แกมมาฟังก์ชัน สามารถเขียนในรูปของ *Igamc* ได้จาก

ผลรวมของ Upper Incomplete Gamma Function ดังสมการ 5.17 และ Lower Incomplete Gamma Function ดังสมการ 5.18

Upper
$$\Gamma(a,x)=\frac{1}{\Gamma}(a)\int_{x}^{\infty}t^{(a-1)}e^{(-t)}dt \tag{5.17}$$

Lower
$$\gamma(a,x)=\frac{1}{\Gamma}(a)\int_{0}^{x}t^{(a-1)}e^{(-t)}dt \tag{5.18}$$

$$\Gamma(a)=\Gamma(a,x)+\gamma(a,x) \tag{5.19}$$

สามารถหา CDF ได้จากสมการ

$$P(\chi_k^2\geq\chi_\alpha^2,k)=\int_{(\chi_\alpha^2,k)}^{\infty}f_\chi^2(u)du=\alpha \tag{5.20}$$

ดังนั้นจึงสามารถเขียนสมการ CDF ในรูปสมการของ *Igamc* ดังนี้

$$F(a,x)=\frac{(\gamma(a,x))}{(\Gamma(a))}=\frac{1}{(\Gamma(a))}\int_{0}^{x}u^{-t}e^{(a-1)}dt \tag{5.21}$$

จากหลักการข้างต้นของการคำนวณสถิติทดสอบของชุดทดสอบทางสถิติเอ็นไอเอสที สามารถคำนวณได้จาก *Igamc* ซึ่งสมการอยู่ในรูปของการปริพันธ์ที่มีความซับซ้อนสูง จึงไม่เหมาะสมสำหรับการพัฒนาเพื่อให้บริการการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์ด้วยวิธีการดังกล่าว ดังนั้นวิทยานิพนธ์นี้ได้นำเสนอการหลักการคำนวณสถิติทดสอบและการพิจารณาการผ่านการทดสอบโดยอ้างอิงการทดสอบไคกำลัง ซึ่งมีรายละเอียดดังนี้

จากการแจกแจงไคกำลังสองและการหาพื้นที่ใต้โค้งปกติโดยการหาค่า CDF ของการแจกแจง ดังสมการที่ 5.20 และ 5.21 นั้นจะเห็นได้ว่าสมการดังกล่าวมีความซับซ้อนสูง และมีขั้นตอนในการคำนวณหลายขั้นตอน ดังนั้นวิทยานิพนธ์จึงนำเสนอการทดสอบความเหมาะสมของการแจกแจง (Test for Goodness of Fit) ซึ่งอ้างอิงการแจกแจงไคกำลังสอง โดยการทดสอบนี้จะนำมาเปรียบเทียบระหว่างความถี่ที่สังเกตที่เกิดขึ้นจากการทดลองจริง (Observed frequency) และความถี่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ที่คาดหวังจะเป็นไปตามทฤษฎี (Expected frequency) ซึ่งจะมีสอดคล้องกับความน่าจะเป็นของจำนวนสุ่มที่มีการแจกแจงแบบไคกำลังสอง โดยสามารถคำนวณสถิติทดสอบดังนี้

$$\text{สถิติทดสอบ คือ} \quad \chi^2=\sum_{i=1}^{k}\left(\frac{(O_i-E_i)^2}{E_i}\right) \tag{5.22}$$

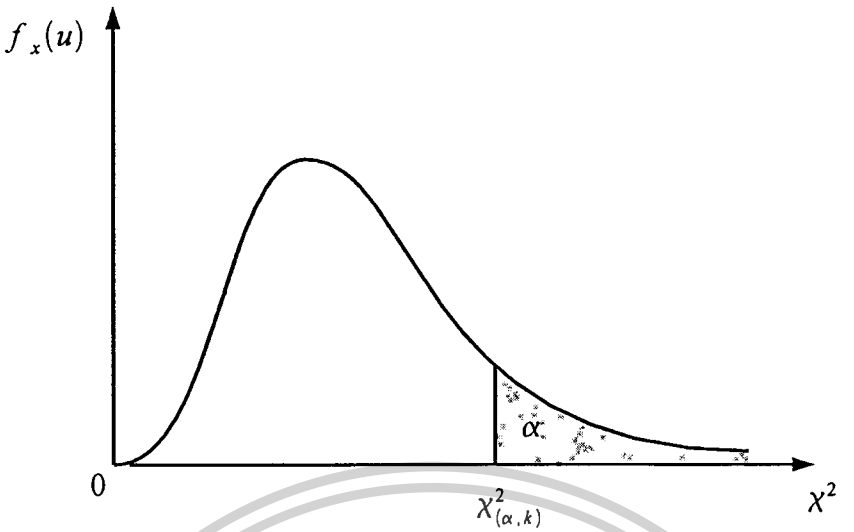
โดย O_i คือ ความถี่ที่ค่าสังเกตที่เกิดขึ้นจากการทดลองจริง (Observed Frequency)

E_i คือ ความถี่ที่ค่าคาดหวังจะเป็นไปตามทฤษฎี (Expected Frequency)

k คือ จำนวนของการจำแนกผลลัพธ์จากการทดลอง หรือจำนวนกลุ่มของข้อมูลที่จัดแบ่ง และ $\sum_{i=1}^{k}O_i=\sum_{i=1}^{k}E_i=n$

เมื่อคำนวณสถิติทดสอบข้างต้นแล้วนั้น สามารถพิจารณาการผ่านการทดสอบโดยอ้างอิงจากหลักการที่นำเสนอ จะเห็นว่าการหาสถิติทดสอบดังกล่าวนี้อยู่ในรูปสมการที่มีความซับซ้อนต่ำ โดยมีประเด็นที่สำคัญคือสามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและค่าทางสถิติได้โดยตรง ทำให้สามารถพิจารณาการผ่านการทดสอบโดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้ ดังรูปที่ 5.2 ซึ่งจะส่งผลให้การทดสอบคุณสมบัติของจำนวนสุ่มมีระยะเวลาในการประมวลผลการทดสอบสั้นลงได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.2 ค่าวิกฤตของการแจกแจงไคกำลังสอง $\chi^2 > \chi^2_\alpha$ บริเวณวิกฤตคือ χ^2 ที่คำนวณได้ [2]

จากหลักการที่นำเสนอทั้งสองหลักการนั้น สามารถนำมาพัฒนาชุดทดสอบคุณสมบัติของจำนวนสุ่มที่จะนำมาให้บริการผ่านระบบออนไลน์ โดยมีเงื่อนไขและขั้นตอนการทดสอบให้เป็นไปตามคุณสมบัติของจำนวนสุ่ม ซึ่งจะกล่าวในรายละเอียดในลำดับถัดไป

5.2 วิธีการทดสอบคุณสมบัติของจำนวนสุ่ม (Randomness Testing Method)

การทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีการทางสถิติ มีการกำหนดเงื่อนไขและคุณสมบัติของชุดการทดสอบตามขั้นตอนวิธีการทดสอบสมมติฐาน ซึ่งสามารถสรุปขั้นตอนได้ ดังนี้

5.2.1 เงื่อนไขและคุณสมบัติของขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่ม

เงื่อนไขและคุณสมบัติของขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่ม แบ่งเป็น 5 ขั้นตอน ดังนี้

ขั้นตอนที่หนึ่ง การตั้งสมมติฐาน

การตั้งสมมติฐานจะกำหนดให้สมมติฐานหลักดังนี้ “จำนวนสุ่มมีคุณภาพเพียงพอที่จะนำไปใช้งาน” โดยการผ่านการตรวจสอบคุณภาพ จะต้องพิสูจน์ให้ได้ว่าไม่มีหลักฐานเพียงพอที่จะปฏิเสธข้อสมมติฐานหลักที่ตั้งไว้

H_0 : จำนวนสุ่มมีคุณภาพเพียงพอที่จะนำไปใช้งาน

H_1 : จำนวนสุ่มไม่มีคุณภาพเพียงพอที่จะนำไปใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ขั้นตอนที่สอง การกำหนดระดับนัยสำคัญ

ระดับนัยสำคัญ(Significance Level: α) ของการทดสอบสมมติฐานทางสถิตินั้น จะเป็นการกำหนดขอบเขตของความผิดพลาดหรือความคลาดเคลื่อนที่จะยอมรับให้เกิดขึ้นได้ ซึ่งการกำหนดระดับนัยสำคัญในการทดสอบคุณสมบัติของจำนวนสุ่มในวิทยานิพนธ์นี้จะเท่ากับ 0.01 และ 0.05 โดยค่าระดับนัยสำคัญจะเป็นสิ่งที่แสดงว่าถ้าในการทดสอบสมมติฐานแล้วเกิดความผิดพลาดหรือความคลาดเคลื่อนน้อยกว่าที่กำหนดไว้ α ก็จะยอมรับสมมติฐานหลัก (H_0) ที่ตั้งไว้ และนั่นคือการปฏิเสธสมมติฐานแย้ง (H_1) ในทางกลับกันถ้าในการทดสอบสมมติฐานแล้วเกิดความผิดพลาดหรือความคลาดเคลื่อนมากกว่าที่กำหนดไว้ α ก็จะปฏิเสธสมมติฐานหลัก (H_0) ที่ตั้งไว้ หรือยอมรับสมมติฐานแย้ง (H_1) นั่นเอง ซึ่งระดับนัยสำคัญจะส่งผลให้การทดสอบมีระดับความเชื่อมั่นว่าผลของการทดสอบที่ได้มามีความผิดพลาดหรือเกิดความคลาดเคลื่อนน้อยกว่าที่กำหนดและผลการทดสอบอยู่ในช่วงหรือขอบเขตที่ยอมรับเท่ากับร้อยละ 95 และร้อยละ 99 นั่นเอง

ขั้นตอนที่สาม การเลือกสถิติทดสอบ

การเลือกสถิติทดสอบจะเลือกจากลักษณะการแจกแจงของชุดจำนวนสุ่ม โดยอ้างอิงการแจกแจงสองแบบได้แก่ การแจกแจงปกติ และการแจกแจงไคกำลังสอง รายละเอียดดังปรากฏในบทที่ 4

ขั้นตอนที่สี่ การกำหนดค่าวิกฤตและขอบเขตวิกฤต

การกำหนดค่าวิกฤต (Critical Point) และบริเวณวิกฤต(Critical Region) เป็นขั้นตอนของกระบวนการเพื่อพิจารณาตัดสินใจเพื่อบ่งชี้การผ่านการทดสอบ โดยในที่นี้การกำหนดขอบเขตวิกฤตและกระบวนการคำนวณค่าสถิติทดสอบ จะเลือกเป็นการทดสอบสองด้านสำหรับการแจกแจงปกติ และทดสอบด้านเดียวสำหรับการแจกแจงไคกำลังสอง

สำหรับการแจกแจงปกติ เป็นการทดสอบสองด้าน สถิติทดสอบคือ Z ระดับนัยสำคัญ 0.01 ระดับความเชื่อมั่นคือร้อยละ 99 ค่าวิกฤตคำนวณได้จากการหาค่า CDF ของการแจกแจงปกติ คือ -2.58 และ 2.58 ซึ่งจะถูกกำหนดให้เป็นช่วงที่ยอมรับสมมติฐานหลักที่ตั้งไว้ ซึ่งหมายความว่า H_0 จะเป็นจริง ก็ต่อเมื่อ H_0 อยู่ในช่วงระหว่าง $-2.58 < Z < 2.58$ สำหรับการทดสอบที่ระดับนัยสำคัญ 0.05 ระดับความเชื่อมั่นคือร้อยละ 95 ค่าวิกฤตคำนวณได้จากการหาค่า CDF ของการแจกแจงปกติ คือ -1.96 และ 1.96 ซึ่งจะถูกกำหนดให้เป็นช่วงที่ยอมรับสมมติฐานหลักที่ตั้งไว้ ซึ่งหมายความว่า H_0 จะเป็นจริง ก็ต่อเมื่อ H_0 อยู่ในช่วงระหว่าง $-1.96 < Z < 1.96$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

สำหรับการแจกแจงไคกำลังสอง เป็นการทดสอบด้านเดียว สถิติทดสอบคือ χ^2 ระดับนัยสำคัญ 0.01 ระดับความเชื่อมั่นคือร้อยละ 99 ค่าวิกฤตคำนวณได้จากการหาค่า CDF ของการแจกแจงปกติ คือ 135.807 ซึ่งจะถูกกำหนดให้เป็นช่วงที่ยอมรับสมมติฐานหลักที่ตั้งไว้ ซึ่งหมายความว่า H_0 จะเป็นจริง ก็ต่อเมื่อ H_0 อยู่ในระดับ $\chi^2 < 135.807$ สำหรับการทดสอบที่ระดับนัยสำคัญ 0.05 ระดับความเชื่อมั่นคือร้อยละ 95 ค่าวิกฤตคำนวณได้จากการหาค่า CDF ของการแจกแจงปกติ คือ 124.342 ซึ่งจะถูกกำหนดให้เป็นช่วงที่ยอมรับสมมติฐานหลักที่ตั้งไว้ ซึ่งหมายความว่า H_0 จะเป็นจริง ก็ต่อเมื่อ H_0 อยู่ในระดับ $\chi^2 < 124.342$

ขั้นตอนที่ห้า การสรุปผลการทดสอบ

การสรุปผลการทดสอบโดยการพิจารณาว่าผ่านหรือไม่ผ่านการทดสอบนั้น จะพิจารณาจากการยอมรับและปฏิเสธข้อสมมติฐานหลักที่ตั้งไว้ H_0 โดยกำหนดให้สอดคล้องกับวิธีการทดสอบ เมื่อ H_0 อยู่ในช่วงที่กำหนดไว้ จะยอมรับสมมติฐานหลัก นั่นคือจะยอมรับว่าจำนวนสุ่มที่นำมาทดสอบมีคุณภาพเพียงพอที่จะนำไปใช้งาน ในกรณีที่ H_0 ไม่ได้อยู่ในขอบเขตที่กำหนดไว้แสดงว่าจำนวนสุ่มที่นำมาทดสอบไม่มีคุณภาพเพียงพอที่จะนำไปใช้งานนั่นเอง

5.2.2 ขอบเขตการทดสอบและการวิเคราะห์ผล

การทดสอบคุณสมบัติของจำนวนสุ่มเป็นไปตามขอบเขตและการวิเคราะห์ผล ดังนี้

5.2.2.1 ขอบเขตการทดสอบสำหรับชุดกำเนิดจำนวนสุ่ม

การทดสอบคุณสมบัติของจำนวนสุ่ม ด้วยวิธีการทางสถิติ ทดสอบคุณสมบัติ 5 คุณสมบัติ ได้แก่ วิธีที่หนึ่ง ทดสอบลักษณะการแจกแจงความน่าจะเป็นและรูปแบบการแจกแจง การซ้ำกันของข้อมูล ความต่อเนื่องของชุดข้อมูล คุณสมบัติความเป็นอิสระเชิงเดี่ยว (Independence) คาบเป็นอิสระ และโอกาสความน่าจะเป็นที่เท่าเทียม(Probability) จำนวนสุ่มที่นำมาทดสอบหลัก เนื่องจากการทดสอบทางสถิติต้องใช้จำนวนสุ่มจำนวนมาก เพื่อให้ได้ผลการทดสอบที่ดีและให้ค่าที่ใกล้เคียงกับข้อมูลจริงมากที่สุด จึงจำเป็นต้องใช้จำนวนสุ่มเทียมที่ได้จากแหล่งกำเนิดที่เป็นฟังก์ชันการสร้างจำนวนสุ่มเทียมด้วยโปรแกรมคอมพิวเตอร์ซึ่งมีสะดวกในการกำเนิด โดยวิทยานิพนธ์นี้กำหนดขนาดชุดจำนวนสุ่มจำนวน 100 ชุด ชุละ 1,000,000 บิต เพื่อเก็บเป็นสถิติและประเมินผลการทดสอบ นอกจากนี้จะทำการเปรียบเทียบการผ่านการทดสอบระหว่างจำนวนสุ่มจากแหล่งกำเนิดเทียมและจำนวนสุ่มจากแหล่งกำเนิดควอนตัมซึ่งได้รับการยอมรับว่าเป็นแหล่งกำเนิดจำนวนสุ่มแท้ จำนวน 100 ชุดเช่นกันเพื่อศึกษาประสิทธิภาพและความแตกต่างของแหล่งกำเนิด

5.2.2.2 การวิเคราะห์ผลการทดสอบ

การวิเคราะห์ผลการทดสอบของชุดวิธีทดสอบที่นำเสนอ จะวิเคราะห์ผล 3 แบบ ได้แก่ แบบที่หนึ่ง การวิเคราะห์ความแตกต่างการพิจารณาสัดส่วนการผ่านการทดสอบ แบบที่สองเก็บ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

สถิติของเวลาทั้งหมดในการประมวลผลการทดสอบ โดยจะทำการพิจารณาเปรียบเทียบผลการทดสอบกับชุดทดสอบทางสถิติเอ็นไอเอสที และหาความแตกต่างของผลการพิจารณาสัดส่วนการผ่านการทดสอบด้วยการพิจารณาจากร้อยละความแตกต่าง (Percentage Different) ตามสมการ 5.23 ด้านการวิเคราะห์ผลจากการลดความซับซ้อนของชุดวิธีทดสอบสามารถวัดได้จากขั้นตอนของการทดสอบที่สั้นลงและเวลาทั้งหมดที่ใช้ในการประมวลผลการทดสอบโดยเฉลี่ย และทำการเปรียบเทียบระหว่างการประมวลผลการทดสอบของหลักการเดิมและหลักการที่นำเสนอ ซึ่งจะแสดงด้วยกราฟเวลาที่แตกต่างและเปรียบเทียบร้อยละของเวลาทั้งหมดที่ใช้ในการประมวลผลการทดสอบโดยเฉลี่ย และการวิเคราะห์ผลแบบที่สาม จะทำการประสิทธิภาพของชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่มที่นำเสนอโดยวัดจากการเปรียบเทียบสัดส่วนการผ่านการทดสอบของจำนวนสุ่มจากแหล่งกำเนิดจำนวนสุ่มแท้และแหล่งกำเนิดจำนวนสุ่มเทียม ซึ่งจะแสดงด้วยตารางเปรียบเทียบสัดส่วนการผ่านการทดสอบ ร้อยละความแตกต่างสามารถหาได้ดังนี้

$$\text{ร้อยละความแตกต่าง} = \frac{|Measured_1 - Measured_2|}{\left(\frac{(Measured_1 + Measured_2)}{2}\right)} \times 100 \qquad (5.23)$$

5.3 รายละเอียดขั้นตอนวิธีการทดสอบ (Testing Methodology)

การทดสอบคุณสมบัติของจำนวนสุ่มห้าวิธีการนั้น แต่ละวิธีการทดสอบจะเป็นการตรวจสอบแต่ละคุณสมบัติของจำนวนสุ่ม ดังที่ได้กล่าวไปแล้วข้างต้น โดยได้ออกแบบการทดสอบที่อ้างอิงจากชุดทดสอบทางสถิติเอ็นไอเอสที ซึ่งมีขอบเขตเงื่อนไขและคุณสมบัติของชุดวิธีทดสอบและการออกแบบการพิจารณาการผ่านการทดสอบและขอบเขตการทดสอบ สถิติทดสอบ ดังที่ได้นำเสนอในหัวข้อ 5.1 ชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่มประกอบด้วย 5 วิธีทดสอบย่อย ดังนี้

วิธีที่ 1 การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)

วิธีที่ 2 การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)

วิธีที่ 3 การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)

วิธีที่ 4 การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)

วิธีที่ 5 การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)

โดยจะกล่าวในรายละเอียดของการทดสอบแต่ละวิธี ลำดับถัดไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่หนึ่ง การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)

วัตถุประสงค์

วัตถุประสงค์ของการทดสอบนี้คือการหาอัตราส่วนของบิตศูนย์และบิตหนึ่งที่อยู่ภายในลำดับหนึ่งๆ และทำการพิจารณาว่าจำนวนของบิตศูนย์และบิตหนึ่งในลำดับว่ามีจำนวนที่ใกล้เคียงกันหรือไม่ ซึ่งจะต้องเป็นไปตามลำดับของจำนวนสุ่มแท้ ซึ่งมีค่าประมาณที่ใกล้เคียงกับ ½ กล่าวคือจำนวนของบิตศูนย์และบิตหนึ่งต้องมีจำนวนเท่ากันนั่นเอง การทดสอบวิธีที่หนึ่งนี้เป็นวิธีการทดสอบคุณสมบัติพื้นฐานอันดับแรก ดังนั้นจึงต้องผ่านการการทดสอบนี้ก่อนการทดสอบคุณสมบัติข้ออื่นๆ [16][17]

ตัวแปรและพารามิเตอร์ที่ใช้ในการทดสอบ

n คือ ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ การทดสอบนี้ n =1,000,000

ε คือ ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิดต่างๆ เช่น ε = 01011001...1100 นั่นคือ $\varepsilon=\varepsilon_1,\varepsilon_2,\varepsilon_3,..,\varepsilon_n$

การแจกแจง

การแจกแจงแบบปกติ

ขั้นตอนการทดสอบ

ขั้นตอนที่ 1 เปลี่ยน ε ให้บิต "1" มีค่าเป็น +1 และบิต "0" ให้มีค่าเป็น -1 ซึ่งเป็นไปตามการแจกแจงของตัวแปรสุ่มเบอร์นูลลิ (Bernoulli random variables) หาค่าตัวแปรสุ่ม X ได้จาก $X=2\varepsilon_i-1$ และผลรวมของตัวแปรสุ่ม (S_n) เท่ากับ $S_n=X_1+X_2+...+X_n$

ตัวอย่างเช่น $\varepsilon=10110011$ จะได้ $S_n=1+(-1)+1+1+(-1)+(-1)+1+1=2$

ขั้นตอนที่ 2 ทำการคำนวณสถิติทดสอบ หาได้จาก $Z_{obs}=\frac{|S_n|}{\sqrt{(n)}}$

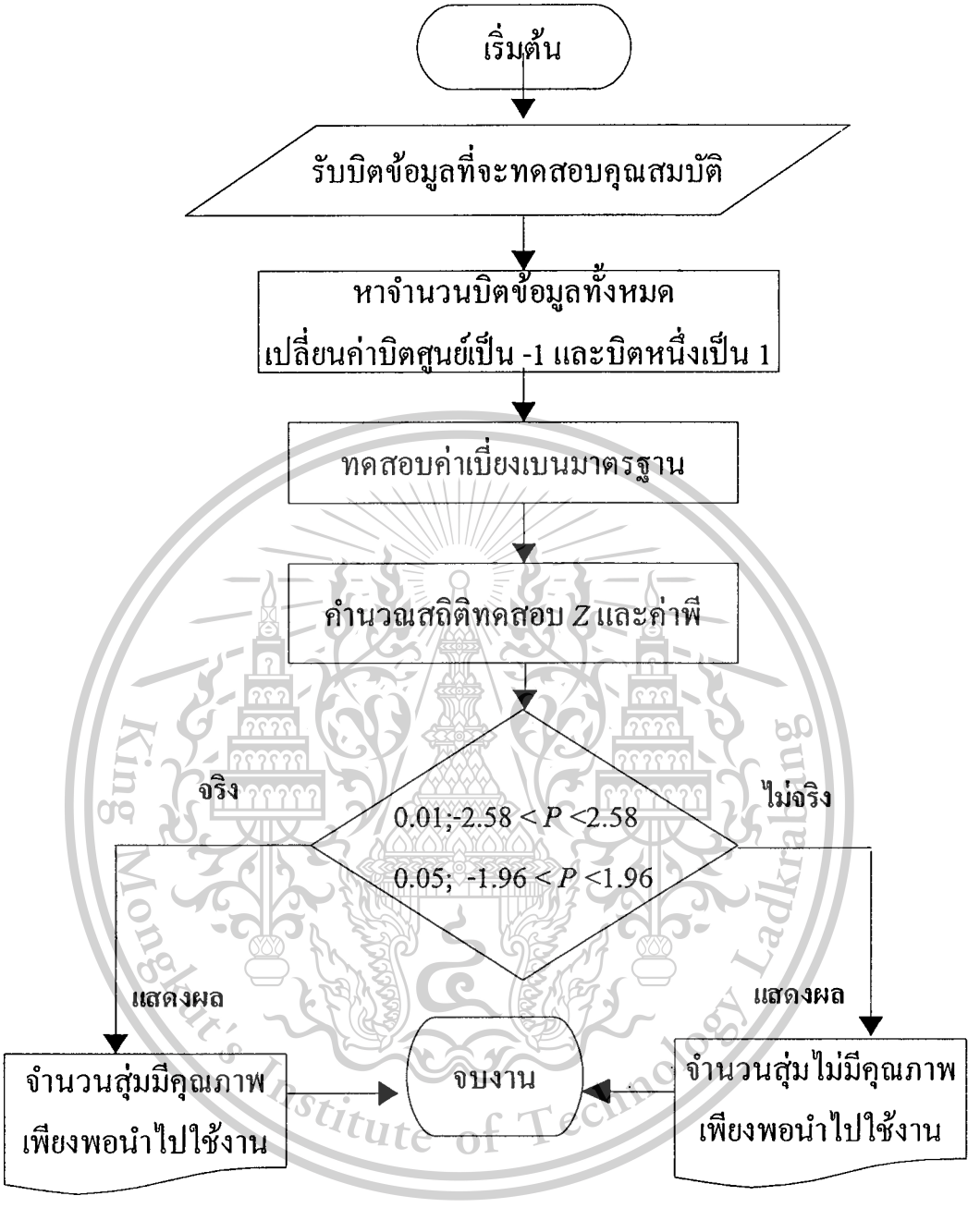
เป็นการหาค่าเบี่ยงเบนเฉลี่ยของจำนวนสุ่มตามเนื้อหาบทที่ 3 โดยอ้างอิงการแจกแจงปกติมาตรฐาน โดยให้ค่าเฉลี่ย $\mu=0$ และค่าเบี่ยงเบนมาตรฐาน $\sigma=1$

ขั้นตอนที่ 3 คำนวณค่าพี จาก $P-value=Z$

ขั้นตอนที่ 4 การสรุปผลการทดสอบ

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่าพีที่คำนวณได้ตกอยู่บริเวณวิกฤต และในทางตรงกันข้ามก็จะยอมรับ H_0 โดยลำดับขั้นตอนของการทดสอบสามารถสรุปได้ตามแผนภาพ (Flow chart) ที่ 5.3 ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.3 แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)

