การพัฒนาชุดการทดสอบคุณสมบัติจำนวนสุ่ม

INVESTIGATION AND DEVELOPMENT OF RANDOM TEST SUITE

เครือวัลย์ วงค์ปัญญา

KRUAWAN WONGPANYA

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2552

KMITL-2009-EN-M-230-161

INVESTIGATION AND DEVELOPMENT OF RANDOM TEST SUITE

KRUAWAN WONGPANYA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2009

KMITL-2009-EN-M-230-161

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การพัฒนาชุดการทดสอบคุณสมบัติจำนวนสุ่ม

Thesis Title Investigation and Development of Random Test Suite

นักศึกษา นางสาวเครือวัลย์ วงศ์ปัญญา

รหัสประจำตัว 48061005

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.กนก เจนจิระพงศ์เวช

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์

หมายเลขวิทยานิพนธ์ KMITL-2009-EN-M-230-161

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.อรลาภ	แสงอรุณ	
รศ.ดร.ชวลิต	เบญจางค์ประเสริฐ	
ดร.เกียรติศักดิ์	ศรีพิมานวัฒน์	
รศ.ดร.อรรถสิทธิ์	หล่าสกุล	
รศ.ดร.กนก	เจนจิระพงศ์เวช	

วัน / เดือน/ ปี ที่สอบ วันอังคารที่ 13 ตุลาคม พ.ศ. 2552 เวลา 09.30-11.30 น.

สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 4

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร.กอบชัย เดชหาญ)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 13 ตุลาคม พ.ศ. 2552

หัวข้อวิทยานิพนธ์	การพัฒนาชุดการทดสอบคุณสมบัติจำนวนสุ่ม
นักศึกษา	นางสาวเครือวัลย์ วงค์ปัญญา
รหัสประจำตัว	48061005
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2552
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร.กนก เจนจิระพงศ์เวช
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์

บทคัดย่อ

วิทยานิพนธ์นี้นำเสนอการพัฒนาชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่ม เพื่อให้มีความมั่นใจในการใช้งานจำนวนสุ่มด้านการสื่อสารปลอดภัย รวมทั้งเป็นแนวทางพัฒนาการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์(Web Service) และการพัฒนาชุดวิธีทดสอบอ้างอิงจากชุดทดสอบทางสถิติเอ็นไอเอสที (National Institute of Standards and Technology Statistical Test Suite) โดยมีวัตถุประสงค์คือ ตรวจสอบหาคุณสมบัติของจำนวนสุ่มแท้และจำนวนสุ่มเทียมก่อนนำไปประยุกต์ใช้งาน เพื่อให้สามารถทราบว่าจำนวนสุ่มดังกล่าวมีคุณสมบัติเพียงพอที่จะนำไปใช้งานหรือไม่ กระบวนสำคัญของการทดสอบคือ การคำนวณสถิติทดสอบ (Test Statistic) และการพิจารณาการผ่านการทดสอบ (Decision Making) เนื่องจากปัญหาของชุดทดสอบอ้างอิงที่ใช้สถิติทดสอบและการพิจารณาการผ่านการทดสอบด้วยหลักการที่มีรูปสมการซับซ้อน รวมทั้งมีขั้นตอนของการทดสอบหลายขั้นตอน ส่งผลให้ใช้เวลาในการประมวลผลนาน ดังนั้นวิทยานิพนธ์นี้จึงนำเสนอการคำนวณสถิติทดสอบและการพิจารณาการผ่านการทดสอบที่มีความซับซ้อนต่ำ เพื่อลดขั้นตอนและเวลาในการประมวลผล จำนวนสองวิธี คือ สถิติทดสอบที่เรียกว่า ค่ามาตรฐาน (Standard Score: Z) สำหรับชุดข้อมูลที่มีการแจกแจงปกติ (Normal Distribution) และสถิติทดสอบไคกำลังสอง (Chi Square : χ^2) สำหรับชุดข้อมูลที่มีการแจกแจงไคกำลังสอง (Chi-square Distribution) นั้น หลักการที่นำเสนอเพื่อการหาสถิติทดสอบดังกล่าวได้รูปสมการที่มีความซับซ้อนต่ำ สามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและค่าทางสถิติได้โดยตรง ทำให้สามารถพิจารณาการผ่านการทดสอบโดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้ได้ การทดสอบคุณสมบัติของจำนวนสุ่มนี้ครอบคลุมห้าวิธีย่อย ได้แก่ การทดสอบความถี่แบบเดี่ยว เพื่อหาลักษณะการแจกแจงความน่าจะเป็นและรูปแบบการแจ้กแจง การทดสอบความต่อเนื่องของจำนวนสุ่ม เพื่อหาการซ้ำกันของข้อมูลและความต่อเนื่องของชุดข้อมูล การทดสอบเพื่อหา

ลักษณะคาบของชุดจำนวนสุ่ม การทดสอบความถี่ของชุดจำนวนสุ่ม เพื่อหาลักษณะการแจกแจงของชุดข้อมูล และการทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล โดยกระบวนการทดสอบทางสถิติทั้งหมดดังกล่าว มีขั้นตอนสำหรับทำการทดสอบทั้งหมดห้าขั้นตอนตามลำดับ ขั้นตอนแรกคือการตั้งสมมติฐาน ตามด้วยขั้นตอนการกำหนดระดับนัยสำคัญ ขั้นตอนการกำหนดค่าวิกฤตและบริเวณวิกฤต ขั้นตอนการเลือกสถิติทดสอบ และขั้นตอนสุดท้ายการสรุปผลการทดสอบ จากการศึกษาวิจัยพบว่า ผลการทดสอบของหลักการที่นำเสนอไม่มีความแตกต่างกับหลักการอ้างอิง ความเบี่ยงเบนเฉลี่ยระหว่างค่าที่ได้จากการทดสอบและค่าทางทฤษฎีน้อยกว่าร้อยละ 1 เวลาของการประมวลผลการทดสอบลดลงร้อยละ 5.85 และชุดวิธีทดสอบสามารถแยกความแตกต่างจากคุณสมบัติของจำนวนสุ่มแท้และจำนวนสุ่มเทียมได้ โดยมีสัดส่วนการผ่านการทดสอบที่ระดับนัยสำคัญที่ 0.05 จำนวน 96 ชุดและ 84 ชุด ส่วนที่ระดับนัยสำคัญที่ 0.01 มีสัดส่วนจำนวน 99 ชุด และ 93 ชุด ตามลำดับ จึงเป็นการยืนยันคุณภาพของชุดทดสอบที่ได้พัฒนาขึ้น

Thesis Title	Investigation and Development of Random Test Suite
Student	Miss Kruawan Wongpanya
Student ID.	48061005
Degree	Master of Engineering
Program	Information Engineering
Year	2009
Thesis Advisor	Assoc. Prof. Dr. Kanok Jenchirapongvet
Thesis Co-Advisor	Dr. Keattisak Sripimanwat

ABSTRACT

This thesis presents the simplified method of random test suite based on the National Institute of Standards and Technology Statistical Test Suite (NIST STS). Random number is used to generate a secret key that is an essential part for cryptographic system. Secret key is one of the most important section of an encryption method and must be verified to pass the random test in order to make it harder for outsiders to predict the pattern of the secret key. However, the verification method is required complex and redundant statistical computation, that may not be possible for the internet application. Thus, the reduction and simplified method of this random testing procedure is then important. The proposed technique are based on the Standard Score (Z) and Chi Square (χ^2) for normal distribution and chi square distribution respectively. In these techniques, the decision making and conclusion can be determined from the critical value of Z and χ^2 directly. The randomness testing consist of five test sets. Firstly, the Frequency (Monobit) Test, the purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as that would be expected for a truly random sequence. Next, Runs Test, is that to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. Discrete Fourier Transform (Spectral) Test, is that the third test set to detect periodic features in the tested sequence that would indicate a deviation from the assumption of randomness. As the forth, Frequency Test within a Block, is a test set to determine whether the frequency of ones in an M-bit block is approximately M/2, as would be expected under an assumption of randomness. Lastly, the purpose of this test, Test for the Longest Run of Ones in a Block, is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be

expected in a random sequence. Consequently, the hypothesis-testing procedures for randomness testing consist of five steps in sequence as *a)* state the null hypothesis and the alternative hypothesis *b)* select a significance level and confidence level *c)* determine a suitable test statistic that based on statistical distribution *d)* compute test statistic and compare the test statistic with the significance level for decision-making *e)* decide whether the null hypothesis should be rejected and report result. As a result, the proposed method gives the same results as that of the NIST STS method. Next, the deviation of randomness assumption is less than 1 percent. For testing comparison of true (quantum) random number with general software generated random number at the significant level 0.05, there are 96 and 84 passed packages respectively. Meanwhile at level of 0.01, there are 99 and 93 packages respectively. These confirm the success of the proposed simplified method.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดี ด้วยความช่วยเหลือและสนับสนุนจากหลายๆ ฝ่ายด้วยกันโดยผู้เขียนขอขอบพระคุณดังต่อไปนี้

ขอขอบคุณ รศ.ดร.กนก เจนจิระพงศ์เวช อาจารย์ผู้ควบคุมวิทยานิพนธ์ ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังและ ดร.เกียรติศักดิ์ ศรีพิมานวัฒน์ อาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วมและนักวิจัยจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ในการให้ความรู้ คำแนะนำและคำปรึกษาที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์เล่มนี้ ผู้เขียนรู้สึกซาบซึ้งในความอนุเคราะห์และขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบคุณภาควิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังที่ประสิทธิ์ประสาทวิชาความรู้ ที่เป็นพื้นฐานในการทำวิทยานิพนธ์เล่มนี้

ขอขอบคุณศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ อุทยานวิทยาศาสตร์ประเทศไทย ในการใช้สถานที่เพื่อทำวิจัยในวิทยานิพนธ์เล่มนี้

ขอขอบคุณทีมงานผู้ช่วยนักวิจัย หน่วยปฏิบัติการวิจัยการสื่อสารเชิงแสงและควอนตัม (OQC) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ที่ให้ความรู้ ความร่วมมือและความช่วยเหลือเกี่ยวกับการสนับสนุนการเขียนโปรแกรมการทดสอบคุณสมบัติจำนวนสุ่ม

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ทางผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่านไว้ ณ โอกาสนี้

เครือวัลย์ วงค์ปัญญา

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป(ต่อ)

สารบัญตาราง

รายการคำย่อ

AES	Advanced Encryption Algorithm
BS	Beam Splitter
CDF	Cumulative Distribution Function
CLT	Central Limit Theorem
D	Detector
DFT	Discrete Fourier Transform
DNA	Deoxy-ribonucleic acid
Erfc	Complementary Error Function
Igamc	Incomplete Gamma Function
LFSR	Linear feedback shift register
NIST	National Institute of Standards and Technology
NIST STS	National Institute of Standards and Technology Statistical Test Suite
PDF	Probability Density Function
PRNGs	Pseudo Random Number Generator
RNGs	Random Number Generator
S	Sample Space
UCL	Lower Control Limit
Z	Standard score

รายการสัญลักษณ์

การแจกแจงการสุ่มตัวอย่างของค่าเฉลี่ย	$\bar{x}$
การแจกแจงการสุ่มตัวอย่างของสัดส่วน	$\hat{p}$
การแจกแจงแบบไคกำลังสอง	χ_k^2
การแจกแจงปกติ	$X \sim N(\mu, \sigma^2)$
แกมมาฟังก์ชัน	$\Gamma(p)$
ขีดเริ่มการทดสอบ DFT	T
ความถี่ของรันของบิตหนึ่งที่ยาวที่สุด	ν_i
ความถี่ที่ค่าคาดหวังจะเป็นไปตามทฤษฎี	E_i
ความถี่ที่ค่าสังเกตที่เกิดขึ้นจากการทดลองจริง	O_i
ความน่าจะเป็นในการปฏิเสธสมมติฐานหลัก	$P-value$
ความน่าจะเป็นของการเกิดเหตุการณ์ A	$P(A)$
ความน่าจะเป็นในการเกิดความถี่รันสูงสุด	pi_i
ความแปรปรวนของตัวอย่าง	S^2
ความแปรปรวนของประชากรปกติ	σ^2
ความยาวของชุดข้อมูลในแต่ชุด	M
ความยาวของบิตจำนวนสุ่มที่นำมาทดสอบ	n
ค่าเฉลี่ย	μ
ค่าเฉลี่ยของตัวแปรสุ่ม X	$\overline{X}$
คาดคะเนของตัวแปรสุ่ม X	E[X]
ค่ามาตรฐาน	Z
ค่าโมดูลัส	*Modulus*
ค่าสถิติทดสอบ	$\hat{\theta}$
จำนวนของพีคค่าที่เกินทฤษฎี	N_0
จำนวนชุดข้อมูล	N
จำนวนพีคใน M ที่มีค่าน้อยกว่า T	N_1
ผลรวมของจำนวนสุ่ม	S_n
ฟังก์ชันความน่าจะเป็น	$F(x)$
ระดับขั้นความเสรี	k
ระดับขั้นความเสรีการทดสอบรัน	K
ระดับนัยสำคัญ	α

ลำดับของจำนวนสุ่มที่มาจากแหล่งกำเนิด	ε
สถิติทดสอบไคกำลังสอง	χ^2
สมมติฐานหลัก	H_0
สมมติฐานอื่น	H_1
ส่วนเบี่ยงเบนมาตรฐาน	σ
สัดส่วนของบิตศูนย์และบิตหนึ่ง	π
สัมประสิทธิ์ความแปรผัน	CV

บทที่ 1
บทนำ

จำนวนสุ่มถูกนำไปประยุกต์ใช้อย่างกว้างขวาง โดยเฉพาะอย่างยิ่งในด้านการสื่อสารปลอดภัยหรือวิทยาการรหัสลับ ซึ่งเป็นเทคโนโลยีเพื่อรักษาความปลอดภัยของข้อมูลจากการถูกโจรกรรม นอกจากนี้จำนวนสุ่มยังสามารถนำไปประยุกต์ใช้งานในด้านอื่นๆ เช่น การคำนวณทางวิทยาศาสตร์ การคำนวณทางคณิตศาสตร์ด้วยวิธีมอลติคาร์โล (Monte Carlo Method) การจำลองการทำงานของโปรแกรม (Simulation) และการทดสอบอุปกรณ์อิเล็กทรอนิกส์และการสื่อสาร เป็นต้น จำนวนสุ่มเป็นส่วนประกอบสำคัญอย่างหนึ่งของเทคโนโลยีการรักษาความปลอดภัยของข้อมูล ซึ่งความปลอดภัยดังกล่าวขึ้นอยู่กับความปลอดภัยของกุญแจที่สร้างขึ้น ดังนั้นจึงมีความจำเป็นที่ต้องใช้กุญแจรหัสที่ยากต่อการตีความหมายหรือการประมวลลำดับต่อไปของกุญแจจากผู้โจรกรรม กุญแจในการเข้ารหัสลับโดยทั่วไปอาศัยอัลกอริธึม (Algorithms) ที่มีความยากและซับซ้อนของคณิตศาสตร์ แต่ไม่สามารถยืนยันได้ว่าเป็นการสุ่มอย่างแท้จริง ประกอบกับคอมพิวเตอร์ได้รับการพัฒนาขีดความสามารถในการคำนวณและประมวลผลขึ้นไปอย่างมาก ดังนั้นคอมพิวเตอร์สามารถคำนวณได้อย่างรวดเร็วและแม่นยำสูงขึ้นด้วย ผู้โจรกรรมก็จะสามารถหาลำดับของกุญแจในการเข้ารหัสได้โดยใช้เวลาก็น้อยลง ความเสี่ยงในการถูกไขรหัสลับที่ปกป้องข้อมูลสำคัญก็จะเพิ่มมากขึ้นตามไปด้วย ดังนั้นในการสร้างกุญแจรหัสลับจึงควรใช้จำนวนสุ่มที่มีคุณภาพที่ยากต่อการคำนวณหรือถอดรหัสหรือมาจากแหล่งที่ผ่านการทดสอบคุณสมบัติ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องจากปัญหาด้านความปลอดภัยของข้อมูล เป็นประเด็นสำคัญที่ทุกฝ่ายต่างตระหนักกันเป็นอย่างดีว่ามีสาเหตุมาจากเทคโนโลยีการสื่อสารต่าง ๆ ได้รับการพัฒนาไปอย่างรวดเร็ว ส่งผลให้ในแต่ละช่วงเวลาจะมีข้อมูลหลายประเภทถูกส่งจากผู้ส่งไปยังผู้รับปลายทางเป็นจำนวนมาก ดังนั้นการนำเทคโนโลยีด้านการรักษาความปลอดภัยของข้อมูล ที่เรียกว่า การเข้ารหัส (Encryption) จึงถูกนำมาใช้ในงานด้านการสื่อสารเพิ่มมากขึ้น เพื่อป้องกันการถูกโจรกรรมข้อมูลที่มีความสำคัญ ซึ่งวิวัฒนาการการเข้ารหัสข้อมูลนี้ จำเป็นต้องอาศัยข้อมูลจำนวนสุ่ม เป็นองค์ประกอบสำคัญในกระบวนการการเข้ารหัสข้อมูล ซึ่งจำนวนสุ่มที่นำมาใช้สร้างเป็นกุญแจรหัสลับโดยทั่วไปได้จากกระบวนการสุ่มที่ไม่ได้รับการรับรองว่าจำนวนที่กำเนิดมานั้นเป็นจำนวนสุ่มแท้ (True Random Number) เพียงแต่ถูกคาดคะเนว่าเป็นไปได้เท่านั้น เพราะว่าจำนวนสุ่มอาจมีจุดสิ้นสุดและอาจมีการกระจายตัวที่ไม่มากพอสำหรับแหล่งกำเนิดจำนวนสุ่มเทียม (Pseudo-Random Number

Generator) จะกำเนิดจำนวนสุ่มตามจังหวะและโอกาสที่จะกลายเป็นจำนวนสุ่ม แต่ยังไม่สมบูรณ์ ดังนั้นการนำจำนวนสุ่มไปประยุกต์ใช้งาน จะทำให้เกิดความไม่น่าเชื่อถือ เมื่อนำมาใช้เป็นรหัสลับในกระบวนการเข้ารหัสข้อมูล อาจจะทำให้ผู้บุกรุกสามารถถอดรหัสลับได้ ดังนั้นแนวทางในการป้องกันปัญหาที่จะเกิดขึ้นคือการนำจำนวนสุ่มที่มาจากแหล่งกำเนิดจำนวนสุ่มแท้ (True Random Number Generator) มาใช้เป็นองค์ประกอบของกุญแจรหัสลับ โดยจำนวนสุ่มแท้ต้องเป็นจำนวนที่ไม่สามารถคาดเดาลำดับถัดไปได้ ด้วยมีโอกาสความน่าจะเป็นของการเกิดผลลัพธ์เท่าๆกันและไม่มีความสัมพันธ์กัน หัวใจในการสร้างรหัสลับเพื่อป้องกันปัญหาการถูกโจรกรรมข้อมูลมีพื้นฐานที่สำคัญที่ต้องปรับเปลี่ยนหรือสุ่ม (Random) รหัสให้มีความหลากหลายและเป็นจำนวนสุ่มที่มีคุณภาพ และที่สำคัญคือ หลังจากตรวจสอบจำนวนสุ่มได้ตามต้องการแล้วนำมาใช้งานหรือสร้างรหัสลับแล้วต้องไม่ให้บุคคลอื่นล่วงรู้ถึงรหัสสำคัญหลังจากการสุ่มสร้างแล้วโดยเด็ดขาด ปัญหาในการตรวจสอบคุณสมบัติของจำนวนสุ่มพบว่า ไม่สามารถตรวจวัดจำนวนสุ่มที่จะนำมาใช้เป็นกุญแจรหัสลับเพื่อเก็บข้อมูลที่สำคัญได้ด้วยการมองเห็นหรือการพิจารณาจากภายนอก จึงจำเป็นต้องใช้กระบวนการหรือเครื่องมือมาช่วยตัดสินใจ เพื่อพิสูจน์ให้ได้ว่าจำนวนสุ่มนั้นเป็น "จำนวนสุ่มอย่างเพียงพอ (Sufficiency Random)" [1] สาเหตุเนื่องมาจากการ ไม่มีหน่วยวัดคุณสมบัติของจำนวนสุ่มเหล่านี้ว่าเป็นจำนวนสุ่มที่มีความสมบูรณ์หรือไม่ อย่างไร ดังนั้นในวิทยานิพนธ์จึงนำหลักการและกระบวนการทดสอบทางสถิติมาใช้ทดสอบคุณสมบัติของจำนวนสุ่มเพื่อวัตถุประสงค์ดังกล่าว ซึ่งจะสามารถวัดค่าจำนวนสุ่มและบ่งบอกออกมาในรูปแบบของปริมาณได้ ทั้งนี้เพื่อเพิ่มความมั่นใจในขอบเขตที่ยอมรับได้ จึงทำการสำรวจวิธีการทดสอบคุณสมบัติของจำนวนสุ่มพบชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่มหลายชุด ดังแสดงตามตารางที่ 1.1 และชุดทดสอบทางสถิติเอ็นไอเอสที (NIST STS) เป็นชุดทดสอบที่ถูกอ้างอิงมากที่สุด[1] เนื่องจากเป็นชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่มที่ออกแบบเพื่อทดสอบจำนวนสุ่มสำหรับนำไปประยุกต์ใช้งานด้านวิทยาการรหัสลับ โดยได้รับการยอมรับจากวงการอุตสาหกรรมอย่างกว้างขวาง เนื่องด้วยเป็นชุดวิธี ทดสอบที่มีความเข้มงวดหรือมีเงื่อนไขในการทดสอบมากที่สุด นอกจากนี้ยังสามารถทดสอบจำนวนสุ่มหลายรูปแบบอีกด้วย ดังนั้นวิทยานิพนธ์นี้จึงนำเสนอศึกษาและพัฒนาชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่มโดยอ้างอิงชุดวิธีทดสอบดังกล่าว

ตารางที่ 1.1 การสำรวจชุดวิธีการทดสอบความคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ

