที่โหนดแรก การตัดนี้จะทำให้โหนดแรกส่งข้อมูลเปลี่ยนไป $-(a_1u+b_1v)$ และข้อมูลเข้าทางซ้ายและขวาของโหนดที่สองเป็น $-(b_1/a_1)v$ กับ $-(a_1/b_1)u$ แทน โดยการเปลี่ยนทางซ้ายไป $-a_1$ และเปลี่ยนทางขวาไป $-b_1$ โหนดที่สองจะมีข้อมูลที่ส่งเปลี่ยนไป $+(a_1u+b_1v)$ ซึ่งจะไปหักล้างกับการเปลี่ยนที่โหนดแรก

เนื่องจากเวกเตอร์ข้อมูลและเวกเตอร์ผลกระทบเป็นเวกเตอร์ k มิติบนฟิลด์ $\Im$ ดังนั้นหากมีโหนดเข้ารหัสมากกว่า $|\Im|^{3k}$ จะต้องมีโหนดบางคู่ที่ตรงตามเงื่อนไขข้างต้น และสามารถทำการตัดตามที่แสดงไว้ เพื่อหาการเข้ารหัสเครือข่ายอีกแบบที่มีโหนดเข้ารหัสไม่เกิน $|\Im|^{3k}$ ได้

อัลกอริทึมของ Iwama et al. นั้นจะเริ่มจากการเลือกโหนดเข้ารหัสและโหนดทางแยกออกมาจากโหนดทั้งหมดที่ไม่ใช่ต้นทางและปลายทาง การเลือกนี้เป็นไปได้มากที่สุด

$$O\left(\binom{N}{C}^2\right) = O(N^{2C}) \tag{1}$$

เมื่อ N คือจำนวนโหนด และ C คือจำนวนโหนดเข้ารหัส หลังจากเลือกโหนดเข้ารหัสและโหนดทางแยกแล้ว จะทำการเพิ่มโหนด u_i และ v_i บนเส้นเชื่อมซ้ายและเส้นเชื่อมขวาของโหนดเข้ารหัส p_i และเพิ่มโหนด w_i ที่เส้นเชื่อมออกจากโหนด p_i เพิ่มโหนด x_i บนเส้นเชื่อมเข้าของโหยดทางแยก q_i และเพิ่มโหนด y_i และ z_i ที่เส้นเชื่อมออกทางซ้ายและทางขวาจากโหนด q_i ตามลำดับดังภาพที่ 3 และสร้างเซตของโหนด 2 เซตคือ OUT และ IN



ภาพที่ 3 ตำแหน่งการเพิ่มโหนดบนเส้นเชื่อม

$$OUT = \{s_1, \ldots, s_k, w_1, \ldots, w_C, y_1, \ldots, y_C, z_1, \ldots, z_C\} \quad (2)$$

$$IN = \{t_1, \ldots, t_k, u_1, \ldots, u_C, v_1, \ldots, v_C, x_1, \ldots, x_C\} \quad (3)$$

จากนั้นทำ perfect matching ระหว่างเซต OUT และ IN และทำการหา vertex disjoint path ที่ในกราฟที่เชื่อมจาก OUT ไปยัง IN โดยไม่ผ่านโหนดเข้ารหัสและโหนดทางแยกที่เลือกไว้ เพื่อหาว่ามีรูปแบบการเชื่อมต่อที่เป็นไปได้หรือไม่ โดยการหา vertex disjoint path นี้ใช้อัลกอริทึมของ Fortune *et al.* (1980) ซึ่งใช้เวลาเป็นพหุนามบน N แต่อาจเป็นเอกซ์โพเนนเชียลบน C ก็ได้

ถ้าหากมี vertec disjoint path ที่ใช้ได้ อัลกอริทึมจะทำการเลือกการเข้ารหัสเครือข่ายและตรวจสอบว่าการเข้ารหัสเครือข่ายนั้นใช้งานได้หรือไม่ ซึ่งการเข้ารหัสเครือข่ายนี้เป็นได้มากที่สุด $|\Im|^{2C}$ เนื่องจากแต่ละโหนดเข้ารหัส มีการเข้ารหัสเครือข่ายได้ $|\Im|^2$ รูปแบบและโหนดเข้ารหัสมีทั้งหมด C โหนด

เวลาที่ใช้ทำงานของอัลกอริทึมเมื่อรวมทุกขั้นตอนแล้วคือ $O\left(N^{2C} \cdot (3C+k)! |\Im|^{2C} \cdot f(N,C)\right)$ เมื่อ $f(N,C)$ เป็นเวลาในการหา vertex disjoint path ตามอัลกอริทึมของ Fortune *et al.* (1980)

อุปกรณ์และวิธีการ

อุปกรณ์

1. อุปกรณ์สำหรับวิเคราะห์และพิสูจน์เชิงทฤษฎี
   1.1 สมุดบันทึก
   1.2 ดินสอและยางลบ

2. อุปกรณ์ในการสำหรับหาข้อมูลและบันทึกผล
   2.1 เครื่องคอมพิวเตอร์
   2.2 ระบบปฏิบัติการวินโดส์
   2.3 ชุดโปรแกรมไมโครซอฟท์ออฟฟิส