หมายเหตุ: ถ้าค่าพีมีค่าใกล้ศูนย์แสดงว่า จำนวนบิต “0” และบิต “1” มีจำนวนใกล้เคียงกัน ถ้าค่าพีมีค่าเป็นบวกแสดงว่าจำนวนสุ่มที่นำมาทดสอบมีจำนวนบิต “1” มากกว่า บิต “0” และถ้าค่าพีมีค่าเป็นลบแสดงว่าจำนวนสุ่มที่นำมาทดสอบมีจำนวนบิต “0” มากกว่า บิต “1” นั่นเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สอง การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)

วัตถุประสงค์

เพื่อหาผลรวมของรัน (Run) ที่เกิดขึ้นในลำดับ เมื่อรันคือลำดับที่ไม่มีการถูกบิตอื่นคั้นกลาง ประกอบด้วยที่บิตที่เหมือนกันอยู่ภายในขอบเขตของบิตหัวบิตท้ายที่ตรงกันข้าม ตัวอย่างของรัน เช่น 0111111111111111111111111110 เป็นต้น การทดสอบนี้เพื่อพิจารณาว่าจำนวนรันของบิตศูนย์และบิตหนึ่งเป็นไปตามลำดับของจำนวนสุ่มหรือไม่ นอกจากนี้การทดสอบนี้จะพิจารณาได้ว่าการอัตราการเกิดหรือความถี่และการเปลี่ยนแปลงการเกิดรันของบิตศูนย์และบิตหนึ่งมีลักษณะเป็นอย่างไร [18][19]

ตัวแปรและพารามิเตอร์ที่ใช้ในการทดสอบ

n คือ ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ การทดสอบนี้ n =1,000,000

ε คือ ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิดต่างๆ เช่น ε = 01011001...1100 นั่นคือ $\varepsilon=\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots,\varepsilon_n$

การแจกแจง

การแจกแจงแบบปกติ

ขั้นตอนการทดสอบ

กำหนดให้ Z_{obs} คือจำนวนรวมของรันของหนึ่งที่ต่อเนื่อง

ขั้นตอนที่ 1 คำนวณการทดสอบขั้นแรกว่าผ่านการทดสอบเชิงความถี่แบบเดี่ยวหรือไม่ โดยคำนวณสัดส่วน (π) ของบิตศูนย์และบิตหนึ่ง ตามสมการ $\pi=\frac{\sum \varepsilon_j}{n}$ ตัวอย่างเช่น $\varepsilon=1011001101$ n= 10 ดังนั้นจะได้ $\pi=\frac{6}{10}=\frac{3}{5}$ เป็นต้น

ขั้นตอนที่ 2 พิจารณาว่าสัดส่วนข้างต้นอยู่ในขอบเขตที่สามารถทำการพิจารณาการทดสอบด้วยวิธีที่สองนี้ได้หรือไม่ โดยพิจารณาจากขอบเขตของ Stirling's formula [24] เมื่อสามารถตรวจสอบได้ว่า $\left|\pi-\frac{1}{2}\right|\geq\tau$ โดย $\tau=\frac{2}{\sqrt{10}}$ แล้วจะถือว่าการทดสอบนี้อยู่นอกขอบเขตของการทดสอบ แต่ถ้าสัดส่วนนี้ไม่เป็นไปตามเงื่อนไขข้างต้น จะถือว่าไม่ผ่านการทดสอบโดยจะทำการปฏิเสธ H_0 จากตัวอย่าง $\left|\frac{3}{5}-\frac{1}{2}\right|\geq\frac{2}{\sqrt{10}}$ แสดงว่าจำนวนสุ่มนี้อยู่ในขอบเขตที่กำหนดและสามารถทดสอบในลำดับต่อไปได้

ขั้นตอนที่ 3 คำนวณค่าสถิติทดสอบ $Z_{(n(obs))}=\sum_{k=1}^{n-1} r(k)+1$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

ตัวอย่างเช่น $\varepsilon=1011001101$ จะได้ $V_{(n(obs))}=(1+0+1+1+0+0+1+1+0+1)+1=7$

ขั้นตอนที่ 4 คำนวณการผ่านการทดสอบโดยอ้างอิงการทดสอบจำนวนรัน[19] จากสมการ

$$Z=\frac{\left|Z_{(n(obs))}-2n\pi(1-\pi)\right|}{(2\sqrt{(n)}\pi(1-\pi))}$$

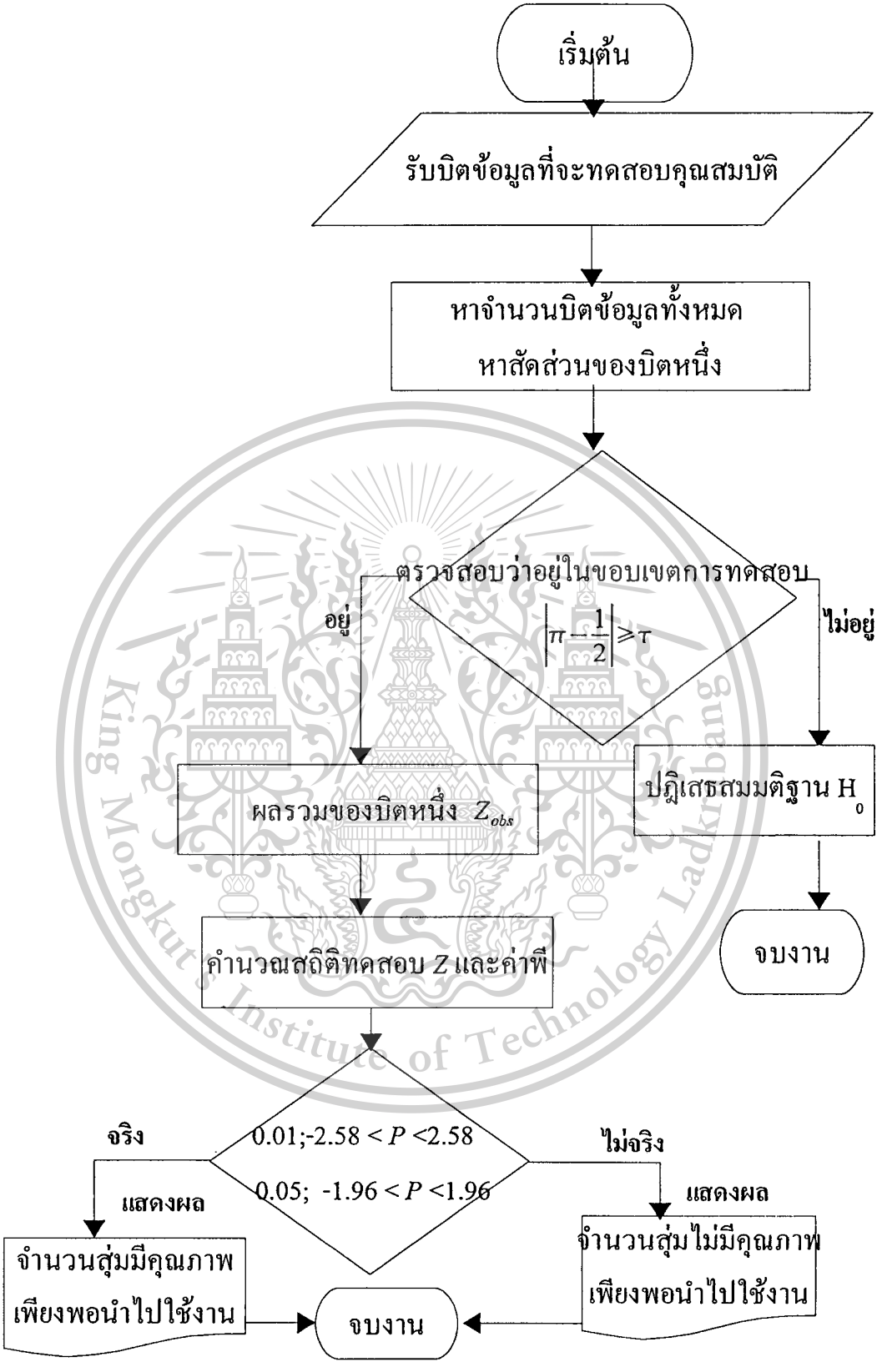
ขั้นตอนที่ 5 คำนวณค่าพีจาก $P-value=Z$

ขั้นตอนที่ 6 การสรุปผลการทดสอบ

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่าพีที่คำนวณได้ตกอยู่บริเวณวิกฤต และในทางตรงกันข้ามก็จะยอมรับ H_0 โดยลำดับขั้นตอนของการทดสอบสามารถสรุปได้ตามแผนภาพ (Flow chart) ที่ 5.4 ดังนี้

หมายเหตุ: ค่า Z_{obs} ที่ใหญ่มาก จะแสดงให้เห็นว่าการเปลี่ยนในลำดับของจำนวนสุ่มนั้นเกิดขึ้นเร็วมาก สำหรับค่า Z_{obs} ที่เล็กจะบ่งบอกว่าการเปลี่ยนค่าในลำดับของจำนวนสุ่มนั้นเกิดขึ้นน้อย ซึ่งหมายถึงการเปลี่ยนค่าจากบิตหนึ่งเป็นบิตศูนย์หรือเปลี่ยนสวนทางกันนั้นมีมากหรือน้อยเกินไป ตัวอย่างจำนวนสุ่มที่มีการเปลี่ยนบ่อย เช่น 0101010101 เป็นต้น และตัวอย่างลำดับของจำนวนสุ่มที่มีความถี่ของการเปลี่ยนแปลงน้อยกว่าที่คาดไว้ในลำดับจำนวนสุ่ม เช่นลำดับหนึ่งมีบิตหนึ่งติดกัน 100 บิต ตามด้วยบิตศูนย์ติดกัน 73 บิต และตามด้วยบิตหนึ่งอีก 127 บิต (รวมเป็น 300 บิต) ตามที่คาดการไว้ควรจะมีรันเท่ากับ 150 ครั้ง แต่ลำดับของจำนวนสุ่มนี้มีรันเพียงแค่ 3 ครั้งเท่านั้น เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.4 แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สาม การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)

วัตถุประสงค์

เพื่อตรวจสอบค้นหาจำนวนพีค (Peak) ที่มีความสูงเกินกว่าช่วงที่กำหนดไว้ โดยการแทนลักษณะรูปแบบที่ซ้ำกันเป็นช่วงๆ (Periodic) ของลำดับบิตข้อมูลด้วยการแปลงดีสครีตฟูเรียทรานส์ฟอร์ม (Discrete Fourier Transform:DFT) ของลำดับจำนวนสุ่ม การทดสอบนี้จะสามารถบ่งชี้การเบี่ยงเบน (Deviation) ที่คำนวณได้ว่าแตกต่างไปจากสมมติฐานของการสุ่ม (Assumption of randomness) มากน้อยเพียงใด โดยตรวจสอบได้จากการพิจารณาว่าชุดจำนวนสุ่มที่ทำการแปลง DFT แล้วนั้นมีจำนวนพีคที่มีค่าต่ำกว่าค่าที่กำหนดไว้(ค่า T)และค่าสูงเกินค่าที่กำหนดไว้ T มีจำนวนแตกต่างกันเกินเกินร้อยละ 5 หรือไม่[20]

ตัวแปรและพารามิเตอร์ที่ใช้ในการทดสอบ

n คือ ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ การทดสอบนี้ n =1,000,000

ε คือ ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิดต่างๆ เช่น ε = 01011001...1100 นั่นคือ $\varepsilon=\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots,\varepsilon_n$

การแจกแจง

การแจกแจงแบบปกติ

ขั้นตอนการทดสอบ

ขั้นตอนที่ 1 เปลี่ยน ε ให้บิต "1" มีค่าเป็น +1 และบิต "0" ให้มีค่าเป็น -1 ซึ่งเป็นไปตามการแจกแจงของตัวแปรสุ่มเบอร์นูลลิ (Bernoulli random variables) หาค่าตัวแปรสุ่ม X ได้จาก $X=2\varepsilon_i-1$ และผลรวมของตัวแปรสุ่ม (S_n) เท่ากับ $S_n=X_1+X_2+\ldots+X_n$

ตัวอย่างเช่น $\varepsilon=10110011$ จะได้ $S_n=1+(-1)+1+1+(-1)+(-1)+1+1=2$

ขั้นตอนที่ 2 ประยุกต์ใช้ DFT ซึ่งจะเป็นการเปลี่ยนค่า X ให้อยู่ในรูปแบบของจำนวนเชิงซ้อน (Complex variable) โดยหาได้จาก $S=DFT(X)$ ซึ่งเป็นการแสดงถึงองค์ประกอบที่มีคาบของลำดับของจำนวนสุ่มที่มีความถี่แตกต่างกัน

ขั้นตอนที่ 3 คำนวณค่าค่าโมดูลัส (Modulus) จาก $M=modulus(S')\equiv|S'|$ เมื่อ S' คือลำดับย่อยครึ่งแรกของจำนวนที่นำมาทดสอบ $\frac{n}{2}$ การหาค่าโมดูลัสจะเป็นการหาค่าพีคที่สูงที่สุดนั่นเอง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ขั้นตอนที่ 4 คำนวณที่กำหนดไว้จาก $T=\sqrt{2.995732274}n$ ซึ่งเป็นค่าที่มีค่าเท่ากับร้อยละ 95 ของความสูงของพืดที่สูงที่สุด ภายใต้ข้อสมมติฐานของการสุ่มและร้อยละ 95 ของค่าที่ได้จากการทดสอบนั้นจะต้องมีค่าไม่เกินค่า T ด้วย

ขั้นตอนที่ 5 คำนวณค่า $N_0=0.95\frac{n}{2}$ เมื่อ N_0 คือ จำนวนของค่าพืดที่มีความสูงเกินร้อยละ 95 และมีค่าน้อยกว่าค่า T

ขั้นตอนที่ 6 คำนวณค่า N_1 เมื่อ N_1 คือ จำนวนพืดในโมดูลัสที่มีค่าน้อยกว่าค่า T

ขั้นตอนที่ 7 คำนวณ $Z=\frac{(N_1-N_0)}{(\sqrt{(n(0.95)(0.05)/2)})}$ เมื่อ Z คือ ค่าความแตกต่างขององค์ประกอบเชิงความถี่ที่สังเกตและค่าคาดหวังตามทฤษฎีไม่เกินร้อยละ 5

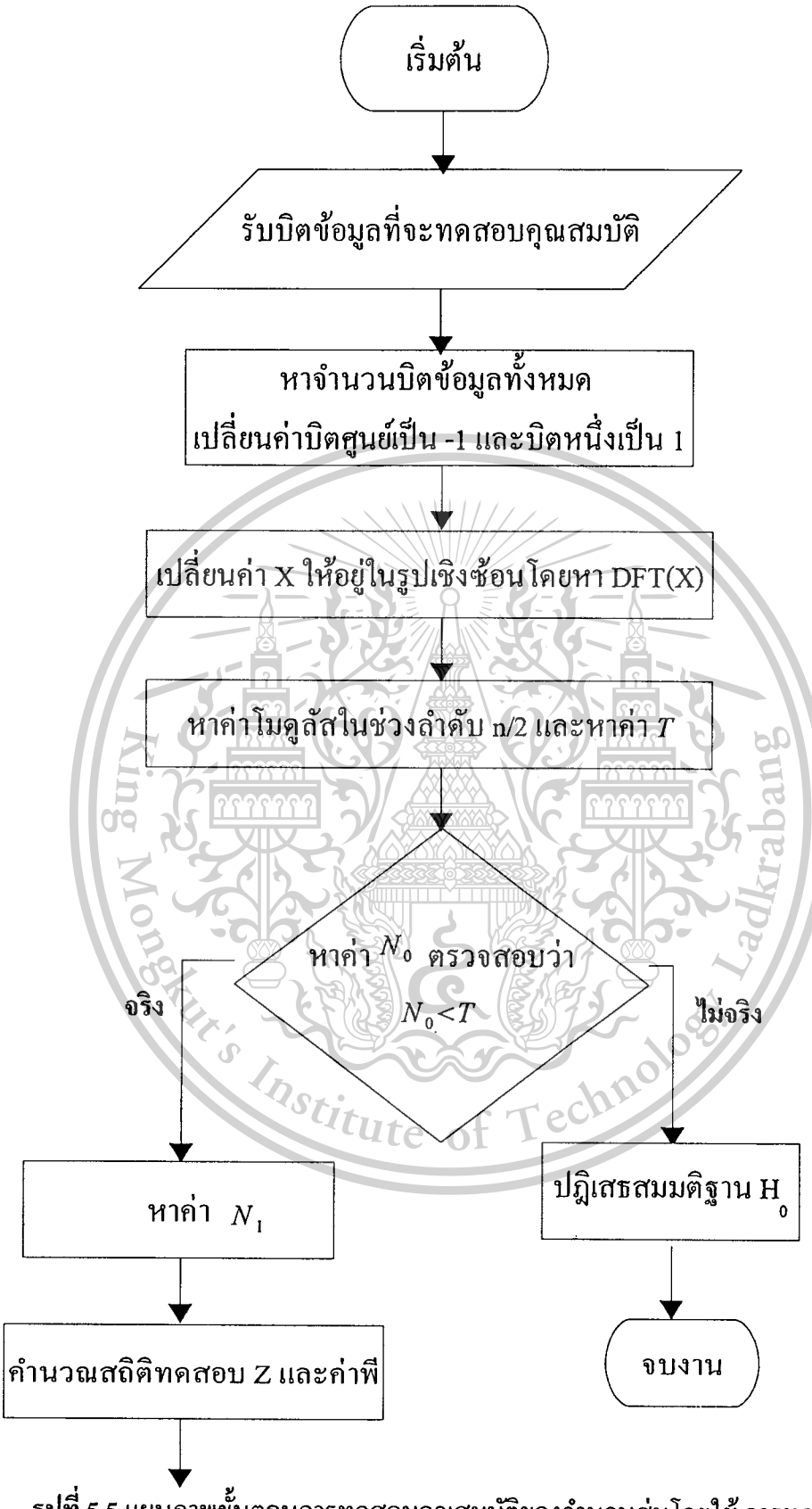
ขั้นตอนที่ 8 คำนวณค่าพีจาก $P-value=Z$

ขั้นตอนที่ 9 การสรุปผลการทดสอบ

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่าพีที่คำนวณได้ตกอยู่บริเวณวิกฤตและในทางตรงกันข้ามก็จะยอมรับ H_0 โดยลำดับขั้นตอนของการทดสอบสามารถสรุปได้ตามแผนภาพ (Flow chart) ที่ 5.5 ดังนี้

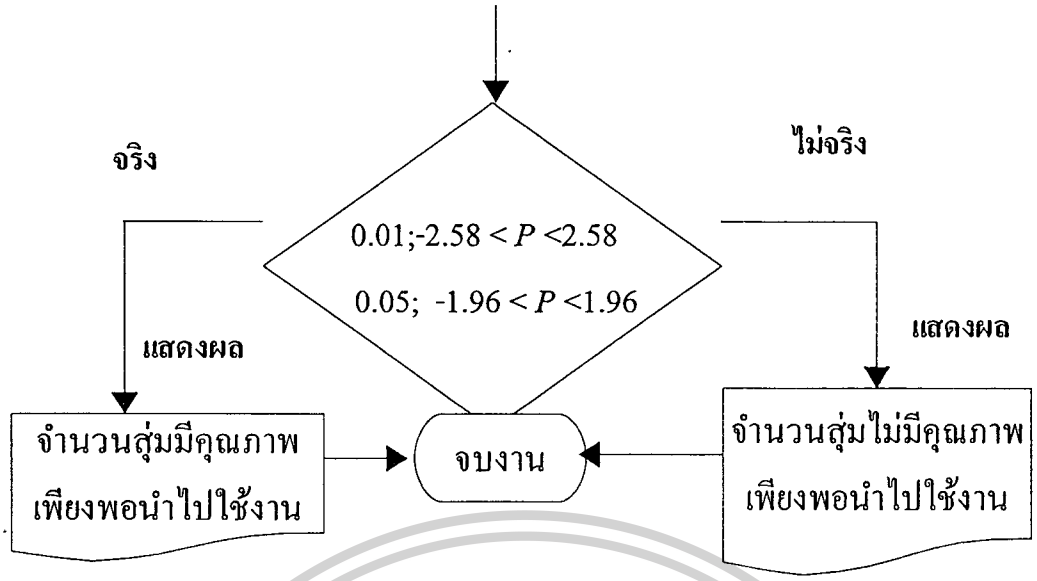
หมายเหตุ: ถ้าค่าที่คำนวณได้ Z มีค่าต่ำมาก จะแสดงให้เห็นว่าจำนวนพืดที่มีค่าต่ำกว่าค่า T นั้นมีจำนวนเล็กน้อยและจำนวนพืดที่มีความสูงเกินค่า T มีจำนวนมากกว่าร้อยละ 5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.5 แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้ การทดสอบลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.5 (ต่อ) แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้ การทดสอบลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)

King Mongkut's Institute of Technology Ladkrabang

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สี่ การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)

วัตถุประสงค์

เพื่อหาอัตราส่วน (สัดส่วน) ของบิตหนึ่งภายในชุดข้อมูล (Block) ขนาด M บิต เป้าหมายคือพิจารณาว่าจำนวนบิตหนึ่งภายในชุดข้อมูลขนาด M บิตจะมีค่าประมาณ ½ หรือไม่ ซึ่งคุณสมบัตินี้จะเป็นไปตามหลักของความเป็นจำนวนสุ่ม [11][12][21]

ตัวแปรและพารามิเตอร์ที่ใช้ในการทดสอบ

M คือ ความยาวของชุดข้อมูลในแต่ชุด

n คือ ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ การทดสอบนี้ n =1,000,000

ε คือ ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิดต่างๆ เช่น ε = 01011001...1100

นั่นคือ $\varepsilon=\varepsilon_1,\varepsilon_2,\varepsilon_3,..,\varepsilon_n$

การแจกแจง

การแจกแจงแบบไคกำลังสอง

ขั้นตอนการทดสอบ

ขั้นตอนที่ 1 แบ่งข้อมูลออกเป็นชุด โดยแต่ละชุดหาได้จาก $N=\left[\frac{n}{M}\right]$ บิตที่เหลือให้ตัดทิ้ง

ขั้นตอนที่ 2 พิจารณาสัดส่วนของบิตหนึ่ง π_i ในแต่ละชุดข้อมูลขนาด M จากสมการ

$$\pi_i=\frac{\left(\sum_{j=1}^{M}\varepsilon_{((j-1)M+j)}\right)}{M}\text{ ; สำหรับ }1\leqslant i\leqslant N$$

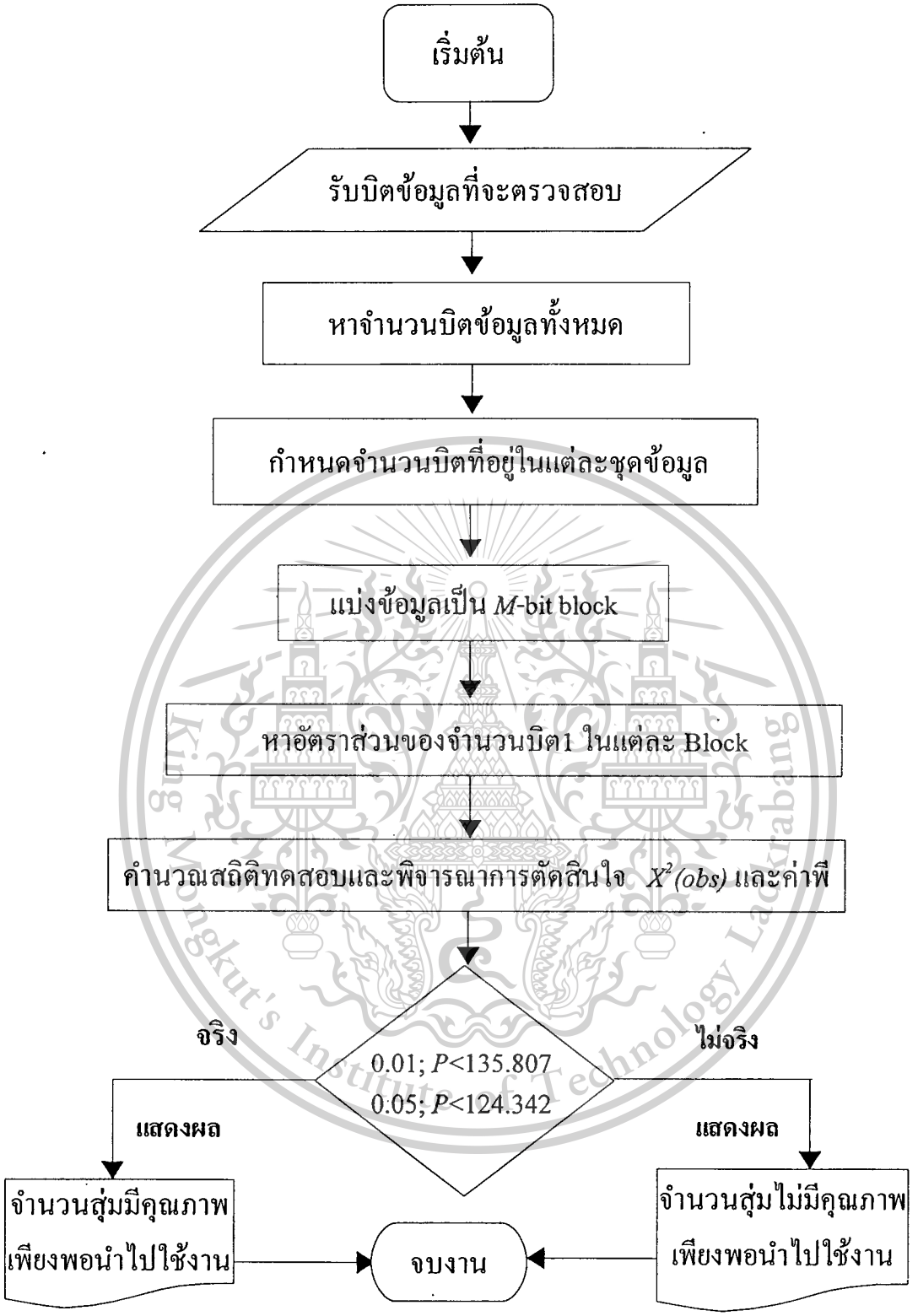
ขั้นตอนที่ 3 คำนวณสถิติทดสอบ $\chi^2(obs)=4M\sum_{i=1}^{N}(\pi_i-1/2)^2$

ขั้นตอนที่ 4 คำนวณค่าพีจาก $P-value=\chi^2$

ขั้นตอนที่ 5 การสรุปผลการทดสอบ

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่าพีที่คำนวณได้ตกอยู่บริเวณวิกฤต และในทางตรงกันข้ามก็จะยอมรับ H_0 โดยลำดับขั้นตอนของการทดสอบสามารถสรุปได้ตามแผนภาพ (Flow chart) ที่ 5.6 ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 5.6 แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่ห้า การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)