ปีที่คิดค้น	ผู้คิดค้น/สถาบัน	ชื่อชุดการทดสอบ	สำหรับการประยุกต์ใช้งาน
1969 (2512)	โดนัล นุช (Donald Knuth)/ มหาวิทยาลัยแสตนฟอร์ด (Stanford University)	การทดสอบนุช (Knuth Test)	การจำลองการทำงาน
1995 (2538)	จอร์ช มาร์แซกเลีย (George Marsaglia) / มหาวิทยาลัยฟลอริดา (Florida State University)	การทดสอบดายฮาร์ด (DIEHARD Test)	การจำลองการทำงาน
1998 (2541)	เฮเลน กัสตาฟสัน (Helen Gustafson)/ มหาวิทยาลัยเทคโนโลยีแห่งควีนส์แลนด์ (Queensland University of Technology)	การทดสอบคริปท์เอ็กซ์เอส (Crypt-XS Test)	วิทยาการรหัสลับสำหรับจำนวนสุ่มที่กำเนิดโดยอาศัยอัลกอริธึมทางคณิตศาสตร์
1998 (2541)	จอห์น วอล์กเกอร์ (John Walker) / Random.org	การทดสอบอีเอ็นที (ENT Test)	การจำลองการทำงานและวิทยาการรหัสลับ
2001 (2544)	แอนดรู รัคคิน (Andrew Rukhin) / NIST	ชุดทดสอบทางสถิติเอ็นไอเอสที (NIST STS)	วิทยาการรหัสลับ
2001 (2544)	หลุยส์ โฟเลย์ (Louise Foley) / Random.org	โครงการนำร่องเอ็มเอสไอเอสเอส (Previous MSISS Project)	ด้านการจำลองการทำงานและวิทยาการรหัสลับ

จากการศึกษาชุดทดสอบอ้างอิง [2] พบว่าการคำนวณสถิติทดสอบเพื่อพิจารณาการผ่านการทดสอบนั้น จะพิจารณาจากการยอมรับและปฏิเสธข้อสมมติฐานที่ตั้งไว้ ชุดทดสอบอ้างอิงใช้สถิติทดสอบที่สอดคล้องกับการแจกแจงของข้อมูลสองแบบ ได้แก่ การแจกแจงปกติ (Normal Distribution) และการแจกแจงไคกำลังสอง (Chi-square Distribution) โดยใช้สถิติทดสอบ Complementary Error Function (*Erfc*) และ Incomplete Gamma Function (*Igamc*) ตามลำดับ [3] ซึ่งการคำนวณหาค่า *Erfc* และ *Igamc* รูปสมการมีความซับซ้อน เมื่อเก็บข้อมูลจำนวนมากหรือทำการทดสอบคุณสมบัติของจำนวนสุ่มหลายครั้งแล้ว จะทำให้ต้องใช้เวลาในการคำนวณและประมวลผลมาก

1.2 ความมุ่งหมายและวัตถุประสงค์ของการวิจัย

การทดสอบสมมติฐานเชิงสถิติ เป็นการทดสอบทางสถิติเพื่อแก้ปัญหาที่ต้องการตัดสินใจว่าจะยอมรับหรือปฏิเสธข้อสมมติฐานที่ได้ตั้งไว้ ทั้งนี้โดยเลือกสถิติทดสอบมาคำนวณหาค่าเพื่อให้สามารถสรุปว่าสมมติฐานนั้นเป็นจริงเพราะว่าไม่มีหลักฐานเพียงพอที่จะปฏิเสธนั่นเอง วิทยานิพนธ์นี้จึงได้นำหลักการดังกล่าวมาประยุกต์ใช้ในการทดสอบคุณลักษณะบางประการของสิ่งที่ต้องการจะศึกษาได้ นั่นคือ การทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ โดยใช้การพิสูจน์ทางคณิตศาสตร์เพื่อตรวจหาคุณสมบัติของการกำเนิดจำนวนสุ่มให้สอดคล้องกับนิยามและทฤษฎีโดยอาศัยการรับรองจากทฤษฎีความน่าจะเป็น (Probability Theory)

วิทยานิพนธ์นี้นำเสนอการพัฒนาชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่ม เพื่อให้ผู้ใช้งานมีความมั่นใจในการใช้งานจำนวนสุ่มด้านการสื่อสารปลอดภัย เนื่องจากเป็นหลักการทดสอบทางสถิติที่จำเป็นต้องเก็บข้อมูลจำนวนมาก รวมไปถึงแนวคิดการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์(Web Service) ดังนั้นจึงมุ่งพัฒนาการทดสอบดังกล่าวให้มีความ ซับซ้อนต่ำและยังคงสามารถพิสูจน์ได้ว่าจำนวนสุ่มนั้นเป็นจำนวนสุ่มเพียงพอที่จะนำมาประยุกต์ใช้งานด้านวิทยาการรหัสลับได้ โดยวัตถุประสงค์ของงานวิจัยมีดังต่อไปนี้

1.2.1 เพื่อศึกษาวิธีการทดสอบคุณสมบัติจำนวนสุ่มด้วยวิธีทางสถิติ
1.2.2 เพื่อศึกษากระบวนการพิจารณาตัดสินใจของการทดสอบคุณสมบัติของจำนวนสุ่ม
1.2.3 เพื่อพัฒนาวิธีการทดสอบให้มีความซับซ้อนต่ำและลดการใช้เวลาในการคำนวณ
1.2.4 จัดทำชุดวิธีการทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ
1.2.5 เพื่อเป็นแนวทางพัฒนาการให้บริการทดสอบคุณสมบัติจำนวนสุ่มด้วยวิธีทางสถิติผ่านระบบออนไลน์

1.3 ขอบเขตการวิจัย

วิทยานิพนธ์นี้ได้นำเสนอการศึกษาและพัฒนาวิธีการทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ โดยอ้างอิงจากชุดวิธีทดสอบคุณสมบัติของจำนวนสุ่มด้วยชุดทดสอบทางสถิติ เอ็นไอเอสที การทดสอบดังกล่าวครอบคลุมการทดสอบคุณสมบัติของจำนวนสุ่มห้าประการ [2] โดยคุณสมบัติเหล่านี้เป็นคุณสมบัติพื้นฐานของจำนวนสุ่มที่จะนำไปประยุกต์ใช้งานด้านวิทยาการรหัสลับได้แก่

- ทดสอบความถี่แบบเดี่ยว (Frequency (Monobit) Test) เพื่อหาลักษณะการแจกแจงความน่าจะเป็นและรูปแบบการแจกแจง
- ทดสอบความต่อเนื่องของจำนวนสุ่ม (Runs Test) เพื่อหาการซ้ำกันของข้อมูลและความต่อเนื่องของชุดข้อมูล
- ทดสอบเพื่อหาลักษณะคาบของชุดจำนวนสุ่ม (Discrete Fourier Transform Test)
- ทดสอบความถี่ของชุดจำนวนสุ่ม (Frequency Test within a Block) เพื่อหาลักษณะการแจกแจงของชุดข้อมูล
- ทดสอบความยาวของจำนวนสุ่มที่ซ้ำในชุดข้อมูล (Tests for the Longest Run of Ones in a Block)

กระบวนการทดสอบทางสถิติดังกล่าวมีขั้นตอนทั้งหมดห้าขั้นตอนตามลำดับดังนี้ คือ

- ขั้นตอนที่หนึ่งการตั้งสมมติฐาน
- ขั้นตอนที่สองการกำหนดระดับนัยสำคัญ (Significance Level : α)
- ขั้นตอนที่สามการกำหนดค่าวิกฤต (Critical Value)และบริเวณวิกฤต (Critical Region)
- ขั้นตอนที่สี่การเลือกสถิติทดสอบ (Test statistic)
- ขั้นตอนที่ห้าการสรุปผลการทดสอบ

วิทยานิพนธ์นี้ได้นำเสนอการพัฒนาวิธีการทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติในส่วนของการเลือกสถิติทดสอบ การกำหนดค่าวิกฤตและขอบเขตวิกฤต ซึ่งเป็นส่วนสำคัญในการกระบวนการพิจารณาการตัดสินใจของการทดสอบ โดยมีกระบวนการทำงานอยู่สอง รูปแบบคือ การคำนวณเพื่อพิจารณาการตัดสินใจของการทดสอบ โดยใช้ค่ามาตรฐาน (Standard Score: Z) สำหรับชุดข้อมูลที่มีการแจกแจงแบบปกติ และการคำนวณเพื่อตัดสินใจของการทดสอบโดยใช้สถิติทดสอบไคกำลังสอง (Test statistic Chi-Square : χ^2) สำหรับชุดข้อมูลที่มีการแจกแจงไคกำลังสองนั้นจะเป็นการลดขั้นตอนของกระบวนการทดสอบคุณสมบัติของจำนวนสุ่มรวมทั้งการคำนวณสถิติทดสอบและการพิจารณาการตัดสินใจที่มีความซับซ้อนต่ำ โดยจะส่งผลให้เวลาที่ใช้ทดสอบลดลงและยังคงมีประสิทธิภาพการทดสอบโดยสามารถพิสูจน์ได้ว่าจำนวนสุ่มนั้นเป็นจำนวนสุ่มเพียงพอที่จะนำมาประยุกต์ใช้งานด้านวิทยาการรหัสลับได้

การศึกษาและการพัฒนาการทดสอบคุณสมบัติของจำนวนสุ่มนี้ ทำการทดสอบจำนวนสุ่มที่ได้จากการกำเนิดด้วยโปรแกรมคอมพิวเตอร์และจำนวนสุ่มจากแหล่งกำเนิดควอนตัม ตัวอย่างจำนวนสุ่มชุดละ 1,000,000 บิต จำนวน 100 ชุด

1.4 ขั้นตอนในการวิจัย

งานวิจัยนี้มุ่งเน้นการศึกษาและพัฒนาการทดสอบคุณสมบัติจำนวนสุ่มด้วยวิธีทางสถิติ เพื่อนำจำนวนสุ่มมาใช้ในการงานด้านวิทยาการรหัสลับ ซึ่งมีขั้นตอนการทำงานดังต่อไปนี้

1.4.1 ศึกษาคุณสมบัติของจำนวนสุ่ม ประเภทของจำนวนสุ่มและการนำไปประยุกต์ใช้งาน

1.4.2 การสำรวจและศึกษาชุดทดสอบคุณสมบัติของจำนวนสุ่มที่นำมาใช้ในงานวิทยาการรหัสลับด้วยวิธีทางสถิติที่มีใช้ในปัจจุบัน วิเคราะห์ชุดทดสอบที่มีความเหมาะสมและเป็นมาตรฐาน

1.4.3 ศึกษาขั้นตอนและวิธีการทดสอบทางสถิติ ข้อกำหนด และทฤษฎีความน่าจะเป็น การแจกแจงแบบต่างๆ

1.4.4 ศึกษาวิธีทดสอบ โดยแยกตามคุณสมบัติของจำนวนสุ่ม เพื่อแยกความแตกต่างระหว่างจำนวนสุ่มแท้และจำนวนสุ่มเทียม

1.4.5 ศึกษาการทำงานของโปรแกรมของชุดทดสอบอ้างอิง

1.4.6 ศึกษากระบวนการใช้วิธีคำนวณสถิติทดสอบ การพิจารณาตัดสินใจของวิธีทดสอบที่มีการใช้ *Erfc* สำหรับจำนวนสุ่มที่มีการแจกแจงปกติ

1.4.7 ศึกษากระบวนการใช้สถิติทดสอบ การพิจารณาตัดสินใจของวิธีทดสอบที่มีการใช้สถิติทดสอบเป็น *Igamc* สำหรับจำนวนสุ่มที่มีการแจกแจงไคกำลังสอง

1.4.8 ออกแบบโปรแกรมทดสอบเพื่อนำกระบวนการใช้สถิติทดสอบ Z สำหรับจำนวนสุ่มที่มีการแจกแจงปกติ

1.4.9 ออกแบบโปรแกรมทดสอบนำกระบวนการใช้สถิติทดสอบ χ^2 สำหรับจำนวนสุ่มที่มีการแจกแจงไคกำลังสอง

1.4.10 วิเคราะห์ผลการทดสอบและเปรียบเทียบสัดส่วนการผ่านการทดสอบระหว่างหลักการเดิมและหลักการใหม่และการสรุปผลการวิจัย

1.5 รายละเอียดของวิทยานิพนธ์

วิทยานิพนธ์นี้แบ่งเนื้อหาออกเป็นบทย่อย 7 บท ซึ่งรายละเอียดของแต่ละบทมีดังต่อไปนี้

บทที่ 1 แสดงความเป็นมาและความสำคัญของปัญหาที่วิจัยวัตถุประสงค์การทำวิจัยขอบเขตการวิจัยและขั้นตอนการวิจัย

บทที่ 2 แสดงภาพรวมของจำนวนสุ่มและการทดสอบคุณสมบัติของจำนวนสุ่ม รวมทั้งการนำไปประยุกต์ใช้งานด้านต่างๆ

บทที่ 3 แสดงทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้องอันได้แก่ พื้นฐานความน่าจะเป็นและตัวแปรสุ่ม

บทที่ 4 แสดงทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้องอันได้แก่ การวิเคราะห์ข้อมูลและสถิติ ทฤษฎีการสุ่มตัวอย่าง การแจกแจงการสุ่มตัวอย่างและสถิติอ้างอิงหรือสถิติอนุมาน

บทที่ 5 เสนอการออกแบบโปรแกรมทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ ประกอบด้วย การนำเสนอหลักการพิจารณาการทดสอบ วิธีดำเนินการวิจัย ขั้นตอนวิธีการดำเนินการวิจัยและขอบเขตเงื่อนไขและคุณสมบัติของวิธีการทดสอบคุณสมบัติของจำนวนสุ่ม

บทที่ 6 แสดงผลการทดสอบคุณสมบัติของจำนวนสุ่มและการเปรียบเทียบผลการทดสอบกับชุดโปรแกรมอ้างอิงชุดทดสอบทางสถิติ เอ็นไอเอสที

บทที่ 7 แสดงบทสรุปของงาน ปัญหาและอุปสรรคที่เกิดขึ้น และข้อเสนอแนะแนวทางในการแก้ไขปัญหา

บทที่ 2
จำนวนสุ่มและการทดสอบคุณสมบัติ

การติดต่อสื่อสารและการรับส่งข้อมูลที่สำคัญภายในหน่วยงานต่างๆ จะมีผลกระทบต่อสังคม เศรษฐกิจ ความมั่นคงของประเทศ ดังนั้นเพื่อเป็นการปกป้องข้อมูลที่สำคัญเหล่านี้ วิทยาการรหัสลับ (Cryptography) โดยการเข้ารหัสข้อมูลจึงเป็นกระบวนการสำคัญที่จะช่วยปกป้องข้อมูลจากผู้ไม่ประสงค์ดี วัตถุประสงค์สำคัญของการวิทยาการรหัสลับคือ เพื่อการรักษาความลับ (Confidentiality) การรักษาความสมบูรณ์ (Integrity) การระบุถึงตัวบุคคลได้ (Authentication) การป้องกันการปฏิเสธความรับผิด (Non-repudiation) และการควบคุมการเข้าถึงข้อมูล (Access Control) จุดสำคัญคือให้ผู้ส่งและผู้รับสามารถติดต่อสื่อสารกันแบบลับบนช่องสื่อสารทั่วไปได้อย่างปลอดภัย วิทยาการรหัสลับมีหลักการพื้นฐาน คือ เปลี่ยนแปลงข้อความปกติ (Plaintext) ที่ผู้ส่งต้องการส่งไปให้ผู้รับให้เป็นข้อความที่ถูกเข้ารหัสไว้ (Ciphertext) โดยไม่สามารถอ่านและเข้าใจข้อความดังกล่าวได้ กระบวนการเข้ารหัส (Encryption) สามารถทำได้ดังนี้ ผู้ส่งจะใช้กุญแจในการเข้ารหัสและผู้รับซึ่งทราบกุญแจที่ใช้ในการเข้ารหัสดังกล่าวจะสามารถถอดรหัส (Decryption) เพื่อแปลงข้อความกลับเพื่อให้สามารถอ่านข้อความเดิมที่สามารถเข้าใจได้ แต่บุคคลที่สาม (Eavesdropper) จะไม่สามารถเข้าใจข้อความนั้น เนื่องจากไม่ทราบกุญแจที่ใช้เข้ารหัสของผู้ส่งและผู้รับ หัวใจสำคัญประการหนึ่ง คือ ความปลอดภัยจากการโจรกรรมข้อมูล ซึ่งความปลอดภัยของระบบวิทยาการรหัสลับทั้งแบบสมมาตร (Symmetrical Cryptography) และอสมมาตร (Asymmetrical Cryptography) ขึ้นอยู่กับความปลอดภัยของกุญแจที่สร้างขึ้นจากกระบวนการสุ่มโดยอาศัยข้อสมมติฐานที่ไม่สามารถพิสูจน์ได้ และได้รับการพัฒนามากขึ้นตามลำดับ การสร้างรหัสลับมีพื้นฐานสำคัญที่ต้องปรับเปลี่ยนหรือสุ่มให้มีความหลากหลายและเป็นจำนวนสุ่มที่มีคุณภาพ [3]

เนื่องจากจำนวนสุ่มที่ใช้เป็นกุญแจรหัสลับโดยทั่วไป ได้จากกระบวนการสุ่มที่ไม่ได้รับการรับรองว่าจำนวนที่กำเนิดมานั้นเป็นจำนวนสุ่มแท้ เพียงแต่ได้รับการคาดคะเนว่าเป็นไปได้เท่านั้น เพราะว่าจำนวนสุ่มอาจมีจุดสิ้นสุดและอาจมีการกระจายตัวที่ไม่มากเพียงพอ โดยแหล่งกำเนิดจำนวนสุ่มเทียมจะกำเนิดจำนวนสุ่มตามจังหวะโอกาสที่จะกลายเป็นจำนวนสุ่มแต่ยังไม่สมบูรณ์ การนำจำนวนสุ่มไปประยุกต์ใช้งาน จะทำให้เกิดความไม่น่าเชื่อถือ เมื่อนำมาใช้เป็นรหัสลับในกระบวนการเข้ารหัสข้อมูล จะสามารถถอดรหัสลับได้ง่ายขึ้น ปัจจัยหนึ่งเนื่องมาจากเทคโนโลยีและคอมพิวเตอร์ที่ได้รับการพัฒนาอย่างรวดเร็ว รหัสลับที่มีความซับซ้อนสูงถูกถอดได้

ในระยะเวลาที่รวดเร็วขึ้น ดังนั้นแนวทางในการป้องกันปัญหาที่จะเกิดขึ้นคือการนำจำนวนสุ่มที่มาจากกระบวนการสุ่มอย่างแท้จริง มาใช้เป็นกุญแจรหัสลับ จำนวนสุ่มอย่างแท้จริงต้องเป็นจำนวนที่ไม่สามารถคาดเดาลำดับถัดไปได้ โดยมีโอกาสความน่าจะเป็นของการเกิดผลลัพธ์เท่าๆกัน ไม่มีความสัมพันธ์กัน

2.1 จำนวนสุ่ม (Ramdom Numbers)

จำนวนสุ่ม คือ จำนวนที่เกิดขึ้นโดยไม่สามารถคาดเดาต่อผลลัพธ์ที่จะตามมา โดยมีโอกาสความน่าจะเป็นของการเกิดผลลัพธ์เท่าๆกัน มีการกระจายตัวของข้อมูลแบบสม่ำเสมอ โดยจำนวนที่ได้จากการสุ่มแต่ละครั้งจะไม่มีรูปแบบของความสัมพันธ์กันเลย ไม่มีลำดับของเหตุการณ์[4]

นิยาม

ให้ x_n เป็นลำดับของจำนวนสุ่ม เมื่อ n= 1,2,3...

x_n เป็นตัวแปรสุ่มที่มีค่าที่เป็นไปได้ 2 ค่า คือ “0” และ “1”

ถ้า $P(x_n = 1 /$ กรณีอื่น$) = 0.5$

2.1.1 คุณสมบัติของจำนวนสุ่ม

การสร้างจำนวนสุ่มเป็นการลำดับการสร้างตัวเลขที่ยากแก่การจัดรูปแบบ จึงทำให้ลำดับที่เกิดขึ้นกลายเป็นจำนวนสุ่มได้ การสร้างจำนวนสุ่มที่มีมาแต่โบราณ ได้แก่ การทอดลูกเต๋า การโยนเหรียญ การเล่นไพ่ เป็นต้น คุณสมบัติที่สำคัญของจำนวนสุ่ม [4] ได้แก่

ก. จำนวนที่เกิดขึ้นโดยปราศจากความคาดหวังต่อผลลัพธ์ที่ได้

ข. ความน่าจะเป็นของการเกิดผลลัพธ์เท่าๆกัน

ค. มีความเป็นอิสระต่อกันตามหลักสถิติ

ง. ไม่มีลำดับของผลลัพธ์ที่เกิดขึ้น

จ. ไม่สามารถคาดเดาผลลัพธ์ที่จะเกิดขึ้นได้

ฉ. จำนวนสุ่มที่สร้างขึ้นไม่มีอิทธิพลต่อการสร้างจำนวนสุ่มอื่นๆ ในลำดับถัดไป

2.1.2 ประเภทของชุดกำเนิดจำนวนสุ่ม (Random Number Generators :RNGs)

จำนวนสุ่มที่มีใช้งานสร้างหรือการกำเนิดจากหลายแหล่ง ซึ่งมีความแตกต่างด้านกายภาพ คุณลักษณะและการแปลงค่า ซึ่งสามารถแยกประเภทออกเป็นสองประเภท ดังนี้

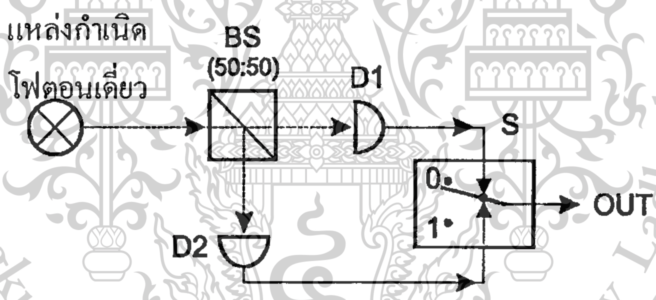
แหล่งกำเนิดจำนวนสุ่มแท้ (True Random Number Generator) และแหล่งกำเนิดจำนวนสุ่มเทียม (Pseudo random Number Generators :PRNGs)