วิธีการ

1. พัฒนาและปรับปรุงอัลกอริทึมสำหรับการเข้ารหัสเครือข่ายสำหรับปัญหาการสื่อสารระหว่างต้นทางและปลายทางหลายคู่

เราใช้แนวคิดของ Iwama *et al.* ที่พิจารณาขีดจำกัดบนของจำนวนโหนดเข้ารหัสมาพัฒนาต่อเพื่อหาขีดจำกัดบนที่แน่นยิ่งขึ้น และพิสูจน์ขีดจำกัดบนที่แน่นขึ้นนี้โดยใช้หลักทางพีชคณิตเชิงเส้นและทฤษฎีบทของ Dilworth

ผลและวิจารณ์

ผล

1. พัฒนาและปรับปรุงอัลกอริทึมสำหรับการเข้ารหัสเครือข่ายสำหรับปัญหาการสื่อสารระหว่างต้นทางและปลายทางหลายคู่

จากการศึกษาอัลกอริทึมของ Iwama *et al.* พบว่าเราสามารถลดขีดจำกัดบนของจำนวนโหนดเข้ารหัสลงได้โดยการตัดและการเปลี่ยนการเข้ารหัสเครือข่ายที่โหนดต่างๆ โดยวิธีการที่ Iwama *et al.* แสดงไว้นั้นพิจารณาเฉพาะในกรณีที่โหนดเข้ารหัสทั้งสองมีข้อมูลเข้าเหมือนกันเท่านั้น เราจึงพิจารณาในกรณีที่กว้างขึ้นกล่าวคือข้อมูลเข้าของโหนดเข้ารหัสไม่จำเป็นต้องเหมือนกันทั้งหมด

เราสามารถลดขีดจำกัดบนของจำนวนโหนดเข้ารหัสจาก $|\Im|^{3k}$ เป็น $k^2|\Im|^{2k}$ ได้ ขีดจำกัดบนที่แน่นขึ้นนี้ทำให้เวลาในการทำงานของอัลกอริทึมของ Iwama *et al.* ลดลงเช่นกัน ในการพิสูจน์เรามีนิยามเพิ่มเติมดังนี้

นิยาม *ผลกระทบจากโหนด v ไปยังเส้นเชื่อม L* หมายถึงค่าที่ส่งบนเส้นเชื่อม L เมื่อต้นทางทั้งหมดส่งข้อมูลเป็น 0 และบังคับให้โหนด v มีข้อมูลออกเป็น 1 เขียนแทนด้วย $e_L(v)$ หากเส้นเชื่อม L ไม่สามารถไปถึงได้จาก v เราจะให้ผลกระทบนี้เป็น 0 และใช้ $e_i(v)$ แทนผลกระทบจากโหนด v ไปยังเส้นเชื่อมเข้าปลายทาง t_i เมื่อ $1 \le i \le k$

นิยาม *เวกเตอร์ผลกระทบจากโหนด v* แทนด้วย $E(v)$ คือเวกเตอร์ของผลกระทบจากโหนด v ไปยังปลายทางแต่ละตัว $E(v) = [e_1(v), e_2(v), \ldots, e_k(v)]$

นิยาม *เวกเตอร์ผลกระทบจากโหนด v ไม่ผ่านเส้นเชื่อม L* คือเวกเตอร์ผลกระทบจากโหนด v หลังจากตัดเส้นเชื่อม L ออกจากกราฟ เขียนแทนด้วย $X_L(v)$ และให้ *เวกเตอร์ผลกระทบจากโหนด v ที่ผ่านเส้นเชื่อม* L คือเวกเตอร์ผลกระทบ $I_L(v) = E(v) - X_L(v)$

เราพิจารณาว่าเครือข่ายสามารถมองเป็นเซตลำดับที่นิยามความสัมพันธ์ $\prec$ ดังนี้ สำหรับโหนด u และ v ใดๆในเซต เราจะกล่าวว่า $u \prec v$ ก็ต่อเมื่อมีบางเส้นเชื่อมเข้าของ v ไปถึงได้จาก u หรืออาจกล่าวได้ว่า u เป็นบรรพบุรุษของ v

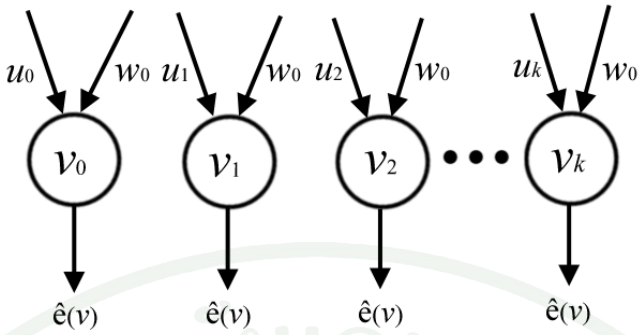
ทฤษฎีบทย่อยที่ 1 *ถ้าหากมีโหนดเข้ารหัสมากกว่า* $k^2|\Im|^k$ *ในเซตลำดับ* C *แล้วจะต้องมี ปฏิโซ่* $C' \subseteq C$ *ที่มีขนาด* $k+1$ *หรือมี โซ่* $C' \subseteq C$ *ที่มีขนาด* $k|\Im|^k+1$