วัตถุประสงค์

เป้าหมายคือการหารันที่ยาวที่สุด (Longest run) ของบิตหนึ่งภายในชุดข้อมูลขนาด M วัตถุประสงค์คือเพื่อพิจารณาว่าความยาวที่สุดของรันของบิตหนึ่งภายในลำดับชุดข้อมูลที่ถูกตรวจสอบมีความสอดคล้องกับความยาวที่สุดของรันของบิตหนึ่งภายในลำดับจำนวนสุ่มหรือไม่ [22][23] [24]

ตัวแปรและพารามิเตอร์ที่ใช้ในการทดสอบ

n คือ ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ การทดสอบนี้ n =1,000,000

ε คือ ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิดต่างๆ เช่น ε = 01011001...1100 นั่นคือ $\varepsilon = \varepsilon_1, \varepsilon_2, \varepsilon_3, .., \varepsilon_n$

M คือ ความยาวของชุดข้อมูลในแต่ชุด ซึ่งถูกกำหนดไว้ด้วยทฤษฎีของแรนดอมวอล์ก (Random Walk) [25] ซึ่งกำหนดไว้ 3 ค่า ได้แก่ $M=8$ $M=128$ และ $M=10,000$ เมื่อกำหนดค่า n เป็นไปตามตารางนี้

ค่า n ที่น้อยที่สุด	M
128	8
6272	128
750,000	10,000

N คือ จำนวนชุดข้อมูลซึ่งจะต้องสอดคล้องกับข้าง M ที่แสดงข้างต้น

การแจกแจง

การแจกแจงแบบไคกำลังสอง (Chi-Square Distribution)

ขั้นตอนการทดสอบ

ขั้นตอนที่ 1 แบ่งข้อมูลจำนวนสุ่มออกเป็นชุดข้อมูลขนาด M บิต

ขั้นตอนที่ 2 หาค่าความถี่ของรันของบิตหนึ่งที่ยาวที่สุด (ν_i) ที่เกิดขึ้นตามตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ตารางที่ 5.1 แสดงค่า M และความถี่ของการตรวจพบบิตหนึ่งที่เกิดขึ้นซ้ำกัน

ν_i	$M=8$	$M=128$	$M=10{,}000$
ν_0	น้อยกว่าหรือเท่ากับ 1	น้อยกว่าหรือเท่ากับ 4	น้อยกว่าหรือเท่ากับ 10
ν_1	2	5	11
ν_2	3	6	12
ν_3	มากกว่าหรือเท่ากับ 4	7	13
ν_4		8	14
ν_5		มากกว่าหรือเท่ากับ 9	15
ν_6			มากกว่าหรือเท่ากับ 16

นอกจากนี้ทำการการพิจารณาเลือกค่าระดับขั้นความเสรี(K) จากข้อกำหนดนี้

กรณีที่หนึ่ง $K=3 \quad M=8$

$\nu_0 = 1 \quad \nu_1 = 2 \quad \nu_2 = 3 \quad \nu_3 = 4$

$pi_0 = 0.21484375 \quad pi_1 = 0.3671875 \quad pi_2 = 0.23046875 \quad pi_3 = 0.1875$

กรณีที่สอง $K=5 \quad M=128$

$\nu_0 = 4 \quad \nu_1 = 5 \quad \nu_2 = 6 \quad \nu_3 = 7 \quad \nu_4 = 8 \quad \nu_5 = 9$

$pi_0 = 0.1174035788 \quad pi_1 = 0.242955959 \quad pi_2 = 0.249363483$

$pi_3 = 0.17517706 \quad pi_4 = 0.102701071 \quad pi_5 = 0.112398847$

กรณีที่สาม $K=6 \quad M=10{,}000$

$\nu_0 = 10 \quad \nu_1 = 11 \quad \nu_2 = 12 \quad \nu_3 = 13 \quad \nu_4 = 14 \quad \nu_5 = 15 \quad \nu_6 = 16$

$pi_0 = 0.0882 \quad pi_1 = 0.2092 \quad pi_2 = 0.2483 \quad pi_3 = 0.1933$

$pi_4 = 0.1208 \quad pi_5 = 0.0675 \quad pi_6 = 0.0727$

ขั้นตอนที่ 3 คำนวณสถิติทดสอบ $\chi^2(obs)=\dfrac{\sum_{i=0}^{K}(\nu_i - N\pi_i)^2}{(N\pi_i)}$ โดยค่า K และ N หา

ได้จากตารางที่ 5.2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ตารางที่ 5.2 แสดงค่า M K และ N ที่สอดคล้องกับทฤษฎี

M	K	N
8	3	16
128	5	49
10,000	6	75

ขั้นตอนที่ 4 คำนวณค่าพีจาก $P-value=\chi^2$

ขั้นตอนที่ 5 การสรุปผลการทดสอบ

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่าพีที่คำนวณได้ตกอยู่บริเวณวิกฤต และในทางตรงกันข้ามก็จะยอมรับ H_0 โดยลำดับขั้นตอนของการทดสอบสามารถสรุปได้ตามแผนภาพ (Flow chart) ที่ 5.7 ดังนี้

หมายเหตุ ความผิดปกติของบิตหนึ่งที่ยาวที่สุดจะบ่งบอกว่ามีความผิดปกติของของบิตศูนย์ที่ยาวที่สุดด้วยเช่นกันและถ้าค่า χ^2 มีขนาดใหญ่แสดงว่าลำดับที่ถูกทดสอบมีกลุ่มของบิตหนึ่งมากกว่าบิตศูนย์

King Mongkut's Institute of Technology Ladkrabang

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.



รูปที่ 5.7 แผนภาพขั้นตอนการทดสอบคุณสมบัติของจำนวนสุ่มโดยใช้การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

บทที่ 6
ผลการทดสอบและการเปรียบเทียบ

จากการออกแบบการพัฒนาชุดวิธีทดสอบคุณสมบัติจำนวนสุ่มดังบทที่ 5 นี้ กระบวนสำคัญของการทดสอบคือ การคำนวณสถิติทดสอบและการพิจารณาการผ่านการทดสอบ ซึ่งได้นำเสนอหลักการคำนวณสถิติทดสอบและการพิจารณาการผ่านการทดสอบ แยกตามประเภทของการแจกแจงของชุดจำนวนสุ่ม 2 แบบ ได้แก่ วิธีที่หนึ่ง สำหรับจำนวนสุ่มที่มีการแจกแจงแบบปกติจะคำนวณได้จากค่ามาตรฐาน *(Z)* และวิธีที่สองสำหรับจำนวนสุ่มที่มีการแจกแจงไคกำลังสอง (χ^2) จะคำนวณได้จากสถิติทดสอบไคกำลังสอง (χ^2)

จากหลักการที่นำเสนอ จะเห็นว่าการหาสถิติทดสอบดังกล่าวนี้อยู่ในรูปสมการที่มีความเรียบง่าย และมีความซับซ้อนต่ำ สามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและค่าทางสถิติได้โดยตรง ทำให้สามารถพิจารณาการผ่านการทดสอบโดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้ ซึ่งคาดว่าการใช้กระบวนการคำนวณดังที่นำเสนอจะส่งผลให้การทดสอบคุณสมบัติของจำนวนสุ่มมีระยะเวลาสั้นลง และเป็นแนวทางที่จะพัฒนาการทดสอบคุณสมบัติจำนวนสุ่มผ่านระบบออนไลน์ได้ โดยกำหนดเงื่อนไขและคุณสมบัติของการทดสอบตามบทที่ 5

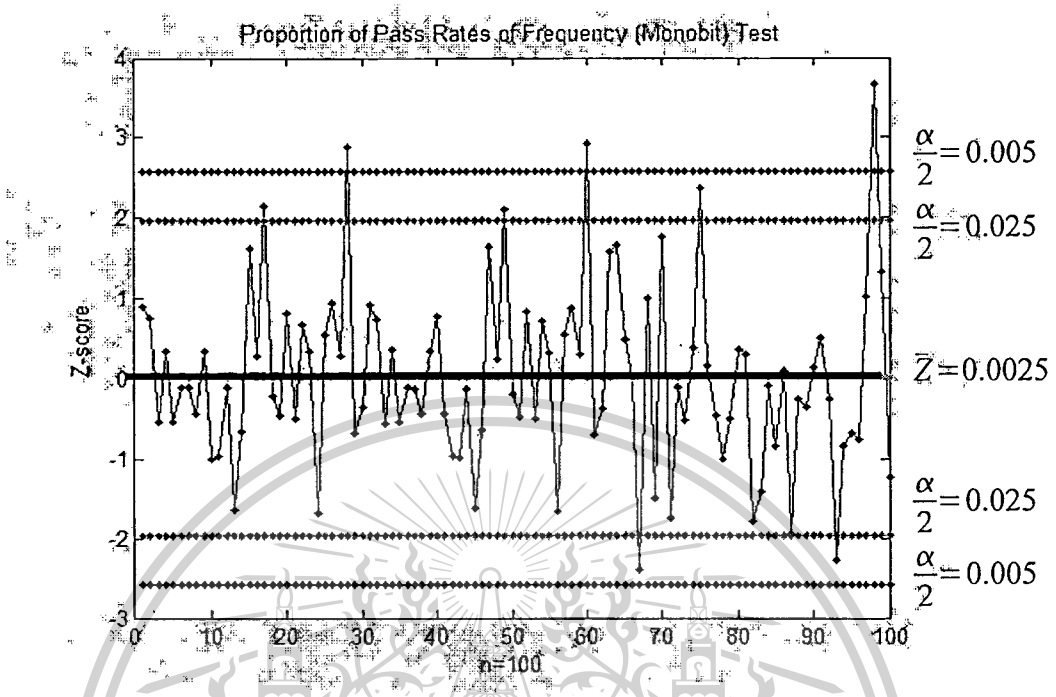
บทที่ 6 นี้กล่าวถึงผลการทดสอบและการวิเคราะห์ผลการทดสอบของชุดวิธีทดสอบที่นำเสนอทั้งหมด 5 วิธีทดสอบ โดยการวิเคราะห์ผลการทดสอบของชุดวิธีทดสอบที่นำเสนอ 3 แบบดังนำเสนอในบทที่ 5 ซึ่งมีรายละเอียดของผลการทดสอบและการวิเคราะห์ผล ดังนี้

6.1 การวิเคราะห์ความแตกต่างของการพิจารณาสัดส่วนการผ่านการทดสอบ

วิทยานิพนธ์ฉบับนี้ ได้ทำการทดสอบคุณสมบัติของจำนวนสุ่มเพื่อใช้เป็นกุญแจรหัสลับของวิทยาการรหัสลับ เนื่องจากการทดสอบทางสถิติต้องใช้จำนวนสุ่มจำนวนมาก เพื่อให้ได้ผลการทดสอบที่ดีและให้ค่าที่ใกล้เคียงกับข้อมูลจริงมากที่สุด จึงจำเป็นต้องใช้จำนวนสุ่มเทียมที่ได้จากแหล่งกำเนิดที่เป็นฟังก์ชันการสร้างจำนวนสุ่มเทียมด้วยโปรแกรมคอมพิวเตอร์ซึ่งมีความสะดวกในการกำเนิด ซึ่งเก็บตัวอย่างจำนวนสุ่มจำนวน 100 ชุด ชุดละ 1,000,000 บิต เพื่อเก็บผลทางสถิติและประเมินผลการทดสอบ ซึ่งวิธีผลการทดสอบตามลำดับชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่ม 5 วิธี ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่หนึ่ง การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)



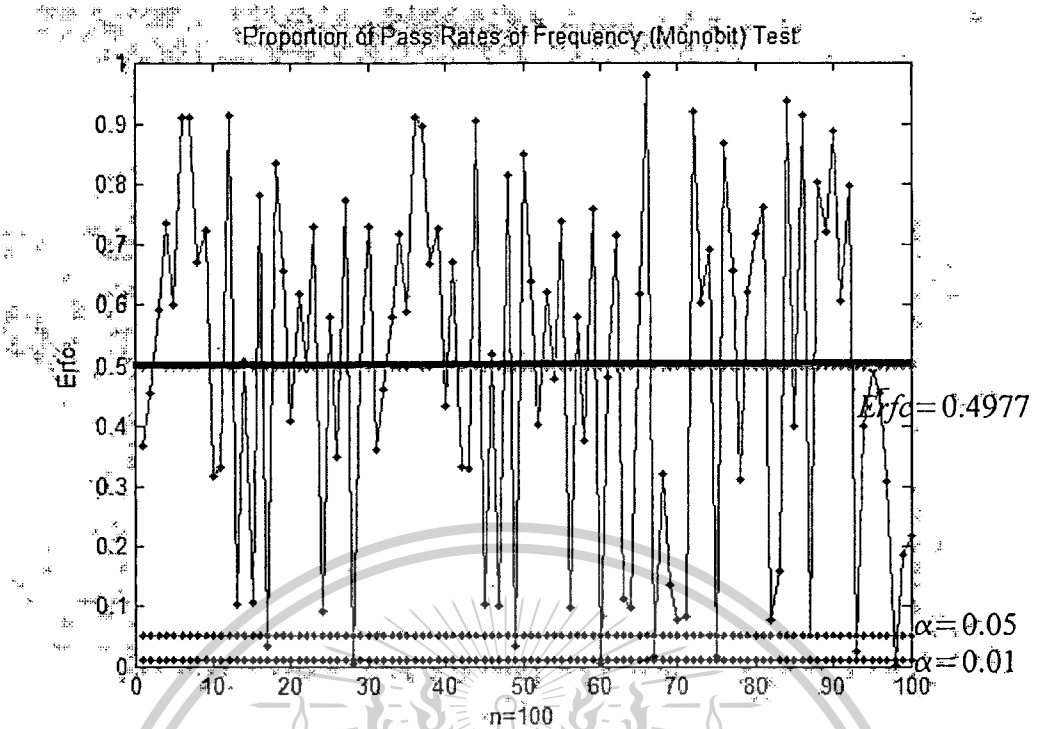
รูปที่ 6.1 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 1 โดยใช้ Z

จากรูปที่ 6.1 สัดส่วนการผ่านการทดสอบโดยค่า Z ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Z=0.0225$ มีค่าเบี่ยงเบนไปจากค่าทางทฤษฎี 0.0225 นั่นคือจำนวนทั้งสองมีจำนวนใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 28 49 60 67 75 93 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 8 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 92

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 28 60 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็นร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 6.2 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 1 โดยใช้ *Erfc*

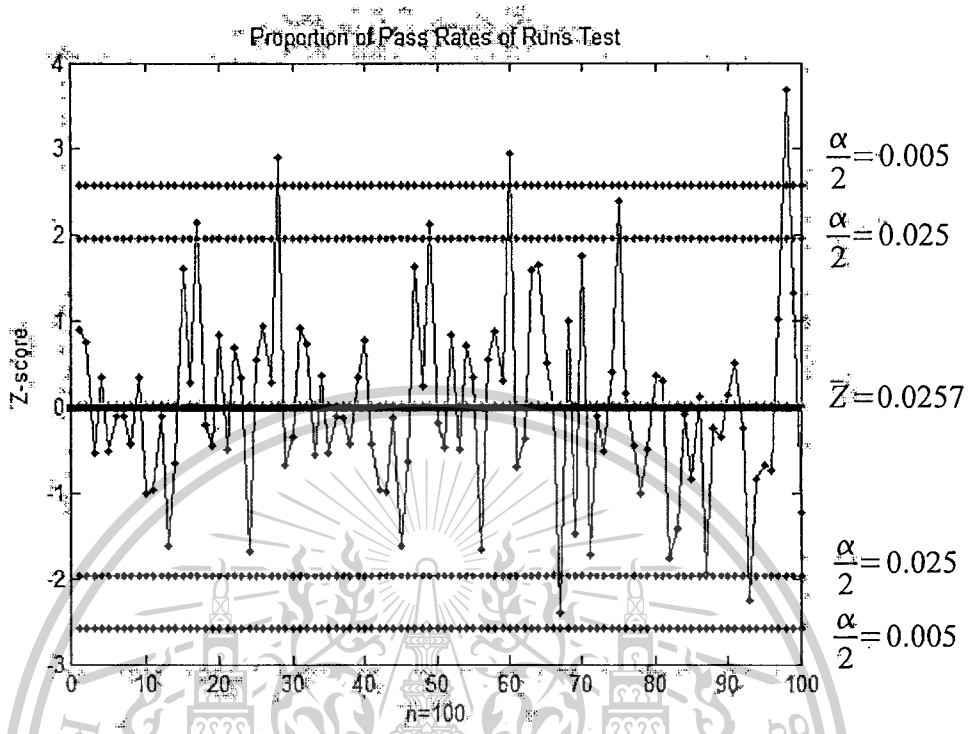
จากรูปที่ 6.1 สัดส่วนการผ่านการทดสอบ ค่า *Erfc* ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Erfc = 0.4977$ มีค่าเบี่ยงเบนไปจากค่าทางทฤษฎี 0.0023 นั่นคือจำนวนทั้งสองมีจำนวนใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 28 49 60 67 75 93 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 8 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 92

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 28 60 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สอง การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)



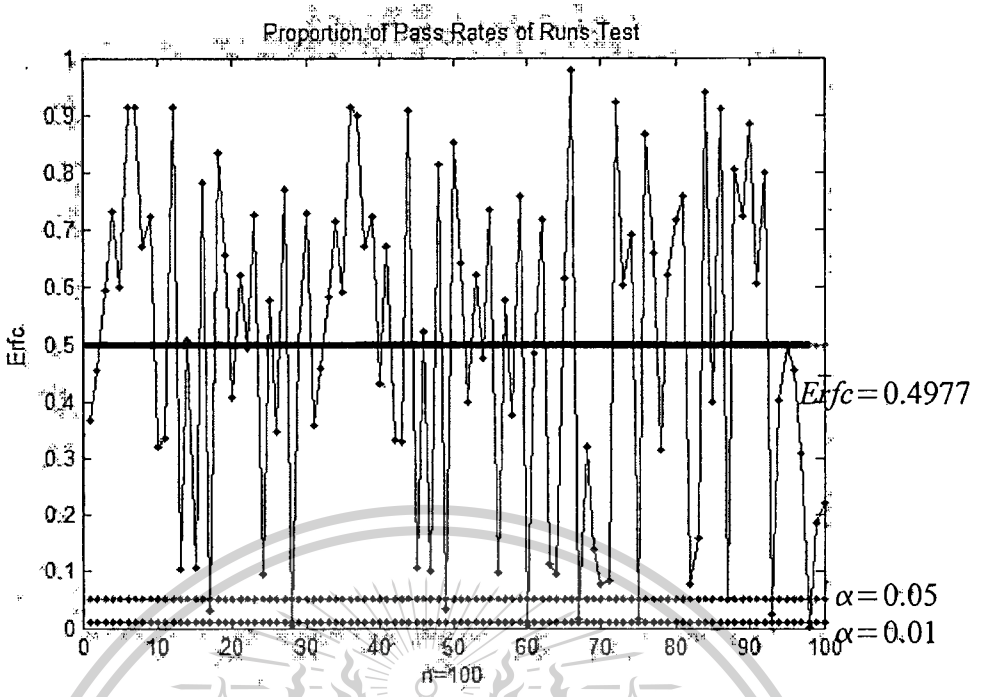
รูปที่ 6.3 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 2 โดยใช้ Z

จากรูปที่ 6.3 สัดส่วนการผ่านการทดสอบค่า Z ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Z=0.0257$ เบี่ยงเบนไปจากค่าทางทฤษฎี 0.0257 นั่นคือจำนวนการรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความถี่การเกิดรันเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 28 49 60 67 75 93 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 8 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 92

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 28 60 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็นร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 6.4 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 2 โดยใช้ *Erfc*

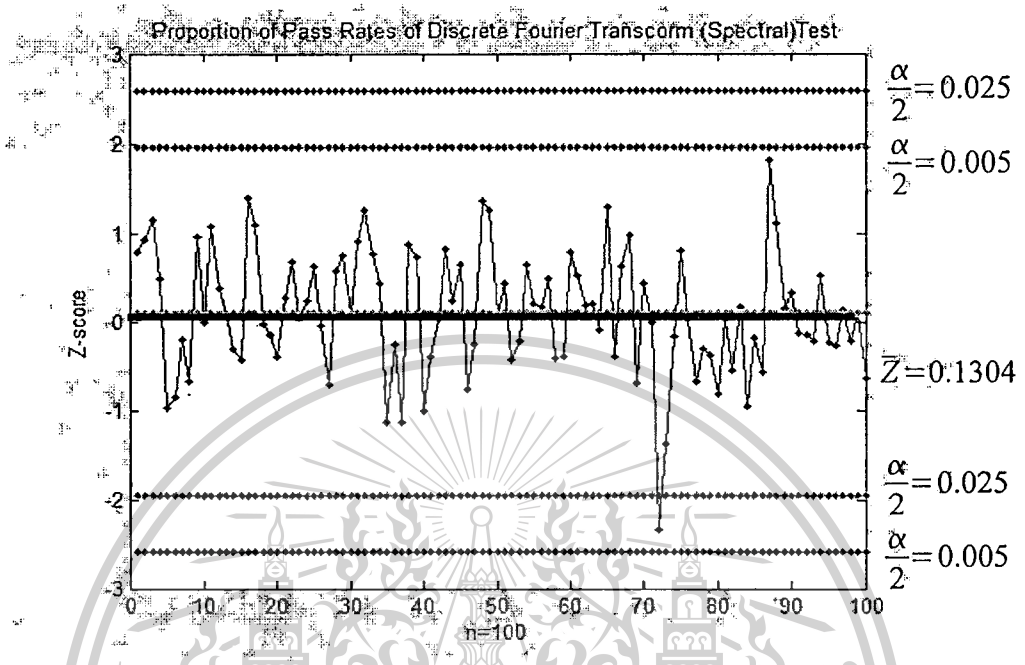
จากรูปที่ 6.4 สัดส่วนการผ่านการทดสอบค่า *Erfc* ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Erfc = 0.4979$ เบี่ยงเบนไปจากค่าทางทฤษฎี 0.0021 นั่นคือจำนวนการรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความถี่การเกิดรันเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 28 49 60 67 75 93 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 8 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 92

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 28 60 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็นร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สาม การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)



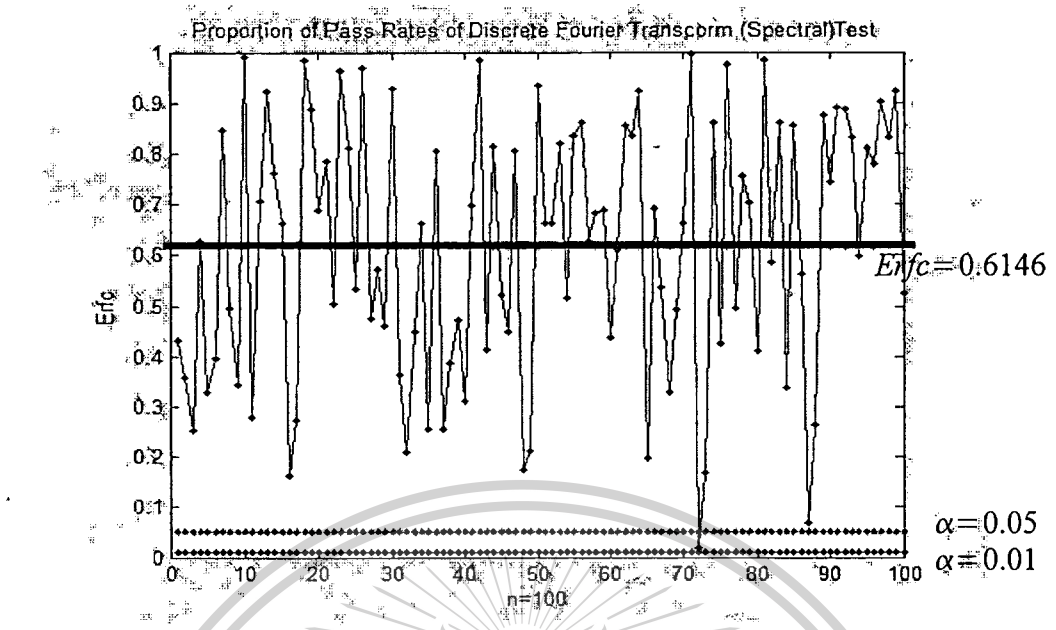
รูปที่ 6.5 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 3 โดยใช้ Z

จากรูปที่ 6.5 สัดส่วนการผ่านการทดสอบค่า Z ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Z=0.1304$ เบี่ยงเบนไปจากค่าทางทฤษฎี 0.1304 นั่นคือมีค่าความแตกต่างต่ำกว่าร้อยละ 5 ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 72 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 1 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 99

ระดับนัยสำคัญเท่ากับ 0.01 ไม่มีชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 6.6 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 3 โดยใช้ *Erfc*

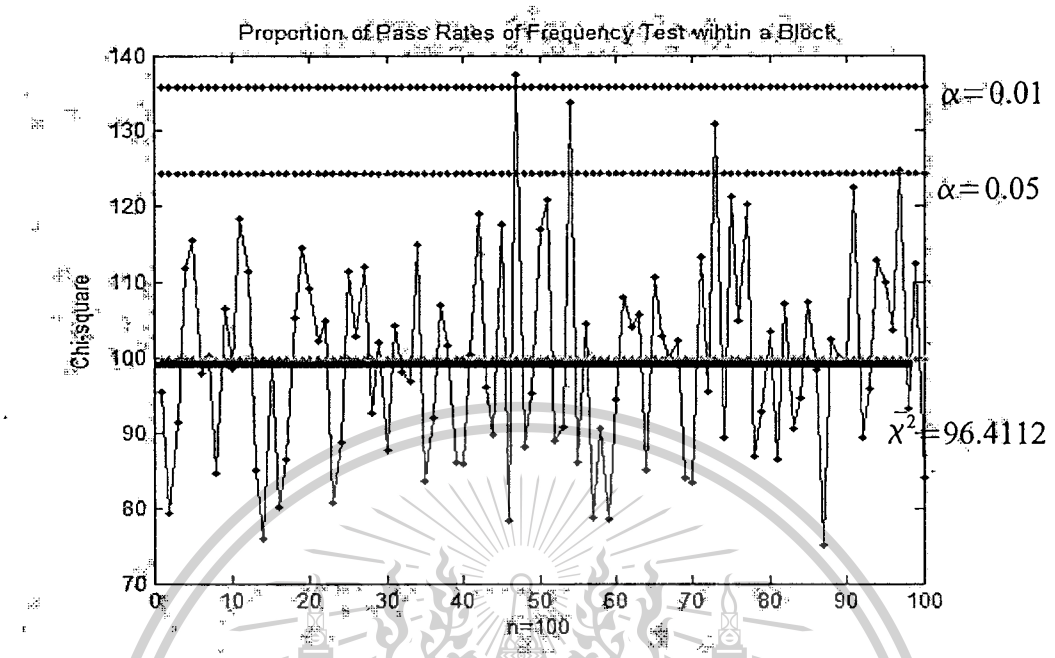
จากรูปที่ 6.6 สัดส่วนการผ่านการทดสอบค่า *Erfc* ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Erfc = 0.6146$ เบี่ยงเบนไปจากค่าทางทฤษฎี 0.1146 นั่นคือมีค่าความแตกต่างต่ำกว่าร้อยละ 5 ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 72 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 1 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 99

