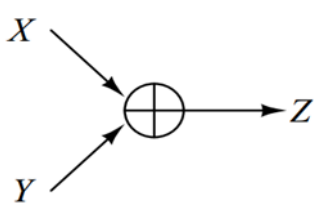
รหัสวัฏจักรสำหรับช่องสื่อสารบวกเลขฐานสอง

สมพงค์ จิตต์มั่น
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

ที่มาและความสำคัญ

การสื่อสารแบบผู้ใช้หลายคน (multiuser communication) เป็นแนวคิดการสื่อสารที่น่าสนใจ มีการวิจัยพัฒนาและประยุกต์ใช้อย่างต่อเนื่องในช่วงหลายทศวรรษที่ผ่านมา การสื่อสารรูปแบบนี้อาศัยหลักการให้ผู้ใช้ทั้งหมด(หรือบางส่วน) ส่งสารพร้อมกันไปตามช่องสื่อสารร่วม โดยมีวัตถุประสงค์ให้ผู้รับสามารถถอดรหัสเพื่อรับสารที่ถูกต้อง ช่องสื่อสารแบบผู้ใช้หลายคนที่นิยมใช้แบบหนึ่ง คือ ช่องสื่อสารบวกเลขฐานสอง (binary adder channel) ในที่นี้ เราสนใจช่องสื่อสารบวกเลขฐานสองสำหรับผู้ใช้สองคน (2-user binary adder channel) กล่าวคือ ให้ X และ Y ใน $\{0,1\}^n$ แทนสาร (message) ของผู้ใช้คนที่หนึ่งและคนที่สองตามลำดับ แล้วส่งสารในรูปแบบ Z=X+Y (ผลบวกแบบจำนวนตรรกยะ) ผ่านช่องสื่อสาร ผู้รับมีหน้าที่ถอดรหัสแยกสารเป็นสารเดิม ผลลัพธ์จาก [2] แสดงให้เห็นว่าเอกภพสัมพัทธ์ของ X และ Y มีผลต่อการถอดรหัส Z



รูปที่ 1 ช่องสื่อสารบวกเลขฐานสอง

รหัสเชิงเส้นฐานสองคู่กันเติมเต็ม (linear complementary dual code) เป็นรหัสที่ประยุกต์ใช้กับช่องสื่อสารบวกเลขฐานสองสำหรับผู้ใช้สองคน ผลการศึกษาใน [2] กล่าวถึงขั้นตอนวิธีสำหรับถอดรหัสจากช่องสื่อสารบวกเลขฐานสองโดยรหัสเชิงเส้นฐานสองคู่กันเติมเต็ม เมื่อ X เป็นสมาชิกในรหัส C และ Y เป็นสมาชิกในส่วนเติมเต็ม $C^{\perp}$

รหัสวัฏจักร (cyclic code) เป็นรหัสที่สามารถประยุกต์กับเรจิสเตอร์แบบเลื่อน (shift register) ได้โดยตรง จึงเป็นรหัสที่เหมาะอย่างยิ่งที่จะใช้ในระบบคอมพิวเตอร์และการสื่อสารผ่านคอมพิวเตอร์ ด้วยเหตุนี้เองการศึกษารหัสวัฏจักรคู่กันเติมเต็มจึงเป็นรหัสที่น่าสนใจสำหรับใช้กับช่องสื่อสารบวกเลขฐานสองสำหรับผู้ใช้สองคน ในงานวิจัยนี้ เราศึกษา การสร้าง การจำแนก และการนับจำนวนรหัสวัฏจักรคู่กันเติมเต็ม

ผลการวิจัย

เมื่อกำหนดความยาว n ของรหัส เรานำเสนอเงื่อนไขที่จำเป็นและเพียงพอสำหรับการสร้างและจำแนกรหัสวัฏจักรฐานสองคู่กันเติมเต็มความยาว n เพื่อการประยุกต์กับช่องสื่อสารบวกเลขฐานสองสำหรับผู้ใช้สองคน นอกจากนี้ยังได้นับจำนวนรหัสเหล่านี้เพื่อยืนยันว่าเรามีรหัสมากพอสำหรับการประยุกต์ใช้ ในเชิงทฤษฎีเราได้ขยายการศึกษาและได้ผลลัพธ์ให้ครอบคลุมรหัสวัฏจักรฐาน q คู่กันเติมเต็ม (เมื่อ q>2) [3] นอกจากนี้ เราได้ขายแนวคิดและได้ผลลัพธ์ซึ่งเป็นนัยทั่วไปครอบคลุมรหัสวัฏจักรเชิงค่าคงที่คู่กันเติมเต็ม [3] และรหัสอาบีเลียนคู่กันเติมเต็ม [1]

เอกสารอ้างอิง

[1] Jitman, S., Ling, S., Liu, H., Xie, X.: Abelian codes in principal ideal group algebras, IEEE Trans. Inform. Theory 59, 3046-3058 (2013).

[2] Massey, J. L.: Linear codes with complementary duals, Disc. Math. 106–107, 337–342(1992)

[3] Sangwisut, E., Jitman, S., Ling, S., Udomkavanich, P.: Hulls of Cyclic and Negacyclic Codes over Finite Fields, Finite Fields Appl. 33, 232-257(2015).