ทฤษฎีบทย่อยนี้เป็นสิ่งที่เห็นได้ค่อนข้างชัดเจน โดยจากทฤษฎีบทของ Dilworth (1950) เรารู้ว่าขนาดที่ใหญ่ที่สุดของปฏิโซ่จะเท่ากับจำนวนโซ่น้อยที่สุดที่สามารถแบ่งได้จากเซตลำดับ ดังนั้นหากไม่มีปฏิโซ่ที่มีขนาดถึง $k+1$ จะต้องมีโซ่ขนาดอย่างน้อย $k|\Im|^k+1$ ในทำนองเดียวกันหากไม่มีโซ่ที่ขนาดถึงโซ่ที่มีขนาดถึง $k|\Im|^k+1$ จะมีปฏิโซ่ขนาดอย่างน้อย $k+1$

ทฤษฎีบทย่อยที่ 2 *ถ้าหากมีโหนดเข้ารหัสจำนวนมากกว่า* $k^2|\Im|^{2k}$ *แล้วจะต้องมีเซตของโหนดเข้ารหัส* C' *ที่เวกเตอร์ผลกระทบเหมือนกัน และ* C' *เป็นปฏิโซ่ที่ขนาด* $k+1$ *หรือเป็นโซ่ที่ขนาด* $k|\Im|^k+1$

พิสูจน์ จากการที่เวกเตอร์ผลกระทบเป็นเวกเตอร์ในปริภูมิ k มิติบนฟิลด์ $\Im$ ดังนั้นเวกเตอร์ผลกระทบจะแตกต่างกันได้มากสุด $|\Im|^k$ แบบ หากเรามีโหนดเข้ารหัสมากกว่า $k^2|\Im|^{2k}$ แล้วจะต้องมีบางเซตของโหนดเข้ารหัสที่เวกเตอร์ผลกระทบเหมือนกันซึ่งมีขนาดมากกว่า $k^2|\Im|^k$ และจากทฤษฎีบทย่อยที่ 1 แสดงว่าต้องมีเซต C' อยู่ในนี้

หลังจากนี้เราจะแสดงว่าในกรณีที่มีปฏิโซ่ขนาดมากกว่า k หรือโซ่ขนาดมากกว่า $k|\Im|^k$ ซึ่งมีเวกเตอร์ผลกระทบเหมือนกันแล้ว เราสามารถเปลี่ยนการเข้ารหัสเครือข่ายให้โหนดเข้ารหัสลดลงได้โดยการส่งข้อมูลปลายทางไม่เปลี่ยนแปลง



ภาพที่ 4 ปฏิโซ่ขนาด k+1 ที่มีเวกเตอร์ผลกระทบเหมือนกัน

ทฤษฎีบทย่อยที่ 3 *ให้ C เป็นปฏิโซ่ของโหนดเข้ารหัสที่มีเวกเตอร์ผลกระทบเหมือนกัน และมีขนาดมากกว่า* $k+1$ *สำหรับการเข้ารหัสเครือข่าย* σ *ที่ใช้โหนดเข้ารหัส* Q *โหนดจะมีการเข้ารหัสเครือข่าย* σ' *ที่ใช้โหนดเข้ารหัส* Q-1 *โหนดและส่งข้อมูลไปยังปลายทางได้เหมือนกับ* σ

พิสูจน์ ให้โหนดในปฏิโซ่คือ $v_0, v_1, \ldots, v_k$ มีข้อมูลเข้าทางซ้ายเป็น $u_0, u_1, \ldots, u_k$ ตามลำดับ ดังภาพที่ 4 และมี $\sigma(v_i) = (a_i, b_i)$ เนื่องจากข้อมูลเข้าแต่ละโหนดมาจากผลรวมเชิงเส้นของข้อมูลต้นทาง k ตัว เราจึงสามารถหา r_i ที่ทำให้ $u_0 = \sum_{i=1}^{k} r_i u_i$ ได้ หากเราทำการตัดทางซ้ายที่โหนด v_0 จะทำให้ข้อมูลที่ส่งของ v_0 เปลี่ยนไป $-u_0 a_0$ หรือเท่ากับ $-\sum_{i=1}^{k} r_i u_i a_0$ เมื่อเราทำการเปลี่ยนทางซ้ายที่โหนด v_i ไป $a_0 r_i$ สำหรับ $1 \le i \le k$ แล้วผลรวมของข้อมูลออกที่เปลี่ยนไปจากโหนด v_1 ถึง v_k คือ $+\sum_{i=1}^{k} r_i u_i a_0$ ดังนั้นเราสามารถหาการเข้ารหัสเครือข่ายใหม่ที่เปลี่ยนให้ $\sigma'(v_0)=(0,b_0)$ และ $\sigma'(v_0)=(a_i + a_0 r_i, b_0)$ เมื่อ $1 \le i \le k$ โดยที่ผลการส่งข้อมูลไปยังปลายทางเหมือน σ ได้