2.1.2.1 แหล่งกำเนิดจำนวนสุ่มแท้

แหล่งกำเนิดจำนวนสุ่มแท้เป็นแหล่งกำเนิดที่ไม่สามารถคาดเดาได้ เช่น แหล่งกำเนิดเอนโทรปี (Entropy) โดยใช้กระบวนการกลั่น (Distillation Process) เพื่อเป็นการแทนค่าทางดิจิทัลจากแหล่งกำเนิดเป็นค่าศูนย์หรือหนึ่ง การกำเนิดจำนวนสุ่มแท้จากแหล่งกำเนิดเอนโทรปี เนื่องจากประกอบด้วยปริมาณทางกายภาพที่มีจำนวนมหาศาล ตัวอย่างแหล่งกำเนิด ดังนี้

ก. แหล่งกำเนิดจากแหล่งกำเนิดเชิงควอนตัม

แหล่งกำเนิดจากแหล่งกำเนิดเชิงควอนตัมด้วยโฟตอนเดี่ยวซึ่งจะใช้หน่วยที่เล็กที่สุดของแสง เรียกว่า โฟตอน (Photon) ดังขั้นตอนการกำเนิดจำนวนสุ่มดังรูปที่2.1 [5] สร้างโดยจัดอุปกรณ์ให้โฟตอนเคลื่อนที่ผ่านอุปกรณ์กระจกแยกลำแสง (Beam Splitter: BS) เมื่อแยกแสงที่ผ่านเข้ามาเป็นสองทิศทาง ได้แก่สะท้อนและทะลุผ่านกระจกดังกล่าวนี้ ซึ่งกระจกจะมีสัมประสิทธิการสะท้อนและการทะลุผ่านเท่ากัน ซึ่งจะส่งผลให้โฟตอนเคลื่อนที่ผ่านไปในทิศทางใดทิศทางหนึ่งไปยังหน่วยรับแสง (Detector : D) นั้นมีโอกาสเท่าเทียมกัน และนำไปแทนค่าเป็นค่าทางดิจิทัล คือค่าศูนย์และค่าหนึ่งได้



รูปที่ 2.1 องค์ประกอบและหลักการกำเนิดจำนวนสุ่มเชิงควอนตัมชนิดกระจกแยกลำแสง

ข. แหล่งกำเนิดจากธาตุกัมมันตรังสี

แหล่งกำเนิดจากธาตุกัมมันตรังสี (Radioactive Source) อาศัยคุณสมบัติที่เกิดจากการปลดปล่อยอนุภาค (Emitting Particles) ซึ่งจะคายพลังงานออกมาในรูปของรังสีชนิดต่างๆ ไปยังเครื่องตรวจนับแบบดูดกลืน (Absorbing Counter) โดยการเกิดกระบวนการนี้เป็นช่วงเวลาที่ไม่สามารถทำนายการเกิดปรากฏการณ์นี้ได้อย่างสมบูรณ์

ค. แหล่งกำเนิดจากสัญญาณรบกวนจากบรรยากาศ

แหล่งกำเนิดจากสัญญาณรบกวนจากบรรยากาศ (Atmospheric Noise) [4] เป็นสัญญาณรบกวนวิทยุ (Radio Noise) เกิดขึ้นจากความแปรปรวนของบรรยากาศที่ห่อหุ้มโลก เช่น ฟ้าแลบฟ้าผ่า ก่อให้เกิดคลื่นวิทยุแผ่กระจายออกไปรอบโลก ซึ่งสัญญาณรบกวนจากปรากฏการณ์ต่างๆ

เหล่านี้เกิดขึ้นอยู่ตลอดเวลา แม้จะไม่มีพายุฝนฟ้าคะนองก็ตาม สามารถดักจับสัญญาณรบกวนดังกล่าวได้โดยใช้สายอากาศ(Antenna) สัญญาณรบกวนเหล่านี้จะมีรูปแบบที่ไม่แน่นอนและไม่สามารถคาดเดาได้ ดังนั้นจึงสามารถนำมาใช้เป็นแหล่งกำเนิดจำนวนสุ่มได้ นอกจากนี้ยังสามารถใช้สัญญาณรบกวนที่เกิดจากแหล่งกำเนิดอื่นๆ ในที่ทำงานหรือห้องปฏิบัติการ เช่น พัดลมระบายอากาศของคอมพิวเตอร์ หรืออุปกรณ์ที่มีการทำงานในลักษณะที่ทำให้เกิดการสั่นได้ด้วย เป็นต้น ทั้งนี้ขึ้นอยู่กับรูปแบบการประยุกต์ที่เหมาะสม

ง. แหล่งกำเนิดจากสัญญาณรบกวนที่เกิดจากอุปกรณ์สารกึ่งตัวนำ

แหล่งกำเนิดจากสัญญาณรบกวนที่เกิดจากอุปกรณ์สารกึ่งตัวนำ (Semiconductor) เกิดจากการทำงานของอุปกรณ์ในสภาวะที่ไม่มีเสถียรภาพหรือผิดปกติสามารถปลดปล่อยสัญญาณรบกวนหรือสัญญาณสุ่มออกมาได้

ผลลัพธ์จากชุดกำเนิดจำนวนสุ่มแท้นี้จะถูกนำไปประยุกต์ใช้โดยตรง และถูกนำไปเป็นลำดับตั้งต้น (Seed) สำหรับกำเนิดจำนวนสุ่มในชุดกำเนิดจำนวนสุ่มเทียมอีกด้วย การอาศัยคุณสมบัติความเป็นจำนวนสุ่มจากปรากฏการณ์เกี่ยวกับกฎของธรรมชาติในการสร้างจำนวนสุ่ม มีข้อดี คือ สามารถสร้างจำนวนสุ่มได้เรื่อยๆ ไม่มีที่สิ้นสุดและไม่เป็นคาบหรือมีเวลาแน่นอน ไม่สามารถสร้างซ้ำขึ้นใหม่ได้ เพราะเป็นการสร้างที่ไม่มีลำดับ แต่มีข้อด้อย คือ จากการพิจารณาการสุ่มที่เกิดขึ้นตามธรรมชาติ จะต้องอาศัยการสังเกตและระยะเวลานานมาก จึงทำให้ความถี่ของการเกิดการสุ่มต่ำมาก และการสร้างหรือการแทนค่าเพื่อให้เป็นจำนวนสุ่มแท้สำหรับการใช้งานทำได้ยากกว่าการกำเนิดจำนวนสุ่มเทียม

2.1.2.1 แหล่งกำเนิดจำนวนสุ่มเทียม

หลักการโดยทั่วไป การกำเนิดจำนวนสุ่มประเภทนี้ทำได้โดยนำลำดับจำนวนสุ่มแท้เป็นลำดับตั้งต้น (Seed) หนึ่งชุดหรือมากกว่านั้น เพื่อกำเนิดจำนวนสุ่มเทียมลำดับต่อไปโดยเครื่องคอมพิวเตอร์หรือหน่วยประมวลผลโดยมีแบบแผนหรืออัลกอริทึม ในการกำเนิดที่แน่นอน จำนวนสุ่มเทียมที่ได้จากการสร้างสามารถคาดเดาได้จากฟังก์ชันของลำดับตั้งต้น กล่าวคือ ทุกจำนวนสุ่มเทียมที่ถูกสร้างขึ้นถูกจำกัดการกำเนิดด้วยลำดับตั้งต้นและการคาดเดากระบวนการกำเนิดจำนวนสุ่มเทียมนำไปสู่การคำนวณเทอมหรือรูปแบบของจำนวนสุ่มดังกล่าว เนื่องจากแต่ละองค์ประกอบของลำดับสุ่มเทียมสามารถสร้างหรือกำเนิดชุดจำนวนสุ่มเทียมใหม่ได้จากลำดับตั้งต้น

2.1.3 การประยุกต์ใช้งานจำนวนสุ่ม

จำนวนสุ่มถูกนำไปประยุกต์ใช้งานได้หลากหลาย ดังตัวอย่างที่จะนำเสนอต่อไปนี้

2.1.3.1 วิทยาการรหัสลับ

การนำไปใช้เป็นรหัสลับในเทคโนโลยีด้านการรักษาความปลอดภัยของข้อมูล เรียกว่าวิทยาการรหัสลับ ที่ถูกนำมาใช้เพื่อปกป้องข้อมูลที่สำคัญจากผู้ไม่ประสงค์ดีที่จะเข้ามาล่วงรู้ในช่อง

การสื่อสาร ซึ่งการเข้ารหัสข้อมูลนี้ จำเป็นต้องอาศัยข้อมูลจำนวนสุ่ม เป็นองค์ประกอบสำคัญในกระบวนการการสร้างรหัสข้อมูล โดยไม่ให้บุคคลที่สามสามารถถอดรหัสและอ่านข้อมูลสำคัญดังกล่าวได้ หลักการที่เกี่ยวข้องกับวิทยาการรหัสลับที่จำเป็นต้องใช้กุญแจรหัสเป็นองค์ประกอบได้แก่ การลงลายมือชื่อดิจิทัล (Digital Signatures) การเข้ารหัสข้อความเพื่อระบุถึงตัวบุคคล (Message Authentication Codes) วิธีการเข้ารหัส (Encryption Algorithms) [6][7]

2.1.3.2 การทดสอบอุปกรณ์อิเล็กทรอนิกส์และการสื่อสาร

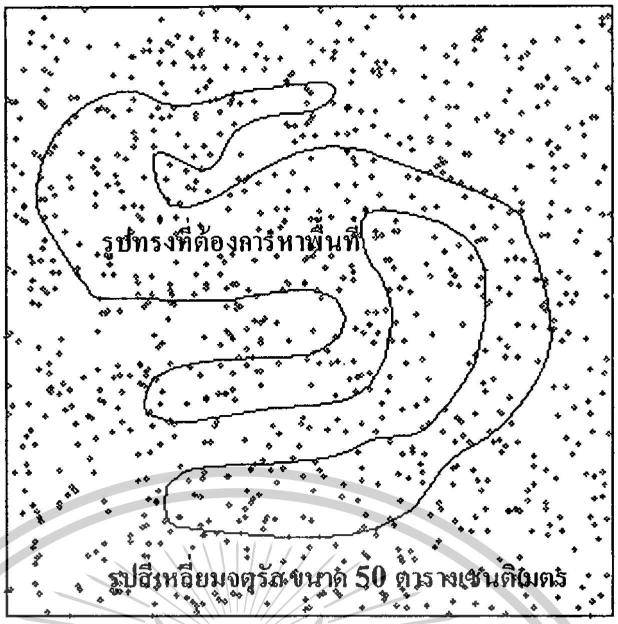
การทดสอบอุปกรณ์อิเล็กทรอนิกส์และการสื่อสารหรือการแก้ปัญหาของเครื่องมือ การทดสอบประสิทธิภาพของอุปกรณ์ดังกล่าว เพื่อให้สามารถทราบถึงการทำงานของอุปกรณ์รวมทั้งกรณีที่ทำให้อุปกรณ์ไม่สามารถทำงานได้ และประเมินอายุการใช้งานของอุปกรณ์ดังกล่าวได้ เพื่อหาวิธีแก้ไขและป้องกันการเกิดกรณีที่อุปกรณ์ไม่สามารถทำงานได้ก่อนหมดอายุการใช้งาน โดยสุ่มสถานการณ์มีความเป็นไปได้ทั้งหมดลงไป เพื่อจำลองการทำงานให้รูปแบบ หรือสถานการณ์ต่างๆ กันออกไป ซึ่งการจำลองนี้ได้ใส่ความเป็นไปได้ทั้งหมดแบบสุ่มลงไป เพื่อให้สามารถทดสอบอุปกรณ์ดังกล่าวว่าสามารถทำงานได้ในทุกกรณีอย่างแท้จริง

2.1.3.2 การจำลองการสืบทอดทางพันธุกรรม

การสืบทอดทางพันธุกรรม อาศัยสารพันธุกรรม หรือดีเอ็นเอ (Deoxy-ribonucleic acid : DNA) ซึ่งเป็นกรดนิวคลีอิก (Nucleic acid) ที่ทำหน้าที่เก็บข้อมูลทางพันธุกรรมของสิ่งมีชีวิต เป็นส่วนผสมของพ่อและแม่ถ่ายทอดไปสู่รุ่นถัดๆ ไป เป็นการคัดสรรทางธรรมชาติก่อนเกิดเป็นวิวัฒนาการ ดีเอ็นเอมีหน้าที่สำคัญสองประการ คือ การจำลองตัวเอง ดีเอ็นเอของสิ่งมีชีวิตมีความสามารถสร้างและจำลองตัวมันเอง ขณะเกิดกระบวนการแบ่งเซลล์ เพื่อสร้างดีเอ็นเอที่เหมือนเดิมทุกประการให้แก่เซลล์ใหม่ และการถ่ายทอดข้อมูลผ่านอาร์เอ็นเอ ดีเอ็นเอสามารถถูกถอดรหัสเพื่อทำหน้าที่กำหนดการเรียงตัวของกรดอะมิโนทำให้สิ่งมีชีวิตสามารถสืบทอดลักษณะประจำพันธุ์และดำรงเผ่าพันธุ์อยู่ได้ วิทยาการทางคอมพิวเตอร์ได้ใช้แนวคิดการสืบทอดทางพันธุกรรมนี้มาเป็นเทคนิคที่เรียกว่าขั้นตอนวิธีแบบพันธุกรรม (Genetic algorithm) ซึ่งจำลองการกระบวนการถ่ายทอดสารพันธุกรรมนี้ขึ้น โดยอาศัยกระบวนการสุ่มเพื่อจำลองกระบวนสร้างให้ออกมาได้ลัพธ์เสมือนจริงที่สุดหรือเหมือนธรรมชาติสร้างมากที่สุดเพื่อประโยชน์ดังกล่าว

2.1.3.2 การประมาณค่าทางคณิตศาสตร์

ศึกษาการทำงานของตัวแบบทางคณิตศาสตร์ที่ซับซ้อนบางอย่างอาจจะยากที่จะคำนวณถึงสิ่งที่เป็นไปได้ทั้งหมดอย่างครบถ้วนสมบูรณ์ เช่น การคาดสภาพอากาศล่วงหน้า การคาดการณ์อุณหภูมิล่วงหน้าเป็นต้น โดยสร้างสถานการณ์จำลองจำนวนมากภายใต้พฤติกรรมเชิงสุ่มของตัวแปร และทำนายให้ใกล้เคียงกับเหตุการณ์หรือความเป็นจริงที่จะเกิดขึ้นมากที่สุดหรือ ตัวอย่างดังรูปที่ 2.2 วิธีมอลติคาร์โล (Monte Carlo Method) การหาพื้นที่ของรูปทรงที่คำนวณได้ยาก ขั้นตอนการคำนวณคร่าวๆ สามารถทำได้โดยการนำรูปทรงที่ต้องการหาพื้นที่ไปวางบนรูปทรงเรขา-



รูปที่ 2.2 การคำนวณหาพื้นที่รูปทรงต่างๆ โดยใช้วิธี Monte Carlo

คณิตที่ทราบขนาด จากนั้นทำการกระจายจำนวนสุ่มลงไปเต็มพื้นที่และนับจุดที่ปรากฏบนพื้นที่ที่ต้องการหาเทียบกับจำนวนจุดที่สุ่มลงไปทั้งหมด เป็นหลักการที่จะทำให้ทราบถึงพื้นที่ของรูปทรงที่ต้องการทราบได้ เป็นต้น

จากเนื้อหาข้างต้นจะพบว่าจำนวนสุ่มถูกนำไปประยุกต์ใช้อย่างกว้างขวาง ดังนั้นเพื่อการนำจำนวนสุ่มไปใช้งานได้อย่างปลอดภัยและมีประสิทธิภาพสูงสุด จึงจำเป็นต้องมีการทดสอบคุณสมบัติของจำนวนสุ่มก่อนการนำไปใช้งาน ซึ่งจะกล่าวถึงรายละเอียดในลำดับถัดไป

2.2 การทดสอบคุณสมบัติของจำนวนสุ่ม (Randomness Testing)

การทดสอบคุณสมบัติของจำนวนสุ่มก่อนนำไปประยุกต์ใช้งานมีความจำเป็นอย่างยิ่ง เพื่อเป็นการบ่งบอกให้ทราบขั้นต้นว่าจำนวนสุ่มดังกล่าวมาจากแหล่งกำเนิดจำนวนสุ่มอย่างแท้จริงหรือไม่ และมีคุณสมบัติเพียงพอที่จะนำไปประยุกต์ใช้งานเพื่อความปลอดภัยหรือไม่ แต่เนื่องจากไม่สามารถตรวจวัดจำนวนสุ่มที่จะนำมาใช้เป็นกุญแจรหัสลับเพื่อเก็บข้อมูลที่สำคัญได้ด้วยการมองด้วยตาเปล่า จึงจำเป็นต้องใช้กระบวนการหรือเครื่องมือมาช่วยตัดสินใจ เพื่อพิสูจน์ให้ได้ว่าจำนวนสุ่มนั้นเป็นจำนวนสุ่มอย่างเพียงพอ [1] จากการที่ไม่มีหน่วยวัดคุณสมบัติของจำนวนสุ่มเหล่านี้ว่าเป็นจำนวนสุ่มที่มีความสมบูรณ์หรือไม่อย่างไร ดังนั้นจึงนำหลักการและกระบวนการทดสอบทางสถิติมาใช้ทดสอบคุณสมบัติของจำนวนสุ่มเพื่อวัตถุประสงค์ดังกล่าว ซึ่งจะสามารถวัดค่าและบ่งบอกออกมาในรูปแบบของปริมาณได้ ทั้งนี้เพื่อเพิ่มความมั่นใจในขอบเขตที่ยอมรับได้

การทดสอบทางสถิติ จะใช้หลักการทางคณิตศาสตร์เพื่อคำนวณและตรวจหาคุณสมบัติของการกำเนิดจำนวนสุ่มให้สอดคล้องกับนิยามและทฤษฎี โดยนำจำนวนสุ่มที่เกิดจากกระบวนการกำเนิดมาทดสอบโดยใช้ข้อมูลทางสถิติวิเคราะห์และประเมินผลว่าจำนวนสุ่มที่ทำการทดสอบนั้นมีคุณสมบัติของจำนวนสุ่มมากเพียงใดจากผลลัพธ์ที่แสดงออกมา โดยแบ่งเป็นแต่ละชุดวิธีการทดสอบตามคุณสมบัติของจำนวนสุ่มเพื่อตรวจหาความแตกต่างระหว่างจำนวนสุ่มแท้และเทียมในทุกๆคุณสมบัติ

2.2.1 การสำรวจงานวิจัยที่เกี่ยวข้อง (Literature Review)

จากการสำรวจงานวิจัยที่เกี่ยวข้องกับการทดสอบความคุณสมบัติของจำนวนสุ่ม[1] พบว่ามีชุดทดสอบหลายชุดที่อ้างอิงหลักการทางสถิติ และมีวัตถุประสงค์เพื่อทดสอบจำนวนสุ่มเพื่อการนำไปใช้งานด้านวิทยาการรหัสลับ ด้านการจำลองการทำงานทางคณิตศาสตร์ วิทยาศาสตร์และวิศวกรรมศาสตร์ ซึ่งจะมีความแตกต่างด้านเงื่อนไขการทดสอบ ดังจะกล่าวในรายละเอียดต่อไป

การทดสอบคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ มีเป้าหมายเพื่อตรวจหาความแตกต่างระหว่างจำนวนสุ่มแท้และจำนวนสุ่มเทียม จำนวนสุ่มชุดใดชุดหนึ่งไม่ผ่านการทดสอบบางวิธีจะถือว่าไม่ผ่านการทดสอบและไม่ใช่จำนวนสุ่มอย่างแท้จริง สำหรับจำนวนสุ่มชุดใดชุดหนึ่งที่ผ่านการทดสอบทั้งหมด ผลสรุปของการทดสอบทางสถิติจะถือว่าจำนวนสุ่มนั้นเป็นจำนวนสุ่มอย่างแท้จริง ทั้งนี้เป็นการอ้างอิงจากทฤษฎีความน่าจะเป็น ชุดการทดสอบทางสถิติจากการสำรวจพบว่ามีหลายชุดการทดสอบ ดังนี้

การทดสอบนุธ (Knuth Test)

จากการสำรวจพบว่าการทดสอบนุธเป็นชุดการทดสอบที่ถูกนำมาอ้างอิงมากที่สุดในการทดสอบความคุณสมบัติของจำนวนสุ่มด้วยวิธีทางสถิติ ซึ่งคิดค้นโดย โดนัล นุธ (Donald Knuth) เจ้าของหนังสือเรื่อง “The Art of Computer Programming, Volume 2” โดนัล นุธ ได้รับการยกย่องว่าเป็นนักปราชญ์ด้านจำนวนสุ่ม และชุดทดสอบนุธได้รับอ้างอิงเพื่อเป็นมาตรฐานการทดสอบในยุคเริ่มแรก

การทดสอบดายฮาร์ด (DIEHARD Test)

คิดค้นโดย จอร์ช มาร์แซกเลีย (George Marsaglia) ซึ่งเป็นการพัฒนาต่อยอดจากการทดสอบนุธ เพื่อตรวจหาจำนวนสุ่มเทียม [8] และได้รับการแก้ไขจากการทดสอบเดิม เนื่องจากการทดสอบนุธมีเงื่อนไขการผ่านการทดสอบที่ง่าย และพัฒนาเป็นชุดทดสอบที่ใช้บนคอมพิวเตอร์ ถึงแม้ว่าชุดทดสอบนี้ไม่ได้รับการพัฒนาต่อหลังจากจอร์ช มาร์แซกเลีย เกษียณ แต่ชุดทดสอบนี้ก็ได้รับการอ้างอิงอย่างกว้างขวาง

การทดสอบคริปท์ เอ็กซ์เอส (Crypt-XS Test)