ระดับนัยสำคัญเท่ากับ 0.01 ไม่มีชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 100

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สี่ การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)



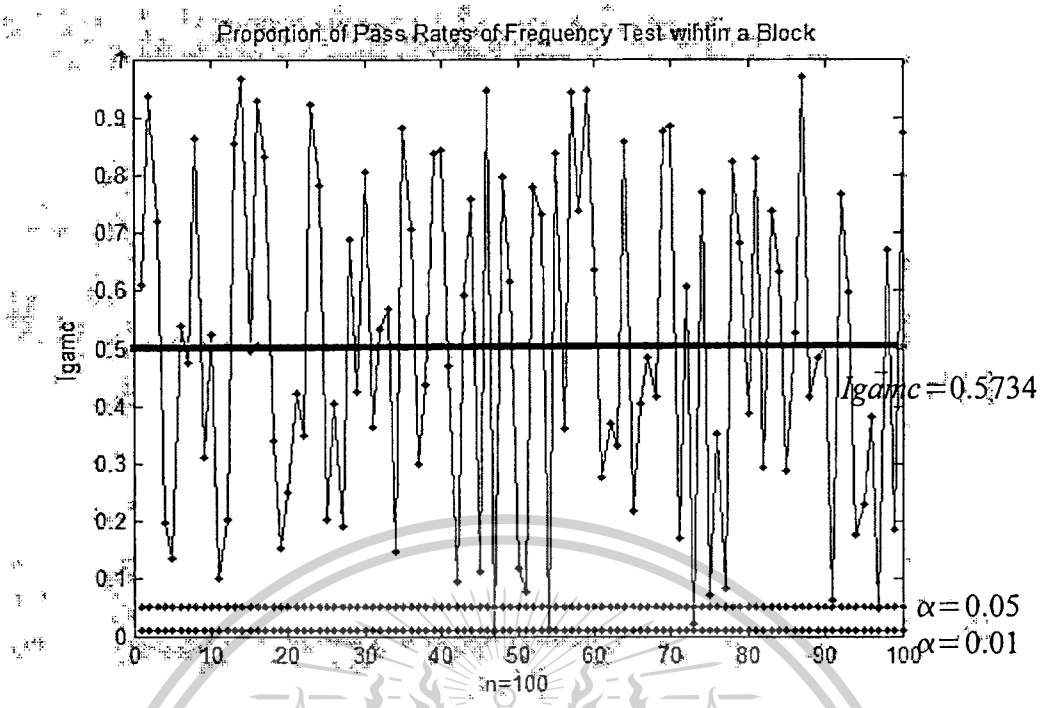
รูปที่ 6.7 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 4 โดยใช้ χ^2

จากรูปที่ 6.7 สัดส่วนการผ่านการทดสอบค่า χ^2 ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $\chi^2=96.4112$ ซึ่งมีค่าเข้าใกล้ค่าระดับขั้นความเสรี (k) ซึ่งเท่ากับ 100 โดยเบี่ยงเบนไปจากค่าทางทฤษฎี 3.5888 ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 47 54 73 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 4 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 96

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 47 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 1 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 99

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 6.8 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 4 โดยใช้ *Igamc*

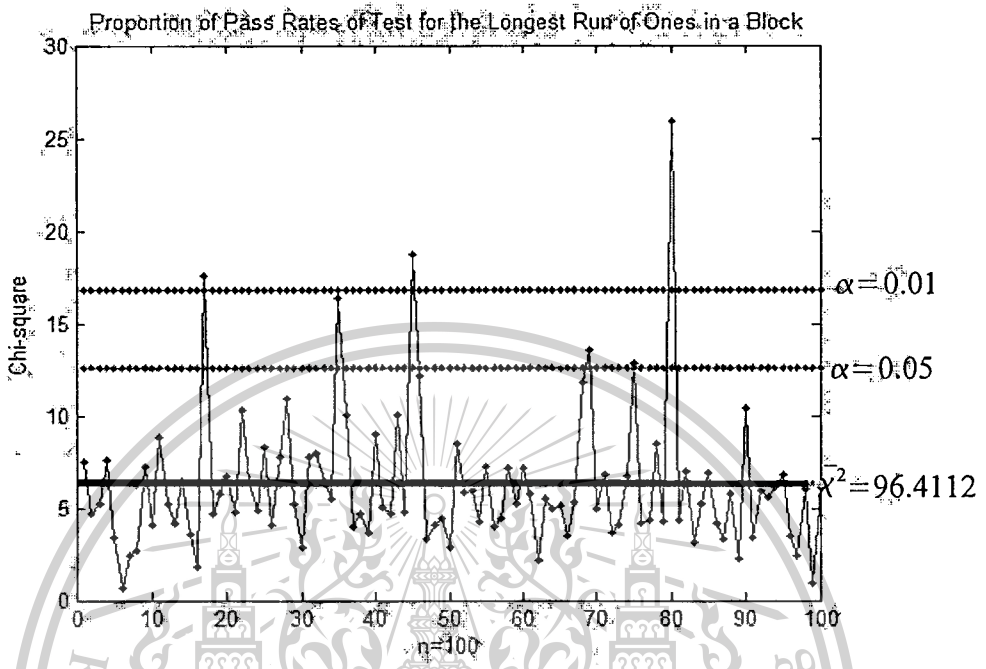
จากรูปที่ 6.8 สัดส่วนการผ่านการทดสอบค่า *Igamc* ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Igamc = 0.5734$ ซึ่งมีค่าเข้าใกล้ 0.5 โดยเบี่ยงเบนจากค่าทางทฤษฎี 0.0734 ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 47 54 73 และ 98 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 4 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 96

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 47 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 1 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 99

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่ห้า การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)



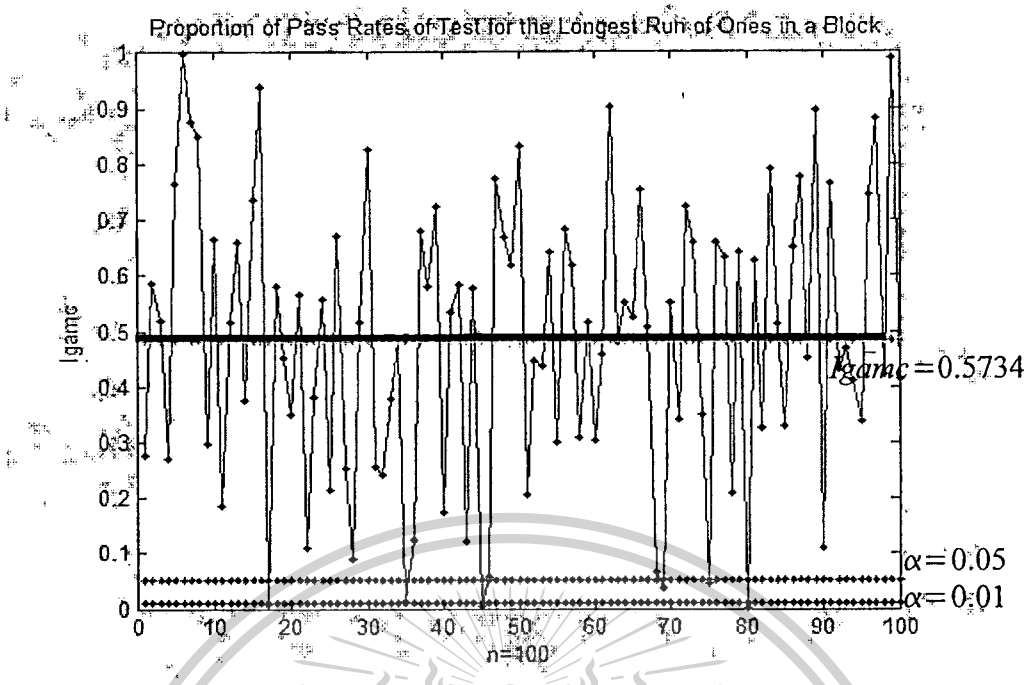
รูปที่ 6.9 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 5 โดยใช้ χ^2

จากรูปที่ 6.9 สัดส่วนการผ่านการทดสอบค่า χ^2 ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $\chi^2=6.4698$ ซึ่งมีค่าเข้าใกล้ค่าระดับขั้นความเสรี (k) ซึ่งเท่ากับ 7 โดยเบี่ยงเบนไปจากค่าทางทฤษฎี 0.0757 นั่นคือจำนวนรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความยาวของการเกิดรันของทั้งบิตศูนย์และบิตหนึ่งใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 35 45 69 75 และ 80 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 6 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 94

ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 45 และ 80 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็นร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



รูปที่ 6.10 สัดส่วนการผ่านการทดสอบ (Proportion of Passing Rates) วิธีที่ 5 โดยใช้ *Igamc*

จากรูปที่ 6.10 สัดส่วนการผ่านการทดสอบค่า *Igamc* ที่คำนวณได้มีการกระจายตัวรอบที่ค่าเฉลี่ยที่ $Igamc = 0.4418$ ซึ่งมีค่าเข้าใกล้ 0.5 โดยเบี่ยงเบนไปจากค่าทางทฤษฎี 0.0582 นั่นคือ จำนวนการรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความยาวของการเกิดรันของทั้งบิตศูนย์และบิตหนึ่งใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

ระดับนัยสำคัญเท่ากับ 0.05 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 35 45 69 75 และ 80 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 6 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 94

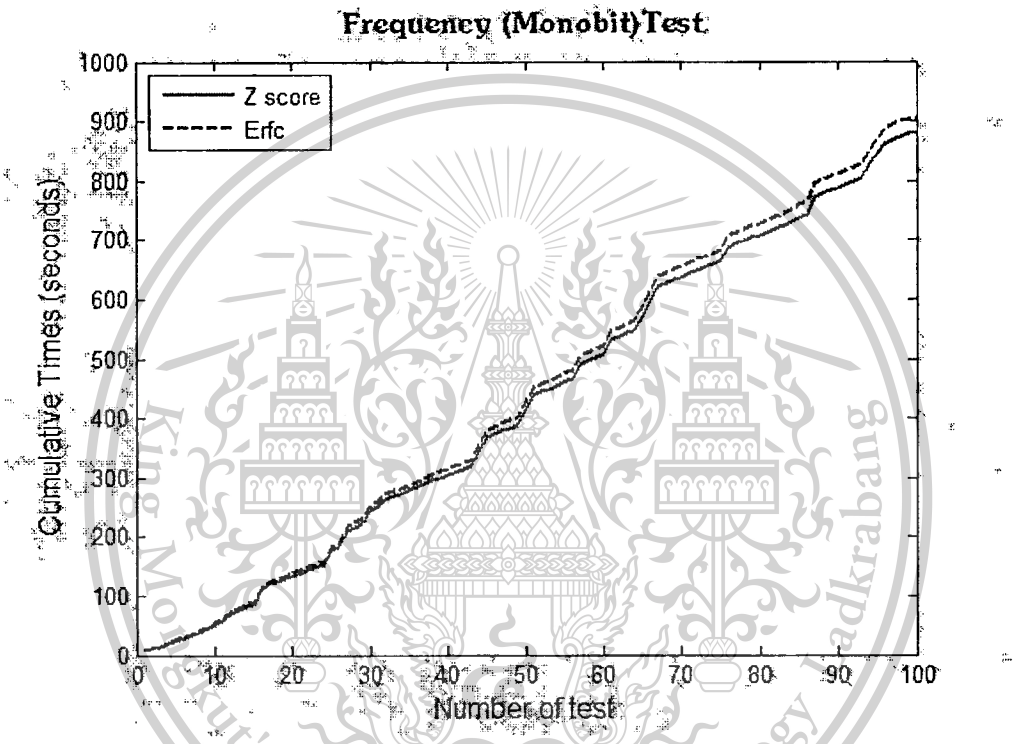
ระดับนัยสำคัญเท่ากับ 0.01 ชุดของจำนวนสุ่มที่ไม่ผ่านการทดสอบ ได้แก่ ชุดที่ 17 45 และ 80 รวมชุดจำนวนสุ่มที่ไม่ผ่านการทดสอบ จำนวน 3 ชุด ดังนั้นสัดส่วนการผ่านการทดสอบเป็น ร้อยละ 97

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

6.2 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบ

การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบสามารถแสดงด้วยกราฟเวลาที่ใช้ในการประมวลผลสะสมและเปรียบเทียบร้อยละของเวลาทั้งหมดที่ใช้ในการประมวลผลการทดสอบโดยเฉลี่ย ซึ่งวิธีผลการทดสอบตามลำดับชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่ม 5 วิธี ดังนี้

วิธีที่หนึ่ง การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)



รูปที่ 6.11 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 1 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง *Erfc*

จากรูปที่ 6.11 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 1 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง *Erfc*

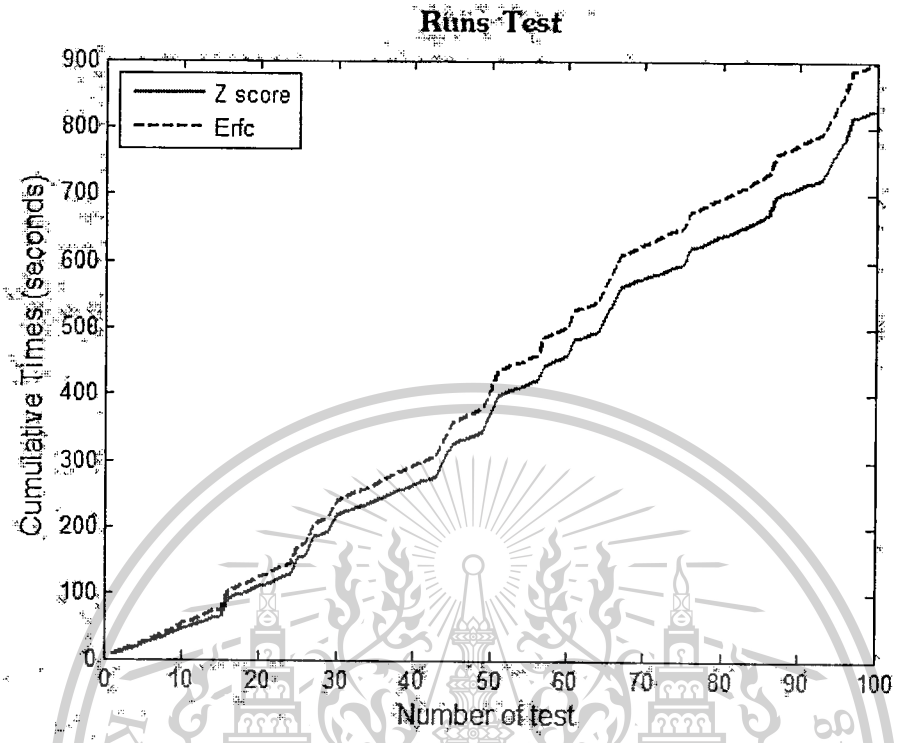
หลักการที่นำเสนอ Z ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 881.26 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 8.8126 วินาที

หลักการอ้างอิง *Erfc* ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 907.48 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 9.0748 วินาที

ทั้งสองหลักการใช้เวลาการประมวลผลต่างกันโดยเฉลี่ยร้อยละ 2.9317

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สอง การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)



รูปที่ 6.12 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 2 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง *Erfc*

จากรูปที่ 6.12 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 2 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง *Erfc*

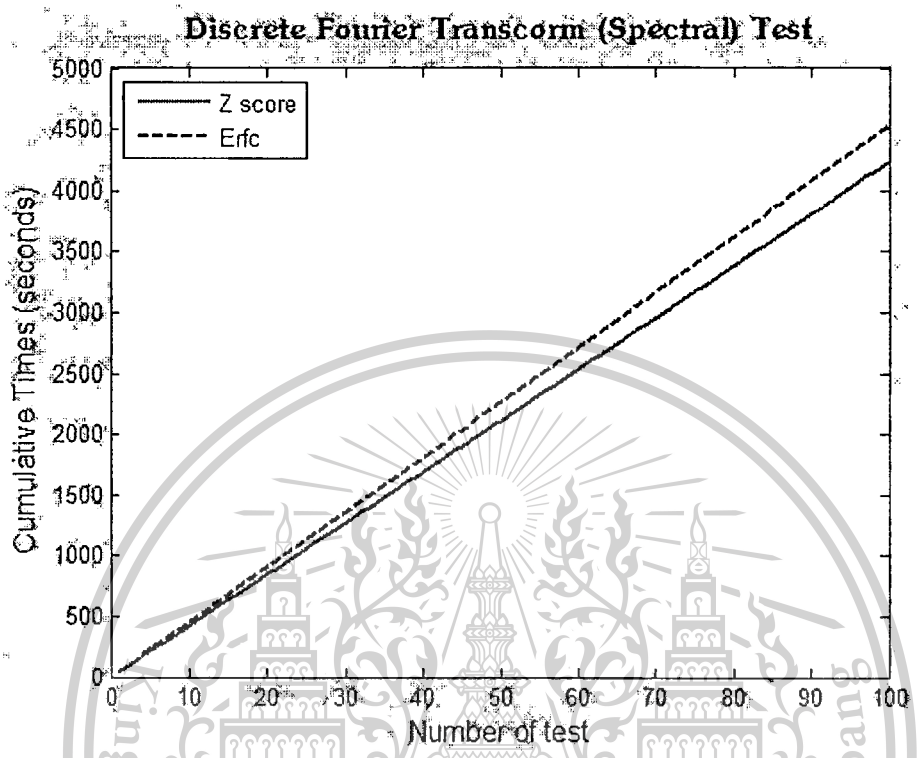
หลักการที่นำเสนอ Z ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 827.65 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 8.2765 วินาที

หลักการอ้างอิง *Erfc* ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 898.82 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 8.9882 วินาที

ทั้งสองหลักการใช้เวลาการประมวลผลต่างกันโดยเฉลี่ยร้อยละ 8.2446

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สาม การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)



รูปที่ 6.13 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 3 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง $Erfc$

จากรูปที่ 6.13 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 3 ระหว่างหลักการที่นำเสนอ Z และหลักการอ้างอิง $Erfc$

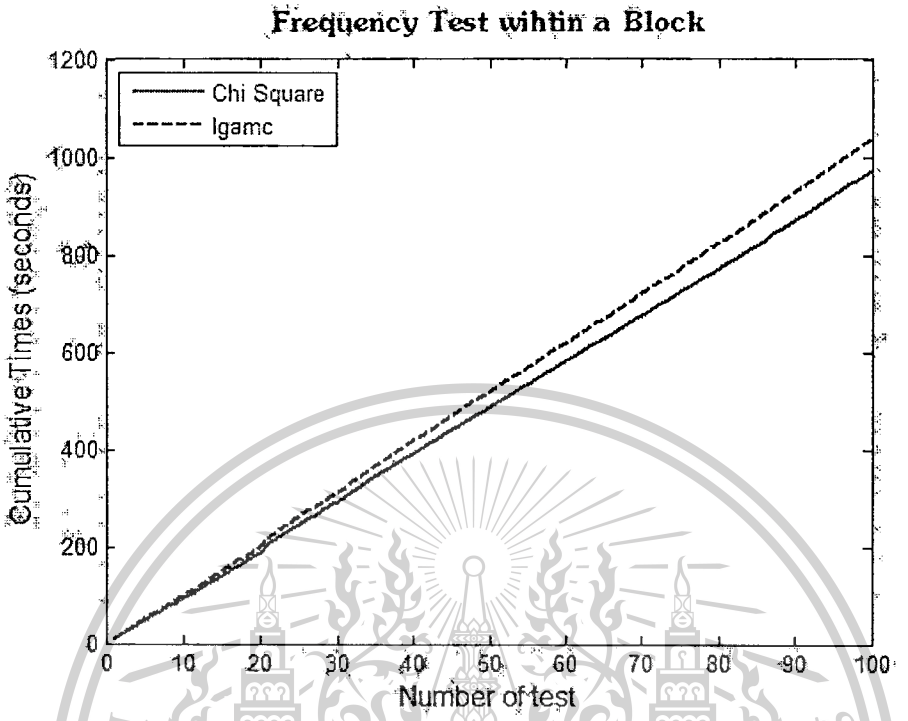
หลักการที่นำเสนอ Z ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 4685.19 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 46.8519 วินาที

หลักการอ้างอิง $Erfc$ ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 4964.49 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 49.6449 วินาที

ทั้งสองหลักการใช้เวลาการประมวลผลต่างกันโดยเฉลี่ยร้อยละ 6.2306

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่สี่ การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)



รูปที่ 6.14 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 4 ระหว่างหลักการที่นำเสนอ χ^2 และหลักการอ้างอิง *Igamc*

จากรูปที่ 6.14 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 4 ระหว่างหลักการที่นำเสนอ χ^2 และหลักการอ้างอิง *Igamc*

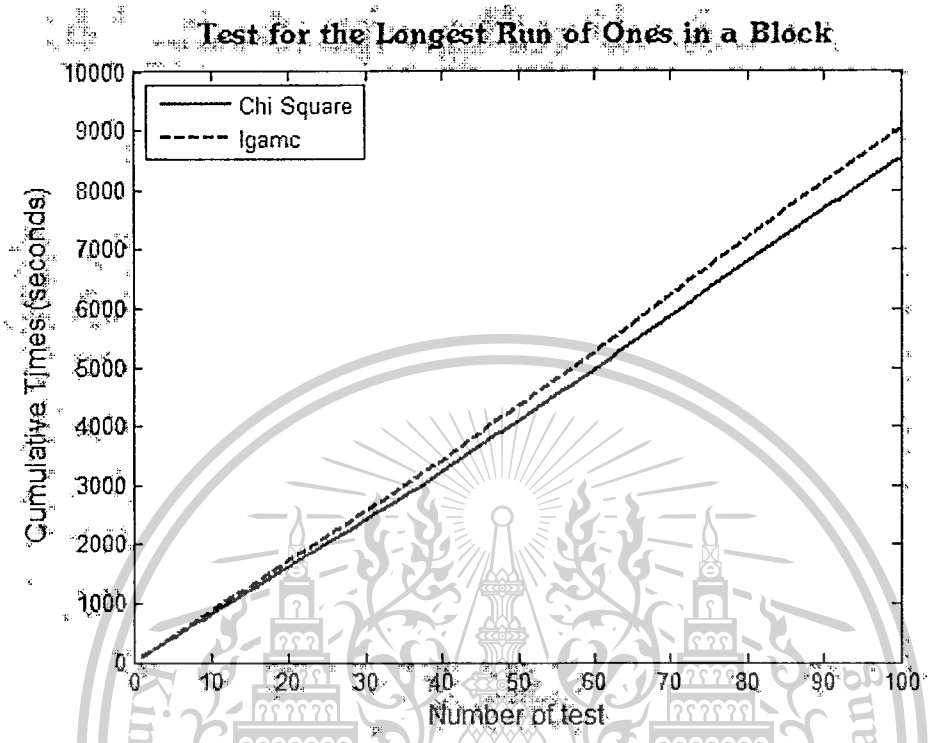
หลักการที่นำเสนอ χ^2 ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 1129.03 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 11.2903 วินาที

หลักการอ้างอิง *Igamc* ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 1190.60 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 11.9060 วินาที

ทั้งสองหลักการใช้เวลาการประมวลผลต่างกันโดยเฉลี่ยร้อยละ 5.3086

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

วิธีที่ห้า การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)



รูปที่ 6.15 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 5 ระหว่างหลักการที่นำเสนอ χ^2 และหลักการอ้างอิง *Igamc*

จากรูปที่ 6.15 การเปรียบเทียบเวลาที่ใช้ในการประมวลผลการทดสอบของวิธีที่ 5 ระหว่างหลักการที่นำเสนอ χ^2 และหลักการอ้างอิง *Igamc*

หลักการที่นำเสนอ χ^2 ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 7407.27 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 74.0727 วินาที

หลักการอ้างอิง *Igamc* ใช้เวลาในการประมวลผลการทดสอบสะสม 100 ชุด เป็น 7909.53 วินาที เฉลี่ยต่อการทดสอบหนึ่งครั้งเป็น 79.0953 วินาที

ทั้งสองหลักการใช้เวลาการประมวลผลต่างกันโดยเฉลี่ยร้อยละ 6.5583

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

6.3 การเปรียบเทียบความแตกต่างของสัดส่วนการผ่านการทดสอบระหว่างแหล่งกำเนิดจำนวนสุ่มแท้และจำนวนสุ่มเทียม

ตารางที่ 6.1 ตารางเปรียบเทียบความแตกต่างของสัดส่วนการผ่านการทดสอบระหว่างแหล่งกำเนิดจำนวนสุ่มแท้แลจำนวนสุ่มเทียม

วิธีการทดสอบ	ระดับนัยสำคัญ	แหล่งกำเนิดจำนวนสุ่มเทียม	แหล่งกำเนิดจำนวนสุ่มแท้
Frequency Test	0.05	92	97
	0.01	97	99
Runs Test	0.05	92	97
	0.01	97	99
Discrete Fourier Transform (Spectral) Test	0.05	99	100
	0.01	100	100
Frequency Test within a Block	0.05	96	97
	0.01	99	100
Test for the Longest Run of Ones in a Block	0.05	94	96
	0.01	97	100

การเปรียบเทียบความแตกต่างของสัดส่วนการผ่านการทดสอบระหว่างแหล่งกำเนิดจำนวนสุ่มแท้ซึ่งได้จากแหล่งกำเนิดควอนตัมและจำนวนสุ่มเทียมได้จากการกำเนิดจำนวนสุ่มเทียมโดยใช้โปรแกรมบนคอมพิวเตอร์ ทั้งนี้ทำการทดสอบจำนวนสุ่มจำนวน 100 ชุด ชุดละ 1,000,000 บิต จากนั้นทำการเปรียบเทียบสัดส่วนการผ่านการทดสอบ ได้ผลการทดสอบดังตารางที่ 6.1