สำหรับกรณีที่เป็นโซ่นั้นจะทำยากขึ้นและคิดแบบปฏิโซ่ไม่ได้เนื่องจากการเปลี่ยนการเข้ารหัสของโหนดในโซ่จะมีผลกับข้อมูลเข้าและเวกเตอร์ผลกระทบของโหนดอื่นๆในโซ่ด้วย โดยในที่นี้เราจะเริ่มพิจารณาจากกรณีที่โซ่มีเพียง 2 โหนดก่อน

ทฤษฎีบทย่อยที่ 4 *ถ้ามีคู่โหนด* v_1, v_2 *ที่*

- $v_1 \prec v_2$ *และ*
- *มีข้อมูลเข้าทางซ้ายเหมือนกันคือ* u *และ*
- *มีเวกเตอร์ผลกระทบเหมือนกัน นั่นคือ* $E(v_1) = E(v_2)$ *และ*

- $X_L(v_1) \neq 0$ *เมื่อ* L *คือเส้นเชื่อมเข้าทางซ้ายของ* v_2

จะมีการเข้ารหัสเครือข่าย $\sigma'(v_2) = (0, B)$ *เมื่อ* $\sigma(v_2) = (A, B)$ *และ* $\sigma'(w) = \sigma(w)$ *ทุกๆ* $w \in V - \{v_1, v_2\}$ *ที่ส่งข้อมูลไปยังปลายทางได้เหมือนกับ* σ

พิสูจน์ หากเราทำการปลี่ยนทางซ้ายไป α ที่ v_1 จะได้ว่าข้อมูลที่ส่งจะเปลี่ยนไป $\alpha \cdot u$ และข้อมูลเข้าทางซ้ายของโหนด v_2 จะมีค่าเป็น $u_1(1 + \alpha \cdot e_L(v_1))$ และเมื่อทำการตัดทางซ้ายที่โหนด v_2 ข้อมูลที่ส่งจะเปลี่ยนไป $-A \cdot u_1(1 + \alpha \cdot e_L(v_1))$ หากเราเลือกให้ $\alpha = A/(1 - A \cdot e_L(v_1))$ จะได้ $\alpha \cdot u = A \cdot u_1(1 + \alpha \cdot e_L(v_1))$ ซึ่งหักล้างผลของการเปลี่ยนแปลงไปได้ โดยเราสามารถหาค่า α ได้เสมอเพราะ $A \cdot e_L(v_1) \neq 1$ ที่เป็นเช่นนี้เพราะถ้าหากว่า $A \cdot e_L(v_1) = 1$ จากนิยามเราจะได้ว่า

$$\begin{aligned} X_L(v_1) &= E(v_1) - I_L(v_1) \\ &= E(v_1) - E(v_2) \cdot A \cdot e_L(v_1) \\ &= 0 \end{aligned} \tag{4}$$

ซึ่งขัดแย้งกับเงื่อนไขที่ว่า $X_L(v_1) \neq 0$

ต่อจากนี้เราจะแสดงว่าในการเปลี่ยนการเข้ารหัสของโหนดในโซ่นั้น ถ้าหากเวกเตอร์ผลกระทบของโหนดมีทิศทางเดียวกัน หลังการเปลี่ยนแปลงการเข้ารหัสเวกเตอร์ทั้งสองจะยังมีทิศทางเดียวกันอยู่

ทฤษฎีบทย่อยที่ 5 *ถ้ามีคู่โหนด* v_1, v_2 *ที่*

- $v_1 \prec v_2$ *และ*
- *เวกเตอร์ผลกระทบของทั้งคู่มีทิศทางเดียวกัน หรือเขียนได้ว่า* $E(v_1) = \delta \cdot E(v_2)$

หลังจากการเปลี่ยนทางซ้าย(หรือทางขวา)ของโหนด v_2 *และเวกเตอร์ผลกระทบใหม่ของโหนด* v_1 , $E'(v_1)$ *จะยังมีทิศทางเดียวกับ* $E(v_2)$ *อยู่*

พิสูจน์ เมื่อให้ L คือเส้นเชื่อมเข้าทางซ้ายของ v_2 หาก $I_L(v_1) = 0$ การเปลี่ยนทางซ้ายที่ v_2 ไม่มีผลใดๆกับ $E(v_1)$ อยู่แล้ว ดังนั้นเราจะแสดงการพิสูจน์ในกรณีที่ $I_L(v_1) \neq 0$ สมมติให้ $\sigma(v_2) = (a_2, b_2)$ เมื่อพิจารณาเวกเตอร์ผลกระทบเรารู้ว่า

$$E(v_1) = X_L(v_1) + I_L(v_1) = \delta \cdot E(v_2) \tag{5}$$

$$I_L(v_1) = e_L(v_1) \cdot a_2 \cdot E(v_2) \tag{6}$$

ดังนั้น $X_L(v_1)$ จะต้องมีทิศทางเดียวกับ $E(v_2)$ เมื่อทำการเปลี่ยนทางซ้ายที่โหนด v_2 เวกเตอร์ $I'_L(v_1)$ จะมีขนาดเปลี่ยนไปแต่ทิศทางยังคงเดิมอยู่ ส่วน $X_L(v_1)$ นั้นไม่เปลี่ยนแปลงแต่อย่างใด จึงสามารถสรุปได้ว่าเวกเตอร์ $E'(v_1)$ มีขนาดเปลี่ยนไปแต่ยังคงมีทิศทางเดียวกับ $E(v_2)$ อยู่ ส่วนการเปลี่ยนทางขวานั้นสามารถพิสูจน์ได้ในทำนองเดียวกัน

