คำนำ

หนังสือเล่มนี้ เขียนขึ้นเพื่อเป็นเอกสารประกอบการสอนวิชาทฤษฎีรหัสเบื้องต้นที่เปิดสอนในระดับปริญญาตรีที่มหาวิทยาลัยรามคำแหง โดยจะเน้นแนวความคิดทางคณิตศาสตร์ที่อยู่เบื้องหลังทฤษฎีบทที่เกี่ยวกับรหัสแก้ไขข้อผิดพลาด

ในบทที่หนึ่ง จะเป็นเนื้อหาสำหรับปูพื้นความรู้เบื้องต้น ให้รู้จักระบบการสื่อสาร การเข้ารหัสและการถอดรหัส และลักษณะปัญหา ที่นิยมศึกษากันในวิชาทฤษฎีรหัส เพื่อความสมบูรณ์ของเนื้อหา

ในบทที่สอง จะรวบรวมนิยามและทฤษฎีบทของคณิตศาสตร์ที่ต้องใช้ในการศึกษาวิชาทฤษฎีรหัส โดยละการพิสูจน์ทฤษฎีบทบางทฤษฎี ที่สามารถหาอ่านได้จากตำราทางพีชคณิตเชิงเส้นทั่วไป จะพิสูจน์เฉพาะบางทฤษฎีบทเท่านั้น

ในบทที่สาม จะเน้นศึกษารหัสเชิงเส้น ซึ่งเป็นรหัสที่มีประสิทธิภาพ เข้ารหัส-ถอดรหัสได้ง่าย โดยอาศัยโครงสร้างทางคณิตศาสตร์ โดยเฉพาะเรื่องกรุปและปริภูมิเวกเตอร์

ในบทที่สี่ เน้นศึกษารหัสบางรหัสที่รู้จักกันแพร่หลาย

ในบทที่ห้า แนะนำให้รู้จักรหัสวัฏจักร ซึ่งเป็นรหัสที่เข้ารหัสได้ง่าย โดยใช้อุปกรณ์ที่เรียกว่า shift register ตลอดจนศึกษาวิธีเข้ารหัส – ถอดรหัสโดยใช้เมทริกซ์ก่อกำเนิดและเมทริกซ์ตรวจสอบภาวะเสมอ

บทสุดท้าย จะศึกษารหัส BCH ซึ่งเป็นรหัสที่เราสามารถออกแบบให้สามารถแก้ไขข้อผิดพลาดได้หลายตำแหน่ง ซึ่งต้องใช้โครงสร้างทางคณิตศาสตร์ขั้นที่สูงกว่าความรู้พื้นฐาน บทนี้จึงเหมาะกับผู้ที่ต้องการศึกษาทฤษฎีรหัสขั้นสูงต่อไป

จุดประสงค์ของหนังสือเล่มนี้ ก็เพื่อให้เป็นพื้นฐานความรู้เกี่ยวกับทฤษฎีรหัสทั่วไป และเป็นข้อมูลสำหรับผู้ที่ต้องการจะศึกษาค้นคว้าทางด้านนี้ ผู้เขียนหวังว่าข้อมูลที่บรรจุไว้ในที่นี้จะเป็นประโยชน์ต่อการศึกษาในขั้นสูงต่อไป

รองศาสตราจารย์ ดร. สมพร สูตินันท์โอภาส

8 กุมภาพันธุ์ 2551