ชุดทดสอบคริปท์ เอ็กซ์เอส ถูกพัฒนาขึ้นโดยนักวิจัย Information Security Research Centre มหาวิทยาลัยเทคโนโลยีแห่งควีนส์แลนด์ ประเทศออสเตรเลียและเป็นชุดซอฟต์แวร์ที่ใช้ในเชิงธุรกิจ โดยมุ่งเน้นที่จะทดสอบจำนวนสุ่มที่กำเนิดจากอัลกอริทึม หรือ จำนวนสุ่มเทียม

การทดสอบอีเอ็นที (ENT Test)

ปี พ.ศ. 25441(ค.ศ. 1998) จอห์น วอล์กเกอร์ (John Walker) ได้พัฒนาชุดทดสอบอีเอ็นทีเพื่อใช้สำหรับทดสอบเพื่อหาว่าจำนวนสุ่มที่นำมาทดสอบมีคุณสมบัติของความไม่เป็นจำนวนสุ่มหรือไม่ ชุดโปรแกรมทดสอบนี้ถูกใช้เพื่ออธิบายจำนวนสุ่มเทียมที่นำมาใช้ด้านการเข้ารหัสและการประยุกต์ใช้งานด้านอื่นที่เกี่ยวข้องกับความหนาแน่นของข่าวสาร

ชุดทดสอบทางสถิติ เอ็นไอเอสที (NIST STS)

ปี พ.ศ. 2544 (ค.ศ. 2001) NIST ได้พัฒนาชุดทดสอบชื่อ เอ็นไอเอสที [2] เป็นชุดทดสอบที่ประกอบด้วยวิธีการทดสอบทั้งหมด 16 วิธี ซึ่งถูกพัฒนาขึ้นเพื่อใช้สำหรับทดสอบคุณสมบัติของจำนวนสุ่มของลำดับไบนารีที่กำเนิดขึ้นโดยฮาร์ดแวร์หรือซอฟต์แวร์ที่จะนำไปใช้สำหรับงานด้านวิทยาการรหัสลับ ชุดทดสอบนี้เป็นผลงานวิจัยระหว่าง Computer Security Division และ the Statistical Engineering Division ของ NIST ซึ่งเป็นชุดซอฟต์แวร์ที่รองรับการทดสอบชุดข้อมูลจำนวนสุ่มที่อยู่ในแบบฟอร์มของไบนารี และยังสามารถทดสอบได้ทั้งจำนวนสุ่มที่มาจากการกำเนิดโดยใช้อัลกอริธึมและจำนวนสุ่มที่มาจากการพัฒนาชุดกำเนิดจำนวนสุ่มด้วยหลักการใหม่ ชุดทดสอบของเอ็นไอเอสที ถือได้ว่าเป็นชุดทดสอบมาตรฐานที่ใหญ่และครอบคลุมการทดสอบคุณสมบัติของจำนวนสุ่มมากที่สุด

โครงการนำร่องเอ็มเอสไอเอสเอส (Previous MSISS Project)

ปี พ.ศ. 2544 (ค.ศ. 2001) หลุยส์ โฟเลย์ (Louise Foley)ได้นำเสนอชุดวิธีการทดสอบประกอบด้วยวิธีการทดสอบ 5 วิธีและ Random.org ใช้เป็นมาตรฐานการทดสอบทดแทนชุดโปรแกรมทดสอบอีเอ็นที ซึ่งมีคำแนะนำว่า เป็นชุดทดสอบที่ใช้งานได้ง่าย และมีความเหมาะสมอย่างตรงไปตรงมา

จากการวิเคราะห์ของ Random.org [9] ชุดวิธีการทดสอบสองชุดที่ใกล้เคียงกันและถูกอ้างอิงมากที่สุด ได้แก่ ชุดทดสอบทางสถิติ เอ็นไอเอสที และการทดสอบดายฮาร์ด ด้วยเหตุผลที่ดังนี้ หนึ่ง เป็นมาตรฐานที่ยอมรับกันอย่างกว้างขวางจากการสำรวจและในวงการอุตสาหกรรม

ถ้าผ่านการทดสอบของเอ็นไอเอสที สามารถกล่าวได้ว่าผ่านมาตรฐานการทดสอบในเชิงอุตสาหกรรม และสามารถนำไปเปรียบเทียบระหว่างชุดการกำเนิดจำนวนสุ่มได้ง่าย

สอง เป็นชุดการทดสอบที่เข้มงวดมากที่สุด โดยออกแบบเพื่อทดสอบสำหรับใช้จำนวนสุ่มสำหรับวิทยาการรหัสลับ ซึ่งต้องผ่านเงื่อนไขการทดสอบมากที่สุด

สาม ถูกนำมาเข้ารหัสแบบ Advanced Encryption Algorithm (AES) ซึ่งเป็นการเข้ารหัสที่ถูกเชื่อว่าสามารถปกป้องข่าวสารด้านความลับของรัฐบาลได้

สี่ ออกแบบเพื่อทดสอบจำนวนสุ่มในรูปแบบของไบนารี ลำดับไบนารี

จากเหตุผลข้างต้น จึงเป็นเหตุผลที่วิทยานิพนธ์นี้เลือกศึกษาและพัฒนาชุดวิธีการทดสอบโดยอ้างอิงชุดทดสอบทางสถิติเอ็นไอเอสที ซึ่งเป็นชุดวิธีทดสอบทางสถิติที่ครอบคลุมการทดสอบคุณสมบัติของจำนวนสุ่มมากที่สุด และมุ่งเน้นสำหรับการนำจำนวนสุ่มไปใช้งานด้านวิทยาการรหัสลับโดยใช้หลักการทดสอบสมมติฐานทางสถิติ ชุดทดสอบทางสถิติ เอ็นไอเอสที มีรายละเอียดดังตารางที่ 2.1 และ 2.2 ชุดทดสอบนี้มีวัตถุประสงค์เพื่อแยกความแตกต่างจากคุณสมบัติของจำนวนสุ่มแท้และจำนวนสุ่มเทียม เป็นการหาจุดบกพร่องของจำนวนสุ่มเทียม และสรุปผลเพื่อบ่งบอกว่าจำนวนสุ่มที่นำมาทดสอบ ไม่ได้กำเนิดจากแหล่งกำเนิดจำนวนสุ่มอย่างแท้จริง นอกจากนี้ได้เปรียบเทียบวิธีการทดสอบระหว่างวิธีทดสอบทางสถิติเอ็นไอเอสทีและชุดการ ทดสอบอื่นๆ ดังตารางที่ 2.3

ตารางที่ 2.1 ภาพรวมการทดสอบของชุดทดสอบทางสถิติเอ็นไอเอสที

ชุดทดสอบทางสถิติ เอ็นไอเอสที		
วิธีการทดสอบ	ข้อผิดพลาดที่ค้นพบ (Defect Detected)	คุณสมบัติ (Property)
Frequency (Monobit)	มีจำนวนบิต "0" หรือ "1" มากเกินไป	เท่าเทียมกัน (global)
Frequency (block)	มีจำนวนบิต "0" หรือ "1" มากเกินไป	เท่าเทียมกัน (local)
Runs test	การแกว่ง(Oscillation) ของจำนวนบิต "0" และ "1" เร็วหรือช้าเกินไป	ไม่อิสระอย่างต่อเนื่อง (local)
Longest run of ones in a block	การแกว่ง(Oscillation) ของจำนวนบิต "0" และ "1" เร็วหรือช้าเกินไป	ไม่อิสระอย่างต่อเนื่อง (global)
Binary matrix rank	ความคลาดเคลื่อนจากขอบเขตการแจกแจงที่คาดหวังไว้	ไม่เป็นอิสระเชิงเส้น
Discrete Fourier transform (spectral)	รูปแบบที่เกิดขึ้นซ้ำๆ กัน	คาบไม่เป็นอิสระ
Non-overlapping template matching	รูปแบบเฉพาะที่ปรากฏขึ้นผิดปกติ (ไม่เป็นระเบียบ)	คาบ ไม่เป็นอิสระและเท่าเทียมกัน
Overlapping template matching	รูปแบบเฉพาะที่ปรากฏขึ้นผิดปกติ (ไม่เป็นระเบียบ)	คาบ ไม่เป็นอิสระและเท่าเทียมกัน
Maurer's universal statistical	ลำดับถูกบีบอัด	ไม่เป็นอิสระและเท่าเทียมกัน
Linear complexity	Linear feedback shift register (LFSR) สั้นเกินไป	ไม่เป็นอิสระ
Serial	ไม่มี uniformity ในการแจกแจงร่วมกันสำหรับ m-length sequence	เท่าเทียมกัน
Approximate entropy	ไม่มี uniformity ในการแจกแจงร่วมกันสำหรับ m-length sequence	เท่าเทียมกัน

ตารางที่ 2.1 (ต่อ) ภาพรวมการทดสอบของชุดทดสอบทางสถิติเอ็นไอเอสที

วิธีการทดสอบ	ข้อผิดพลาดที่ค้นพบ (Defect Detected)	คุณสมบัติ (Property)
Cumulative sums (Cusum)	มีจำนวนบิต "0" หรือ "1" มากเกินไปที่จุดแรกหรือหลังในลำดับ	ไม่เป็นอิสระอย่างต่อเนื่อง
Random excursions	ความคลาดเคลื่อนจากการแจกแจงของจำนวนของการตรวจสอบของ random walk ที่สถานะหนึ่งๆ	ไม่เป็นอิสระอย่างต่อเนื่อง
Random excursions variants	ความคลาดเคลื่อนจากการแจกแจงของจำนวนของการตรวจสอบ(ตรงข้ามกับ random walk) ที่สถานะหนึ่งๆ	ไม่เป็นอิสระอย่างต่อเนื่อง

ตารางที่ 2.2 ภาพรวมชุดทดสอบทางสถิติ เอ็นไอเอสที ตามคุณสมบัติของจำนวนสุ่ม

ลักษณะของ String ที่ตรงกับลักษณะของ Random Walk	ลักษณะของรูปแบบ (Pattern)		ความซับซ้อนและการบีบอัด (Complexity/ Compression)
Frequency	Runs	Longest Run	Rank
Block Frequency	Aperiodic Template	Universal Statistical	Spectral
Cumulative Sum	Periodic Template	Serial	Lempel - ZivComplexity
Random Excursions (Variant)	Approximate Entropy		Linear Complexity

ตารางที่ 2.3 การเปรียบเทียบวิธีการทดสอบระหว่างวิธีทดสอบทางสถิติ เอ็นไอเอสที และชุดการทดสอบอื่นๆ [9]

วิธีทดสอบ	นูธ	ดายฮาร์ด	คริปท์เอ็กซ์เอส	เอ็นไอเอสที	อีเอ็นที	เอ็มเอสไอเอสเอส
Frequency	1		1	1		
Serial	1			1		
Gap	1					
Poker/Partition	1					
Coupon Collector's	1					
Permutation	1					
Runs	1	1	1	1		1
Maximum-of-t	1					
Collision	1					
Birthday Spacings	1	1				
Serial Correlation	1				1	
Tests on Subsequences	1					
Overlapping Permutations		1				
Binary rank test for 32x32 matrices		1		1		1
Ranks of 6x8 matrices		1				
Monkey tests on 20-bit words		1				
Monkey tests OPSO, OQSO, DNA		1				

ตารางที่ 2.3 (ต่อ) การเปรียบเทียบวิธีการทดสอบระหว่างวิธีทดสอบทางสถิติ เอ็นไอเอสที และชุดการทดสอบอื่นๆ [9]

วิธีทดสอบ	นุธ	ดายฮาร์ด	คริปท์เอ็กซ์เอส	เอ็นไอเอสที	อีเอ็นที	เอ็มเอสไอเอสเอส
Count the 1's in a stream of bytes		1				
Count the 1's in specific bytes		1				
Parking lot		1				
Minimum distance		1				
Random spheres		1				
Squeeze		1				
Overlapping Sums		1				1
Craps		1				
Binary Derivative			1			
Change Point			1			
Sequence Complexity			1			
Linear Complexity			1	1		
Frequency test within a block				1		
Longest run of 1's in a block				1		
Discrete fourier transform (spectral)				1		

ตารางที่ 2.3 (ต่อ) การเปรียบเทียบวิธีการทดสอบระหว่างวิธีทดสอบทางสถิติ เอ็นไอเอสที และชุดการทดสอบอื่นๆ [9]

วิธีทดสอบ	นูธ	ดายฮาร์ด	คริปท์ เอ็กซ์เอส	เอ็นไอ เอสที	อีเอ็นที	เอ็มเอสไอ เอสเอส
Non-overlapping template matching				1		
Overlapping template matching				1		
Maurer's universal statistical				1		
Approximate Entropy				1	1	
Cumulative sums (cusum)				1		
Random Excursions				1		
Random Excursions Variants				1		
Chi-square					1	1
Arithmetic Mean					1	
Monte Carlo Value for Pi					1	
Reverse arrangements						1
จำนวนวิธีทดสอบ	12	15	6	15	5	5

2.2.2 การวิเคราะห์ชุดทดสอบทางสถิติเอ็นไอเอสที

จากการศึกษาชุดทดสอบทางสถิติ เอ็นไอเอสที ดังตารางที่ 2.1 และ 2.2 และบทวิเคราะห์ของ Information Technology Promotion Agency ของประเทศญี่ปุ่น [9] เป็นบทวิเคราะห์เรื่องการจัดลำดับความสำคัญของการทดสอบ รวมถึงความซ้ำซ้อนของการทดสอบที่มีลักษณะที่เหมือนกันแตกต่างเพียงการตรวจจับบิตที่แตกต่างไปจากเดิมเท่านั้น เช่น Overlapping template matching และ Non-overlapping template matching เป็นต้น จากการวิเคราะห์ข้างต้นได้อ้างอิงมีการเลือกชุดทดสอบชุดเล็กประกอบด้วยเจ็ดวิธีทดสอบ ได้แก่ Frequency (block) Test Longest run of ones in a block Discrete Fourier transform(spectral) Non-overlapping template matching Serial Cumulative sums(cusum) และ Random excursions และการเปรียบเทียบวิธีการทดสอบระหว่างวิธีทดสอบทางสถิติเอ็นไอเอสทีและชุดการทดสอบอื่นๆ ดังตารางที่ 2.3 ดังนั้นวิทยานิพนธ์นี้จึงเสนอการศึกษาและพัฒนาการทดสอบคุณสมบัติจำนวนสุ่มที่อ้างอิงชุดทดสอบทางสถิติเอ็นไอเอสที โดยมีการจัดลำดับความสำคัญและการเปรียบเทียบกับชุดการทดสอบอื่นๆ ซึ่งครอบคลุมการทดสอบคุณสมบัติของจำนวนสุ่ม 5 ประการ ดังที่ได้กล่าวไปแล้วในบทที่ 1 โดยคุณสมบัติเหล่านี้เป็นคุณสมบัติพื้นฐานของจำนวนสุ่มที่จะนำไปประยุกต์ใช้งานด้านวิทยาการรหัสลับและเพื่อเป็นแนวทางการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์ที่มีความซับซ้อนต่ำ เวลาในการประมวลผลและการตัดสินใจรวดเร็วและยังคงมีประสิทธิภาพของการทดสอบคุณสมบัติของจำนวนสุ่มได้เช่นเดียวกันกับวิธีอ้างอิง

บทที่ 3

ความน่าจะเป็นและตัวแปรสุ่ม

การศึกษาและอธิบายคุณลักษณะของการสุ่ม จะนำหลักการตัดสินใจทางวิศวกรรมมาช่วยอธิบาย โดยหลักการดังกล่าวเป็นวิธีทางสถิติที่มีการดำเนินการภายใต้สภาวะควบคุม (Controlled Condition) ผลลัพธ์ที่ได้จากการศึกษาดังกล่าวนี้ เรียกว่า ค่าสังเกต (Observed Value) ซึ่งเป็นค่าที่ใช้ในการตัดสินใจ แต่ค่าสังเกตนี้ไม่สามารถนำมาทำนายความน่าจะเป็นของภาพรวมทั้งหมดได้ ดังนั้นจึงต้องอาศัยทฤษฎีความน่าจะเป็น (Probability Theory) เพื่ออธิบายและวิเคราะห์ลักษณะของการสุ่ม ซึ่งเป็นการอธิบายความคลาดเคลื่อนของข้อมูลว่ามีระดับความน่าเชื่อถือของเหตุการณ์ที่จะเกิดขึ้นว่าเป็นเท่าไหร่ โดยทฤษฎีความน่าจะเป็นมีพื้นฐานมาจากเรื่องเซต ดังนั้นบทนี้จะกล่าวถึงเรื่องเซตพื้นฐานเป็นลำดับแรก [7] แล้วจึงจะอธิบายเรื่องทฤษฎีความน่าจะเป็นในลำดับถัดไป

3.1 เซต (Sets)

เซต (Sets) หมายถึง การรวบรวมสิ่งที่สนใจเป็นกลุ่ม มีสมาชิก (Element) แน่นอน โดยใช้อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ A B C แทนชื่อเซต และอักษรภาษาอังกฤษตัวพิมพ์เล็กแทนสมาชิก a b c โดยจะใช้สัญลักษณ์ $x \in A$ แทน x เป็นสมาชิกของ A และ $x \notin A$ แทน x ไม่เป็นสมาชิกของ A กรณีที่ A เป็นเซตที่ไม่มีสมาชิก จะเรียกเซต A ว่า **เซตว่าง** โดยจะสัญลักษณ์ $A=\phi$ ในการศึกษาเกี่ยวกับเรื่องความน่าจะเป็นนั้น เซตจะถูกนำมาใช้ในการหาค่าความน่า จะเป็นของเหตุการณ์ที่เกี่ยวเนื่องกัน โดยมีตัวดำเนินการเกี่ยวกับเซต (Set Operation) ดังนี้

3.1.1 ยูเนียน (Union)

ยูเนียน (Union) เขียนแทนด้วยสัญลักษณ์ $A \cup B$ หมายถึง ผลการทดลองที่เกิดเป็นเหตุการณ์ A หรือเหตุการณ์ B เขียนแทนด้วย $A \cup B = \{x / x \in A \vee x \in B\}$

3.1.2 อินเตอร์เซคชัน (Intersection)

อินเตอร์เซคชัน (Intersection) เขียนแทนด้วยสัญลักษณ์ $A \cap B$ หมายถึง ผลการทดลองที่เกิดขึ้นเป็นเหตุการณ์ A และเหตุการณ์ B เขียนแทนด้วย $A \cap B = \{x / x \in A \wedge x \in B\}$

3.1.3 คอมพลีเมนต์ (Complement)

คอมพลีเมนต์ (Complement) เขียนแทนด้วยสัญลักษณ์ A' หมายถึง ผลการทดลองที่ไม่ได้เป็นสมาชิกของ A เขียนแทนด้วย $A'=\{x/x\in U, x\notin A\}$

3.1.4 ซับเซท (Subset)

ซับเซท (Subset) เขียนแทนด้วยสัญลักษณ์ $A\subset B$ หมายถึง เหตุการณ์ A จะเป็นซับเซทของเหตุการณ์ B ก็ต่อเมื่อสมาชิกทุกตัวของ A เป็นสมาชิกของ B

การดำเนินการเกี่ยวกับเซตนี้จะนำไปเป็นพื้นฐานอธิบายและการหาค่าความน่าจะเป็นที่จะกล่าวในหัวข้อถัดไป

3.2 ความน่าจะเป็น (Probability)

ความน่าจะเป็น (Probability) [10] คือตัวเลขที่แสดงถึงโอกาสในการเกิดเหตุการณ์ที่สนใจสำหรับการทดลองหนึ่งๆ สามารถหาได้จากอัตราส่วนระหว่างจำนวนครั้งของการเกิดเหตุการณ์นั้นต่อจำนวนครั้งของเหตุการณ์ที่เกิดขึ้นทั้งหมดเช่น ความน่าจะเป็นของการเกิดเหตุการณ์ A หรือ $P(A)$ คือจำนวนครั้งของการเกิดเหตุการณ์ A ที่เกิดขึ้นทั้งหมด N_A ครั้งต่อจำนวนครั้งของเหตุการณ์ที่เกิดขึ้นทั้งหมดในแซมเปิลสเปซ (N) ดังสมการ

$$P(A)=\frac{N_A}{N} \quad ;N\to\infty \tag{3.1}$$

จากสมการความน่าจะเป็นของเหตุการณ์ใดเหตุการณ์หนึ่งมีค่าอยู่ระหว่าง [0,1] ถ้าความน่าจะเป็นของเหตุการณ์ A ที่เกิดขึ้นมีค่าเท่ากับหนึ่ง ($P(A)$=1) แล้ว ผลจากการทดลองนั้นจะมีเหตุการณ์ A เกิดขึ้นเสมอ แต่ถ้าความน่าจะเป็นของเหตุการณ์ A มีค่าเท่ากับศูนย์ แสดงว่าผลของการทดลองจะไม่มีเหตุการณ์ A เกิดขึ้นอย่างแน่นอน นอกจากนี้เมื่อพิจารณาเหตุการณ์ที่เกิดขึ้นสองเหตุการณ์โดย ให้ A เป็นเหตุการณ์ที่หนึ่งและ B เป็นอีกเหตุการณ์ที่สอง จำนวนเหตุการณ์ที่การทดลองครั้งที่หนึ่งจะเกิดเหตุการณ์ A หรือเหตุการณ์ B คือ N_{A+B} ซึ่งจะเรียกเหตุการณ์ที่เกิดนี้ว่าเหตุการณ์ที่ยูเนียนกัน โดยที่เหตุการณ์นี้จะเกิดขึ้นอย่างเป็นอิสระ ก็ต่อเมื่อ $A\cap B=\phi$ ดังนั้นค่าของความน่าจะเป็นในการเกิดเหตุการณ์ A หรือเหตุการณ์ B แสดงดังต่อไปนี้

$$
\begin{aligned}
P(A \cup B) &= \frac{N_{A+B}}{N} \\
&= \frac{N_A}{N} + \frac{N_B}{N} \\
&= P(A) + P(B)
\end{aligned}
$$