จากทฤษฎีบทย่อยที่ 5 นั้น ทำให้เราสามารถเปลี่ยนแปลงการเข้ารหัสของโหนดในโซ่ได้โดยที่เวกเตอร์ผลกระทบยังมีทิศทางคงเดิม ถ้าหากเวกเตอร์เหล่านั้นมีทิศทางเดียวกันอยู่ก่อนจะมีการเปลี่ยน ในลำดับต่อไปเราจะแสดงว่าเราสามารถการเปลี่ยนการเข้ารหัสของโซ่เพื่อให้ข้อมูลปลายทางมีการเปลี่ยนไปตามที่เราต้องการได้

ทฤษฎีบทย่อยที่ 6 *ถ้ามีโซ่ของโหนดเข้ารหัส* $C = \{v_1, \ldots, v_{h+1}\}$ *ที่*

- $v_1 \prec v_2 \prec \ldots \prec v_{h+1}$
- *เวกเตอร์ผลกระทบของ* $v_{h+1} \neq 0$ *และ*
- *มีข้อมูลเข้าทางซ้ายเหมือนกันคือ* u *และ*
- *สำหรับทุกๆ* $v_i \in C$ *ถ้าหากเวกเตอร์ผลกระทบ* $E(v_i) \neq 0$ *เวกเตอร์ผลกระทบต้องมีทิศทางเดียวกับเวกเตอร์ผลกระทบของ* v_{l+1} *หรือมี* δ_i *ที่ทำให้* $\delta_i \cdot E(v_i) = E(v_{h+1})$
- $e_{L(i+1)}(v_i)a_{i+1} \neq 0$ *สำหรับ* $1 \leq i \leq k$ *เมื่อให้ L(i) เป็นเส้นเชื่อมเข้าทางซ้ายของโหนด* v_i *และ* $\sigma(v_i) = (a_i, b_i)$ *สำหรับทุกๆ* $v_i \in C$ *และ*
- *เวกเตอร์ข้อมูลทางขวาของโหนด* v_i *คือ* $\gamma_{(i,1)} y_1 + \gamma_{(i,2)} y_2 + \cdots + \gamma_{(i,i)} y_i$ *เมื่อ* $\gamma_{(i,i)} \neq 0$ *และ* $\gamma_{(i,1)}, \cdots, \gamma_{(i,i)} \in \Im$ *และเวกเตอร์* $y_1, y_2, \cdots, y_i$ *ทั้งหมดตั้งฉากกัน*

สำหรับการเข้ารหัสเครือข่าย σ *และค่าใดๆ* $\gamma'_1, \gamma'_2 \cdots, \gamma'_l \in \Im$ *จะมีการเข้ารหัสเครือข่าย* σ' *ที่* $\sigma'(v_i) = (a'_i, b'_i)$ *สำหรับทุกๆ* $v_i \in C - \{v_{h+1}\}$ *และ* $\sigma'(v_{h+1}) = (a'_{h+1}, b_{h+1})$ *และ* $\sigma'(w) = \sigma(w)$ *สำหรับ* $w \in V/C$ *ที่ทำให้ข้อมูลเข้าของปลายทาง* t_i *เปลี่ยนไป* $(\gamma'_1 y_1 + \gamma'_2 y_2 + \cdots + \gamma'_l y_l) \cdot e_i(v_{h+1})$

พิสูจน์ เราจะพิสูจน์ทฤษฎีบทย่อยนี้ด้วยการพิสูจน์โดยอุปนัย (induction) บน h

ที่มูลฐาน $h = 1$ พิจารณาคู่โหนด v_1 และ v_2 ถ้าหาก $E(v_1) \neq 0$ เราจะทำการเปลี่ยนทางขวาไปB ที่ v_1 เพื่อให้ข้อมูลเข้าที่ปลายทาง i เปลี่ยนไป $\gamma_1' y_1 \cdot e_i(v_2)$ เรารู้ว่า $\delta_1 \cdot E(v_1) = E(v_2)$ ดังนั้นหากเราทำการเปลี่ยนโดยใช้ $B = \dfrac{\gamma_1'}{\delta_1 y_1}$ เราจะได้การเปลี่ยนข้อมูลตามที่ต้องการ