จากตารางที่ 6.1 ตารางเปรียบเทียบความแตกต่างของสัดส่วนการผ่านการทดสอบระหว่างแหล่งกำเนิดจำนวนสุ่มแท้แลจำนวนสุ่มเทียม พบว่าจำนวนสุ่มจากแหล่งกำเนิดจำนวนสุ่มแท้มีสัดส่วนการผ่านการทดสอบที่ระดับนัยสำคัญ 0.05 จำนวน 96 ชุด และที่ระดับนัยสำคัญ 0.01 จำนวน 99 ชุด จำนวนสุ่มจากแหล่งกำเนิดจำนวนสุ่มเทียมมีสัดส่วนการผ่านการทดสอบที่ระดับนัยสำคัญ 0.05 จำนวน 84 ชุด และที่ระดับนัยสำคัญ 0.01 จำนวน 93 ชุด ดังนั้น จำนวนสุ่มจากแหล่งกำเนิดจำนวนสุ่มแท้มีสัดส่วนการผ่านการทดสอบมากกว่าจำนวนสุ่มจากแหล่งกำเนิดจำนวนสุ่มเทียม แสดงว่าแหล่งจำนวนสุ่มแท้มีคุณสมบัติดีกว่าแหล่งกำเนิดจำนวนสุ่มเทียม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

บทที่ 7
สรุปผลการวิจัยและข้อเสนอแนะ

การพัฒนาชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่ม เพื่อให้มีความมั่นใจในการใช้งานจำนวนสุ่มด้านการสื่อสารปลอดภัย รวมทั้งเป็นแนวทางพัฒนาการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์(Web Service) และการพัฒนาชุดวิธีทดสอบอ้างอิงจากชุดทดสอบทางสถิติเอ็นไอเอสที (National Institute of Standards and Technology Statistical Test Suite) โดยมีวัตถุประสงค์คือ ตรวจสอบหาคุณสมบัติของจำนวนสุ่มแท้และจำนวนสุ่มเทียมก่อนนำไปประยุกต์ใช้งาน เพื่อให้สามารถทราบว่าจำนวนสุ่มดังกล่าวมีคุณสมบัติเพียงพอที่จะนำไปใช้งานหรือไม่ กระบวนสำคัญของการทดสอบคือ การคำนวณสถิติทดสอบ (Test Statistic) และการพิจารณาการผ่านการทดสอบ (Decision Making) เนื่องจากปัญหาของชุด ทดสอบอ้างอิงที่ใช้สถิติทดสอบและการพิจารณาการผ่านการทดสอบด้วยหลักการที่มีรูปสมการ ซับซ้อน รวมทั้งมีขั้นตอนของการทดสอบหลายขั้นตอน ส่งผลให้ใช้เวลาในการประมวลผลนาน ดังนั้นวิทยานิพนธ์นี้จึงนำเสนอการคำนวณสถิติทดสอบและการพิจารณาการผ่านการทดสอบที่มีความซับซ้อนต่ำเพื่อลดขั้นตอนและเวลาในการประมวลผล จำนวนสองวิธี คือ สถิติทดสอบที่เรียกว่า ค่ามาตรฐาน (Standard Score: Z) สำหรับชุดข้อมูลที่มีการแจกแจงปกติ (Normal Distribution) และสถิติทดสอบไคกำลังสอง (Chi Square : χ^2) สำหรับชุดข้อมูลที่มีการ แจกแจงไคกำลังสอง (Chi-square Distribution) นั้น หลักการที่นำเสนอเพื่อการหาสถิติทดสอบ ดังกล่าวได้รูปสมการที่มีความซับซ้อนต่ำ สามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและ ค่าทางสถิติได้โดยตรง ทำให้สามารถพิจารณาการผ่านการทดสอบโดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้ได้ การ ทดสอบคุณสมบัติของจำนวนสุ่มนี้ครอบคลุมห้าวิธีย่อย ได้แก่ การทดสอบความถี่แบบเดี่ยว เพื่อหาลักษณะการแจกแจงความน่าจะเป็นและรูปแบบการแจกแจง การทดสอบความต่อเนื่องของจำนวนสุ่ม เพื่อหาการซ้ำกันของข้อมูลและความต่อเนื่องของชุดข้อมูล การทดสอบเพื่อหาลักษณะคาบของชุดจำนวนสุ่ม การทดสอบความถี่ของชุดจำนวนสุ่ม เพื่อหาลักษณะการแจกแจงของชุดข้อมูล และการทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล โดยกระบวนการทดสอบทางสถิติทั้งหมดดังกล่าว มีขั้นตอนสำหรับทำการทดสอบทั้งหมดห้าขั้นตอนตามลำดับ ขั้นตอนแรกคือการตั้งสมมติฐาน ตามด้วยขั้นตอนการกำหนดระดับนัยสำคัญ ขั้นตอนการกำหนดค่าวิกฤตและบริเวณวิกฤต ขั้นตอนการเลือกสถิติทดสอบ และขั้นตอนสุดท้ายการสรุปผลการทดสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

จากหลักการที่นำเสนอ จะเห็นว่าการหาสถิติทดสอบดังกล่าวนี้อยู่ในรูปสมการที่มีความซับซ้อนต่ำ สามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและค่าทางสถิติได้โดยตรง ทำให้สามารถพิจารณาการผ่านการทดสอบโดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้ ซึ่งคาดว่าการใช้กระบวนการคำนวณดังที่นำเสนอจะส่งผลให้การทดสอบคุณสมบัติของจำนวนสุ่มมีระยะเวลาสั้นลง และเป็นแนวทางที่จะพัฒนาการทดสอบคุณสมบัติจำนวนสุ่มผ่านระบบออนไลน์ได้ โดยมีผลการทดสอบและผลการวิเคราะห์ผลการทดสอบเป็นไปตามบทที่ 6 ซึ่งสามารถสรุปผลการพัฒนาชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่ม เพื่อให้ผู้ใช้งานมีความมั่นใจในการใช้งานจำนวนสุ่มด้านการสื่อสารปลอดภัย รวมทั้งเป็นแนวทางพัฒนาการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์ (Web Service) ดังนี้

7.1 สรุปผลการวิจัย

จากผลการทดสอบทั้งห้าวิธีทดสอบที่นำเสนอในบทที่ 6 สามารถสรุปได้ดังตารางที่ 7.1-7.4 ดังนี้

ตารางที่ 7.1 ค่าความน่าจะเป็นเฉลี่ยของแต่ละวิธีการทดสอบ

วิธีการทดสอบ	ความน่าจะเป็น	
	Z score	*Erfc*
Frequency Test	0.0225	0.4977
Runs Test	0.0257	0.4979
Discrete Fourier Transform (Spectral) Test	0.1304	0.6146
วิธีการทดสอบ	ความน่าจะเป็น	
	Chi square	*Igamc*
Frequency Test within a Block	96.4112	0.5734
Test for the Longest Run of Ones in a Block	6.4698	0.4418

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

จากตารางที่ 7.1 ความน่าจะเป็นที่เกิดจากการคำนวณสถิติทดสอบเพื่อนำไปสู่การพิจารณาตัดสินใจการผ่านการทดสอบนั้น สำหรับการคำนวณด้วยหลักการที่นำเสนอ Z ค่า $\bar{Z}$ มีค่าเข้าใกล้ศูนย์ และการคำนวณด้วยหลักการที่อ้างอิง χ^2 ค่า มี $\bar{\chi}^2$ ค่าเข้าใกล้ระดับความเสรี คือที่ 0.05 ซึ่งเป็นการยืนยันการทดสอบตามวิธีการทดสอบดังนี้

วิธีที่ 1 การทดสอบเชิงความถี่แบบเดี่ยว (Frequency (Monobit) Test)

สำหรับชุดจำนวนสุ่มที่ผ่านการทดสอบ แสดงว่าจำนวนบิตศูนย์และจำนวนบิตหนึ่งมีจำนวนใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

วิธีที่ 2 การทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test)

สำหรับชุดจำนวนสุ่มที่ผ่านการทดสอบ แสดงว่าจำนวนการรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความถี่การเกิดรันไม่สูงหรือต่ำ เฉลี่ยตรงกลาง ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

วิธีที่ 3 การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform (Spectral) Test)

สำหรับชุดจำนวนสุ่มที่ผ่านการทดสอบ แสดงว่าชุดจำนวนสุ่มมีจำนวนพีคที่มีค่าต่ำกว่าค่า T และสูงเกินค่า T แตกต่างเกินกันไม่เกินร้อยละ 5 ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

วิธีที่ 4 การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block)

สำหรับชุดจำนวนสุ่มที่ผ่านการทดสอบ แสดงว่าจำนวนบิตศูนย์และจำนวนบิตหนึ่งในแต่ละชุดจำนวนสุ่มมีจำนวนใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

วิธีที่ 5 การทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)

สำหรับชุดจำนวนสุ่มที่ผ่านการทดสอบ จำนวนการรันของบิตศูนย์และบิตหนึ่งมีค่าใกล้เคียงกันและความยาวของการเกิดรันของทั้งบิตศูนย์และบิตหนึ่งใกล้เคียงกัน ซึ่งเป็นไปตามทฤษฎีของการสุ่ม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ตารางที่ 7.2 ค่าเบี่ยงเบนเฉลี่ยของแต่ละวิธีการทดสอบในอัตราส่วนเดียวกัน

วิธีการทดสอบ	ค่าเบี่ยงเบนเฉลี่ยในอัตราส่วนเดียวกัน	
	Z score	*Erfc*
Frequency Test	0.0038	0.0023
Runs Test	0.0043	0.0021
Discrete Fourier Transform (Spectral) Test	0.0217	0.1146
วิธีการทดสอบ	ค่าเบี่ยงเบนเฉลี่ยในอัตราส่วนเดียวกัน	
	Chi square	*Igamc*
Frequency Test within a Block	0.0359	0.0734
Test for the Longest Run of Ones in a Block	0.0757	0.0582

จากการทดสอบชุดการทดสอบคุณสมบัติของจำนวนสุ่มทั้งห้าวิธี สามารถสรุปค่าความเบี่ยงเบนเฉลี่ยจากค่าทฤษฎีในอัตราส่วนเดียวกันได้ดังตารางที่ 7.2 ซึ่งจะเห็นได้ว่าจากการคำนวณด้วยหลักการที่นำเสนอ มีค่าความเบี่ยงเบนเฉลี่ยน้อยกว่าค่าจากการคำนวณด้วยหลักการอ้างอิง จำนวน 2 วิธีทดสอบ ได้แก่ วิธีที่ 3 และวิธีที่ 4 และมีค่าความเบี่ยงเบนเฉลี่ยมากกว่าค่าที่ได้จากการคำนวณด้วยหลักการอ้างอิง จำนวน 3 วิธีทดสอบ ได้แก่ วิธีที่ 1 วิธีที่ 2 และวิธีที่ 5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ตารางที่ 7.3 สัดส่วนการผ่านการทดสอบของแต่ละวิธี

วิธีการทดสอบ	ระดับนัยสำคัญ	หลักการที่นำเสนอ	หลักการที่อ้างอิง	ร้อยละความแตกต่าง
Frequency Test	0.05	92	92	0
	0.01	97	97	0
Runs Test	0.05	92	92	0
	0.01	97	97	0
Discrete Fourier Transform (Spectral) Test	0.05	99	99	0
	0.01	100	100	0
Frequency Test within a Block	0.05	96	96	0
	0.01	99	99	0
Test for the Longest Run of Ones in a Block	0.05	94	94	0
	0.01	97	97	0

จากตารางที่ 7.3 สัดส่วนการผ่านการทดสอบจากหลักการที่นำเสนอและหลักการอ้างอิงในทุกวิธีทดสอบพบว่ามีร้อยละความแตกต่างเท่ากับศูนย์หรือไม่มีความแตกต่างกัน

จากหลักการที่นำเสนอในวิทยานิพนธ์นี้ ได้ทำการประมวลผลและเก็บสถิติของเวลาที่ใช้ในการประมวลผลทั้งหมดของการทดสอบของแต่ละหลักการ และคำนวณร้อยละความแตกต่าง ซึ่งมีผลการทดสอบแสดงดังตารางที่ 7.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ตารางที่ 7.4 เวลาเฉลี่ยในการประมวลผลการทดสอบของแต่ละวิธีการทดสอบ

วิธีการทดสอบ	เวลา (วินาที)		เวลาที่ต่างกัน (%)
	Z score	*Erfc*	
Frequency Test	8.8126	9.0748	2.9317
Runs Test	8.2765	8.9882	8.2446
Discrete Fourier Transform (Spectral) Test	46.8519	49.8649	6.2036
วิธีการทดสอบ	เวลา (วินาที)		เวลาที่ต่างกัน (%)
	Chi square	*Igamc*	
Frequency Test within a Block	11.2903	11.9060	5.3086
Test for the Longest Run of Ones in a Block	74.0727	79.0953	6.5583

จากตารางที่ 7.4 เวลาเฉลี่ยในการประมวลผลการทดสอบของแต่ละวิธี เปรียบเทียบการประมวลผลการทดสอบด้วยหลักการที่นำเสนอและหลักการอ้างอิง พบว่าทุกวิธีทดสอบการประมวลผลการทดสอบด้วยหลักการที่นำเสนอใช้เวลาน้อยกว่าการประมวลผลการทดสอบด้วยหลักการอ้างอิง โดยเวลาที่ใช้ในการประมวลผลทั้งหมดเฉลี่ยลดลงร้อยละ 5.85

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

จากผลการทดสอบทั้งห้าวิธีทดสอบที่นำเสนอในวิทยานิพนธ์นี้ สามารถสรุปได้ดังนี้

หนึ่ง สัดส่วนการผ่านการทดสอบจากหลักการที่นำเสนอและหลักการอ้างอิงในทุกวิธีทดสอบไม่มีความแตกต่างกัน ในแง่ของการพิจารณาการทดสอบ ซึ่งจะเห็นได้จาก ตำแหน่งชุดทดสอบที่ผ่านและไม่ผ่านการทดสอบนั้นคือตำแหน่งชุดจำนวนสุ่มชุดเดียวกัน ดังนั้นสรุปได้ว่าสามารถทดสอบคุณสมบัติของจำนวนสุ่มด้วยหลักการคำนวณสถิติทดสอบและการพิจารณาตัดสินการผ่านการทดสอบที่นำเสนอได้เทียบเท่ากับหลักการที่อ้างอิง หรือไม่มีความแตกต่างกัน

สอง ความน่าจะเป็นที่คำนวณได้จากสถิติทดสอบที่นำเสนอ เมื่อเปรียบเทียบกับหลักการอ้างอิง ความน่าจะเป็นเฉลี่ยมีค่าเข้าใกล้ค่าเฉลี่ยตามทฤษฎี โดยมีความเบี่ยงเบนจากค่าทฤษฎีไม่เกินร้อยละหนึ่ง ดังนั้นสรุปได้ว่าจำนวนสุ่มที่ผ่านการทดสอบนั้น คุณสมบัติของจำนวนสุ่มเป็นไปตามทฤษฎีของการสุ่ม

สาม เวลาในการประมวลผลในการทดสอบคุณสมบัติของจำนวนสุ่ม จากหลักที่นำเสนอใช้เวลาในการประมวลผลในการทดสอบน้อยกว่าหลักการที่อ้างอิง ดังนั้นสรุปได้ว่าหลักการที่นำเสนอมีความซับซ้อนและขั้นตอนในการประมวลผลการทดสอบน้อยกว่าหลักการอ้างอิง และหลักการนี้สามารถนำไปพัฒนาชุดวิธีทดสอบผ่านระบบออนไลน์ที่ต้องมีการแสดงผลในเวลาอันสั้นได้

สี่ การทดสอบคุณสมบัติของจำนวนสุ่มที่มาจากแหล่งอ้างอิงที่แตกต่างกัน โดยจำนวนสุ่มที่ได้จากแหล่งกำเนิดควอนตัมผ่านการทดสอบมากกว่าแหล่งกำเนิดอัลกอริทึม แสดงว่าชุดวิธีทดสอบที่นำเสนอนี้สามารถวัดคุณสมบัติของจำนวนสุ่มที่มาจากแหล่งกำเนิดที่แตกต่างกัน ดังนั้นสรุปได้ว่าชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่มที่นำเสนอสามารถนำไปใช้ในการตรวจสอบคุณภาพของจำนวนสุ่มก่อนการนำไปใช้งานด้านวิทยาการรหัสลับได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

7.2 ปัญหาและอุปสรรคที่พบในงานวิจัย

การทดสอบคุณสมบัติของจำนวนสุ่มเพื่อนำไปประยุกต์ใช้งานงานด้านวิทยาการรหัสลับตามหลักการอ้างอิง ซึ่งมีเงื่อนไขในการทดสอบตามทฤษฎีจำนวนสุ่มอย่างเข้มงวด เพื่อให้สามารถแยกความแตกต่างระหว่างแหล่งกำเนิดจำนวนสุ่มแท้และแหล่งกำเนิดจำนวนสุ่มเทียมได้อย่างชัดเจน จากการศึกษาและสำรวจพบว่ามีวิธีการทดสอบที่ซ้ำซ้อน ดังนั้น จึงพัฒนาชุดการทดสอบให้ยังคงมีความสามารถในการแยกความแตกต่างระหว่างแหล่งกำเนิดจำนวนสุ่มแท้และแหล่งกำเนิดจำนวนสุ่มเทียม โดยนำเสนอหลักการที่สามารถลดความซับซ้อนและขั้นตอนในการทดสอบ รวมทั้งเน้นเฉพาะลักษณะเด่นของการทดสอบแต่ละคุณสมบัติเท่านั้น เพื่อให้เวลาในการประมวลผลลดลงและเพื่อให้สามารถนำไปให้บริการผ่านระบบออนไลน์ (Web Service) ที่ต้องให้มีความเร็วในการประมวลผลให้อยู่ในระดับที่ผู้ใช้งานสามารถรอผลการทดสอบผ่านหน้าจอได้ ซึ่งการทดสอบด้วยวิธีการอื่นก็สามารถทดสอบคุณสมบัติของจำนวนสุ่มได้เช่นกัน แต่จะใช้เวลาในการประมวลผลมากกว่า ดังนั้นวิธีการทดสอบคุณสมบัติที่นำเสนอจึงมีความต้องการการพัฒนาต่อไปเพื่อให้สามารถทดสอบคุณสมบัติของจำนวนสุ่มให้เข้มงวดมากขึ้น และมีความรวดเร็วในการประมวลผลมากกว่าเดิม

การทดสอบการทำงานของชุดวิธีทดสอบ เป็นการทดสอบและเก็บสถิติเกี่ยวกับเวลาของการประมวลผลบนเครื่องคอมพิวเตอร์ส่วนบุคคล และได้ทดลองนำชุดวิธีการทดสอบดังกล่าวนี้ให้บริการผ่านระบบออนไลน์ ซึ่งในระยะเริ่มต้นได้ทำการเก็บสถิติเวลาของการประมวลผลบนเครื่องคอมพิวเตอร์ที่มีระยะใกล้กับเครื่องแม่ข่าย พบว่าชุดทดสอบสามารถทำงานได้อย่างปกติและใช้เวลาเพิ่มจากการประมวลผลบนเครื่องคอมพิวเตอร์ โดยการทดสอบประสิทธิภาพของชุดวิธีการทดสอบนี้ยังไม่ได้ทำการเก็บสถิติด้านเวลาเมื่อทำการประมวลผลการทดสอบผ่านเครื่องลูกข่ายในสถานที่ที่มีระยะทางต่างกันออกไป ซึ่งอาจมีปัจจัยอื่นที่จะส่งผลให้เวลาที่ใช้ในการประมวลผลการทดสอบบนลูกข่ายอีกหลายประการ เช่นความเร็วในการประมวลผลของเครื่องลูกข่าย ความเร็วในการรับส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต และระยะทาง เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

7.3 ข้อเสนอแนะในการพัฒนา

จากปัญหาข้างต้น ดังนั้นจึงมีข้อเสนอแนะให้มีการพัฒนาชุดวิธีทดสอบที่มีประสิทธิภาพดีขึ้น สามารถทดสอบคุณสมบัติของจำนวนสุ่มที่เข้มงวดกว่าเดิม โดยการหาแนวทางแก้ไขความซับซ้อนด้านอื่นที่แตกต่างออกไป เพื่อให้สามารถให้บริการผ่านระบบออนไลน์ได้โดยใช้เวลาในการประมวลผลน้อยลงกว่าเดิม รวมทั้งหาแนวทางแก้ไขปัญหาที่อาจจะมีผลต่อการประมวลผลในการทดสอบนั้น อาจมีการเก็บสถิติเรื่องเวลาในการประมวลผลการทดสอบบนเครื่องลูกข่ายในสถานที่แตกต่างกันออกไปและวิเคราะห์ปัจจัยอื่นๆ เช่น ความเร็วในการประมวลผลของเครื่องลูกข่าย ความเร็วในการรับส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต และระยะทาง เป็นต้น ซึ่งจะส่งผลต่อเวลาที่ใช้ในการประมวลผลการทดสอบ รวมไปถึงการรับความคิดเห็นจากผู้ใช้งานอื่น เพื่อนำคำแนะนำ หรือความคิดเห็นที่แตกต่าง มาปรับปรุงและพัฒนาชุดวิธีทดสอบให้มีประสิทธิภาพดีขึ้นต่อไป

King Mongkut's Institute of Technology Ladkrabang

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

เอกสารอ้างอิง

[1] Charmaine Kenny and Krzysztof Mosurski, **Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators**, The Distributed systems group, Computer Science Department, Trinity College Dublin, April 2005.

[2] Andrew Rukhin, Juan Soto, **A Statistical Test Suite for Random and Pseudorandom Generator for Cryptographic Applications,** NIST Special Publication 800-22, USA, May 15, 2001.

[3] A. Menezes, et al., **Handbook of Applied Cryptography,** CRC Press, Inc., 1997.

[4] Athanasios Papoulis , **Probability, Random Variables and Stochastic Processes Third Edition.** McGrow-hill Book Company, 1991.

[5] QRNG , iD Quantique , Available URL: http://www.idquantique.com/map/map.htm

[6] NIST ,FIPS 140-1, **Security Requirements for Cryptographic Modules Federal Information Processing Standards Publication 140-1,** U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, VA, 1994.

[7] Alberto Leon-Garcia, **Probability and Random Processes for Electrical Engineering** ,Second Edition, 1994.

[8] G. Marsaglia, **DIEHARD Statistical Tests,** Available URL: http://stat.fsu.edu/~geo/diehard.html.

[9] **Random,** Available URL: http://www.random.org .

[10] Donald G. Childers, **Probability and Random Processes Using MATLAB,** Irwin/McGraw-Hill, 1997.

[11] Donald Knuth, **The Art of Computer Programming**,Massachusetts, Grove Press,Inc.,1998.

[12] Milton Abramowitz and Irene Stegun, **Handbook of Mathematical Functions with Formulas Graphs and Mathematical Tables,** National Bureau of Standards. U.S.,1970.

[13] John G. Proakis, **Digital Communications Third Ddition,** McGRAW-Hill International Editions, 1995.

[14] Albert H. Gowker and Gerald J. Lieberman, **Engineering Statistics** Second edition, Prentic Hall, INC, Englewood Cliffs, New Jersey, U.S.A, 1972.

[15] Duglas C. Montgomery and George C. Runger, **Applied Statistics and Probability for**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

Engineers Fourth edition, Wiley Asia Student Edition , 2007.

[16] Kai Lai Chung, **Elementary Probability Theory with Stochastic Processes,** New York: Springer-Verlag, 1979 (especially pp. 210-217).

[17] Jim Pitman, **Probability,** New York: Springer-Verlag, 1993 (especially pp. 93-108).

[18] Jean D. Gibbons, **Nonparametric Statistical Inference,** Second ed. New York: Marcel Dekker, 1985 (especially pp. 50-58).

[19] Anant P. Godbole and Stavros G. Papastavridis, (ed), **Runs and patterns in probability: Selected papers,** Dordrecht: Kluwer Academic, 1994.

[20] R. N. Bracewell, **The Fourier Transform and Its Applications,** New York: McGraw-Hill, 1986.

[21] Nick Maclaren, **Cryptographic Pseudo-random Numbers in Simulation**, Cambridge Security Workshop on Fast Software Encryption, Dec. 1993, pp. 185-190.

[22] F. N. David and D. E. Barton, **Combinatorial Chance,** New York: Hafner Publishing Co., 1962, p. 230.

[23] Anant P. Godbole and Stavros G. Papastavridis (ed), **Runs and Patterns in Probability: Selected Papers,** Dordrecht, Kluwer Academic, 1994.

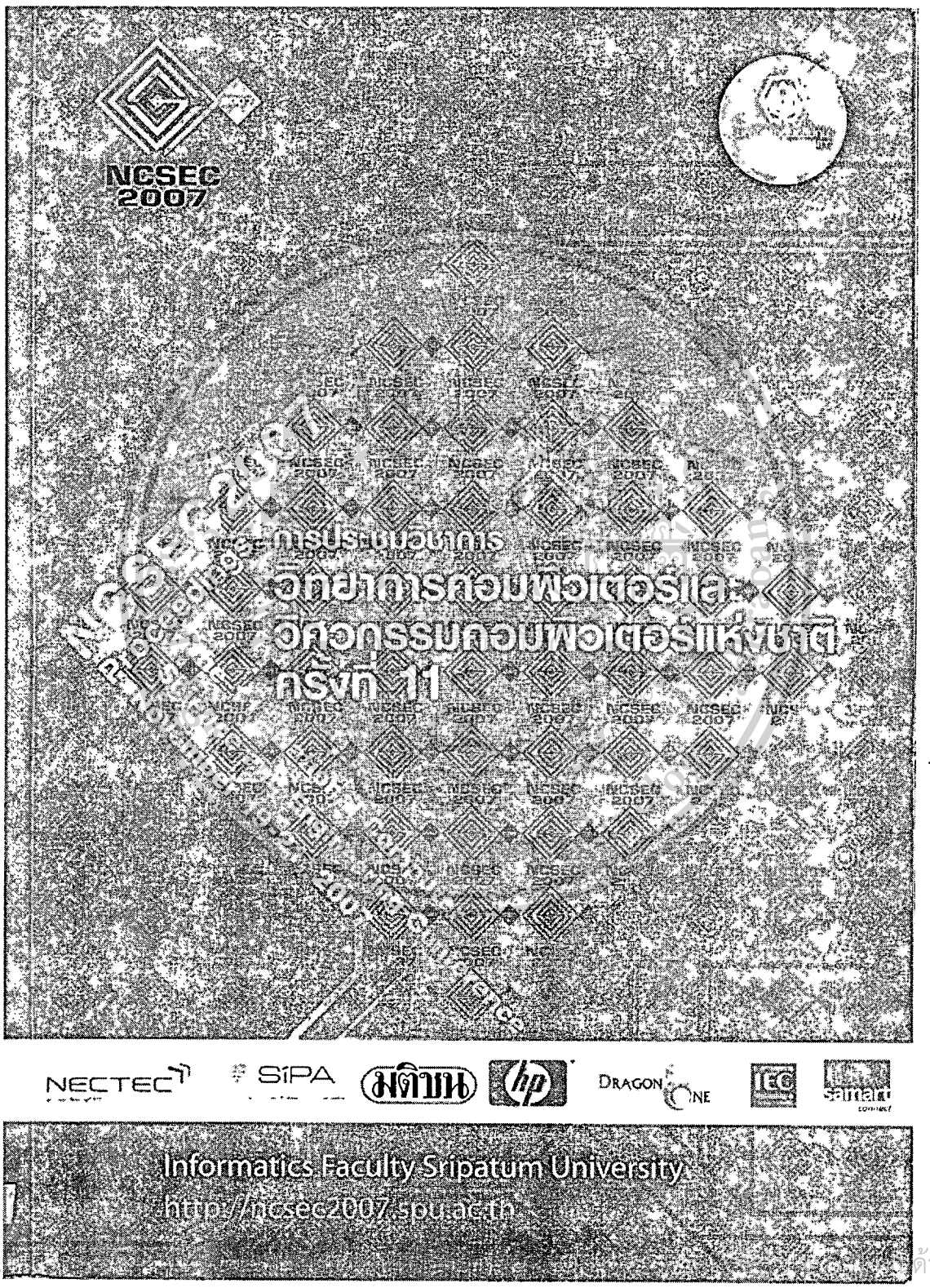
[24] A Wald, J Wolfowitz, **On a Test Whether Two Samples are From the Same Population,** vol. 11, The Annals of Mathematical Statistics, 1940.