ถ้าเหตุการณ์ A และเหตุการณ์ B เป็นเหตุการณ์ที่ไม่เป็นอิสระต่อกันหรือ $A \cap B \neq \phi$ ความน่าจะเป็นของผลจากการทดลองที่เกิดเหตุการณ์ A หรือเหตุการณ์ B แสดงได้ดังนี้

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(A) = P(A \cap B') + P(A \cap B)$$

$$P(B) = P(B \cap A') + P(A \cap B)$$

ดังนั้น $$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$P(A \cap B)$ คือความน่าจะเป็นที่เหตุการณ์ A และเหตุการณ์ B เกิดร่วมกัน เรียกว่า **ความน่าจะเป็นร่วม** เขียนแทนด้วย

$$P(A \cap B) = \frac{N_{AB}}{N} \qquad N \to \infty \tag{3 .2}$$

เมื่อ N_{AB} คือ จำนวนครั้งในการเกิดเหตุการณ์ A และ B พร้อมกันหรือ $A \cap B$

จากสมการที่ (3.1) ถึงสมการที่ (3.2) สามารถสรุปคุณสมบัติของความน่าจะเป็นได้ดังต่อไปนี้

- $P(A) \geq 0$ หมายถึงความน่าจะเป็นคืออัตราส่วนระหว่างจำนวนเหตุการณ์ A ที่เกิดขึ้นต่อจำนวนเหตุการณ์ที่เกิดขึ้นทั้งหมด ดังนั้นจึงทำให้ความน่าจะเป็นมีค่าอยู่ระหว่าง [0,1]
- $P(S) = 1$ คือ ความน่าจะเป็นของแซมเปิลสเปซ (Sample Space: S) จะมีค่าเท่ากับหนึ่งเสมอ
- ถ้าหาก $A \cap B = \phi$ แล้ว $P(A \cup B) = P(A) + P(B)$ และถ้า $A \cap B \neq \phi$ แล้ว จะได้ $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

นอกจากนี้ความน่าจะเป็นอาจหาได้จากประสบการณ์หรือผลลัพธ์ที่เกิดขึ้นก่อนหน้า โดยการวิเคราะห์เงื่อนไขต่างๆ ของการทดลองโดยการสันนิษฐานจากการทดลองที่กระทำซ้ำหลายครั้ง โดยสังเกตจากความถี่ของเหตุการณ์ที่สนใจ ซึ่งจะมีวิธีการกำหนดความน่าจะเป็นให้แก่ผลลัพธ์ของการทดลองอย่างสุ่ม ดังนี้

กรณีที่ 1 ถ้า S เป็นแซมเปิลสเปซแบบจำกัดของการทดลองอย่างสุ่ม มีจำนวนผลลัพธ์เป็น n กำหนดความน่าจะเป็นให้กับผลลัพธ์คือ p_i โดยที่ p_i มีคุณสมบัติดังนี้

- $0 \leq p_i \leq 1$ เมื่อ i = 1,2,3,…,n
- $p_1 + p_2 + p_3 + \ldots + p_n = 1$ เขียนแทนด้วยสัญลักษณ์ $\sum_{i=1}^{n} p_i = 1$

ความน่าจะเป็นของเหตุการณ์ A คือผลรวมของความน่าจะเป็นของผลลัพธ์ทั้งหมดที่เกิดขึ้นในเหตุการณ์ A เขียนแทนด้วย

$$P(A) = \sum_{i=1}^{n} p_i = 1 \qquad (3.3)$$

กรณีที่ 2 ถ้า S เป็นแซมเปิลสเปซแบบอนันต์ของการทดลองอย่างสุ่ม p_i มีคุณสมบัติดังนี้

- $0 \leq p_i \leq 1$ เมื่อ i = 1,2,3,…,n
- $p_1 + p_2 + p_3 + \ldots + p_n = 1$ เขียนแทนด้วยสัญลักษณ์ $\sum_{i=1}^{\infty} p_i = 1$

กรณีที่ 3 ถ้า S เป็นแซมเปิลสเปซแบบจำกัด และผลลัพธ์ของแต่ละตัวมีโอกาสเกิดขึ้นเท่ากัน (Equally Likely) หรือ $p_1 = p_2 = p_3 = \ldots = p_n = 1/n$ แล้ว เขียนแทนด้วย

$$P(A) = \frac{n(A)}{n} \qquad (3.4)$$

3.2.1 ความน่าจะเป็นแบบมีเงื่อนไขและความเป็นอิสระต่อกันเชิงสถิติ

เมื่อเกิดเหตุการณ์บางเหตุการณ์ขึ้นและเหตุการณ์ดังกล่าวนั้นส่งผลทำให้เกิดเหตุการณ์อีกเหตุการณ์หนึ่งตามมาแล้วจะเรียกเหตุการณ์ที่เกิดขึ้นในลักษณะนี้ว่า *เหตุการณ์แบบมีเงื่อนไข* (Conditional Probability) เช่น เมื่อมีเหตุการณ์ A เกิดขึ้นแล้วเหตุการณ์ A ส่งผลให้เกิดเหตุการณ์ B ตามมา สัญลักษณ์ที่ใช้แทนความน่าจะเป็นของการเกิดเหตุการณ์นี้ คือ $P(B|A)$ แต่ถ้ามีเหตุการณ์ A เกิดขึ้นแล้วเหตุการณ์ A ไม่ได้ส่งผลไปยังอีกเหตุการณ์หนึ่ง จะเรียกเหตุการณ์ที่เกิดขึ้นนี้ว่าเป็นเหตุการณ์ที่เป็นอิสระต่อกัน โดยมีความน่าจะเป็นหลายรูปแบบ ดังนี้

กรณีที่ 1 ความน่าจะเป็นแบบมีเงื่อนไข

ความน่าจะเป็นแบบมีเงื่อนไขหาได้จากสมการ

$$P(B/A) = \frac{P(A \cap B)}{P(A)} \tag{3.5}$$

ถ้า $P(A)$ ไม่เท่ากับศูนย์ แล้ว $P(B/A)$ คือความน่าจะเป็นแบบมีเงื่อนไขเมื่อการเกิดของเหตุการณ์ B ขึ้นอยู่กับเหตุการณ์ A

เมื่อเหตุการณ์ A และเหตุการณ์ B เกิดขึ้นอย่างเป็นอิสระต่อกัน ดังนั้นเหตุการณ์ B จะไม่ขึ้นอยู่กับการเกิดของเหตุการณ์ A แล้ว $P(A \cap B) = 0$ ดังนั้น $P(B/A) = 0$ แต่ถ้าความน่าจะเป็นของของเหตุการณ์ A ขึ้นอยู่กับเหตุการณ์ B แล้วความน่าจะเป็นแบบมีเงื่อนไขสามารถหาค่าได้จากสมการ

$$P(A/B) = \frac{P(A \cap B)}{P(B)} \tag{3.6}$$

เมื่อ $P(B)$ ไม่เท่ากับศูนย์แล้ว จากสมการที่ (3.5) และ (3.6) จะได้

$$P(A \cap B) = P(A|B)P(B) \text{ หรือ} \tag{3.7}$$

$$P(A \cap B) = P(B|A)P(A)$$

กำหนดให้ $B_1, B_2, B_3, \ldots, B_n$ เป็นเหตุการณ์ที่มีอิสระต่อกันและผลรวมของเหตุการณ์ที่เกิดขึ้นทั้งหมดเท่ากับแซมเปิลสเปซ (S) เหตุการณ์ A สามารถแสดงความสัมพันธ์กับเหตุการ B ได้ดังต่อไปนี้

$$
\begin{aligned}
A &= A \cap S \\
&= A \cap (B_1 \cup B_2 \cup \ldots \cup B_n) \\
&= (A \cap B_1) \cup (A \cap B_2) \cup \ldots \cup (A \cap B_n)
\end{aligned}
$$

จากสมการที่ (3.7) ความน่าจะเป็นของเหตุการณ์ A สามารถหาได้โดย [7]

$$
\begin{aligned}
P(A) &= P(A \cap B_1) + P(A \cap B_2) + \ldots + P(A \cap B_n) \\
&= P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \ldots + P(A \mid B_n)P(B_n)
\end{aligned} \tag{3.8}
$$

การหาความน่าจะเป็นของเหตุการณ์ที่เกิดขึ้นในขั้นตอนสุดท้าย (Posterior Probability) สามารถหาได้ด้วยหลักการพื้นฐานของกฎของเบย์ (Baye's Theory) เขียนแทนด้วย $P(B_j/A)$ สมมติให้ $B_1, B_2, B_3, \ldots, B_n$ เป็นหนึ่งในเหตุการณ์ที่อยู่ในแซมเปิลสเปซ (S) และกำหนดให้มีเหตุการณ์ A เกิดขึ้น ดังนั้นความน่าจะเป็นที่เกิดเหตุการณ์ B_j จากเหตุการณ์ A จากสมการที่ (3.7) จะแสดงดังสมการ

$$
\begin{aligned}
P(B_j \mid A) &= \frac{P(B_j \cap A)}{P(A)} \\
&= \frac{P(A \mid B_j)P(B_j)}{P(A)}
\end{aligned} \tag{3.9}
$$

และจากสมการที่ (3.8) สมการที่ (3.9) จะสามารถเขียนอีกรูปแบบหนึ่งได้ดังนี้

$$P(B_j \mid A) = \frac{P(A \mid B_j)P(B_j)}{\sum_{i=1}^{n} P(A \mid B_i)P(B_i)} \tag{3.10}$$

กรณีที่ 2 ความน่าจะเป็นที่เป็นอิสระต่อกันทางสถิติ

เมื่อการทดลองมีเหตุการณ์ A และเหตุการณ์ B เกิดขึ้นเหตุการณ์ทั้งสองจะถูกเรียกว่าเป็น **เหตุการณ์ที่เป็นอิสระต่อกันทางสถิติ** ก็ต่อเมื่อผลคูณระหว่างความน่าจะเป็นในการเกิดเหตุการณ์ A และความน่าจะเป็นในการเกิดเหตุการณ์ B มีค่าเท่ากับความน่าจะเป็นร่วมระหว่างเหตุการณ์ A และเหตุการณ์ B ดังสมการ

$$P(A \cap B) = P(A) \times P(B) \tag{3.11}$$

จากสมการที่ (3.7) สามารถที่จะเขียนสมการที่ (3.11) ได้ใหม่ดังนี้

$P(A \mid B) = P(A)$ เมื่อ $P(B) \neq 0$ หรือ

$P(A \mid B) = P(A)$ เมื่อ $P(A) \neq 0$

ดังนั้นจึงสามารถสรุปได้ว่าเหตุการณ์ที่เป็นอิสระต่อกันทางสถิตินั้นต้องเป็นไปตามเงื่อนไขต่อไปนี้

$$P(A \cap B) = P(A) \times P(B)$$

$$P(A \mid B) = P(A)$$

$$P(A \mid B) = P(A)$$

หากเหตุการณ์สองเหตุการณ์เป็นอิสระต่อกันและมีความน่าจะเป็นไม่เท่ากับศูนย์ ซึ่งเหตุการณ์ทั้งสองอาจจะไม่เป็นเหตุการณ์ที่เป็นอิสระต่อกันทางสถิติก็ได้ นอกจากนี้ถ้าหากมีเหตุการณ์เกิดขึ้นมากกว่าสองเหตุการณ์ เช่น $A_1, A_2, A_3, \ldots, A_n$ เหตุการณ์เหล่านี้จะเรียกว่าเป็นเหตุการณ์ที่เป็นอิสระต่อกันทางสถิติก็ต่อเมื่อ

$$P(A_1 \cap A_1 \cap A_3 \cap \ldots \cap A_n) = P(A_1)P(A_2)P(A_3)\ldots P(A_n)$$

3.3 ตัวแปรสุ่ม (Random Variable)

จากการทดลองอย่างสุ่ม ผลลัพธ์ส่วนใหญ่ที่เกิดขึ้นจะเป็นเหตุการณ์ เช่น "หัวหรือก้อย" "มีหรือไม่มี" "มืดหรือสว่าง" เป็นต้น ดังนั้น ถ้าให้ E คือการทดลองที่มี แซมเปิลสเปซ S และ X คือฟังก์ชันที่กำหนดจำนวนจริง จะได้ X(e) ให้กับทุกผลลัพธ์ที่ $e \in S$ โดยจะเรียก X(e) ว่าตัวแปรสุ่ม (Random Variable) [4] ตัวอย่างการสร้างตัวแปรสุ่ม เช่น การโยนเหรียญหนึ่งเหรียญ ความน่าจะเป็นในการเกิดหัวและก้อยมีโอกาสเกิดขึ้นเท่ากันคือ 1/2 ถ้ากำหนดให้เหตุการณ์ A คือเหตุการณ์ในการเกิดหัวและเหตุการณ์ B เป็นเหตุการณ์ในการเกิดก้อย กำหนดให้ตัวแปรสุ่ม x มีค่าเท่ากับ "1" แทนเหตุการณ์ A และตัวแปรสุ่ม x มีค่าเท่ากับ "0" แทนเหตุการณ์ B ดังนั้น จะได้ตัวแปรสุ่ม $X(1)=P(A)=1/2$ และ $X(0)=P(B)=1/2$ โดยตัวแปรสุ่มแบ่งออกเป็นสองชนิดได้แก่ ตัวแปรสุ่มแบบไม่ต่อเนื่อง (Discrete Random Variable) หมายถึงตัวแปรสุ่มที่มีเรนจ์สเปซ (Range Space) เป็นเซตนับได้ (Countable Set) ตัวอย่างเช่น จำนวนนักเรียนในห้องหนึ่ง เป็นต้น และตัวแปรสุ่มแบบต่อเนื่อง (Continuous Random Variable) หมายถึงตัวแปรสุ่มที่มีเรนจ์สเปซเป็นเซตนับไม่ได้ (Uncountable Set) ตัวอย่างเช่น ระยะเวลาการใช้งานหลอดไฟแต่ละหลอดในแต่ละวันของครอบครัวทั้งหมดในประเทศไทย เป็นต้น เมื่อนำหลักการของความน่าจะเป็นมาวิเคราะห์ตัวแปรสุ่มจะได้คุณสมบัติของตัวแปรสุ่มดังต่อไปนี้

3.3.1 ฟังก์ชันความหนาแน่นของความน่าจะเป็น

ฟังก์ชันความหนาแน่นของความน่าจะเป็น (Probability Density Function: PDF) เป็นฟังก์ชันระหว่างตัวแปรสุ่ม X และค่าความน่าจะเป็นของการเกิดตัวแปรสุ่มนั้นหรือ $P(x)$ ซึ่งจะบอกถึงโอกาสในการเกิดเหตุการณ์ดังกล่าว รูปแบบของฟังก์ชันความหนาแน่นของความน่า จะเป็นแบ่งได้ตามรูปแบบของตัวแปรสุ่มดังต่อไปนี้

3.3.1.1 ฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบไม่ต่อเนื่อง

ถ้าหากว่าตัวแปรสุ่มเป็นแบบตัวแปรสุ่มที่ไม่ต่อเนื่องแล้ว จะสามารถเขียนฟังก์ชันความหนาแน่นของความน่าจะเป็นได้ดังสมการ

$$f(x)=\sum_{i=1}^{n} P(x_i)\delta(x-x_i) \tag{3.12}$$

เมื่อ n คือจำนวนเหตุการณ์ที่เกิดขึ้นทั้งหมด และ $P(x_i)$ คือความน่าจะเป็นของเหตุการณ์

3.3.1.2 ฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่อง

สำหรับตัวแปรสุ่มแบบต่อเนื่อง การที่จะกำหนดตัวค่าความน่าจะเป็นให้ตัวแปรสุ่มแบบต่อเนื่องจะไม่สามารถทำได้โดยตรง เนื่องจากจะทำให้ผลของความน่าจะเป็นจะมีค่าเท่ากับศูนย์ [4] ดังนั้นในการหาความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่องจึงต้องหาค่าความน่าจะเป็นระหว่าง ค่าสองค่า เช่น $P(a \le x < b)$ หรือ $P(a \le x < a + \Delta a)$ โดยคุณสมบัติฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่องจะมีคุณสมบัติเหมือนกับตัวแปรสุ่มแบบไม่ต่อเนื่อง ดังนี้คือ

ก. $f(x) \ge 0$

ข. $\int_{-\infty}^{\infty} f(x)dx = 1$

ค. $P(a \le x < b) = \int_{a}^{b} f(x)dx$

3.3.2 ฟังก์ชันแจกแจงสะสม

ฟังก์ชันแจกแจงสะสม(Cumulative Distribution Function: CDF) เป็นฟังก์ชันที่ใช้สำหรับวิเคราะห์ความน่าจะเป็นของตัวแปรสุ่ม โดยฟังก์ชันแจกแจงสะสมเป็นผลรวมของความน่าจะเป็นหรือแทนได้โดย $P(X \le x)$ ซึ่งรายละเอียดของฟังก์ชันแจกแจงสะสมมีดังต่อไปนี้

3.3.2.1 ฟังก์ชันแจกแจงสะสมของตัวแปรสุ่มแบบไม่ต่อเนื่อง

กำหนดให้ X(s) คือตัวแปรสุ่มแบบไม่ต่อเนื่อง (Discrete Random Variable) เมื่อนำหลักการของความน่าจะเป็นมาวิเคราะห์ตัวแปรสุ่มแบบไม่ต่อเนื่อง โดยพิจารณาเฉพาะเพียงเหตุการณ์ที่ $X \le x$ ดังนั้นความน่าจะเป็นของเหตุการณ์ที่เกิดขึ้นนี้คือ $P(X \le x)$ โดยที่ $-\infty \le x \le \infty$ ซึ่งเรียกความน่าจะเป็นของเหตุการณ์ $X \le x$ นี้ว่าฟังก์ชันแจกแจงสะสมของตัวแปรสุ่ม X ดังสมการต่อไปนี้

$$F(x) = P(X \le x) \qquad ; -\infty \le x \le \infty \tag{3.13}$$

เมื่อ $F(x)$ คือฟังก์ชันแจกแจงสะสม

เนื่องจาก $F(x)$ จะแสดงในรูปของความน่าจะเป็น ดังนั้นฟังก์ชันแจกแจงสะสมจึงมีค่าอยู่ระหว่าง $0 \le F(x) \le 1$ และ $F(-\infty) = 0, F(\infty) = 1$ โดยค่าฟังก์ชันแจกแจงสะสมของตัวแปรสุ่ม

แบบไม่ต่อเนื่องสามารถหาได้จากผลรวมของฟังก์ชันความหนาแน่นของความน่าจะเป็นดังสมการต่อไปนี้

$$F_X(x) = \sum_{i=1}^{n} P(x_i) \qquad (3.14)$$

3.3.2.2 ฟังก์ชันแจกแจงสะสมของตัวแปรสุ่มแบบต่อเนื่อง

จากฟังก์ชันความหนาแน่นของความน่าจะเป็นของตัวแปรสุ่มแบบต่อเนื่อง (Continuous Random Variable) ค่าความน่าจะเป็น $P(a < x < b)$ คือความน่าจะเป็นระหว่าง a และ b ถ้าทำการหาค่าของความน่าจะเป็นระหว่าง $-\infty$ ถึงค่าใดค่าหนึ่งเช่น a หรือ $P(-\infty < x < a)$ แล้วค่าความน่าจะเป็นที่ได้จะเรียกว่าฟังก์ชันแจกแจงสะสมของ a หรือ $F(a)$ โดยนิยามของฟังก์ชันแจกแจงสะสมเป็นดังสมการ

$$\begin{aligned} F(a) &= P(X \le a) \\ &= \int_{-\infty}^{a} f(x)dx \end{aligned} \qquad (3.14)$$

เมื่อ a อยู่ระหว่าง $(-\infty, \infty)$

3.3.3 ค่าเฉลี่ยของตัวแปรสุ่ม

นอกจากฟังก์ชันความหนาแน่นของความน่าจะเป็น (PDF) และฟังก์ชันการแจกแจงสะสม (CDF) ที่ใช้อธิบายลักษณะของตัวแปรสุ่ม (Random Variable)แล้ว ยังสามารถวัดคุณสมบัติของตัวแปรสุ่มอีกหลายวิธีที่ใช้บ่งบอกถึงลักษณะของตัวแปรสุ่ม เช่น ค่าเฉลี่ยของตัวแปรสุ่ม (Mean) เป็นต้น โดยค่าเฉลี่ยของตัวแปรสุ่ม X ใช้สัญลักษณ์แทนคือ $\overline{X}$ และใช้สัญลักษณ์ *E[X]* แทนกระบวนการหาค่าเฉลี่ย เรียกว่า การคาดคะเนของตัวแปรสุ่ม X (Expectation of X หรือ Statistical Averaging) ซึ่งค่าเฉลี่ยมีความสัมพันธ์กับค่าของฟังก์ชันความหนาแน่นของความน่าจะเป็นโดยเป็นค่าที่บอกถึงศูนย์กลางของการกระจายของผลลัพธ์ที่ได้จากการทดลอง หรือค่ากึ่งกลางของฟังก์ชันความหนาแน่นของความน่าจะเป็น โดยค่าเฉลี่ยของตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาได้ดังสมการ

$$\bar{X}=E(X)=\sum_{i=1}^{k} x_i P(x_i) \tag{3.15}$$

เมื่อ X_i เป็นตัวแปรสุ่มแบบไม่ต่อเนื่องและ $P(x_i)$ เป็นค่าความน่าจะเป็นของตัวแปรสุ่มแบบไม่ต่อเนื่อง