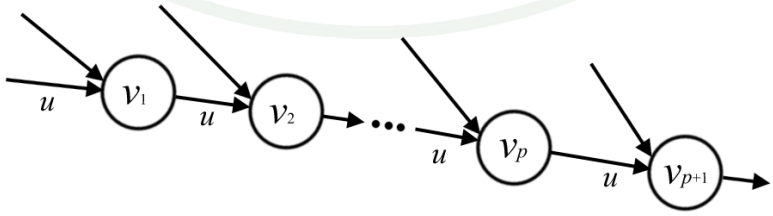
ในกรณีที่ $E(v_1) = 0$ เราจะทำการเปลี่ยนให้ $E(v_1) \neq 0$ ก่อน โดยมีวิธีการคือทำการเปลี่ยนทางซ้ายไป $+e_L(v_1)$ ที่โหนด v_1 การเปลี่ยนนี้ไม่มีผลใดๆกับข้อมูลที่ปลายทางเนื่องจากเวกเตอร์ผลกระทบเป็น 0 และได้ว่า

$$\sigma'(v_1) = (a_1 + \mathrm{e}_{\mathrm{L}2}(\mathrm{v}_1)\ , b_1) \tag{7}$$

จากนั้นเมื่อทำการตัดทางซ้ายที่ v_2 จะทำให้เวกเตอร์ผลกระทบของ v_1 เปลี่ยนเป็น

$$E'(v_1) = X_{L(2)}(v_1) = -e_{L(2)}(v_1) \cdot a_2 \cdot E(v_2) \tag{8}$$

และข้อมูลเข้าปลายทางตัวที่ i เปลี่ยนไป $-a_2 \cdot u \cdot e_i(v_2)$ จากนั้นเมื่อทำการเปลี่ยนทางซ้ายที่ v_1 ไป $-e_{L(2)}(v_1)$ ข้อมูลเข้าปลายทางตัวที่ i จะเปลี่ยนไป $+a_2 \cdot u \cdot e_i(v_2)$ ซึ่งจะหักล้างกับการตัดทางซ้ายที่ v_2 และมีการเข้ารหัส $\sigma''(v_1) = \sigma(v_1)$ และได้ $E(v_1) \neq 0$ ซึ่งสามารถทำการหาการเปลี่ยนการเข้ารหัสได้ดังที่แสดงไว้ข้างต้นแล้ว



ภาพที่ 5 โซ่ขนาด p+1 ที่โหนดมีข้อมูลเข้าทางซ้ายเหมือนกัน

ขั้นอุปนัยตั้งสมมติฐานว่าทฤษฎีเป็นจริงเมื่อ $h = p$ จะแสดงว่าเป็นจริงกับกรณี $h = p+1$ เช่นกัน พิจารณาโหนด v_p และ v_{p+1} ในโซ่ขนาด p+1 ดังภาพที่ 5 ถ้า $E(v_p) = 0$ เราจะทำการเปลี่ยนโดยวิธีการเดียวกับขั้นมูลฐานเพื่อให้

$$E(v_p) = -e_{L(p+1)}(v_p) \cdot a_{p+1} \cdot E(v_{p+1}) \neq 0 \tag{9}$$

หากกำหนดให้ $(\gamma_1' \; y_1 + \gamma_2' y_2 + \cdots + \gamma_p' y_p) \cdot e_i(v_{p+1})$ เป็นการเปลี่ยนแปลงข้อมูลที่ปลายทางตัวที่ i ที่ต้องการโดยการเปลี่ยนทางขวาไป $\frac{\gamma_p'}{\delta_p y_p}$ จะได้ว่าข้อมูลเข้าที่ปลายทางตัวที่ i เปลี่ยนไป $(\phi + \gamma_p' y_p) \cdot e_i(v_{p+1})$ เมื่อ ϕ เป็นเวกเตอร์ที่ขึ้นกับ $y_1, y_2, ..., y_{p-1}$ เท่านั้นดังนั้นจะเหลือการเปลี่ยนของข้อมูลที่เราต้องการอีก

$$\begin{aligned}(\gamma_1' y_1 + \gamma_2' y_2 + \cdots + \gamma_{p-1}' y_{p-1} - \phi) \cdot e_i(v_{p+1}) &= (\gamma_1' y_1 + \gamma_2' y_2 + \cdots + \gamma_{p-1}' y_{p-1} - \phi) \cdot \delta_p \cdot e_i(v_p) \\ &= (\gamma_1'' y_1 + \gamma_2'' y_2 + \cdots + \gamma_{p-1}'' y_{p-1}) \cdot e_i(v_p) \end{aligned} \tag{10}$$

ซึ่งจากสมมติฐานที่ว่าทฤษฎีเป็นจริงที่ $h = p$ แสดงว่าเราสามารถหาการเปลี่ยนนี้จากโหนด $v_1, ..., v_{p-1}$ ได้ และพิสูจน์ว่าทฤษฎีบทย่อยนี้เป็นจริง

จากทฤษฎีบทย่อยนี้ทำให้เราสามารถทำการตัดที่โหนดในโซ่และหาการเปลี่ยนการเข้ารหัสเพื่อมาชดเชยการเปลี่ยนแปลงของข้อมูลที่เกิดจากการตัดนี้ได้

ทฤษฎีบทย่อยที่ 7 *ถ้าหากมีการเข้ารหัสเครือข่าย σ ที่ใช้โหนดเข้ารหัส Q โหนดและมีโซ่ C ของโหนดเข้ารหัสที่มีเวกเตอร์ผลกระทบเหมือนกัน ซึ่งมีขนาดอย่างน้อย $k|\Im|^k + 1$ แล้ว จะมีการเข้ารหัสเครือข่าย σ' ที่มีการส่งข้อมูลไปยังปลายทางเหมือนกับ σ โดยใช้โหนดเข้ารหัสน้อยกว่า Q โหนด*