[25] Pal Revesz, **Random Walk in Random and Non-Random Environments, Singapore:** World Scientific, 1990.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ภาคผนวก ก

Proceeding งานประชุมวิชาการ NCSEC 2007



เอกสารนี้ ... ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

การลดความซับซ้อนของการทดสอบค่ามาตรฐานวิธีข้อสมมติฐานว่างสำหรับการวัดผลการกำเนิดจำนวนสุ่ม

Simplification on Decision of a Null Hypothesis for Random Generating Test

เครือวัลย์ วงค์ปัญญา[1] เกียรติศักดิ์ ศรีพิมานวัฒน์[2] กนก เจนจิระพงศ์เวช[1]

[1]ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ถ. ฉลองกรุง เขตลาดกระบัง กรุงเทพมหานคร 10520 E-mail: s8061005@kmitl.ac.th kjkanok@kmitl.ac.th

[2]ห้องปฏิบัติการวิจัยการสื่อสารเชิงแสงและควอนตัม (OQC) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช) E-mail: keattisak.sripimanwat@nectec.or.th

บทคัดย่อ

บทความนี้ นำเสนอการลดความซับซ้อนของการทดสอบสมมติฐานเชิงสถิติ (Tests of Statistical Hypotheses) ซึ่งอ้างอิงชุดการทดสอบ NIST Statistical Test Suite ที่มุ่งเน้นทดสอบจำนวนสุ่มเพื่อนำไปใช้ประยุกต์ในงานด้านวิทยาการรหัสลับสำหรับการสื่อสาร โดยใช้ค่ามาตรฐาน (Standard Score: Z) เป็นตัวสถิติเพื่อพิจารณาขอมรับและปฏิเสธข้อสมมติฐานว่าง (Null hypotheses) และนำไปสู่การพิจารณาว่าจำนวนสุ่มที่นำมาทดสอบนั้นเป็นจำนวนสุ่มที่เพียงพอต่อการนำไปประยุกต์ใช้งานด้านการสื่อสารหรือไม่ โดยเปรียบเทียบค่าที่ได้จากการคำนวณทางสถิติที่อ้างอิงชุดการทดสอบ NIST Statistical Test Suite ที่ใช้ส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน (Complementary Error Function: $Erfc$) ที่ระดับนัยสำคัญ (α) 0.01 และ 0.05 ตามลำดับ โดยเปรียบเทียบจากอัตราส่วนการผ่านการทดสอบของสัดส่วนประชากรของค่าสถิติทั้งสองชุดวิธีทดสอบจำนวน 100 ครั้ง จากผลการทดสอบและผลการเปรียบเทียบนั้น การตัดสินใจในการพิจารณาขอมรับและปฏิเสธข้อสมมติฐานว่าง (H_0) อยู่ระดับค่าที่ยอมรับได้ที่ความเชื่อมั่นเท่ากับร้อยละ 99 และ 95 ดังนั้น จึงสามารถนำค่ามาตรฐาน (Z) เป็นตัวสถิติสำหรับการทดสอบสมมติฐาน ที่มีชุดจำนวนสุ่มแจกแจงแบบปกติสำหรับการวัดผลการกำเนิดของจำนวนสุ่ม เพื่อพิจารณาว่าจำนวนสุ่มที่ได้มีความเป็นจำนวนสุ่มอย่างพอเพียงที่จะนำไปประยุกต์ใช้งานวิทยาการรหัสลับในการสื่อสารได้ในอนาคต

คำสำคัญ : การคำนวนเชิงสถิติ จำนวนสุ่มสำหรับรหัสลับ

Abstract

This paper presents the simplification on random testing based on NIST Statistical Test Suite, being designed for cryptographic applications which the highest stringent requirements (cryptography) than other applications. This is a test of statistical hypothesis with Standard Score (Z) for making decision of the null hypothesis via the Frequency test at normal probability distribution. Some unbiased mechanical tests applied to decide if a number is the sufficient randomness. These standard scores (Z) are compared to the complementary error function ($Erfc$) according to significance level (α) at 0.01 and 0.05. Meanwhile, the results are tested via the estimation of population proportion with confidences of 99% and 95% respective. As a result; It is able to use for the random generating test that it will be applied for secure communication system.

Keywords: Complementary Error function, Random Generator, Cryptography

1. พื้นฐานการทดสอบจำนวนสุ่ม

หัวใจประการหนึ่งของการติดต่อสื่อสารและข้อมูล คือ ความปลอดภัยจากการโจรกรรม ดังนั้น การติดต่อสื่อสารและข้อมูลที่สำคัญจึงใช้รหัสลับเพื่อรักษาความลับดังกล่าว ซึ่งความปลอดภัยของข้อมูลจากผู้บุกรุก (Eavesdropper) ขึ้นอยู่กับความปลอดภัยของกุญแจที่สร้างขึ้น วิทยาการรหัสลับที่ต้องมีผู้ส่ง (Sender) ทำการเข้ารหัส (Encryption) ต้องนำส่งกุญแจรหัส (Keys) นั้นไปยังผู้รับ (Receiver) ได้รับการพัฒนามากขึ้นตามลำดับ โดยที่การสร้างรหัสลับมีพื้นฐานที่สำคัญที่ต้องปรับเปลี่ยนหรือสุ่ม (Random) ให้มีความหลากหลายและเป็นจำนวนสุ่มที่มีคุณภาพ

จำนวนสุ่มอย่างแท้จริง ต้องเป็นจำนวนที่ไม่สามารถคาดเดาล่วงหน้าได้ โดยมีโอกาสความน่าจะเป็นของการเกิดผลลัพธ์เท่าๆกัน ไม่มีความสัมพันธ์กัน ซึ่งจำนวนสุ่มที่ใช้เป็นกุญแจไขรหัสลับโดยทั่วไปไม่ได้รับการรับรองว่าเป็นจำนวนสุ่มอย่างแท้จริง เพียงแต่ได้รับการคาดคะเนว่าเป็นไปได้เท่านั้น เพราะว่าจำนวนสุ่มอาจมีจุดสิ้นสุดและอาจมีการกระจายตัวที่ไม่มากเพียงพอ

การนำจำนวนสุ่มไปประยุกต์ใช้งานมีความสำคัญมาก เช่น งานที่เกี่ยวข้องกับความมั่นคง การเงินการธนาคาร เมื่อเกิดการโจรกรรมข้อมูลขึ้นจะมีความเสี่ยงต่อการถูกไขรหัสลับได้สูง และความปลอดภัยในการติดต่อสื่อสารและข้อมูลจะลดน้อยลงตามไปด้วย เนื่องจากไม่สามารถตรวจวัดจำนวนสุ่มที่จะนำมาใช้เป็นกุญแจรหัสลับเพื่อเก็บข้อมูลที่สำคัญ ได้ด้วยการมองด้วยตาเปล่า ดังนั้นจึงจำเป็นต้องใช้กระบวนการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

หรือเครื่องมือมาช่วยตัดสินใจ เพื่อพิสูจน์ให้ได้ว่าจำนวนสุ่มนั้นเป็น "จำนวนสุ่มอย่างเพียงพอ (Sufficiently Random)" จากการที่ไม่มีหน่วยวัดคุณสมบัติของจำนวนสุ่มเหล่านี้ว่าเป็นจำนวนสุ่มที่มีความสมบูรณ์หรือไม่อย่างไร ดังนั้นจึงนำหลักการและกระบวนการทดสอบทางสถิติมาใช้ทดสอบคุณสมบัติของจำนวนสุ่มเพื่อวัตถุประสงค์ดังกล่าว ซึ่งจะสามารถวัดค่าและบ่งบอกออกมาในรูปแบบของปริมาณได้ ทั้งนี้เพื่อเพิ่มความมั่นใจในขอบเขตที่ยอมรับได้

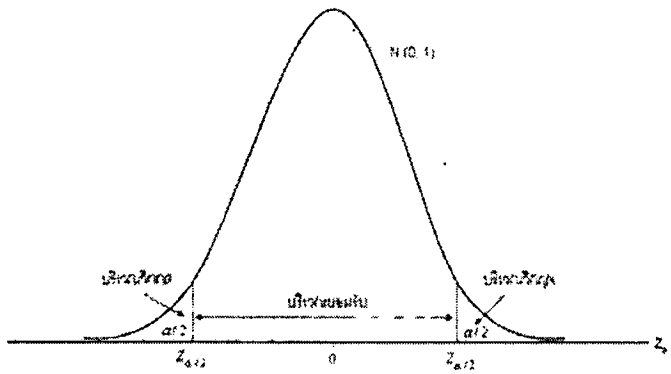
จากการสำรวจพบว่าการทดสอบด้วยวิธีทางสถิติมีอยู่หลายวิธีดังนี้ เช่น DIEHARD Test และ NIST's Statistical Test [1] ซึ่งแต่ละชุดการทดสอบมีวัตถุประสงค์มุ่งเน้นการทดสอบให้สอดคล้องกับแต่ละประเภทของการประยุกต์ใช้งาน โดยที่ DIEHARD Test มุ่งเน้นทดสอบสำหรับจำนวนสุ่มที่จะใช้ในการจำลองการทำงาน (Simulation)และชุดการทดสอบ NIST's Statistical Test Suite ที่เป็นมาตรฐานการทดสอบจะมุ่งเน้นทดสอบจำนวนสุ่มเพื่อนำไปใช้ในงานด้านวิทยาการรหัสลับสำหรับการสื่อสาร และใช้ในเชิงอุตสาหกรรมที่ครอบคลุมการทดสอบคุณสมบัติของจำนวนสุ่มมากที่สุดและมีเงื่อนไขการทดสอบที่เข้มงวดมากที่สุดเป็นต้น [1] ซึ่งแต่ละชุดการทดสอบได้นำหลักการทดสอบสมมติฐานเชิงสถิติมาใช้เพื่อหากระบวนการในการตัดสินใจโดยสถิติที่ใช้ คือ ส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* และ Incomplete Gamma Function *(Igmc)* [2] สำหรับจำนวนสุ่มที่มีการแจกแจงแบบปกติ (Normal probability distribution) และแบบไคกำลังสอง (Chi-square probability distribution) ตามลำดับ

บทความนี้นำเสนอการทดสอบชุดจำนวนสุ่มที่มีการแจกแจงแบบปกติ เมื่อต้องทำการทดสอบชุดจำนวนสุ่มที่มีจำนวนมาก การคำนวณหาค่าส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* จะมีความซับซ้อนและใช้เวลาในการคำนวณมาก เนื่องจากรูปแบบการตัดสินใจในการยอมรับและปฏิเสธมีรูปสมการที่ซับซ้อน ดังนั้น จึงนำเสนอตัวสถิติที่ใช้ในการทดสอบคือ ค่ามาตรฐาน *(Z)* สำหรับการการแจกแจงแบบปกติ ซึ่งมีความซับซ้อนต่ำ และใช้เวลาในการคำนวนน้อยลง

2. การทดสอบความเป็นจำนวนสุ่มด้วยวิธีทางสถิติ

การทดสอบด้วยวิธีทางสถิตินี้แบ่งเป็นสี่ ประเภทได้แก่การทดสอบทั่วไป (General Test) การทดสอบเชิงทดลอง (Empirical Test) การทดสอบเชิงทฤษฎี (Theoretical Test) และการทดสอบเชิงสเปคตรัม (The Spectral Test) [3]

บทความนี้จะทำการทดสอบการทดสอบทั่วไป (General Test) โดยอ้างอิงกับชุดทดสอบ NIST's Statistical Test Suite โดยทำการทดสอบเชิงความถี่ (Frequency Test) [2] เพื่อหาความสัมพันธ์ของบิตศูนย์และบิตหนึ่งทั้งหมดในลำดับ เพื่อทำการตรวจสอบว่า จำนวนบิตศูนย์ และจำนวนบิตหนึ่งมีสัดส่วนอย่างละครึ่ง เป็นคุณสมบัติสำคัญเป็นอับดับแรกของจำนวนสุ่ม ที่เกี่ยวข้องกับโอกาสในการกำเนิด และใช้



รูปที่ 1 *ขอบเขตวิกฤต และขอบเขตยอมรับ*

กระบวนการตัดสินใจว่าสัดส่วนที่ได้จากการทดสอบเป็นไปตามคุณสมบัติของจำนวนสุ่มหรือไม่ด้วยการทดสอบสมมติฐานเชิงสถิติ

2.1 การทดสอบสมมติฐานเชิงสถิติ

การทดสอบสมมติฐานเชิงสถิติ คือการอนุมานเชิงสถิติวิธีหนึ่งเพื่อแก้ปัญหาที่ต้องการตัดสินใจ โดยใช้กระบวนการตัดสินใจว่าจะยอมรับหรือปฏิเสธข้อสมมติฐานที่ได้ตั้งไว้ ทั้งนี้โดยเลือกสถิติเพื่อใช้ในการคำนวนหาค่าเพื่อให้สามารถสรุปว่าสมมติฐานนั้นเป็นจริงหรือจะยอมรับสมมติฐานนั้น เนื่องจากไม่มีหลักฐานเพียงพอที่จะปฏิเสธ [4] โดยข้อสมมติฐานที่ตั้งขึ้นนั้นเขียนอยู่ในรูปแบบสัญลักษณ์ทางคณิตศาสตร์ ซึ่งมีการตั้งสมมติฐานได้สองแบบ ได้แก่สมมติฐานว่าง (Null Hypothesis) แทนด้วย H_0 และสมมติฐานแย้ง (Alternative Hypothesis) แทนด้วย H_1

การกำหนดขอบเขตวิกฤต (Critical Region) ซึ่งเป็นขอบเขตในการปฏิเสธหรือยอมรับสมมติฐานว่าง H_0 ซึ่งอยู่ส่วนปลายภายใต้เส้นโค้งของการแจกแจงความน่าจะเป็นดังรูปที่ 1 มีสองประเภท ได้แก่การทดสอบแบบสองด้าน เขียนแทนด้วยสมการ $-2.58 < Z\text{-}Score < 2.58$ และการทดสอบแบบด้านใดด้านหนึ่งเขียนแทนด้วยสมการ $P\text{-}value > 0.01$ เป็นต้น ค่าวิกฤต (Critical Point) จะแบ่งเขตระหว่างขอบเขตการยอมรับและปฏิเสธสมมติฐานว่าง H_0 ซึ่งแบ่งพื้นที่ได้กราฟออกเป็นหนึ่งร้อยส่วนกำหนดขอบเขตที่ยอมรับและขอบเขตที่ปฏิเสธตามค่าวิกฤตที่กำหนดตามระดับนัยสำคัญ ดังนั้นถ้าค่าสถิติที่คำนวณได้จากข้อมูลตัวอย่างตกอยู่ในขอบเขตวิกฤต จะมีผลทำให้ปฏิเสธสมมติฐานว่าง H_0 นั่นหมายถึงการยอมรับสมมติฐานแย้ง H_1 [4] ระดับนัยสำคัญจะถูกกำหนดค่าไว้ล่วงหน้าก่อนการทำการทดสอบสมมติฐานทางสถิติ ค่าที่นิยมใช้คือ 0.10 และ 0.05 เมื่อมีการทดสอบแบบสองด้านค่า α จะถูกแบ่งครึ่ง โดยค่า α จะบ่งบอกถึงระดับความเชื่อมั่น (Confident Level) ในการยอมรับ H_0 เมื่อ H_0นั้นเป็นจริง แสดงอยู่ในรูปของร้อยละ $(1-\alpha)$ 100 % เช่น ระดับนัยสำคัญ 0.10 หมายถึงระดับความน่าเชื่อมั่นร้อยละ 90

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ชุดจำนวนสุ่มที่นำมาทดสอบโดยทั่วไปจะมีการแจกแจงสองประเภท การแจกแจงความน่าจะเป็นแบบปกติ (Normal probability distribution) การแจกแจงความน่าจะเป็นแบบไคกำลังสอง (Chi-square probability distribution) (Exponential probability distribution) ซึ่งคำนวนสถิติโดยใช้ค่าฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* และ Incomplete Gamma Function *(Igamc)* ตามลำดับ

2.2 สถิติที่ใช้ในการทดสอบ

การทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีการทดสอบสมมติฐานเชิงสถิติ ส่วนที่สำคัญของการทดสอบ นั่นคือการเลือกตัวสถิติที่สอดคล้องกับลักษณะการแจกแจงของชุดข้อมูล เพื่อคำนวนและสรุปผลเพื่อตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้

บทความนี้จะนำเสนอชุดข้อมูลจำนวนสุ่ม (x) ที่มีการแจกแจงแบบปกติ มีลักษณะเป็นเส้นโค้งที่มีความสมมาตรรูปทรงระฆังคว่ำ (Bell Shape) ดังรูปที่ 1 รอบค่ากลางค่าหนึ่ง ซึ่งมีพารามิเตอร์สองตัว คือ ค่าเฉลี่ย (μ) และ ความแปรปรวน (σ^2) และมีฟังก์ชันความหนาแน่น ดังสมการที่ 1

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x_i-\mu)^2}{2\sigma^2}} \quad (1)$$

และชุดทดสอบ NIST Test suite เลือกใช้ตัวสถิติในการคำนวนเป็นส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* [2] และวิธีการทดสอบ DIEHARD เลือกใช้ตัวสถิติเช่นเดียวกันกับชุดทดสอบ NIST Test suite ซึ่งส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* มีความสัมพันธ์กับฟังก์ชันค่าคลาดเคลื่อน (Error function: *Erf*) ดังสมการที่ 2 เพื่อใช้เปรียบเทียบหาความสัมพันธ์ระหว่างส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน *(Erfc)* และค่ามาตรฐาน *(Z)* ที่จะได้ทำการนำเสนอในส่วนต่อไป

$$1 - Erf(z) = Erfc(z) = \frac{2}{\pi}\int_z^{\infty} e^{-u^2} du \quad (2)$$

การหาขอบเขตวิกฤตของชุดการทดสอบ NIST Test suite อ้างอิงจากพื้นที่ใต้กราฟของการแจกแจงแบบปกติ ซึ่งทำได้โดยการหาฟังก์ชันการแจกแจงปกติสะสม (Cumulative Distribution Function: *CDF*) $(\phi(z))$ ดังสมการที่ 3

$$\phi(z) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(x_i-\mu)^2}{2\sigma^2}} \quad (3)$$

ซึ่ง *Erf* มีความสัมพันธ์กับ *CDF* $(\phi(z))$ ดังสมการที่4 [5]

$$\phi(x) = \frac{1}{2}[1 + Erf(\frac{x}{\sqrt{2}})] \quad (4)$$

เนื่องจากการหาปริพันธ์ (Integration) ของ *CDF* และ *Erfc* มีความซับซ้อนในการคำนวน ซึ่งการหา *CDF* สามารถแปลงรูปให้อยู่ในรูปที่ลดความซับซ้อนเรียกว่าค่ามาตรฐาน (standard score) ดังสมการที่ 5

$$z = \frac{x_i - \mu}{\sigma} \quad (5)$$

ซึ่งค่า Z จะมีค่าอยู่ในช่วง $-4 \le z \le 4$ สามารถแปลงให้อยู่ในรูปของเปอร์เซนต์ไทล์ (Percentiles) คือแบ่งพื้นที่ใต้กราฟออกเป็นหนึ่งร้อยส่วน ซึ่งสะดวกและเข้าใจได้ง่ายต่อการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐาน และในการพิจารณาความแตกต่างของการใช้ตัวสถิติ ในการคำนวนเพื่อการตัดสินใจต่างกัน จะทำการพิจารณาได้จากการประมาณค่าสัดส่วนของประชากร (Estimation of population proportion) หรือค่าสถิติที่คำนวนได้ของทั้งสองตัวสถิติที่เลือกใช้ จำนวน 100 ครั้ง เพื่อหาค่าความน่าเชื่อถือในการทดสอบในระดับที่ยอมรับได้

2.3 การประมาณค่าสัดส่วนประชากร

การทดสอบความเป็นจำนวนสุ่มด้วยวิธีทางสถิติ เป็นการวัดค่าที่สามารถบ่งบอกในเชิงปริมาณว่าจำนวนสุ่มนั้นมีความเป็นจำนวนสุ่มเพียงพอที่จะใช้ในการนำไปประยุกต์ใช้งานด้านวิทยาการรหัสลับในการสื่อสาร เพื่อเป็นการเพิ่มความมั่นใจและระดับความน่าเชื่อถือของการทดสอบ จึงทำการประมาณค่าสัดส่วนประชากร (Estimation of population proportion) ที่ผ่านการทดสอบของค่าที่คำนวนได้จากตัวสถิติที่ใช้ในการทดอบ ซึ่งการประมาณค่าสัดส่วนประชากรนี้เป็นการหาค่าใกล้เคียงกับค่าพารามิเตอร์ที่ต้องการทราบ สามารถหาโดยการประมาณค่าความคลาดเคลื่อนมาตรฐาน (Estimated Standard Error) [5] เมื่อแทนค่าสัดส่วน (p) ของความสำเร็จของชุดจำนวนสุ่มที่ใช้ทดสอบดังสมการที่ 6

$$p = \frac{X}{n} \quad (6)$$

และคำนวนช่วงความเชื่อมั่นสองด้าน (1- α)100% ของ p ดังสมการที่ 7

$$\hat{p} - Z_{\alpha/2}\sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \le p \le \hat{p} + Z_{\alpha/2}\sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \quad (7)$$

และคำนวนช่วงความเชื่อมั่นด้านบน (1- α)100% ของ p ดังสมการที่ 8

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

$$p \le \hat{p} + Z_{\alpha/2}\sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \qquad (8)$$

3. การสร้างและวิธีทดสอบ

เนื่องจากการทดสอบสมมติฐานโดยใช้ตัวสถิติในการคำนวนเป็น *Erfc* มีความซับซ้อนและใช้เวลาในการคำนวนนาน จึงได้นำเสนอการใช้ตัวสถิติในการคำนวนเพื่อสรุปการตัดสินใจ เป็นค่ามาตรฐาน *(Z)* ที่มีความซับซ้อนต่ำและใช้เวลาในการคำนวนน้อยกว่า เนื่องจากเป็นสมการที่ลดรูปของฟังก์ชันการแจกแจงปกติสะสมซึ่งมีความสัมพันธ์กับ *Erfc* ดังสมการที่ 2 โดยทำการทดสอบคุณสมบัติของชุดจำนวนสุ่มด้วยการทดสอบเชิงความถี่ (Frequency Test) โดยขั้นตอนการทดสอบแนวคิดที่นำเสนอในบทความนี้จำลองด้วยโปรแกรมคอมพิวเตอร์ โดยกำหนดชุดจำนวนสุ่ม *(n)* ที่ใช้ทดสอบจำนวน 1,000,000 บิต ทดสอบจำนวน 100 ครั้ง และสมมุติฐานที่ตั้งไว้ เป็นดังนี้

H_0 คือ จำนวนสุ่มที่นำมาทดสอบมีความเป็นจำนวนสุ่มอย่างเพียงพอสำหรับการประยุกต์ใช้งานด้านวิทยาการรหัสลับ

H_1 คือ จำนวนสุ่มที่นำมาทดสอบไม่มีความเป็นจำนวนสุ่มอย่างเพียงพอสำหรับการประยุกต์ใช้งานด้านวิทยาการรหัสลับ

กำหนดระดับนัยสำคัญ α เท่ากับ 0.01 และ 0.05 สำหรับตัวสถิติ *Erfc* และเท่ากับ 0.005 และ 0.025 ตามลำดับ สำหรับตัวสถิติ *Z* โดยค่าที่ได้จากการคำนวน *Erfc* เรียกว่า *P-value* และค่าที่ได้จากการคำนวน *Z* เรียกว่า *Z-Score* ซึ่งเป็นค่าที่แสดงถึงโอกาสความน่าจะเป็น

ขอบเขตวิกฤตจะ *P-value* > 0.01 และ คือ *P-value* > 0.05 สำหรับที่ใช้ตัวสถิติ *Erfc* เนื่องจากเป็นการทดสอบด้านเดียวสำหรับขอบเขตวิกฤตที่ใช้ตัวสถิติ *Z* เป็น -2.58 < *Z-Score* <2.58 และ -1.96 < *Z-Score* <1.96 ตามลำดับ เนื่องจากเป็นการทดสอบสองด้าน ทำการทดสอบเชิงความถี่ (Frequency Test) เพื่อตรวจสอบสัดส่วนบิตศูนย์ และบิตหนึ่งว่าเป็นอย่างละครึ่งหรือไม่ นำค่าที่ได้มาทำการตัดสินใจโดยคำนวนตัวสถิติ *Erfc* และ *Z* ซึ่งค่าที่ได้เป็นค่า *P-value* และ *Z-Score* เพื่อพิจารณาขอมรับหรือปฏิเสธ H_0

สรุปผลการทดสอบ จะปฏิเสธ H_0 ถ้า *P-value* และ *Z-Score* ตกอยู่ในขอบเขตวิกฤต และยอมรับ H_0 ถ้า *P-value* และ *Z-Score* ตกอยู่บริเวณที่ยอมรับ จากนั้นพิจารณาเปรียบเทียบความแตกต่างของ *P-value* และ *Z-Score* โดยพิจารณาจากการประมาณค่าสัดส่วนของประชากร (Estimation of population proportion) ดังสมการที่ 6-8 เพื่อหาค่าความน่าเชื่อถือในการทดสอบเมื่อใช้ตัวสถิติเป็นค่ามาตรฐาน *(Z)* เปรียบเทียบกับ *Erfc* ในระดับความน่าเชื่อถือร้อยละ 99 และ 95 ซึ่งจะบ่งบอกได้ว่าสามารถใช้ตัวสถิติเป็นค่ามาตรฐาน *(Z)* แทน *Erfc* ได้