กรณีของตัวแปรสุ่มแบบต่อเนื่องค่าเฉลี่ยสามารถหาค่าได้จากฟังก์ชันความหนาแน่นของความน่าจะเป็นดังต่อไปนี้

$$\bar{X}_i=E(X)=\int_{-\infty}^{\infty} x P_x(x)dx \tag{3.16}$$

3.3.4 ค่าเบี่ยงเบนมาตรฐานและความแปรปรวนของตัวแปรสุ่ม

ค่าเฉลี่ยของตัวแปรสุ่มเป็นเพียงค่าหนึ่งที่ใช้บอกคุณสมบัติของตัวแปรสุ่มแต่ค่านี้ยังไม่สามารถให้รายละเอียดได้อย่างชัดเจน เช่น ถ้าค่าเฉลี่ยมีค่าเท่ากับศูนย์ ค่านี้อาจจะแสดงถึงผลจากการทดลองในเหตุการณ์หนึ่ง ซึ่งให้ผลออกมามีค่าเท่ากับศูนย์ทั้งหมดหรือผลจากการทดลองมีค่าที่ไม่เท่ากับศูนย์รวมมาอยู่ด้วย ดังนั้นเพื่อเป็นการวัดการกระจาย โอกาสของผลการทดลองจึงใช้ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) เขียนแทนด้วย σ_x เพื่อนำมาใช้วัดการกระจายของค่าตัวแปรสุ่มออกจากค่าเฉลี่ยหรือจุดกึ่งกลางของการกระจายตัว โดยค่าเบี่ยงเบนมาตรฐานนั้นสามารถมีได้ทั้งค่าบวกหรือค่าลบ ดังนั้นผลการวัดนี้อาจจะสามารถทำให้อยู่ในรูปแบบของขนาดของการกระจายตัวที่มีค่าเป็นบวกเสมอ โดยนำค่าเบี่ยงเบนมาตรฐานยกกำลังสองจะได้ค่าทางสถิติที่เรียกว่า “**ความแปรปรวน** ”(Variance: σ_x^2) สามารถหาค่าความแปรปรวนได้ดังนี้

ค่าความแปรปรวนของตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาได้จาก

$$\sigma_x^2=E[(X-(\bar{X}_i))^2] \tag{3.17}$$

กระจายสมการได้ $E[X^2-2X(\bar{X}_i)+(\bar{X}_i)^2]=E[X^2]-2(\bar{X}_i)E[X]+(\bar{X}_i)^2$

$$=(\bar{x^2})-2(\bar{X}_i)^2+(\bar{X}_i)^2$$

$$=(\bar{x^2})-(\bar{X_i})^2$$

3.3.5 ค่าเฉลี่ยของตัวแปรสุ่มหลายตัวแปร

การหาค่าเฉลี่ยหรือค่าคาดหวัง (Expected Value) ของตัวแปรสุ่มสองตัวขึ้นไป ตัวแปรสุ่มนั้นสามารถหาได้ดังเช่นการหาค่าเฉลี่ยของตัวแปรสุ่มหนึ่งตัวแปรสุ่มเช่น การหาค่าค่าเฉลี่ยของฟังก์ชัน $Z = g(X,Y)$ สามารถหาได้ดังต่อไปนี้ [7]

$$E(Z) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x,y)f_{X,Y}(x,y)dxdy \tag{3.18}$$

กรณีที่ตัวแปรสุ่ม Z เป็นตัวแปรสุ่มแบบต่อเนื่อง $f_{X,Y}(x,y)$ คือฟังก์ชันความหนาแน่นของความน่าจะเป็นร่วมระหว่างตัวแปรสุ่ม X และตัวแปรสุ่ม Y ในกรณีของตัวแปรสุ่มไม่ต่อเนื่องค่าเฉลี่ยแสดงได้ดังต่อไปนี้

$$E(Z) = \sum_{i}\sum_{n} g(x_i,y_n)p_{X,Y}(x_i,y_n) \tag{3.19}$$

เมื่อ $p_{X,Y}(x_i,y_n)$ คือความน่าจะเป็นร่วมระหว่างตัวแปรสุ่ม X และตัวแปรสุ่ม Y

สำหรับค่าเฉลี่ยของผลคูณของตัวแปรสุ่มคือผลคูณของค่าเฉลี่ยของตัวแปรสุ่มแต่ละตัวแปรสุ่มเมื่อตัวแปรสุ่มในแต่ละตัวแปรสุ่มเป็นอิสระต่อกันดังสมการ

$$E(X_1X_2...X_n) = E(X_1)E(X_2)....E(X_n) \tag{2.20}$$

3.3.6 ค่าความสัมพันธ์ของตัวแปรสุ่มสองตัวแปรสุ่ม

เมื่อทำการหาค่าเฉลี่ยของฟังก์ชัน $G(X,Y) = X^i Y^j$ เรียกว่าโมเมนต์ร่วม โดยที่ i และ j ของตัวแปรสุ่ม X และตัวแปรสุ่ม Y สามารถแสดงได้ดังต่อไปนี้

กรณีของตัวแปรสุ่ม X และตัวแปรสุ่ม Y เป็นตัวแปรสุ่มแบบต่อเนื่องสามารถหาได้จาก

$$E(Z) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^i y^j f_{X,Y}(x,y)dxdy \qquad (3.21)$$

กรณีของตัวแปรสุ่ม X และตัวแปรสุ่ม Y เป็นตัวแปรสุ่มแบบไม่ต่อเนื่องสามารถหาได้จาก

$$E(Z) = \sum_m \sum_n x_m^i y_n^j p_{X,Y}(x_i, y_n) \qquad (3.22)$$

ถ้า i เท่ากับศูนย์จะได้ค่าโมเมนต์ (Moment) ของตัวแปรสุ่ม Y ถ้า j เท่ากับศูนย์จะได้ค่าโมเมนต์ของตัวแปรสุ่ม X หาก i และ j เท่ากับหนึ่งจะเรียกว่าค่าเฉลี่ยหรือ $E(XY)$ นี้ว่าความสัมพันธ์ของตัวแปรสุ่ม X และ Y (Correlation of X and Y) หาก $E(XY) = 0$ จะได้ว่าตัวแปรสุ่ม X และตัวแปรสุ่ม Y ตั้งฉากกัน (Orthogonal)

3.3.7 โควาร์เรียนของตัวแปรสุ่ม

จากการหาความสัมพันธ์ระหว่างตัวแปรสุ่ม X และ Y หากทำการหาค่าเฉลี่ยของฟังก์ชัน แสดงได้ดังต่อไปนี้

$$E\{(X - E[X])^i (Y - E[Y])^j\} \qquad (3.23)$$

จากสมการที่ 3.23 จะได้ข้อสรุปของการหาโควาร์เรียนดังนี้คือ $E\{(X - E[X])^i (Y - E[Y])^j\}$

ถ้า $i = 2$ และ $j = 0$ จะได้ค่าของความแปรปรวนของตัวแปรสุ่ม X และในทำนองเดียวกัน หาก $j = 2$ และ $i = 0$ จะได้ความแปรปรวนของตัวแปรสุ่ม Y หาก $i = 1$ และ $j = 1$ จะเรียกว่า โควาร์เรียน (Covariance) ของตัวแปรสุ่ม X และตัวแปรสุ่ม Y ดังนี้

$$COV(X,Y) = E\{(X - E[X])(Y - E[Y])\} \tag{3.24}$$

หรือ

$$COV(X,Y) = E[XY] - E[X]E[Y] \tag{3.25}$$

หากตัวแปรสุ่มทั้งสองเกิดขึ้นอย่างเป็นอิสระต่อกันแล้วค่าของโควาร์เรียนจะมีค่าเท่ากับศูนย์ ซึ่งสัมประสิทธิ์ความสัมพันธ์ระหว่างตัวแปรสุ่ม X และ ตัวแปรสุ่ม Y สามารถหาได้ดังนี้

$$p_{X,Y} = \frac{COV(X,Y)}{\sigma_X \sigma_Y} = \frac{E[(X - E[X])(Y - E[Y])]}{\sigma_X \sigma_Y} \tag{3.26}$$

เมื่อ σ_X คือส่วนเบี่ยงเบนมาตรฐานของตัวแปรสุ่ม X หรือ $\sigma_X = \sqrt{VAR(X)}$ และ σ_Y คือส่วนเบี่ยงเบนมาตรฐานของตัวแปรสุ่ม Y หรือ $\sigma_Y = \sqrt{VAR(Y)}$

ค่าของ $p_{X,Y}$ จะมีค่าอยู่ระหว่าง [-1,1] ซึ่งจะบ่งบอกถึงระดับความสัมพันธ์ (Correlation) ระหว่างตัวแปรสุ่ม หาก $p_{X,Y}$ มีค่าเท่ากับหนึ่ง นั่นคือตัวแปรสุ่มทั้งสองตัวจะมีความสัมพันธ์กัน และ หาก $p_{X,Y}$ เท่ากับศูนย์ นั่นคือตัวแปรสุ่มทั้งสองไม่มีความสัมพันธ์กัน หากตัวแปรสุ่มสองตัวมีความเป็นอิสระต่อกันตัวแปรสุ่มทั้งสองอาจจะมีความสัมพันธ์กันหรือไม่มีความสัมพันธ์กันก็ได้ [41] เนื่องจากค่าโควาร์เรียนของตัวแปรสุ่มที่มีอิสระต่อกันเท่ากับศูนย์

3.4 การแจกแจงความน่าจะเป็น

การแจกแจงความน่าจะเป็นของตัวแปรสุ่ม ใช้อธิบายพฤติกรรมเกี่ยวกับค่าเฉลี่ยและความแปรปรวนของตัวแปรสุ่ม ซึ่งจะบ่งบอกถึงรูปแบบและลักษณะของชุดตัวแปรสุ่มว่าข้อมูลทั้งชุดมีลักษณะปกติ สมมาตร เบ้ โค้งหรือไม่ อย่างไร และมากน้อยเพียงใด ในวิทยานิพนธ์นี้จะเน้นการแจกแจงปกติและการแจกแจงไคกำลังสอง ซึ่งจะกล่าวในรายละเอียดในลำดับถัดไป

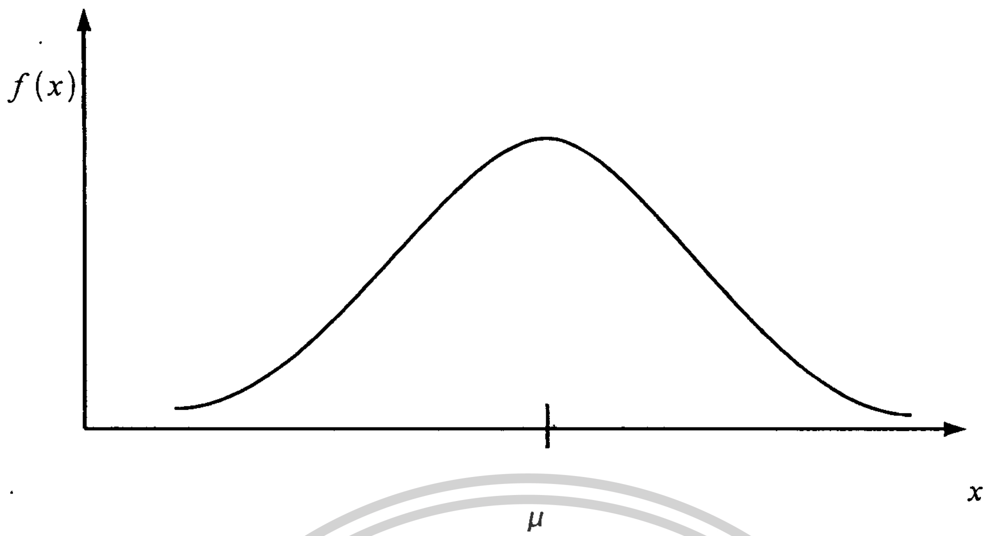
3.4.1 การแจกแจงปกติ

การแจกแจงปกติ (Normal Distribution) มีลักษณะเป็นเส้นโค้งที่มีความสมมาตรรูปทรงระฆังคว่ำ (Bell Shape) ดังรูปที่ 3.1 มีการกระจายตัวรอบค่ากลางค่าหนึ่ง ขนาดของรูปทรงหรือความกว้างของโค้งการแจกแจงจะขึ้นอยู่กับพารามิเตอร์สองค่า คือ ค่าเฉลี่ย (μ) และส่วนเบี่ยงเบนมาตรฐาน (σ)

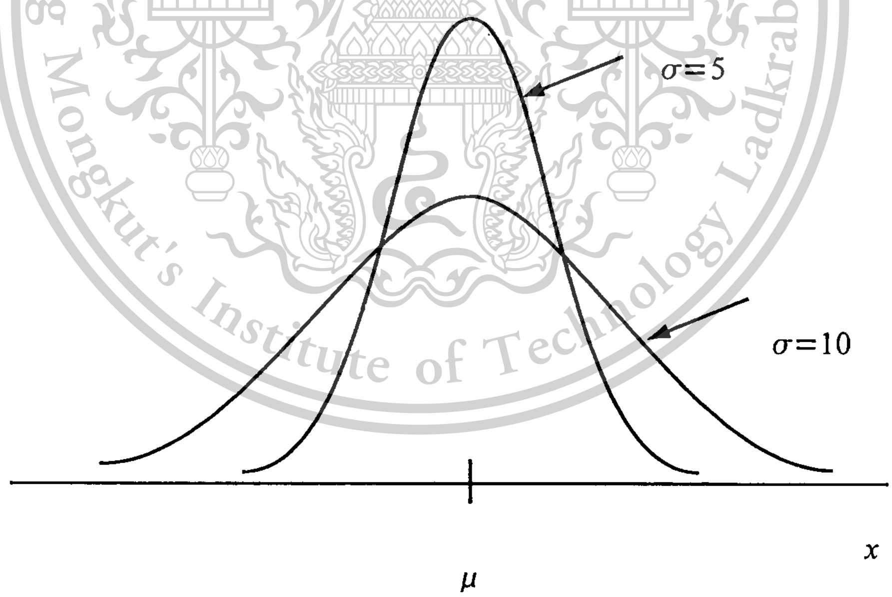
ถ้าให้ X เป็นตัวแปรสุ่มที่มีการแจกแจงปกติ โดยมีค่าเฉลี่ย $\mu(-\infty<\mu<\infty)$ หมายถึงค่าเฉลี่ยเป็นไปได้ทั้งจำนวนจริงลบ จำนวนเต็มศูนย์ หรือจำนวนจริงบวก และความแปรปรวนเป็น $\sigma^2(\sigma^2>0)$ ซึ่งมีฟังก์ชันความหนาแน่นดังนี้

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x_i-\mu)^2}{2\sigma^2}} \quad ; (-\infty<x<\infty) \tag{3.27}$$

การแจกแจงปกติสามารถแสดงในรูปย่อ ด้วยสัญลักษณ์ $X\sim N(\mu,\sigma^2)$ พื้นที่ใต้เส้นโค้งปกติแทนจำนวนความถี่ทั้งหมด N ตัว หรือแทนความถี่ 100% หรือความหนาแน่นของความน่าจะเป็นเท่ากับ 1 และการหาพื้นที่ใต้เส้นโค้งปกติสามารถหาได้จากการหา CDF ซึ่งเป็นการปริพันธ์ (Integration) ของ PDF ดังสมการที่ 3.28 และ 3.29



รูปที่ 3.1 การแจกแจงปกติ



รูปที่ 3.2 การแจกแจงของประชากร 2 กลุ่ม โดยที่ μ เท่ากันแต่ σ แตกต่างกัน

$$F(X)=P(X\leqslant x)=\int_{-\infty}^{x} p(u)\,du \tag{3.28}$$

$$F(X)=\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{x} \mathrm{e}^{-(u-\mu)^2/2\sigma^2}\,du \tag{3.29}$$

คุณสมบัติของการแจกแจงความน่าจะเป็นแบบปกติมีดังต่อไปนี้

- พื้นที่ใต้เส้นโค้งปกติมีค่าเท่ากับ 1 หน่วยเสมอ นั่นคือ $\int_{-\infty}^{\infty}(f(x))dx=1$ กล่าวคือ พื้นที่ใต้เส้นโค้งปกติทางซ้ายของค่าเฉลี่ยเท่ากับ 0.5 และทางด้านขวาเท่ากับ 0.5 เช่นกัน
- $(f(x))\geqslant 0$ สำหรับทุกค่าของ x
- เมื่อลากปลายเส้นโค้งปกติทั้งสองข้างให้ห่างจากค่าเฉลี่ยออกไป เส้นจะเข้าใกล้แกนนอน แต่จะไม่ตัดแกน กล่าวคือ $\lim_{(x\to\infty)} f(x)=0$ และ $\lim_{(x\to-\infty)} f(x)=0$
- $f(\mu+x)=f(\mu-x)$ คือฟังก์ชันความหนาแน่นสมมาตรรอบค่า μ
- ค่าสูงสุดของ $f(x)$ ปรากฏ เมื่อ $x=\mu$ และเรียกจุดที่ $x=\mu$ ว่าแกนสมมาตร ซึ่งเป็นจุดที่แบ่งพื้นที่ออกเป็นสองส่วนเท่ากัน คือร้อยละ 50 ของพื้นที่ใต้โค้งทั้งหมด
- ค่าเฉลี่ยเลขคณิต มัธยฐานและฐานนิยมจะมีค่าเท่ากัน ณ ค่าสูงสุดของ $f(x)$
- จุดเปลี่ยนโค้งของ $f(x)$ อยู่ที่จุด $x=\mu\pm\sigma$ ถ้าค่าเฉลี่ยเท่ากันและค่าของ σ มาก จะทำให้โค้งกว้างกว่าค่าของ σ น้อย ดังรูปที่ 3.2

เนื่องจากเมื่อต้องเปรียบเทียบข้อมูลตัวแปรสุ่มตั้งแต่สองชุดขึ้นไป ว่ามีความเหมือนหรือต่างกันอย่างไรนั้น การเปรียบเทียบจะไม่สามารถนำข้อมูลตัวแปรสุ่มดังกล่าวมาเปรียบเทียบกันได้โดยตรง รวมทั้งการหาปริพันธ์นั้น [10] เป็นสมการที่มีความซับซ้อน จึงมีความจำเป็นจะต้องแปลงรูปฟังก์ชันให้อยู่ในรูปสมการที่สามารถหาปริพันธ์อย่างง่าย หรือแปลงให้อยู่ในรูปมาตรฐานก่อน การแปลงให้อยู่ในรูปมาตรฐานสามารถทำด้วยการแปลงค่าเฉลี่ยของคะแนนดิบให้เป็นศูนย์ และทำค่าความแปรปรวนของคะแนนดิบให้มีค่าเท่ากับหนึ่ง ดังแสดงในรูปที่ 3.3 และจะเรียกตัวแปรสุ่มดังกล่าวว่า "ค่ามาตรฐาน (Standard score : Z) [12] [13] จากนั้นจึงทำการเปรียบเทียบกันได้

3.4.1.1 ค่ามาตรฐาน (Standard score : Z)

ค่ามาตรฐาน (Standard score : Z) คือค่าที่มาจากการแปลงค่าการแจกแจงปกติให้อยู่ในรูปแบบอย่างง่าย แทนสัญลักษณ์ด้วย $Z \sim N(0,1)$ การแปลงข้อมูลให้เป็นค่ามาตรฐานที่มีค่าเฉลี่ยเลขคณิตเท่ากับศูนย์ และส่วนเบี่ยงเบนมาตรฐานเท่ากับหนึ่ง ทั้งนี้ทำได้ด้วยการนำค่าเฉลี่ย μ หักออกจากทุกค่าของตัวแปร และนำค่า σ มาหารออกจากทุกค่าของตัวแปร ดังรูปที่ 3.3 และรูปที่ 3.4 จะได้ค่ามาตรฐานดังสมการ

ถ้า x_i เป็นค่าที่ i ของตัวแปร x_i แล้ว ค่ามาตรฐานของ x_i คือ

$$z_i = \frac{(x_i - \mu)}{\sigma} \quad \text{เมื่อ i คือ 1, 2,..., n} \tag{3.30}$$

สมการที่ (3.27)(3.29)และ (3.30) หาปริพันธ์ของตัวแปรสุ่มแบบปกติมาตรฐานได้ดังนี้

$$F(X) = P(X \leqslant x)$$

$$F(Z) = P(Z \leqslant \frac{x_i - \mu}{\sigma})$$

$$F(Z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{(x_i-\mu)/\sigma} e^{-z^2} dz \tag{3.31}$$

ค่ามาตรฐานจะถูกนำมาใช้ในการวัดตำแหน่งที่หรือตำแหน่งสัมพัทธ์ของข้อมูล เปรียบเทียบข้อมูลและใช้เป็นพื้นฐานของการคำนวณพื้นที่ใต้โค้งปกติหรือฟังค์ชันความน่าจะเป็นสะสม ดังรูปที่ 3.5 โดยพื้นที่ใต้โค้งปกติในช่วง $-1 \leqslant Z \leqslant 1$ มีค่าประมาณ 68.26% ช่วง $-2 \leqslant Z \leqslant 2$ มีค่าประมาณ 95.44% และช่วง $-3 \leqslant Z \leqslant 3$ มีค่าประมาณ 99.72% ถ้า Z มีค่าเท่ากับศูนย์ หมายถึงข้อมูลมีค่าเท่ากับค่าเฉลี่ย ถ้า Z น้อยกว่าศูนย์ หมายถึงข้อมูลมีค่าน้อยกว่าค่าเฉลี่ย และถ้า Z มีค่ามากกว่าศูนย์ หมายถึงข้อมูลมีค่ามากกว่าค่าเฉลี่ย คุณสมบัติของค่า Z มีดังนี้

3.4.1.2 ค่าเฉลี่ยและความแปรปรวนของการแจกแจงปกติ

ค่าเฉลี่ย (Mean) คือ $E(X)=\int_{-\infty}^{\infty}\frac{x}{\sigma\sqrt{2\pi}}e^{\frac{-1}{2}[\frac{(x-\mu)}{\sigma}]^2}dx$

ให้ $z=\frac{(x-\mu)}{\sigma}$ ดังนั้น $x=\sigma z+\mu$ และ $dx=\sigma dz$

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

$$=\sigma\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}z\,e^{\frac{-1}{2}z^2}dz+\mu\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{\frac{-1}{2}z^2}dz$$