พิสูจน์ เนื่องจากเวกเตอร์ข้อมูลของเส้นเชื่อมมีได้มากที่สุด $|\Im|^k$ รูปแบบ ดังนั้นจะต้องมีเซต $C' \in C$ ที่มีขนาดอย่างน้อย $k+1$ เขียนแทนด้วย $v_1, v_2, \cdots, v_{k+1}$ เมื่อ $v_1 \prec v_2 \prec \cdots \prec v_{k+1}$ และให้ L_i เป็นเส้นเชื่อมเข้าทางซ้ายของโหนด v_i หากมีคู่โหนด v_i, v_j ที่มี $X_{L_j}(v_i) \neq 0$ เราสามารถลดโหนดเข้ารหัสได้โดยทฤษฎีบทย่อยที่ 4 พิจารณากรณีที่ $X_{L_j}(v_i) = 0$ ให้ y_i เป็นเวกเตอร์ข้อมูลบนเส้น

เชื่อมเข้าทางขวาของโหนด v_i เราจะสร้างเซต $C'' \in C'$ ที่ตรงตามเงื่อนไขในทฤษฎีบทย่อยที่ 6 โดยเริ่มจาก $C'' = \{y_1\}$ และให้ $y'_1 = y_1$ จากนั้นทำซ้ำดังนี้

1. ให้ j เป็นค่าอันดับน้อยที่สุดที่ v_j ยังไม่อยู่ใน C'' ถ้าหาก y_j เป็นผลรวมเชิงเส้นของ $y'_1, y'_2, \cdots, y'_{j-1}$ หยุดทำซ้ำ
2. แสดงว่ามีเวกเตอร์ y'' ที่เป็นอิสระเชิงเส้นกับ $y'_1, y'_2, \cdots, y'_{j-1}$ และทำให้ $y_j = \gamma_{(j,1)} y'_1 + \gamma_{(j,2)} y'_2 + \cdots + \gamma_{(j,j-1)} y'_{j-1} + y''$ สำหรับ $\gamma_{(j,1)}, \gamma_{(j,2)}, \cdots, \gamma_{(j,j-1)} \in F$ เพิ่ม v_j ใน C'' และให้ $y'_j = y''$ วนกลับข้อ 1

เนื่องจากเวกเตอร์ข้อมูลเหล่านี้เป็นเวกเตอร์ใน k มิติ เราสามารถวนซ้ำได้มากที่สุด k รอบ หลังจากนั้นจะพบเวกเตอร์ข้อมูลที่ขึ้นกับ k เวกเตอร์ที่มีอยู่ก่อนหน้าเสมอ

จะเห็นว่าเซต $D = C'' + \{v_j\}$ ตรงตามเงื่อนไขแต่ละข้อในทฤษฎีบทย่อยที่ 6 อย่างชัดเจนอยู่แล้ว และในข้อที่ว่า $e_{L(i+1)}(v_i) \cdot a_{i+1} \neq 0$ นั้นเป็นจริงเพราะว่า $X_{L(i+1)}(v_i) = 0$ และจากที่ $E(v_i) = E(v_{i+1})$ ทำให้ได้ว่า $e_{L(i+1)}(v_i) \cdot a_{i+1} = 1$

เมื่อมีเซตที่ตรงทฤษฎีบทย่อยที่ 6 แล้ว เราสามารถทำการตัดทางขวาที่โหนด v_j ทำให้โหนดนี้ไม่เป็นโหนดเข้ารหัสและทำให้ข้อมูลที่ปลายทางเปลี่ยนไป

$$(\gamma'_1 \ y_1 + \gamma'_2 y_2 + \cdots + \gamma'^{'}_{j-1} y_{j-1}) \cdot e_i(v_j) \tag{11}$$

ซึ่งจากทฤษฎีบทย่อยที่ 6 เราสามารถทำการเปลี่ยนการเข้ารหัสเครือข่ายของโหนด $v_1, v_2, \ldots, v_{j-1}$ ที่มีการเปลี่ยนแปลงที่ข้อมูลที่ปลายทางหักล้างกับการตัดทางขวานี้ได้

จากทฤษฎีบทย่อยที่ 3 และทฤษฎีบทย่อยที่ 7 เราสามารถสรุปจำนวนโหนดเข้ารหัสได้ทั้งในกรณีโซ่และปฏิโซ่แล้ว ในทฤษฎีบทของเราจะกล่าวถึงจำนวนโหนดเข้ารหัสทั้งหมดในเครือข่าย

ทฤษฎีบทที่ 2 *หากมีการเข้ารหัสเครือข่ายที่ใช้งานได้โดยใช้โหนดเข้ารหัสมากกว่า* $k^2|\Im|^{2k}$ *โหนด จะมีการเข้ารหัสเครือข่ายอีกแบบหนึ่งที่ใช้งานโดยมีโหนดเข้ารหัสอยู่ไม่เกิน* $k^2|\Im|^{2k}$ โหนด