เหตุการณ์ / ระดับสำคัญ	α = 0.01		α = 0.05	
	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
1.ทดสอบด้วยค่า*P-value*				
ช่วงความเชื่อมั่น	≤0.99	≤0.01	≤0.94	≤0.06
สัดส่วนการทดสอบ	1	0	0.94	0.06
2.ทดสอบด้วยค่า*Z-Score*				
ช่วงความเชื่อมั่น	0.85-0.99	0.01-0.15	0.78-0.92	0.08-0.22
สัดส่วนการทดสอบ	0.92	0.08	0.85	0.15
3. เปรียบเทียบ *P-value* และ *Z-Score*				
ช่วงความเชื่อมั่น	0.04-0.12		0.01-0.15	
สัดส่วนการทดสอบ	0.06		0.10	

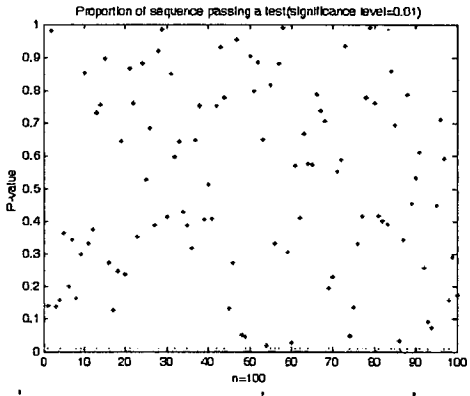
ตารางที่ 1 เปรียบเทียบระดับความเชื่อมั่นของสัดส่วนที่ผ่านและไม่ผ่านการทดสอบด้วยวิถีเชิงความถี่ของค่า *P-value* และ *Z-Score*

4. ผลการทดสอบ

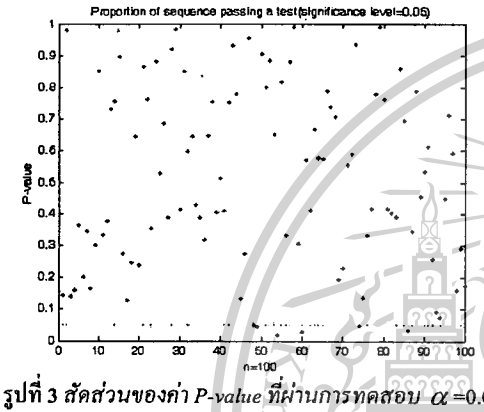
ผลการทดสอบเชิงความถี่ทั้งหมด 100 ครั้ง ที่ระดับนัยสำคัญเท่ากับ 0.01 หมายถึงระดับความน่าเชื่อถือเป็นร้อยละ 99 ค่า *P-value* ที่ผ่านการทดสอบทั้งหมด 100 ครั้ง คิดเป็นร้อยละ 100 เมื่อนำมาคำนวนหาอัตราการผ่านการทดสอบของสัดส่วนประชากรแบบด้านเดียว คำนวนจากสมการที่ 8 ค่า *P-value* จะต้องอยู่ในช่วง $P \le 0.99$ และค่า *Z-Score* ที่ผ่านการทดสอบทั้งหมด 100 ครั้ง คิดเป็นร้อยละ 92 เมื่อนำมาคำนวนหาอัตราการผ่านการทดสอบของสัดส่วนประชากรแบบสองด้าน คำนวนจากสมการที่ 7 ค่า *Z-Score* จะต้องอยู่ในช่วง $0.85 \le P \le 0.99$ เมื่อเปรียบเทียบค่าแตกต่างในการพิจารณาขอมรับและปฏิเสธ H_0 ระหว่าง ค่า *P-value* และค่า *Z-Score* คิดเป็นร้อยละ 6 ดังนั้นค่า *P-value* และค่า *Z-Score* ที่ผ่านการทดสอบมีความน่าเชื่อถือในระดับร้อยละ 99 ที่ระดับนัยสำคัญเท่ากับ 0.01 ดังตารางที่ 1 และรูปที่ 2-3

ผลการทดสอบเชิงความถี่ทั้งหมด 100 ครั้ง ที่ระดับนัยสำคัญเท่ากับ 0.05 ระดับความน่าเชื่อถือเป็นร้อยละ 95 ค่า *P-value* ที่ผ่านการทดสอบทั้งหมด 100 ครั้ง คิดเป็นร้อยละ 94 เมื่อนำมาคำนวนหาอัตราการผ่านการทดสอบของสัดส่วนประชากรแบบด้านเดียว คำนวนจากสมการที่ 8 ค่า *P-value* จะต้องอยู่ในช่วง $P \le 0.94$ และค่า *Z-Score* ที่ผ่านการทดสอบทั้งหมด 100 ครั้ง คิดเป็นร้อยละ 85 เมื่อนำมาคำนวนหาอัตราการผ่านการทดสอบของสัดส่วนประชากรแบบสองด้าน คำนวนจากสมการที่ 7 ค่า *Z-Score* จะต้องอยู่ในช่วง $0.78 \le P \le 0.92$ เมื่อเปรียบเทียบค่าแตกต่างในการพิจารณาขอมรับและปฏิเสธ H_0 ระหว่าง ค่า *P-value* และ

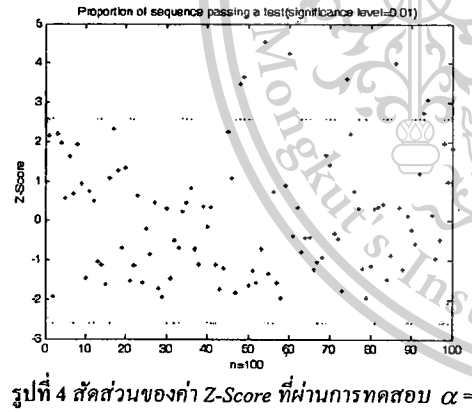
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.



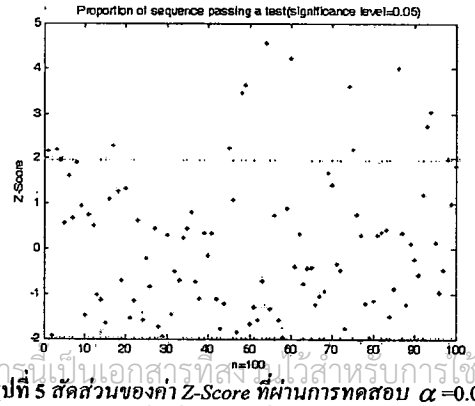
รูปที่ 2 *สัดส่วนของค่า P-value ที่ผ่านการทดสอบที่* α =0.01



รูปที่ 3 *สัดส่วนของค่า P-value ที่ผ่านการทดสอบ* α =0.05



รูปที่ 4 *สัดส่วนของค่า Z-Score ที่ผ่านการทดสอบ* α =0.01



รูปที่ 5 *สัดส่วนของค่า Z-Score ที่ผ่านการทดสอบ* α =0.05

ค่า *Z-Score* คิดเป็นร้อยละ 10 ดังนั้นค่า *P-value* และค่า *Z-Score* ที่ผ่านการทดสอบมีความน่าเชื่อถือในระดับร้อยละ 95 ที่ระดับนัยสำคัญเท่ากับ 0.05 ดังตารางที่ 1 และรูปที่ 4-5

5. การพัฒนางานวิจัยในอนาคต

การลดความซ้ำซ้อนของสถิติที่ใช้ในการตัดสินใจ Incomplete Gamma Function *(Igmc)* และทำการทดสอบด้วยวิธีอื่น เพื่อให้สามารถหาวิธีตัดสินใจยอมรับได้ว่าจำนวนสุ่มมีคุณสมบัติความเป็นจำนวนสุ่มเพียงพอต่อการนำไปใช้งานหรือไม่ โดยโปรแกรมการทดสอบนี้ผู้ใช้งานทั่วไปสามารถทำความเข้าใจได้ง่ายและสามารถนำโปรแกรมการทดสอบความเป็นจำนวนสุ่มได้สะดวก โดยโปรแกรมการทดสอบความเป็นจำนวนสุ่มชุดนี้มุ่งเน้นเพื่อทดสอบความเป็นจำนวนสุ่มของกุญแจรหัสลับที่จะใช้ในการเข้ารหัสสำหรับวิทยาการรหัสลับในระบบการสื่อสารทั่วไป

6. สรุป

การทดสอบความเป็นจำนวนสุ่มของ NIST's Statistical Test Suite มีความซับซ้อนสูง วิธีการที่นำเสนอใช้ค่ามาตรฐาน *(Z)* เป็นตัวสถิติในการคำนวนเพื่อพิจารณาการตัดสินใจ เพื่อพิจารณายอมรับหรือปฏิเสธความเป็นจำนวนสุ่ม จากผลการทดสอบเชิงความความถี่ของชุดจำนวนสุ่มมีการแจกแจงแบบปกติ โดยเปรียบเทียบกับการใช้ส่วนเติมเต็มฟังก์ชันค่าความคลาดเคลื่อน *(Erfc)* เป็นตัวสถิติคำนวน ซึ่งค่าอยู่ในช่วงที่ยอมรับได้ในระดับความเชื่อมั่นเท่ากับร้อยละ 99 และ 95 วิธีการที่นำเสนอนี้สามารถลดความซับซ้อนของการทดสอบสมมติฐานเชิงสถิติ (Tests of Statistical Hypotheses) ที่มุ่งเน้นทดสอบจำนวนสุ่มเพื่อนำไปใช้ประยุกต์ในงานด้านวิทยาการรหัสลับสำหรับการสื่อสารได้

เอกสารอ้างอิง

[1] Charmaine Kenny and Krzysztof Mosurski, **Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators,** The Distributed systems group, Computer Science Department, Trinity College Dublin, April 2005.

[2] Andrew Rukhin, Juan Soto, **A Statistical Test Suite for Random and Pseudorandom Generator for Cryptographic Applications,** NIST Special Publication 800-22. USA. May 15 2001.

[3] Donald Knuth. **The Art of Computer Programming,** Massachusetts. Grove Press,Inc. 1998

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

[4] ศุภชัย นาทะพันธ์. ความน่าจะเป็นและสถิติ. กรุงเทพมหานคร บริษัทซีเอ็ดยูเคชั่น จำกัด(มหาชน), 2547.

[5] Milton Abramowitz and Irene Stegun. **Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables.** National Bureau of Standards. U.S.1970.



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ภาคผนวก ข

Proceeding งานประชุมวิชาการ AICT 2008



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

Simplification of Frequency Test for Random Number Generation Based on Chi-Square

Kruawan Wongpanya[1] Keattisak Sripimanwat[2] and Kanok Jenjerapongvej [1]
[1] Department of Information Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand.
s8061005@kmitl.ac.th, kjkanok@kmitl.ac.th
[2] Optical and Quantum Communications Laboratory
National Electronics and Computer Technology Center (NECTEC), Thailand. keattisak.sripimanwat@nectec.or.th

Abstract—**This paper presents the simplified method of random test suite based on the frequency (block) test. The test is used to check the first property of random numbers which is to have the same probabilities of being "1" and "0". Random numbers are used for the secret key generation which is an essential part for cryptographic system. Before encryption, secret keys need to pass the random test in order to make it harder for outsiders to predict the pattern of the secret keys. Basically, the decision making of whether the secret keys are truly random, is based on the test statistics computation. Due to the motivation that the classical method based on the NIST Statistical Test Suite (NIST STS) is complex and redundant, the reduction of this random testing procedure is then proposed. The introduced technique does not need to compute the Incomplete Gamma Function (*Igamc*) nor the P-value for the decision making of test results unlike that of the classical method. Thus, it results to the reduction in the testing decision time. In this technique, the decision making and conclusion can be determined from the critical value of chi-square (x^2) directly. Its results without having to compute *Igamc* is compared to that of the classical method. In the test, the significance level (α) is set to be 0.01 or 0.05 in order to obtain the critical values and the critical regions. Resulting to the confidence of 99% or 95% respectively. Next, overall performance is evaluated by computing the percentage difference in order to demonstrate that the proposed value gives the same result as that of the classical method. Therefore, this proposed technique can be applied as that of the conventional based on the frequency (block) test.**

I. INTRODUCTION

The random number is utilized in various applications such as in the Monte Carlo simulation method, stochastic optimization, and cryptography for the secure communication system. Generally, the sender encodes information (plaintext) using the secret key. The result is in the form of incomprehensible messages called cipher text to be sent through the channel. When the receiver gets the messages, it will decode them using the secret key that is transmitted from the sender. However, the problem is that sometimes the transmitted key may be intercepted by the eavesdropper. If the secret key is generated by the non-randomness generator such that the secret key is not truly random, then the eavesdropper may be able to guess the value of the secret key. Thus, it needs a random number generator (*RNGs*) in order to employ the secret key.

Random number should have the same probabilities of being "1" and "0". Each number should be independent from the prior sequence and unpredictable. Therefore, properties of random number must be tested before using. Since that properties cannot be proved by sight, so the statistical tests must be used to test for its random performance. In order to validate result, a large number of samples should be realized.

Amongst many statistical test suites reported in the literature, the National Institute of Standards and Technology (NIST) test suite is preferred the most due to its meeting the industrial standard [1]. However in this paper, it will prove that some procedures of the NIST test suite could be simplified. This will result in the reduction of the random testing procedure and lower the random testing time.

In this paper, it is organized as follows. In Section II, the principle of statistic hypothesis test and fundamental are explained. The proposed method to reduce the complexity of the random test is then described in the next section. Finally, tested results will be presented to validate the proposed design in Section IV, and followed by the conclusion of the proposed design and its contribution in the section V.

II. PRELIMINARIES

This section introduces the basics of statistic hypothesis tests, test statistic, and the percentage difference. In that hypothesis, the significance level (α) is the criterion used for either accepting or rejecting the null hypothesis (H_0) as follows. First, the difference between the results of the experiment and H_0 is computed. If the probability (*P-value*) of the difference is equal to or larger than α, then H_0 is accepted.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

978-0-7695-3162-5/08 $25.00 © 2008 IEEE
DOI 10.1109/AICT.2008.42

IEEE computer society
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

Otherwise, H_0 is rejected [2]. In addition, the determination of *P-value* depends on the type of distribution. For instance, for the normal distribution, *P-value* is generally computed by *Erfc* [3] which is shown in Equation (1). For the Chi-square distribution, the *P-value* is computed by *Igamc* [3] which is shown in Equation (2).

$$Erfc(z) = \frac{2}{\pi}\int_{z}^{\infty} e^{-u^2}\,du \tag{1}$$

$$Q(a,x) = \frac{\Gamma(a,x)}{\Gamma(a)} = \frac{1}{\Gamma(a)}\int_{x}^{\infty} u^{-t}e^{a-1}dt \tag{2}$$

$$\Gamma(z) = \frac{1}{\Gamma(a)}\int_{0}^{\infty} t^{z-1}e^{-t}\,dt \tag{3}$$

where Γ represents the gamma function, and a is an integer.

III. Random Number Testing Procedure

This section presents the testing procedure, the proposed method, and their parameters. Finally, measurement of randomness will be presented based on the frequency (block) test.

A. General Specifications

The paper follows the statistic hypothesis test. The null hypothesis *(H_0)* is defined as the sequence of random numbers and the alternative hypothesis *(H_1)* is as for the sequence of non-random numbers. For its significance levels *(α)*, if it is set as 0.01 or 0.05, for example, it means that the sequence is considered to be random with the confidence of 99 % or 95% respectively. Basically, the critical value of α affects to the critical region. If the *P-value* is more than α then H_0 is accepted. Otherwise, H_0 is rejected. Next, the random sequence data are generated by three principle sources. Those are pseudo-random number generators (*PRNGs*) based on software generator, the quantum photonic source [4], and the atmospheric noise source [5].

B. The Frequency (block) test

Based on the block test, the focus is the proportion of ones *(bit "1")* within *M*-bit blocks that is approximately *M/2*, as would be expected under an assumption of randomness [1]. In this paper, the random testing is simulated by computer programming. This procedure is divided into six steps as those in [1].

Step I: Set length of input data *(n)* in which the input data is broken up into *(N)* blocks, and test in sequence of one block at a time. In the experiment, n and N are set to be as 2000 and 100 respectively. Thus, the length of each block *(M)* where $M = n/N$ is equal to 20.

Step II: determine the proportion (π_i) of ones *(bit "1")* in each *M*-bit block using the Equation (4)

$$\pi_i = \frac{\sum_{j=1}^{M} \varepsilon_{(i-1)M+j}}{M} \tag{4}$$

Step III: compute the test statistic, chi-square (x^2) according to Equation (5).

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \tag{5}$$

where O is the observed value and E is the expected value.

Step IV: decide for tested results by input x^2 value from step III in *the Igamc*'s computational process as in Equation (2) Computed value is called *P-value*.

Step V: compare *P-value* with α. If the *P-value* is more than α, then H_0 is accepted. Otherwise, H_0 is rejected.

Step VI: conclude the tested results; if H_0 is rejected, the tested result indicates that the sequence is non-random and vice versa, and repeat step I to VI with different random input data for 100 loop times *(L)*.

C. The simplified procedure

Due to the computation of *P-value* of NIST STS is a special function which is very complex and time-consuming. So that the proposed method trends to the simply that random test suite by reducing the testing procedures. This technique is done by making decision and comparison to α in order to conclude the tested result in *step III*. [6]. Thus, the probability distribution function is computed as

$$f(\chi^2) = \frac{1}{2_{k/2}\Gamma(\frac{k}{2})} u^{(k/2)-1}e^{-u/2} \quad \text{for } \chi 2 > 0 \tag{6}$$

where Γ represents the gamma function which is shown in Equation (3) and k is degree of freedom. If x^2 value is equal to or less than the critical value, H_0 is rejected. Otherwise, H_0 is accepted. The tested result is concluded as in *step VI*, the proposed technique does neither need to compute the *Igamc* significantly nor the *P-value* in *step IV* in order to compare with α in *step V*. Then, the tested results must be evaluated by considering the percentage difference in order to evaluate the similarity or the difference of the testing as shown in the Equation (7).

$$Percentage\ Diff = \frac{|Mearsured_{\,1} - Mearsured_{\,2}|}{\left(\frac{Mearsured_{\,1} + Mearsured_{\,2}}{2}\right)} X100\% \tag{7}$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

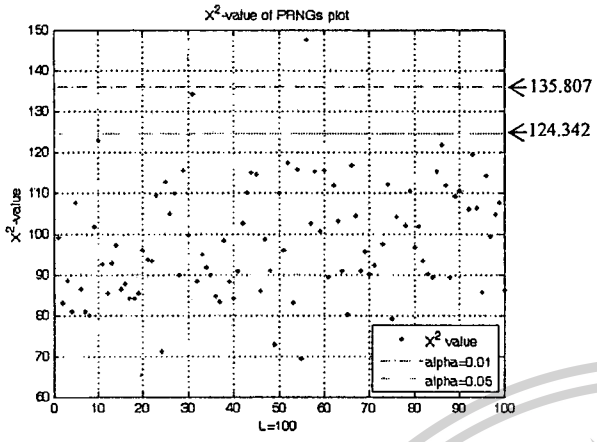


Fig.1. Distribution of *PRNGs* Test based on x^2 value
(passed in case of below the critical line and vice versa)

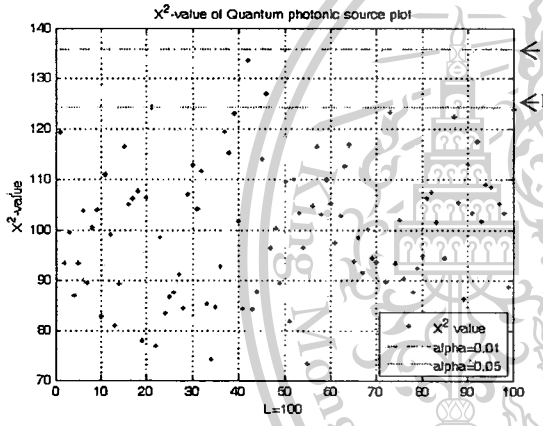


Fig.2. Distribution of the quantum photonic source
Test based on x^2 value
(passed in case of below the critical line and vice versa)

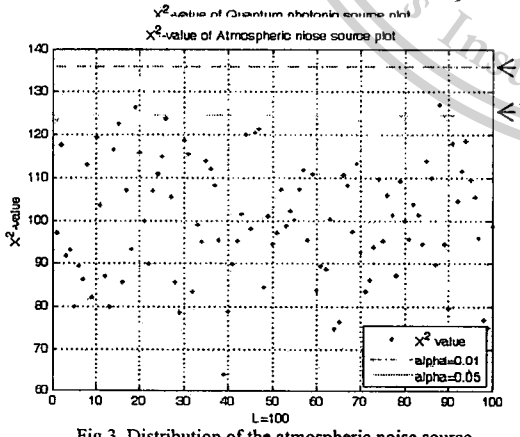


Fig.3. Distribution of the atmospheric noise source
Test based on x^2 value
(passed in case of below the critical line and vice versa)

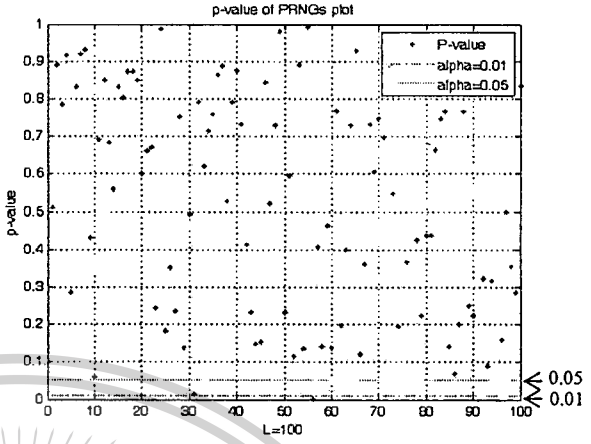


Fig.4. Distribution of *PRNGs* Test based on *P-value*
(passed in case of above the critical line and vice versa)

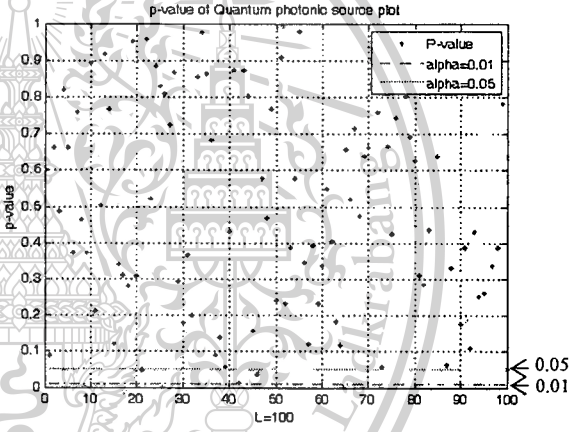


Fig.5. Distribution of the quantum photonic source based on *P-value*
(passed in case of above the critical line and vice versa)

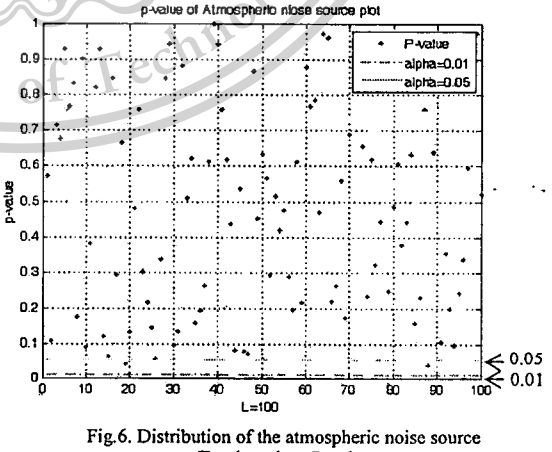


Fig.6. Distribution of the atmospheric noise source
Test based on *P-value*
(passed in case of above the critical line and vice versa)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

TABLE I THE COMPARISON PERCENTAGES BETWEEN *P-VALUE* AND x^2 *VALUE* FROM THE DIFFERENT SOURCES

Sources (conditions) \ Significance level (Results)		α = 0.01		α = 0.05	
		Passed (%)	Failed (%)	Passed (%)	Failed (%)
PRNGs	χ^2-value	99	1	98	2
	P-value	99	1	98	2
	Percentage Difference	0	0	0	0
Quantum photonic source [4]	χ^2-value	100	0	97	3
	P-value	100	0	97	3
	Percentage Difference	0	0	0	0
Atmospheric noise source [5]	χ^2-value	100	0	98	2
	P-value	100	0	98	2
	Percentage Difference	0	0	0	0

IV. TESTED RESULTS

The calculated results are shown in Table I. and the proportion of three sources test based on x^2 values and *P-values* are shown in Fig.1 to Fig.6.

Fig.1 to Fig.3 shows the performances of result distribution based on x^2 value from *PRNGs*, the quantum photonic source, and the atmospheric noise source. In sequence of those three sources, at α of 0.01, the passed rates are 99, 100, and 100%.Similarly, at α of 0.05, the passed rates are 98, 97, and 98% respectively. Next, Fig.4 to 6 shows the tests that also based on *P-value* from *PRNGs*, the quantum photonic source, and the atmospheric noise source. In sequence of those three sources, at α of 0.01, the passed rates are 99, 100, and 100%. Similarly, at α of 0.05, the passed rates are 98, 97, and 98% respectively.

Table I is the summarized results. It shows that the compared percentage difference between *P-value* and x^2 value from the different source is zero. Eventually, this proves that the proposed method could be used effectively as one of the classical random test suite based on frequency (block) test method.

CONCLUSION

As a key factor for secured communications, evidence of random number must be proved of its randomness. Promising on complexity reduction of NIST's *P-value* method, a simplified version based on the frequency (block) test has been proposed. That is done without computing the *Igamc* nor *P-value*. Comparison of the proposed method of x^2 values and the respective *P-value*'s shows that the percentage difference is zero. Therefore, this presents the equal random testing procedure where a simpler method is found. Finally, it can be concluded as a new simplified method that can be used to test randomness of the future secret key purpose.

REFERENCES

[1] Andrew Rukhin, Juan Soto, "A Statistical Test Suite for Random and Pseudorandom Generator for Cryptographic Applications", *NIST Special Publication 800-22. USA*,May 2001.

[2] Suphachai Natapan. *Probability and statistics. Se-education public company limited, Bangkok, Thailand*, 2004.

[3] Milton Abramowitz and Irene Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, *National Bureau of Standards. U.S.*,.1970.