เนื่องจาก $\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{\frac{-1}{2}z^2}dz$ เป็นการแจกแจงปกติมาตรฐานที่มีค่า $\mu=0$ และ $\sigma=1$ ดังนั้นผลการหาปริพันธ์ของ $\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{\frac{-1}{2}z^2}dz$ คือ 1 ส่วน $\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{\frac{-1}{2}z^2}dz$ หาค่าได้เท่ากับศูนย์ นั่นคือ

$$=\sigma(0)-\mu(1)$$

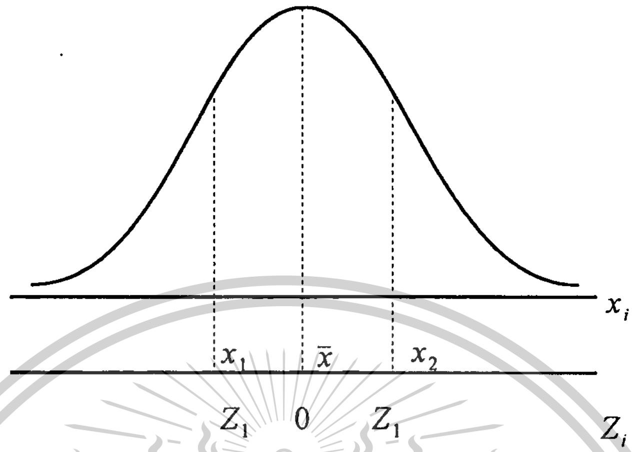
$$E(X)=\mu \tag{3.32}$$

ความแปรปรวน (Variance) คือ $V(X)=E((X-\mu)^2)$

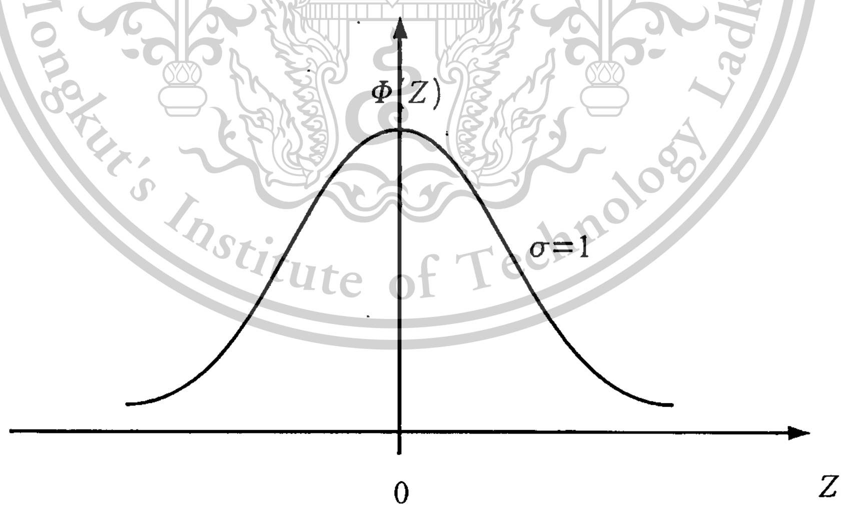
$$=\int_{-\infty}^{\infty}(x-\mu)^2\frac{1}{\sigma\sqrt{2\pi}}e^{\frac{-1}{2}[\frac{(x-\mu)}{\sigma}]^2}dx$$

ให้ $z=\frac{(x-\mu)}{\sigma}$ ดังนั้น $x=\sigma z+\mu$ และ $dx=\sigma dz$

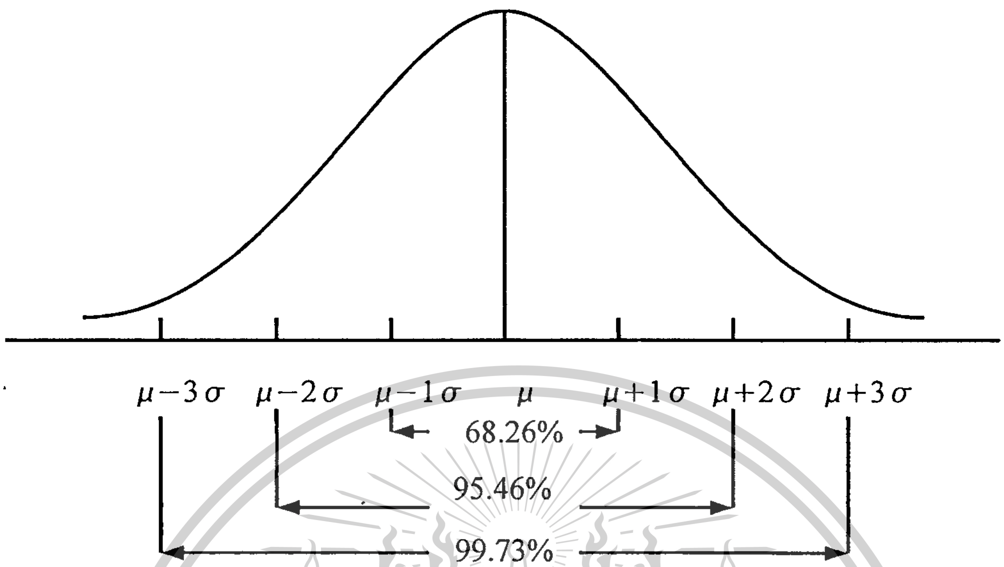
$$=\int_{-\infty}^{\infty}(\sigma z)^2\frac{1}{\sigma\sqrt{2\pi}}e^{\frac{-1}{2}z^2}(\sigma dz)$$



รูปที่ 3.3 การแปลงค่าจาก x_i เป็น Z_i



รูปที่ 3.4 การแจกแจงปกติมาตรฐาน



รูปที่ 3 .5 พื้นที่ใต้เส้นโค้งปกติ

ให้ $u=z$ และ $dv=z\,\mathrm{e}^{\frac{-1}{2}z^2}dz$ โดย $du=dz$ $v=-\mathrm{e}^{\frac{-1}{2}z^2}$

$$=\sigma^2\left(\frac{-z}{\sqrt{2\pi}}\mathrm{e}^{\frac{-1}{2}z^2}\Big|_{-\infty}^{\infty}+\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{\frac{-1}{2}z^2}dz\right)$$

$$=\sigma^2(0+1)$$

$$V(X)=\sigma^2 \tag{3.33}$$

3.4.2 การแจกแจงแบบไคกำลังสอง

การแจกแจงแบบไคกำลังสอง เป็นการแจกแจงความน่าจะเป็นของค่าความแปรปรวน (S^2) ของชุดข้อมูลตัวแปรสุ่ม โดยพิจารณาการแจกแจงของสถิติทดสอบ χ^2

เมื่อให้ $Z_1, Z_2, Z_3, .., Z_k$ เป็นตัวแปรสุ่มที่มีการแจกแจงปกติมาตรฐานและเป็นอิสระต่อกัน มีค่าเฉลี่ย $\mu=0$ และค่าความแปรปรวน $\sigma^2=1$ จะได้ตัวแปรสุ่มที่มีการแจกแจงแบบไคกำลังสอง ดังนี้

$$X^2 = Z_1^2 + Z_2^2 + Z_3^2 + \ldots + Z_k^2$$

สามารถหาฟังก์ชันความหนาแน่นได้จาก

$$f(X^2) = \frac{1}{2_{k/2}\Gamma(\frac{k}{2})} u^{(k/2)-1} e^{-u/2} \quad ; \quad \mu > 0 \qquad (3.34)$$

$$= 0 \quad ; \quad \mu \text{ มีค่าอื่นๆ}$$

เมื่อ $\Gamma(p)$ คือ แกมมาฟังก์ชัน (Gamma Function) [14] และการแจกแจงไคกำลังสองมีระดับขั้นความเสรี k เขียนแทนด้วย X_k^2 ดังรูปที่ 3.6

3.4.2.1 ค่าเฉลี่ยและความแปรปรวนของการแจกแจงแบบไคกำลังสอง

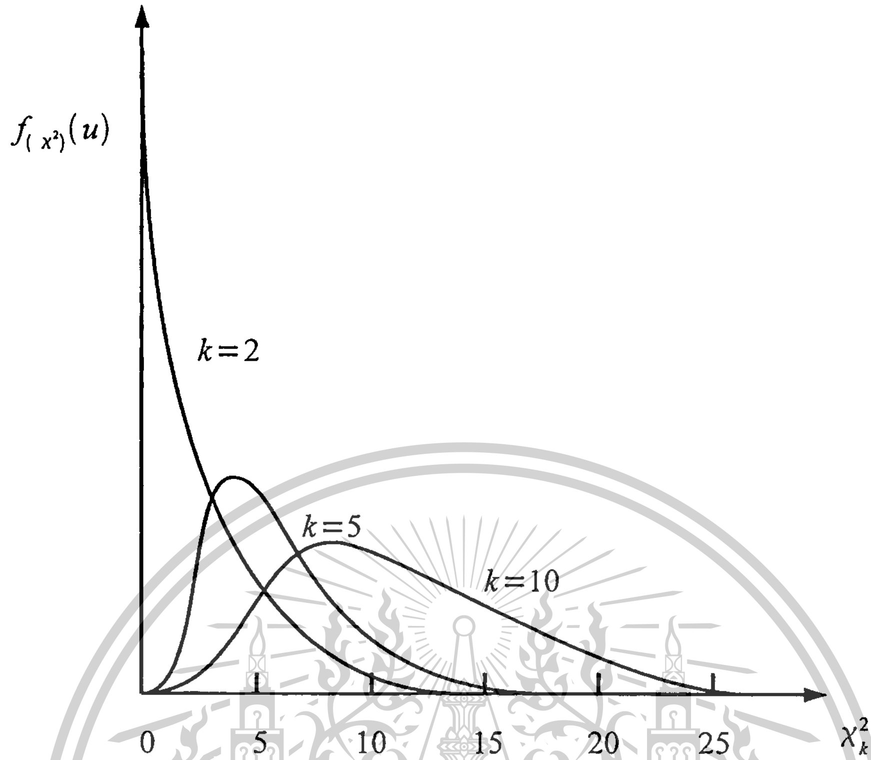
- ค่าเฉลี่ย (Mean) คือ $E(X) = \mu = k$
- ความแปรปรวน (Variance) คือ $V(X) = \sigma^2 = 2k$

คุณสมบัติของการแจกแจงความน่าจะเป็นแบบปกติมีดังต่อไปนี้

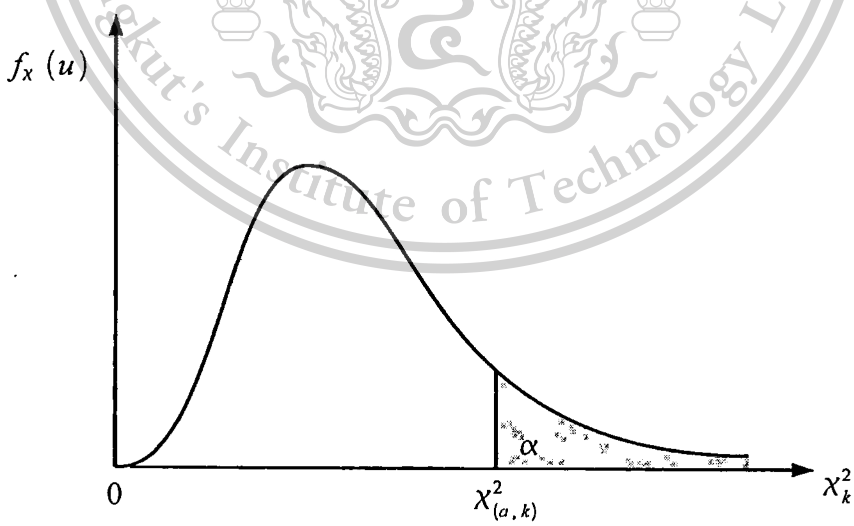
- X_k^2 เป็นตัวแปรสุ่มที่มีค่าไม่ติดลบ และกราฟของการแจกแจงความน่าจะเป็นมีลักษณะเบ้ขวา
- เมื่อ $k \to \infty$ แล้ว X_k^2 จะมีลักษณะเหมือนการแจกแจงปกติ
- การหาค่าความน่าจะเป็นของ X_k^2 หรือการหาพื้นที่ใต้โค้งไคกำลังสอง กำหนดให้ X_{α}^2, k คือค่าวิกฤต (Critical Value) ของการแจกแจงไคกำลังสอง และระดับขั้นความเสรี (Degree of Freedom) เป็น k แสดงดังรูปที่ 3.7 การหาความน่าจะเป็นของการแจกแจงไคกำลังสอง หาได้จากสมการ

$$P(X_k^2 \geq X_{\alpha}^2, k) = \int_{(X_{\alpha}^2, k)}^{\infty} f_X^2(u)\,du = \alpha \qquad (3.35)$$

- ตัวสถิติ $X_{(n-1)}^2$ ที่ใช้ในการทดสอบมีค่าเท่ากับ $\frac{((n-1)S^2)}{\sigma^2}$



รูปที่ 3.6 การแจกแจงไคกำลังสองมีระดับขั้นความเสรี k ต่างๆ



รูปที่ 3.7 ค่าวิกฤตของการแจกแจงไคกำลังสอง [14]

บทที่ 4
การวิเคราะห์ข้อมูลและสถิติ

การเก็บตัวอย่างจำนวนสุ่มมาทำการศึกษาและวิเคราะห์คุณสมบัติเพื่อนำไปประยุกต์ใช้งานนั้น จะต้องอาศัยความน่าจะเป็นและสถิติ [14][15] มาช่วยศึกษาและหาคำตอบว่าจำนวนสุ่มนั้นมีคุณสมบัติเป็นอย่างไร โดยใช้หลักเกณฑ์เพื่อพิจารณาในคุณสมบัติดังต่อไปนี้ ผลการวิเคราะห์ข้อมูลจำนวนสุ่ม ความน่าจะเป็นและการแจกแจงข้อมูลจำนวนสุ่ม เป็นต้น

4.1 การวิเคราะห์ข้อมูลเบื้องต้น (Data Analysis)

การวิเคราะห์ข้อมูลเบื้องต้นเป็นการใช้คณิตศาสตร์และสถิติมาช่วยในการศึกษาชุดข้อมูลสารสนเทศ (Information) โดยสิ่งสำคัญที่สามารถบ่งบอกคุณลักษณะหรือเป็นตัวแทนของชุดข้อมูลได้แก่ ค่ากลาง การกระจายของข้อมูล และรูปแบบของการแจกแจงของข้อมูล ซึ่งผลการวิเคราะห์คุณลักษณะดังกล่าวจะสามารถนำมาวางแผนและตัดสินใจในการนำข้อมูลสารสนเทศเหล่านั้นไปใช้ประโยชน์ต่อไป

4.1.1 การวัดค่ากลางของข้อมูล (Measure of central value)

การนำความรู้ทางคณิตศาสตร์มาช่วยหาความสัมพันธ์ของข้อมูลนั้น จะช่วยทำให้สามารถสรุปผลและตัดสินใจได้ว่า ชุดข้อมูลที่ควรจะเป็นนั้นมีลักษณะอย่างไร โดยค่าที่คำนวณได้นี้จะมีค่าหรือมีแนวโน้มลู่เข้าหาค่ากลางค่าหนึ่ง ซึ่งจะเรียกว่าค่าแนวโน้มสู่ศูนย์กลาง (Central Tendency or Location) ซึ่งสามารถวัดค่าดังกล่าวได้จากสถิติสามชนิด ดังนี้ ค่าเฉลี่ยเลขคณิต มัธยฐาน และฐานนิยม

4.1.1.1 ค่าเฉลี่ยเลขคณิต (Arithmetic Mean or Mean)

ค่าเฉลี่ยเลขคณิต ใช้สัญลักษณ์แทน $\bar{X}$ หรือ μ โดยค่าเฉลี่ยเลขคณิตจะเป็นตัวแทนของข้อมูล ซึ่งสามารถหาค่าเฉลี่ยเลขคณิตได้จาก

$$\bar{X} = \frac{\sum_{i=1}^{n} x_i}{n} \quad ; \text{n คือ จำนวนทั้งหมด} \qquad (4.1)$$

4.1.1.2 มัธยฐาน (Median)

มัธยฐาน เป็นค่าที่มีตำแหน่งอยู่กึ่งกลางของข้อมูลทั้งหมด โดยเรียงลำดับข้อมูลจากค่าน้อยที่สุดไปหาค่ามากที่สุด ซึ่งค่าดังกล่าวจะแสดงให้ทราบว่ามีจำนวนข้อมูลที่มีมากกว่าหรือน้อยกว่าค่ามัธยฐานหรือไม่และเป็นจำนวนเท่าไหร่ โดยสามารถหาค่ามัธยฐานได้จาก

$$\text{ตำแหน่งของข้อมูลที่อยู่ตรงกลาง} \quad \tilde{X} = \begin{cases} X_{((n+1)/2)} & ; \text{n เป็นจำนวนคี่} \\ \dfrac{\left(X_{(n/2)} + X_{((n/2)+1)}\right)}{2} & ; \text{n เป็นจำนวนคู่} \end{cases} \qquad (4.2)$$

4.1.1.3 ฐานนิยม (Mode)

ฐานนิยม เป็นค่าของข้อมูลที่มีความถี่สูงสุด โดยการหาค่ามัธยฐานและฐานนิยมเป็นการหาค่ากลางของข้อมูลโดยการประมาณและทำอย่างรวดเร็ว ซึ่งค่าทั้งสองอาจจะไม่ใช่ตัวแทนของชุดข้อมูลที่ดีที่สุดเนื่องจากอาจมีค่าต่ำสุดและสูงสุดของข้อมูลแตกต่างกันมาก ทั้งนี้ตัวแทนของชุดข้อมูลควรเป็นค่าเฉลี่ยเลขคณิต ซึ่งเป็นค่ากลางที่ได้มาจากการนำข้อมูลทั้งหมดมาเฉลี่ยกัน

4.2 การวัดการกระจายของข้อมูล (Measure of Dispersion)

การวัดเฉพาะค่ากลางเพื่อใช้อธิบายการแจกแจงของข้อมูลนั้น ยังไม่สามารถอธิบายคุณลักษณะของชุดข้อมูลได้เพียงพอ ดังนั้นจึงต้องใช้คณิตศาสตร์อื่นมาช่วยวิเคราะห์ว่าข้อมูลชุดเพิ่มเติมเพื่อให้สามารถสรุปได้ว่าข้อมูลมีความหมายแตกต่างกันอย่างไร เนื่องจากข้อมูลทั้งหมดอยู่ภายใต้ความเบี่ยงเบนโดยธรรมชาติ ดังนั้นจึงมีความจำเป็นต้องพิจารณาความเบี่ยงเบนที่เรียกว่า "การกระจาย (Dispersion)" อธิบายคุณสมบัติของชุดข้อมูลเพิ่มเติม ซึ่งเป็นความเบี่ยงเบนนี้สามารถวัดได้ด้วยตัวสถิติสามชนิด ได้แก่ พิสัย (Range) ความแปรปรวน (Variance) และสัมประสิทธิ์ความแปรผัน (Coefficient of Variation) ซึ่งมีรายละเอียดดังนี้

4.2.1 พิสัย (Range)

พิสัย เป็นตัวสถิติที่ใช้คำนวณการกระจายของข้อมูลได้ง่ายที่สุด ซึ่งเป็นการพิจารณาค่ามากที่สุดและค่าที่ต่ำที่สุดของชุดข้อมูล ดังสมการที่ 4.3

$$R = x_{max} - x_{min} \qquad (4.3)$$

4.2.2 ความแปรปรวน (Variance)

ความแปรปรวนเป็นการวัดการกระจายของข้อมูลโดยใช้ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: S) ซึ่งได้จากการวัดการกระจายของข้อมูลทุกค่าที่กระจายอยู่รอบค่าเฉลี่ยของชุดข้อมูล วิธีนี้เป็นวิธีที่นักสถิติยอมรับว่าเป็นวิธีที่ใช้วัดการกระจายได้ดีที่สุด โดยค่าความเบี่ยงเบนหาได้จาก

$$S=\sqrt{\left(\frac{\sum_{i=1}^{n}(x_i-\bar{X})}{(n-1)}\right)} \tag{4.4}$$

$\bar{X}$ แทนค่าเฉลี่ยเลขคณิต

n แทนจำนวนตัวอย่างทั้งหมด

โดยค่าความแปรปรวนสามารถหาได้จากการยกกำลังสองของส่วนเบี่ยงเบนมาตรฐาน ดังสมการที่ 4.5

$$S^2=\frac{\sum_{i=1}^{n}(x_i-\bar{X})}{(n-1)} \tag{4.5}$$

n-1 คือระดับขั้นความเสรี (Degree of Freedom)

ระดับความเป็นอิสระ (Degree of freedom) ซึ่งเขียนแทนด้วย k คือ จำนวนข้อมูลที่เป็นอิสระและไม่ขึ้นกับข้อบังคับใดๆ โดยสามารถเปลี่ยนเป็นค่าใดๆ ได้อย่างอิสระ นั่นคือ ระดับความเป็นอิสระเท่ากับจำนวนตัวอย่างทั้งหมดลบด้วยจำนวนพารามิเตอร์ที่ประมาณได้จากตัวอย่าง

4.2.3 สัมประสิทธิ์ความแปรผัน (Coefficient of Variation: CV)

สัมประสิทธิ์ความแปรผันถูกนำมาใช้ในการเปรียบเทียบความเบี่ยงเบนของข้อมูลตั้งแต่สองชุดขึ้นไปซึ่งสามารถหาได้จากสมการที่ 4.6

$$\text{CV}=\frac{S}{\bar{X}} \tag{4.6}$$

4.3 การสุ่มตัวอย่างและการแจกแจงการสุ่มตัวอย่าง

การทดลองหรือการแก้ปัญหาต่างๆ สามารถศึกษาและเข้าใจถึงปัญหาต่างๆได้โดยการจำลองการแก้ปัญหา ซึ่งจะทำการสุ่มตัวอย่างเพื่อทำการทดสอบและหาแนวทางแก้ปัญหาหรือหาคำตอบ การสุ่มตัวอย่างนั้นจะเป็นการเก็บข้อมูลจากประชากร (Population) บางส่วน เพื่อประมาณค่าลักษณะที่สนใจศึกษาของประชากร เช่น ค่าเฉลี่ย ค่าความเบี่ยงเบน เป็นต้น โดยที่การประมาณ