พิสูจน์ หากเรามีโหนดเข้ารหัสมากกว่า $k^2|\Im|^{2k}$ จากทฤษฎีบทย่อยที่ 2 จะได้ว่าเรามีโซ่หรือปฏิโซ่ ซึ่งตรงตามเงื่อนไขใน ทฤษฎีบทย่อยที่ 3 หรือทฤษฎีบทย่อยที่ 7 ดังนั้นเราสามารถหาการเข้ารหัสเครือข่ายใหม่ที่มีโหนดเข้ารหัสไม่เกิน $k^2|\Im|^{2k}$ ได้

วิจารณ์

วิธีการหาขีดจำกัดบนของจำนวนโหนดเข้ารหัสในงานวิจัยนี้เป็นการพัฒนาต่อจากงานของ Iwama *et al.* โดยสามารถลดโหนดเข้ารหัสในกรณีที่มีข้อมูลเข้าขึ้นต่อกันหรือข้อมูลเข้าที่เหมือนกันเพียงข้างเดียวเท่านั้นได้ จากเดิมที่ต้องมีข้อมูลเข้าเหมือนกันทั้งสองข้าง อย่างไรก็ตาม วิธีการนี้โหนดเข้ารหัสยังจำเป็นต้องมีเวกเตอร์ผลกระทบที่เหมือนกันอยู่ หากพิจารณาในกรณีที่เวกเตอร์ผลกระทบไม่เหมือนกันด้วยน่าจะสามารถหาขีดจำกันบนของจำนวนโหนดเข้ารหัสที่แน่นกว่านี้ได้อีก

สรุปและข้อเสนอแนะ

สรุป

งานวิจัยนี้เสนอวิธีการลดขีดจำกัดบนของโหนดเข้ารหัสจากเดิมที่เป็น $|\Im|^{3k}$ ให้เหลือ $k^2|\Im|^{2k}$ โหนด โดยใช้หลักการทางพีชคณิตและทฤษฎีบทของ Dilworth ในการพิสูจน์ความถูกต้องของขีดจำกัดบนใหม่ ซึ่งขีดจำกัดบนที่แน่นขึ้นนี้ทำให้อัลกอริทึมในการคำนวณการเข้ารหัสเครือข่ายที่มีการสื่อสารระหว่างต้นทางปลายทางหลายคู่ใช้เวลาในการทำงานลดลงไปด้วย

ข้อเสนอแนะ

ในงานวิจัยนี้เพียงแค่หาขีดจำกัดบนของจำนวนโหนดเข้ารหัสใหม่เท่านั้น ยังไม่ได้ทำการปรับปรุงอัลกอริทึม หากออกแบบอัลกอริทึมใหม่โดยคำนึงถึงลักษณะเครือข่ายด้วย น่าจะสามารถพัฒนาอัลกอริทึมให้มีประสิทธิภาพและใช้เวลาในการทำงานน้อยลงกว่านี้ได้อีก

เอกสารและสิ่งอ้างอิง

Ahlswede, R., N. Cai, S. R. Li, and R. W. Yeung. 2000. Network information flow. **IEEE Transactions on Information Theory**

Dilworth, R. P. 1950. A Decomposition Theorem for Partially Ordered Sets. **Annals of Mathematics.** Vol. 51. No 1

Fortune, S., J. Hopcroft, and J. Wyllie. 1980. The directed subgraph homeo-morphism problem. **Theoret. Comput. Sci.**

Iwama, K., H. Nishimura, M. Paterson, R. Raymond, and S. Yamashita. 2008. Polynomial-time construction of linear network coding. **ICALP 2008**.

Jaggi, S., P. Sanders, P. A. Chou, M. Effros, S. Egner, and L. Tolhuizen. 2005. Polynomial time algorithms for multicast network code construction. **IEEE Transactions on Information Theory**. Vol. 51. No 6

Lehman, A. R. and E. Lehman. 2003. Complexity classification of network information flow problems. **In Proc. 41st Annual Allerton Conference on Communication, Control, and Computing.**

Li, S-Y. R., R. W. Yeung, and N. Cai. 2003. Linear network coding. **IEEE Transactions on Information Theory**

Wang, C.C. and N. B. Sheoff. 2007. Beyond the butterfly a graph-theoretic characterization of the feasibility of network coding with two simple unicast sessions. **IEEE International Symposium on Information Theory**

ประวัติการศึกษาและการทำงาน

ชื่อ	นายมุนินทร์ เอี่ยมโอภาส
เกิดวันที่	16 เมษายน 2528
สถานที่เกิด	อำเภอพญาไท จังหวัดกรุงเทพมหานคร
ประวัติการศึกษา	วศ.บ. (วิศวกรรมไฟฟ้า) มหาวิทยาลัยเกษตรศาสตร์
ตำแหน่งปัจจุบัน	-
สถานที่ทำงานปัจจุบัน	-
ผลงานดีเด่น/ผลงานทางวิชาการ	-
ทุนการศึกษาที่ได้รับ	ได้รับทุนโครงการบัณฑิตศึกษา ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2551)