[4] web service : "http://www.randomnumber.info"

[5] web service : "http://www.random.org"

[6] Albert H. Gowker and Gerald J. Lieberman, *Engineering Statistics* second edition. *Prentic-Hall, INC, Englewood Cliffs, New Jersey, U.S.A*, 1972

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

ภาคผนวก ค พื้นที่ใต้โค้งการแจกแจงปกติมาตรฐาน Z

$$F(Z)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{(x_i-\mu)/\sigma} e^{-z^2}dz$$

α	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.0000	0.0040	0.0080	0.0120	0.0160	0.0199	0.0239	0.0279	0.0319	0.0359
0.1	0.0398	0.0438	0.0478	0.0517	0.0557	0.0596	0.0636	0.0675	0.0714	0.0753
0.2	0.0793	0.0832	0.0871	0.0910	0.0948	0.0987	0.1026	0.1064	0.1103	0.1141
0.3	0.1179	0.1217	0.1255	0.1293	0.1331	0.1368	0.1406	0.1443	0.1480	0.1517
0.4	0.1554	0.1591	0.1628	0.1664	0.1700	0.1736	0.1772	0.1808	0.1844	0.1879
0.5	0.1915	0.1950	0.1985	0.2019	0.2054	0.2088	0.2123	0.2157	0.2190	0.2224
0.6	0.2257	0.2291	0.2324	0.2357	0.2389	0.2422	0.2454	0.2486	0.2517	0.2549
0.7	0.2580	0.2611	0.2642	0.2673	0.2704	0.2734	0.2764	0.2794	0.2823	0.2852
0.8	0.2881	0.2910	0.2939	0.2967	0.2995	0.3023	0.3051	0.3078	0.3106	0.3133

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ ดัดแปลง เผยแพร่ หรือแสวงหาประโยชน์ทางการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ลบข้อความนี้ทิ้ง และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use. Forbidden to modify the content, and cite the document when use.

α	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.9	0.3159	0.3186	0.3212	0.3238	0.3264	0.3289	0.3315	0.3340	0.3365	0.3389
1.0	0.3413	0.3438	0.3461	0.3485	0.3508	0.3531	0.3554	0.3577	0.3599	0.3621
1.1	0.3643	0.3665	0.3686	0.3708	0.3729	0.3749	0.3770	0.3790	0.3810	0.3830
1.2	0.3849	0.3869	0.3888	0.3907	0.3925	0.3944	0.3962	0.3980	0.3997	0.4015
1.3	0.4032	0.4049	0.4066	0.4082	0.4099	0.4115	0.4131	0.4147	0.4162	0.4177
1.4	0.4192	0.4207	0.4222	0.4236	0.4251	0.4265	0.4279	0.4292	0.4306	0.4319
1.5	0.4332	0.4345	0.4357	0.4370	0.4382	0.4394	0.4406	0.4418	0.4429	0.4441
1.6	0.4452	0.4463	0.4474	0.4484	0.4495	0.4505	0.4515	0.4525	0.4535	0.4545
1.7	0.4554	0.4564	0.4573	0.4582	0.4591	0.4599	0.4608	0.4616	0.4625	0.4633
1.8	0.4641	0.4649	0.4656	0.4664	0.4671	0.4678	0.4686	0.4693	0.4699	0.4706
1.9	0.4713	0.4719	0.4726	0.4732	0.4738	0.4744	0.4750	0.4756	0.4761	0.4767
2.0	0.4772	0.4778	0.4783	0.4788	0.4793	0.4798	0.4803	0.4808	0.4812	0.4817
2.1	0.4821	0.4826	0.4830	0.4834	0.4838	0.4842	0.4846	0.4850	0.4854	0.4857

This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

α	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
2.2	0.4861	0.4864	0.4868	0.4871	0.4875	0.4878	0.4881	0.4884	0.4887	0.4890
2.3	0.4893	0.4896	0.4898	0.4901	0.4904	0.4906	0.4909	0.4911	0.4913	0.4916
2.4	0.4918	0.4920	0.4922	0.4925	0.4927	0.4929	0.4931	0.4932	0.4934	0.4936
2.5	0.4938	0.4940	0.4941	0.4943	0.4945	0.4946	0.4948	0.4949	0.4951	0.4952
2.6	0.4953	0.4955	0.4956	0.4957	0.4959	0.4960	0.4961	0.4962	0.4963	0.4964
2.7	0.4965	0.4966	0.4967	0.4968	0.4969	0.4970	0.4971	0.4972	0.4973	0.4974
2.8	0.4974	0.4975	0.4976	0.4977	0.4977	0.4978	0.4979	0.4979	0.4980	0.4981
2.9	0.4981	0.4982	0.4982	0.4983	0.4984	0.4984	0.4985	0.4985	0.4986	0.4986
3.0	0.4987	0.4987	0.4987	0.4988	0.4988	0.4989	0.4989	0.4989	0.4990	0.4990

This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ภาคผนวก ง พื้นที่ใต้โค้งการแจกแจงแบบไคกำลัง

$$P(\chi_k^2 \geq \chi_\alpha^2, k) = \int_{(\chi_\alpha^2, k)}^{\infty} f_\chi^2(u)\,du = \alpha$$

Df \area	.995	.990	.975	.950	.900	.750	.500	.250	.100	.050	.025	.010	.005
1	0.00004	0.00016	0.00098	0.00393	0.01579	0.10153	0.45494	1.32330	2.70554	3.84146	5.02389	6.63490	7.87944
2	0.01003	0.02010	0.05064	0.10259	0.21072	0.57536	1.38629	2.77259	4.60517	5.99146	7.37776	9.21034	10.59663
3	0.07172	0.11483	0.21580	0.35185	0.58437	1.21253	2.36597	4.10834	6.25139	7.81473	9.34840	11.34487	12.83816
4	0.20699	0.29711	0.48442	0.71072	1.06362	1.92256	3.35669	5.38527	7.77944	9.48773	11.14329	13.27670	14.86026
5	0.41174	0.55430	0.83121	1.14548	1.61031	2.67460	4.35146	6.62568	9.23636	11.07050	12.83250	15.08627	16.74960
6	0.67573	0.87209	1.23734	1.63538	2.20413	3.45460	5.34812	7.84080	10.64464	12.59159	14.44938	16.81189	18.54758
7	0.98926	1.23904	1.68987	2.16735	2.83311	4.25485	6.34581	9.03715	12.01704	14.06714	16.01276	18.47531	20.27774

This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

Df \area	.995	.990	.975	.950	.900	.750	.500	.250	.100	.050	.025	.010	.005
8	1.34441	1.64650	2.17973	2.73264	3.48954	5.07064	7.34412	10.21885	13.36157	15.50731	17.53455	20.09024	21.95495
9	1.73493	2.08790	2.70039	3.32511	4.16816	5.89883	8.34283	11.38875	14.68366	16.91898	19.02277	21.66599	23.58935
10	2.15586	2.55821	3.24697	3.94030	4.86518	6.73720	9.34182	12.54886	15.98718	18.30704	20.48318	23.20925	25.18818
11	2.60322	3.05348	3.81575	4.57481	5.57778	7.58414	10.34100	13.70069	17.27501	19.67514	21.92005	24.72497	26.75685
12	3.07382	3.57057	4.40379	5.22603	6.30380	8.43842	11.34032	14.84540	18.54935	21.02607	23.33666	26.21697	28.29952
13	3.56503	4.10692	5.00875	5.89186	7.04150	9.29907	12.33976	15.98391	19.81193	22.36203	24.73560	27.68825	29.81947
14	4.07467	4.66043	5.62873	6.57063	7.78953	10.16531	13.33927	17.11693	21.06414	23.68479	26.11895	29.14124	31.31935
15	4.60092	5.22935	6.26214	7.26094	8.54676	11.03654	14.33886	18.24509	22.30713	24.99579	27.48839	30.57791	32.80132
16	5.14221	5.81221	6.90766	7.96165	9.31224	11.91222	15.33850	19.36886	23.54183	26.29623	28.84535	31.99993	34.26719
17	5.69722	6.40776	7.56419	8.67176	10.08519	12.79193	16.33818	20.48868	24.76904	27.58711	30.19101	33.40866	35.71847
18	6.26480	7.01491	8.23075	9.39046	10.86494	13.67529	17.33790	21.60489	25.98942	28.86930	31.52638	34.80531	37.15645
19	6.84397	7.63273	8.90652	10.11701	11.65091	14.56200	18.33765	22.71781	27.20357	30.14353	32.85233	36.19087	38.58226

This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

Df \area	.995	.990	.975	.950	.900	.750	.500	.250	.100	.050	.025	.010	.005
20	7.43384	8.26040	9.59078	10.85081	12.44261	15.45177	19.33743	23.82769	28.41198	31.41043	34.16961	37.56623	39.99685
21	8.03365	8.89720	10.28290	11.59131	13.23960	16.34438	20.33723	24.93478	29.61509	32.67057	35.47888	38.93217	41.40106
22	8.64272	9.54249	10.98232	12.33801	14.04149	17.23962	21.33704	26.03927	30.81328	33.92444	36.78071	40.28936	42.79565
23	9.26042	10.19572	11.68855	13.09051	14.84796	18.13730	22.33688	27.14134	32.00690	35.17246	38.07563	41.63840	44.18128
24	9.88623	10.85636	12.40115	13.84843	15.65868	19.03725	23.33673	28.24115	33.19624	36.41503	39.36408	42.97982	45.55851
25	10.51965	11.52398	13.11972	14.61141	16.47341	19.93934	24.33659	29.33885	34.38159	37.65248	40.64647	44.31410	46.92789
26	11.16024	12.19815	13.84390	15.37916	17.29188	20.84343	25.33646	30.43457	35.56317	38.88514	41.92317	45.64168	48.28988
27	11.80759	12.87850	14.57338	16.15140	18.11390	21.74940	26.33634	31.52841	36.74122	40.11327	43.19451	46.96294	49.64492
28	12.46134	13.56471	15.30786	16.92788	18.93924	22.65716	27.33623	32.62049	37.91592	41.33714	44.46079	48.27824	50.99338
29	13.12115	14.25645	16.04707	17.70837	19.76774	23.56659	28.33613	33.71091	39.08747	42.55697	45.72229	49.58788	52.33562
30	13.78672	14.95346	16.79077	18.49266	20.59923	24.47761	29.33603	34.79974	40.25602	43.77297	46.97924	50.89218	53.67196

This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ภาคผนวก จ

Source Code ชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่ม

1. วิธีทดสอบที่หนึ่ง

```
%--------Frequency Test-------------

clc;
clear;
tic
%-------call input file--------------------
fid = fopen('Qran4.txt','r');
fclose(fid);
%--------core test--------------------
n = length(a)
x=2*a-1;
Sn=sum(x)
So=abs(Sn)/sqrt(n);
Z_score=So

toc
% Significance level is 0.01 and then it is seperated to 0.005

if -2.58<=Z_score&Z_score<=2.58 ;

    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n');
end


% Significance level is 0.05 and then it is seperated to 0.025

if -1.96<=Z_score&Z_score<=1.96 ;
    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
else
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

```
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n' );
end
toc
```

2. วิธีทดสอบที่สอง

```
%--------Runs Test-------------
clc;
clear;
tic
fid = fopen('rng12.txt','r');
fclose(fid);
n = length(a)
phi=sum(a)/n
tor=2/sqrt(n)
phi1=abs(phi-1/2)

if phi1>=tor %that means if phi < tor is else case
  Z_score=0

else
    Vobs=sum(a)+1
    Z_score=abs((Vobs-2*n*phi*(1-phi)))/(2*sqrt(n)*phi*(1-phi))
end
toc
% Significance level is 0.01 and then it is seperated to 0.005

if -2.58<=Z_score&Z_score<=2.58 ;

    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n');
end

% Significance level is 0.05 and then it is seperated to 0.025

if -1.96<=Z_score&Z_score<=1.96 ;
    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

```
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n' );
end
toc
```

3. วิธีทดสอบที่สาม

```
clear;
clc;

tic
fid = fopen('rng2.txt','r');
fclose(fid);
n = length(a)
X=2*a-1;
S=fft(X);   %S=DFT(X)
M=abs(S);   %The modulus r of a complex number z = a + ib is written
| z | and defined by | z | = sqrt(a^2+b^2)

       count = 0;
       upperBound = sqrt(2.995732274*n);
       for i = 1:n/2-1
          if M(i)<upperBound
             count=count+1;
          end
       end
       percentile = count/(n/2)*100
       N_1 = count      % number of peaks less than h =
sqrt(2.995732274*n)
       N_o = 0.95*n/2
       Z_score = ((N_1 - N_o)/sqrt(n/2.*0.95*0.05))

 toc
 % Significance level is 0.01 and then it is seperated to 0.005

if -2.58<=Z_score&Z_score<=2.58 ;

    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n');
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

```
end


% Significance level is 0.05 and then it is seperated to 0.025

if -1.96<=Z_score&Z_score<=1.96 ;
    fprintf('\tThe probability (under the null hypothesis of
randomness) is Critical Region<=%f <= Critical Region\n',Z_score);
    fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) is %f > Critical Region or %f < Critical Region
\n',Z_score);
    fprintf('\tnot accept the sequence as random\n' );
end
toc
```

4. วิธีทดสอบที่สี่

```
%--------Frequency Block Test-------------
clc;
clear;
tic
fid = fopen('rng7.txt','r');
a= abs(48- fread(fid,'uint8'));
fclose(fid);

 %-------------------------------------------------------------------%

n=length(a) ;                    % find a length of sequence
M=100;
N=n/M ;                          % set a number of block sequence
%-------------------------------------------------------------------%
fprintf('r1')
fid=fopen('rng1.txt','r');
A= abs(48- fread(fid,[M,N]));

fclose(fid);
 %-------------------------------------------------------------------
------%

meanA=mean(A);                          %find phi and fine a x2(obs)

%-------------------------------------------------------------------%
x=((meanA-1/2).^2)/0.5 ;                %find chi square
probability
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

```
Xobs=sum(x)
Z_score=Xobs
toc

if Z_score<=135.807;
     fprintf('\tThe probability (under the null hypothesis of
randomness) = %f <= Critical Region\n',Z_score);
     fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) = %f > Critical Region\n',Z_score);
    fprintf('\tnot accept the sequence as random\n' );
end

if Z_score<=124.342;
     fprintf('\tThe probability (under the null hypothesis of
randomness) = %f <= Critical Region\n',Z_score);
     fprintf('\taccept the sequence as random\n');
else
    fprintf('\tThe probability (under the null hypothesis of
randomness) = %f > Critical Region\n',Z_score);
    fprintf('\tnot accept the sequence as random\n' );
end
toc
```

5. วิธีทดสอบที่ห้า

```
clc;
clear;
tic
fid=fopen('Rng1.txt','r');
A=fread(fid);
cha=char(A);
a=cha'
 %-------------------------------------------------------------------%

n=length(a)

%-------------------------------------------------------------------%
if  n <= 128

        fprintf ('\t\t   n=%f is too short\n', n);

   elseif  n < 6272
        K = 4;
        M = 8;
        P=[0.21484375 0.3671875 0.23046875 0.1875];
    elseif  n < 75000
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

```
        K = 6;
        M = 128;
        P=[0.1174035788 0.242955959 0.249363483 0.17517706
0.102701071 0.112398847];

    else
        K = 7;
        M = 10000;
        P=[0.0882 0.2092 0.2483 0.1933 0.1208 0.0675 0.0727];

end
 N=floor(n/M);
 result=zeros(N,M);

 %%
   for i=1:N
       run=0;

       counter=zeros(n,1);
       for j=((i-1)*M+1):i*M
        if a(j)=='1'
            run=run+1;
            v=run
            sprintf('found! j=%d run=%d ',j,run) %maxrun=%d
        else
            if run>0
                MaxRun=max(v)
                counter(MaxRun)=counter(MaxRun)+1;
                sprintf('j=%d i=%d M=%d a(%d)=%c run=%d
counterMax(%d)=%d',j,i,M,j,a(j),run,run,counter(MaxRun))
                run=0;
                v=0;
            end
            run=0;
            v=0;
        end

       end

        if run>0
            MaxRun=max(v)
            counter(run)=counter(run)+1;
                  sprintf('j=%d i=%d M=%d a(%d)=%c run=%d
counterMax(%d)=%d',j,i,M,j,a(j),run,run,counter(MaxRun))
            run=0;
            v=0;
        end
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

```
        output='';
        for k=1:M
            output=sprintf('%s%c',output,a(k+(i-1)*M));
        end
       for k=1:M
            output=sprintf('%s (%d-%d)',output,k,counter(k));
            result(i,k)=counter(k);
        end
        disp(output);
    end
    result
    Y=sum(result)
    len=length(Y)
if len==8
    Y(4)=Y(4);%+Y(5);%+Y(6)+Y(7)+Y(8);
    Z=Y(1:4)
    U=Z-(N.*P);
    U1=N.*P;
    U2=U.^2;
    U3=U2./U1;
    Chi2=sum(U3)
    P_value1=gammainc(Chi2./2,N./2)
    P_value=1-P_value1
elseif len==128
    Y(4)=Y(4); %Y(1)+Y(2)+Y(3)+
    Y(9)=Y(9)+Y(10);%+Y(11);%+Y(12)+Y(13)+Y(14)+Y(15)+Y(16);
    Z=Y(4:9)
    U=Z-(N.*P);
    U1=N.*P;
    U2=U.^2;
    U3=U2./U1;
    Chi2=sum(U3)
    P_value1=gammainc(Chi2./2,N./2)
    P_value=1-P_value1
elseif len==10000
    Y(10)=Y(10);%Y(1)+Y(2)+Y(3)+Y(4)+Y(5)+Y(6)+Y(7)+Y(8)+Y(9)+
    Y(16)=Y(16);%+Y(17)+Y(18);%+Y(19)+Y(20)+Y(21)+Y(22)+Y(23);
    Z=Y(10:16)
    U=Z-(N.*P);
    U1=N.*P;
    U2=U.^2;
    U3=U2./U1;
    Chi2=sum(U3)
    P_value1=gammainc(Chi2./2,N./2)
    P_value=1-P_value1
end
        toc
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.

รายการคำศัพท์

ก

กรดนิวคลิอิก	Nucleic acid
กระจกแยกลำแสง	Beam Splitter
กระบวนการกลั่น	Distillation Process
การเข้ารหัส	Encryption
การเข้ารหัสข้อความเพื่อระบุถึงตัวบุคคล	Message Authentication Codes
การควบคุมการเข้าถึงข้อมูล	Access Control
การแจกแจงการสุ่มตัวอย่าง	Sampling Distributions
การแจกแจงไคกำลังสอง	Chi-square Distribution
การแจกแจงแบบปกติมาตรฐาน	Standard Normal Distribution
การแจกแจงปกติ	Normal Distribution
การทดสอบคริปท์ เอ็กซ์เอส	Crypt-XS
การทดสอบความต่อเนื่องของจำนวนสุ่ม	Runs Test
การทดสอบความเป็นอิสระ	Test for independence
การทดสอบความลักษณะคาบของชุดจำนวนสุ่ม	Discrete Fourier Transform (Spectral) Test
การทดสอบความยาวของจำนวนสุ่มที่ซ้ำ	Tests for the Longest Run of Ones in a
ในชุดข้อมูล	Block
การทดสอบความเหมาะสมของการแจกแจง	Test for Goodness of Fit
การทดสอบคุณสมบัติของจำนวนสุ่ม	Randomness Testing
การทดสอบเชิงความถี่ของชุดจำนวนสุ่ม	Frequency Test within a Block
การทดสอบเชิงความถี่แบบเดี่ยว	Frequency (Monobit) Test
การทดสอบดายฮาร์ด	DIEHARD Test
การทดสอบนุช	Knuth Test
การทดสอบสมมติฐาน	Test of Hypotheses
การทดสอบสมมติฐานด้านเดียว	One-tailed Test
การทดสอบสมมติฐานสองด้าน	One-tailed Test
การทดสอบหลายสัดส่วน	Test for proportions
การทดสอบอีเอ็นที	ENT
การบีบอัด	Compression

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

การประมาณค่า	Estimation
การป้องกันการปฏิเสธความรับผิด	Non-repudiation
การพิจารณาการผ่านการทดสอบ	Decision Making
การระบุถึงตัวบุคคล	Authentication
การรักษาความลับ	Confidentiality
การรักษาความสมบูรณ์	Integrity
การลงลายมือชื่อดิจิทัล	Digital Signatures
การวัดการกระจายของข้อมูล	Measure of Dispersion
การวัดค่ากลางของข้อมูล	Measure of central value
การวิเคราะห์ข้อมูล	Data Analysis
การสุ่มตัวอย่าง	Random Sampling
การอนุมานเชิงสถิติ	Statistical Inference
แกมมาฟังก์ชัน	Gamma Function
ข	
ข้อความที่ถูกเข้ารหัส	Ciphertext
ข้อความปกติ	Plaintext
ข้อมูลสารสนเทศ	Information
ขีดจำกัดควบคุมบน	Upper Control Limit
ขีดจำกัดควบคุมล่าง	Lower Control Limit
ค	
ความซับซ้อน	Complexity
ความถี่ที่คาดหวัง	Expected Frequency
ความถี่ที่สังเกต	Observed Frequency
ความน่าจะเป็น	Probability
ความน่าจะเป็นแบบมีเงื่อนไข	Conditional Probability
ความเป็นอิสระเชิงเดี่ยว	Independence
ความแปรปรวน	Variance
ความยาวของรันที่ยาวที่สุด	Longest Run
คอมพลีเมนต์	Complement
ค่าคลาดเคลื่อนมาตรฐาน	Standard Error
ค่าแนวโน้มสู่ศูนย์กลาง	Central Tendency or Location
ค่าเบี่ยงเบนมาตรฐาน	Standard Deviation

King Mongkut's Institute of Technology Ladkrabang
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ค่ามาตรฐาน	Standard Score
ค่าวิกฤติ	Critical value
ค่าสังเกต	Observed Value
เครื่องตรวจนับแบบดูดกลืน	Absorbing counter
โครงการนำร่องเอ็มเอสไอเอสเอส	Previous MSISS Project
จ	
จำนวนสุ่ม	Random Numbers
จำนวนสุ่มแท้	True Random Number
จำนวนสุ่มอย่างเพียงพอ	Sufficiently Random
ช	
ชุดข้อมูล	Block
ชุดทดสอบทางสถิติเอ็นไอเอสที	National Institute of Standards and Technology Statistic Test Suite
ซ	
ซับเซท	Subset
เซต	Sets
แซมเปิลสเปซ	Sample Space
ฐ	
ฐานนิยม	Mode
ด	
ดีสครีตฟูเรียทรานสฟอร์ม	Discrete Fourier Transform
ต	
ตัวแปรสุ่ม	Random Variable
ตัวแปรสุ่มแบบต่อเนื่อง	Continuous Random Variable
ตัวแปรสุ่มแบบไม่ต่อเนื่อง	Discrete Random Variable
ตัวสถิติ	Statistic
ตัวอย่าง	Sample
ถ	
ถอดรหัส	Decryption
ท	
ทฤษฎีขีดจำกัดสู่ศูนย์กลาง	Central Limit Theorem
ทฤษฎีความน่าจะเป็น	Probability Theory

King Mongkut's Institute of Technology Ladkrabang
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ทฤษฎีแรนดอมวอล์ก	Random Walk Theory
บ	
บริเวณยอมรับ	Acceptance Region
บริเวณวิกฤต	Critical Region
บุคคลที่สาม	Eavesdropper
ป	
ปริพันธ์	Integration
พ	
พารามิเตอร์	Parameter
พิสัย	Range
พีค	Peak
ฟ	
ฟังก์ชันความหนาแน่นของความน่าจะเป็น	Probability Density Function
ฟังก์ชันแจกแจงสะสม	Cumulative Distribution Function
ฟังก์ชันพิเศษ	Special Function
โฟตอน	Photon
ภ	
ภายใต้สภาวะควบคุม	Controlled Condition
ม	
มัธยฐาน	Median
ย	
ยูเนียน	Union
ร	
ร้อยละความแตกต่าง	Percentage Different
ระดับขั้นความเสรี	Degree of Freedom
ระดับความเชื่อมั่น	Confidence Level
ระดับความเป็นอิสระ	Degree of freedom
ระดับนัยสำคัญ	Significance Level
เรนจ์สเปซ	Range Space
ล	
ลำดับตั้งต้น	Seed

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ว

วิทยาการรหัสลับ	Cryptography
วิทยาการรหัสลับแบบสมมาตร	Symmetrical Cryptography
วิทยาการรหัสลับแบบอสมมาตร	Asymmetrical Cryptography
วิธีการเข้ารหัส	Encryption Algorithms
วิธีมอลติคาร์โล	Monte Carlo Method

ส

สถิติทดสอบ	Test Statistic
สถิติทดสอบไคกำลังสอง	Test Statistic Chi Square
สมมติฐานของการสุ่ม	Assumption of randomness
สมมติฐานหลัก	Null Hypotheses
สมมติฐานอื่น	Alternative Hypotheses
สมาชิก	Element
สัญญาณรบกวนจากบรรยากาศ	Atmospheric noise
สัญญาณรบกวนวิทยุ	Radio Noise
สัดส่วนการผ่านการทดสอบ	Proportion of Passing Rates
สัดส่วนของประชากร	Population proportion
สัมประสิทธิ์ความแปรผัน	Coefficient of Variation
สายอากาศ	Antenna
สารพันธุกรรม	Deoxy-ribonucleic Acid
สุ่ม	Random

ห

หน่วยรับแสง	Detector
แหล่งกำเนิดธาตุกัมมันตรังสี	Radioactive Source
แหล่งกำเนิดจำนวนสุ่มเทียม	Pseudo-Random Number Generator
แหล่งกำเนิดจำนวนสุ่มแท้	True Random Number Generator

อ

อัลกอริธึม	Algorithms
อินเตอร์เซคชัน	Intersection
อุปกรณ์สารกึ่งตัวนำ	Semiconductor
เอนโทรปี	Entropy

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
This material is reserved for educational use only, not allowed for commercial use.
Forbidden to modify the content, and cite the document when use.

ประวัติผู้เขียน

ชื่อ-นามสกุล นางสาวเครือวัลย์ วงค์ปัญญา

วัน เดือน ปีเกิด 17 กันยายน 2524 จังหวัดพะเยา

ประวัติการศึกษา 2542 มัธยมศึกษาปีที่ 6 โรงเรียนฟากกว๊านวิทยาคม จังหวัดพะเยา

2546 คณะวิทยาศาสตร์ สาขาฟิสิกส์ มหาวิทยาลัยนเรศวร

จังหวัดพิษณุโลก

2548 ศึกษาต่อระดับปริญญาโท ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

งานวิจัยที่สนใจ จำนวนสุ่ม การทดสอบคุณสมบัติของจำนวนสุ่ม สถิติและวิทยาการรหัสลับ

King Mongkut's Institute of Technology Ladkrabang

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

This material is reserved for educational use only, not allowed for commercial use.

Forbidden to modify the content, and cite the document when use.