ค่ามีสองวิธี คือ การประมาณค่าแบบจุดและการประมาณค่าแบบช่วง ซึ่งการประมาณค่าต่างๆ ของประชากรที่ต้องการทราบคุณลักษณะนั้นจะมีความถูกต้องและน่าเชื่อถือได้มากน้อยเพียงไรนั้นย่อมขึ้นอยู่กับการหาขนาดของตัวอย่างสุ่ม การประมาณค่าของสิ่งที่ต้องการทราบคุณลักษณะของประชากร เรียกว่า “พารามิเตอร์ (Parameter)” โดยจะได้จากการคำนวณค่าจาก“ตัวสถิติ (Statistic)” ซึ่งเป็นตัวแทนของตัวอย่างสุ่มทั้งหมด

4.3.1 การสุ่มตัวอย่าง

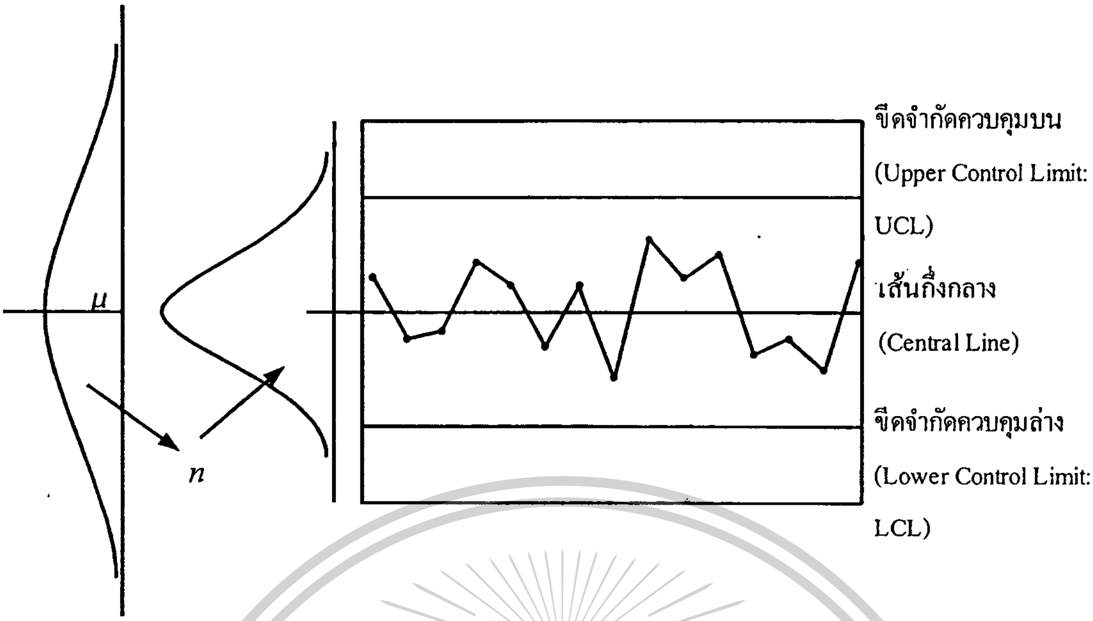
การสุ่มตัวอย่าง (Random Sampling) เป็นการใช้เทคนิคทางสถิติที่เกี่ยวข้องกับหลักการความน่าจะเป็น ซึ่งเป็นการสำรวจหรือการเก็บข้อมูลบางส่วนของประชากรภายใต้เงื่อนไขที่ไม่เปลี่ยนแปลงจำนวน n ครั้ง

หลักสำคัญในการสุ่มตัวอย่างคือ หน่วยตัวอย่างของประชากรต้องมีโอกาสที่จะถูกเลือกเท่ากัน สามารถใช้วิธีการสุ่มได้หลายวิธี เช่น วิธีการจับฉลาก วิธีการเปิดตารางตัวเลขสุ่ม เป็นต้น ประโยชน์ที่ได้รับจากการสุ่มตัวอย่าง คือทำให้ประหยัดค่าใช้จ่าย เวลา และกำลังคน ในการทำการประมาณลักษณะที่สนใจศึกษาของประชากรทั้งหมด เช่น การหาเวลาในการทำงานของเครื่องใช้ไฟฟ้าตลอดอายุการใช้งาน หรือทดสอบประสิทธิภาพของการผลิตว่ามีคุณภาพดีและสามารถใช้งานได้เป็นปรกติหรือไม่ เป็นต้น การสุ่มตัวอย่างเป็นการนำข้อมูลบางส่วนที่ต้องการศึกษาเพื่ออ้างอิงถึงประชากร เพื่อนำมาผลที่ได้มาสรุปว่าประชากรทั้งหมดมีคุณภาพเป็นอย่างไร ในการทดสอบนั้นผลสรุปจะมีความแม่นยำมากน้อยเพียงใดจะขึ้นอยู่กับจำนวนข้อมูลและตัวอย่างที่เลือกนำมาทดสอบ กล่าวคือตัวอย่างที่สุ่มตัวมานั้นจะต้องมีลักษณะที่เหมือนกับประชากรทั้งหมด เพื่อสามารถประมาณค่าที่ได้จากตัวอย่างใกล้เคียงกับประชากร นอกจากนี้ปริมาณของตัวอย่างก็มีผลต่อความแม่นยำดังกล่าวด้วย ถ้าสุ่มเก็บข้อมูลมากความแม่นยำจะเพิ่มสูงขึ้น

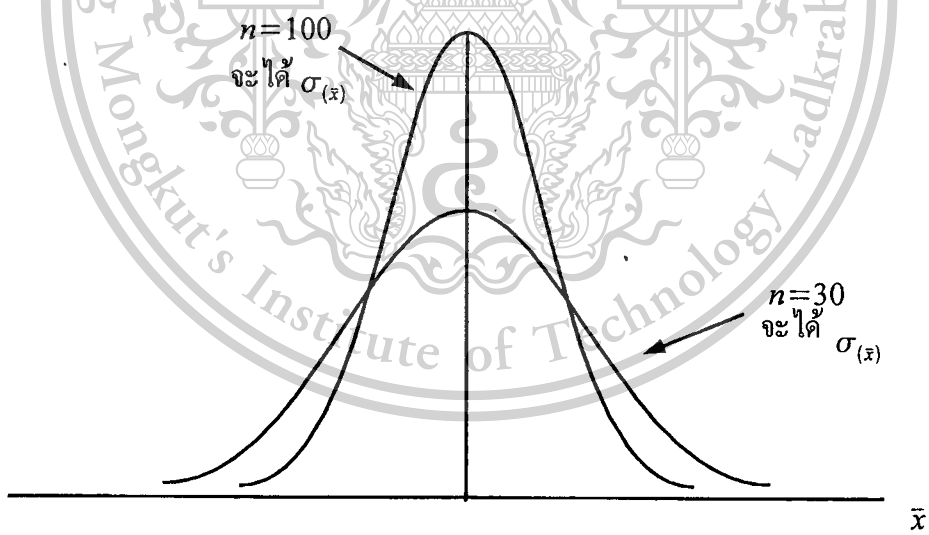
4.3.1.1 การแจกแจงการสุ่มตัวอย่าง

การแจกแจงการสุ่มตัวอย่าง (Sampling Distributions) คือการแจกแจงความน่าจะเป็นของตัวสถิติที่จะคำนวณได้จากกลุ่มตัวอย่าง เช่น ถ้าเป็นการแจกแจงความน่าจะเป็นของ $\bar{x}$ จะเรียกว่าการแจกแจงการสุ่มตัวอย่างของค่าเฉลี่ย ถ้าเป็นการแจกแจงความน่าจะเป็นของ $\hat{p}$ จะเรียกว่าการแจกแจงการสุ่มตัวอย่างของสัดส่วน เป็นต้น การแจกแจงการสุ่มตัวอย่างของตัวสถิติขึ้นอยู่กับขนาดของประชากร ขนาดของตัวอย่าง และวิธีการเลือกสุ่มตัวอย่าง

ตัวสถิติ (Statistic) คือฟังก์ชันของตัวอย่างสุ่มที่ได้ขึ้นกับพารามิเตอร์ที่ไม่ทราบค่า ค่าสถิติคือค่าที่คำนวณได้จากตัวอย่างสุ่ม เนื่องจากตัวอย่างที่สุ่มจากประชากรเดียวกัน อาจมีได้หลายชุดต่างๆ กัน เช่น การสุ่มตัวอย่างมา 2 กลุ่ม จากประชากรชุดเดียวกันและคำนวณหาค่าเฉลี่ย ($\bar{x}$) จะพบว่า ค่าเฉลี่ยของตัวอย่าง (Sample Mean) คือ $(\bar{x}_1)$ และ $(\bar{x}_2)$ ซึ่งแตกต่างกัน ดังนั้นค่าสถิติที่คำนวณได้จากตัวอย่างชุดหนึ่ง จึงเป็นค่าเพียงค่าหนึ่งของตัวสถิติเท่านั้น



รูปที่ 4.1 ความผันแปรของค่าเฉลี่ยตัวอย่างรอบค่าเฉลี่ยของประชากร [15]



รูปที่ 4.2 การเปรียบเทียบการแจกแจงเมื่อ n เพิ่มขึ้น [2]

ตัวสถิติจะถูกนำมาใช้สรุปค่าพารามิเตอร์ของประชากร โดยตัวสถิติมักใช้สัญลักษณ์แทนด้วยอักษรลาตินและค่าพารามิเตอร์จะใช้สัญลักษณ์แทนด้วยอักษรกรีก เช่น

	ตัวสถิติ	พารามิเตอร์
ค่าเฉลี่ย	$\bar{x}$	μ
ค่าความแปรปรวน	S^2	σ^2
สัดส่วน	$\hat{p}$	p

การแจกแจงการสุ่มตัวอย่างของค่าเฉลี่ยเป็นการพิจารณาค่าเฉลี่ยตัวอย่าง $\bar{x}$ เพื่อใช้สำหรับอนุมานค่าเฉลี่ยประชากร μ โดยได้จากการสุ่มตัวอย่างจากประชากรขนาด n จำนวน ดังนั้นผลลัพธ์ที่ได้คือ $(\bar{x_1}),(\bar{x_2}),(\bar{x_3}),...,(\bar{x_{15}})$ เมื่อ n เท่ากับ 15 ซึ่งแสดงให้เห็นถึงความผันแปรของค่าเฉลี่ยตัวอย่างรอบค่าเฉลี่ยของประชากร ดังรูป 4.1 จากทั้ง 15 จุด แต่ละจุดแทน $(\bar{x_1}),(\bar{x_2}),(\bar{x_3}),...,(\bar{x_{15}})$ ตามลำดับ ซึ่งแต่ละจุดสุ่มมาจากประชากรที่มีการแจกแจงปกติเท่ากับ n ดังนั้นค่าสังเกต $x_i(x_1, x_2, x_3, .., x_n)$ แต่ละตัวของแต่ละ $\bar{x}$ ก็จะมีการแจกแจงปกติเช่นเดียวกับประชากร โดยมีผลรวมเชิงเส้นตรงของตัวแปรสุ่มแบบปกติ เป็นดังนี้

$$\bar{x}=\frac{(x_1, x_2, x_3, .., x_n)}{n}$$

การแจกแจงปกตินี้มีค่าเฉลี่ยเท่ากับ

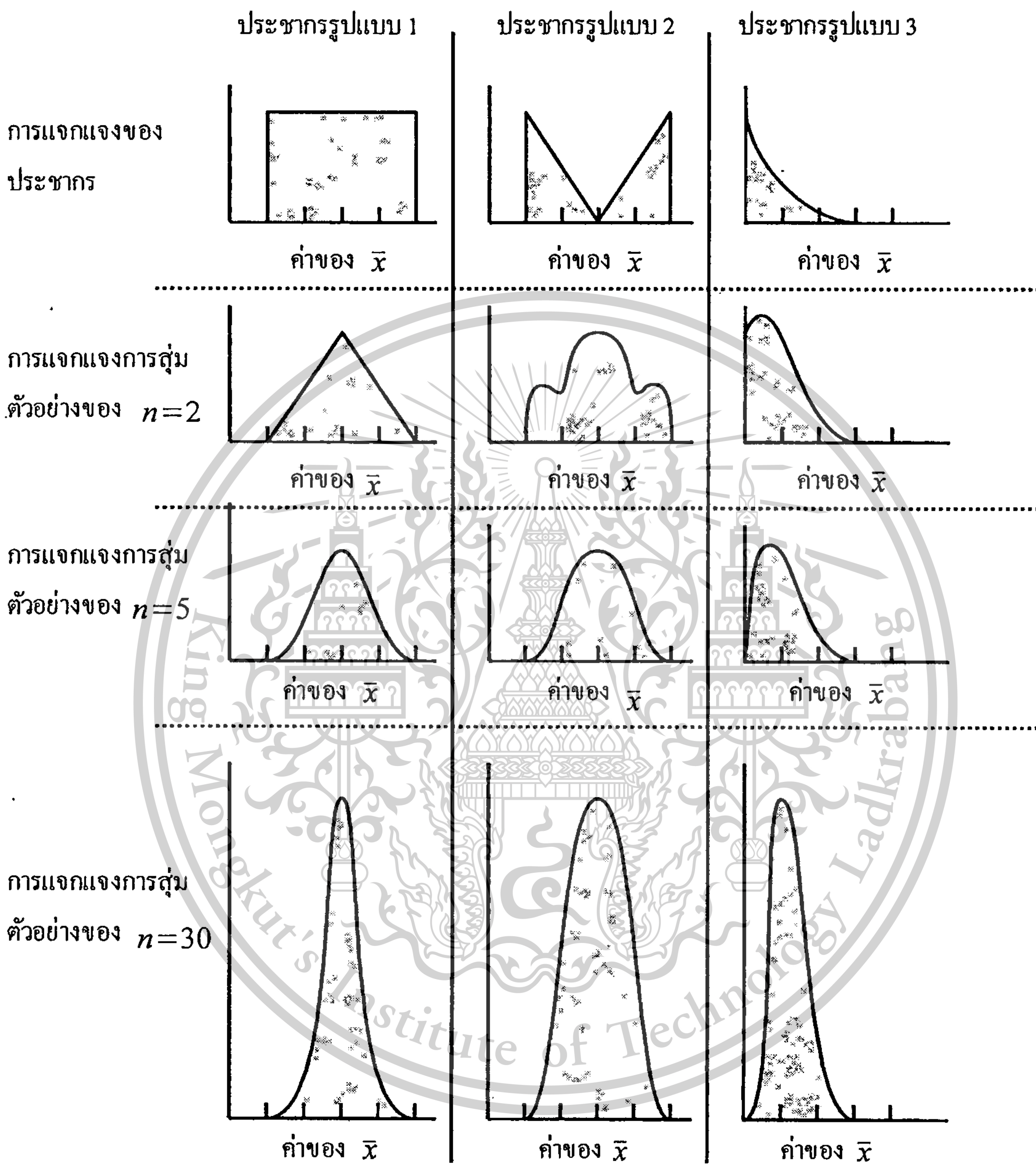
$$\mu_{(\bar{x})}=\bar{x}=\frac{(\bar{x}_1, \bar{x}_2, \bar{x}_3, .., \bar{x}_n)}{n}$$

$$=\mu$$

ความแปรปรวนหาได้จาก $$\sigma^2_{(\bar{x})}=\frac{(\sigma^2_1, \sigma^2_2, \sigma^2_3, .., \sigma^2_n)}{n^2}$$

$$=\frac{\sigma^2}{n} \tag{4.7}$$

จากสมการที่ 4.7 พบว่า เมื่อค่า n เพิ่มขึ้น ค่า $\sigma^2_{(\bar{x})}$ จะลดลง และผลที่ตามมาคือ รูปร่างและขนาดของการแจกแจงของ $\bar{x}$ จะขึ้นอยู่กับค่าของ n ดังรูปที่ 4.2



รูปที่ 4.3 การใช้ทฤษฎีขีดจำกัดสู่ศูนย์กลางกับตัวอย่างประชากร 3 รูปแบบ [2]

4.3.1.2 ทฤษฎีขีดจำกัดสู่ศูนย์กลาง (Central Limit Theorem: CLT)

กล่าวถึงการประมาณการแจกแจงปกติสำหรับ $\bar{x}$ จะทำได้เมื่อตัวอย่างสุ่มมีขนาดใหญ่ $n \geqslant 30$ โดยไม่สนใจว่าประชากรจะมีการแจกแจงเป็นแบบใด ผลที่ได้คือ การแจกแจงการสุ่มตัวอย่างของค่าเฉลี่ย $\bar{x}$ จะประมาณเป็นการแจกแจงปกติด้วยค่าเฉลี่ย μ และค่าความแปรปรวน $\frac{\sigma^2}{n}$ หรือ $N(\mu, \frac{\sigma^2}{n})$ ดังรูป 4.3

จากรูป 4.3 แถวบนแสดงถึงการแจกแจงแต่ละประเภทของประชากร ซึ่งไม่ได้เป็นการแจกแจงแบบปกติ แต่เมื่อตัวอย่างสุ่มมีขนาดเพิ่มขึ้น หรือมีจำนวนมากกว่า 30 แล้วนั้น การแจกแจงทั้ง 3 รูปแบบของประชากรจะมีการแจกแจงการสุ่มตัวอย่างของค่าเฉลี่ยประมาณเป็นการแจกแจงแบบปกติ

4.4 การอนุมานเชิงสถิติ (Statistical Inference)

การแก้ปัญหาเพื่อให้ได้มาซึ่งผลสรุปและคำตอบนั้น ได้นำวิธีการทางสถิติมาช่วยหาคำตอบ เนื่องจากว่าสามารถคำนวณออกมาในรูปแบบของปริมาณที่วัดค่าได้ การหาผลสรุปของปัญหาทางสถิติโดยทั่วไป เป็นการทดสอบลักษณะของประชากรจากกลุ่มตัวอย่าง (Sample) ที่เป็นตัวแทนของกลุ่มประชากรที่ต้องการศึกษาทั้งหมด เนื่องจากการศึกษาจำนวนกลุ่มประชากรทั้งหมดบางครั้งอาจมีจำนวนมากหรือมีจำนวนเป็นอนันต์ ซึ่งทำให้เสียเวลาและเสียงบประมาณอย่างมาก รวมทั้งไม่สะดวกในทางปฏิบัติอีกด้วย ตัวอย่างเช่น ในการผลิตหม้อหุงข้าวขึ้นมาใหม่หนึ่งรุ่น เพื่อหาอายุการใช้งานของหม้อหุงข้าวรุ่นนี้ ถ้าทำการทดสอบการใช้งานของหม้อหุงข้าวทุกใบ จะทำให้เสียงบประมาณและเวลาเป็นอย่างมาก ดังนั้นจึงแก้ปัญหาโดยการเลือกสุ่มหม้อหุงข้าวมาจำนวนหนึ่งและทดสอบการทำงานเพื่อดูอายุการใช้งาน และจากข้อมูลนี้จะสามารถประมาณอายุการใช้งานโดยเฉลี่ยของหม้อหุงข้าวรุ่นที่ผลิตใหม่นี้ได้ เป็นต้น [15]

การแก้ไขปัญหาด้วยวิธีการใช้วิธีการทางสถิติดังกล่าวเรียกว่า การอนุมานเชิงสถิติ (Statistical Inference) [15] คือ วิธีการต่างๆ ที่ใช้ในการอนุมานหรือหาข้อสรุปในทางสถิติที่เกี่ยวข้องกับกลุ่มประชากร โดยอาศัยข้อเท็จจริงบางส่วนที่ได้มาจากข้อมูลในกลุ่มตัวอย่าง แล้วมุ่งไปสู่ความสนใจเกี่ยวกับคุณสมบัติของกลุ่มประชากร ซึ่งแสดงออกมาได้ด้วยตัวเลข เช่น ค่าเฉลี่ยเลขคณิตของประชากร (Mean) ส่วนเบี่ยงเบนมาตรฐานของประชากร หรือสัดส่วนของประชากร (Population proportion) เป็นต้น การอนุมานเชิงสถิติ (Statistical Inference) แบ่งออกเป็นสองแบบ ได้แก่ การประมาณค่า(Estimation) และการทดสอบสมมติฐาน (Test of Hypotheses) ซึ่งในวิทยานิพนธ์นี้เน้นการใช้การทดสอบสมมติฐานเป็นหลัก ดังนั้นจึงจะกล่าวรายละเอียดการประมาณค่าเพียงเล็กน้อย และจะกล่าวในรายละเอียดของการทดสอบสมมติฐานในลำดับต่อไป

4.4.1 การประมาณค่า (Estimation)

การประมาณค่า(Estimation) คือวิธีการที่ใช้ค่าสถิติของตัวอย่างเพื่อประมาณค่าพารามิเตอร์หรือคุณลักษณะของข้อมูล เพื่อที่จะให้ทราบค่าที่ใกล้เคียงของพารามิเตอร์นั้นๆ เช่น ค่าเฉลี่ย ค่าความแปรปรวน ค่าพิสัย เป็นต้น ซึ่งค่าเหล่านี้เรียกว่าค่าแนวโน้มสู่ศูนย์กลาง(Central Tendency or Location) หรือเรียกว่าค่าสถิติของข้อมูล ซึ่งเป็นตัวแทนหรือสื่อให้ทราบว่าข้อมูลมีลักษณะอย่างไร ดังการวิเคราะห์ข้อมูลเบื้องต้นที่ได้กล่าวมาแล้วในข้างต้น

4.4.2 การทดสอบสมมติฐาน (Test of Hypotheses)

การทดสอบสมมติฐาน (Test of Hypotheses) คือการอนุมานเชิงสถิติวิธีหนึ่งเพื่อแก้ปัญหาที่ต้องการตัดสินใจ โดยใช้กระบวนการตัดสินใจว่าจะยอมรับหรือปฏิเสธข้อสมมติฐานที่เกี่ยวข้องกับข้อมูล(ประชากร) ที่ตั้งไว้ เพื่อสรุปลักษณะบางอย่างของประชากร(พารามิเตอร์) การหาคำตอบเพื่อให้ทราบว่าสมมติฐานนั้นจริงหรือไม่ จะต้องทำการตรวจสอบข้อมูลอย่างทั่วถึง จึงจะสรุปผลได้ ฉะนั้นจึงต้องใช้วิธีการสุ่มตัวอย่างจากข้อมูลที่กำลังทำการศึกษา และใช้คุณลักษณะของตัวอย่างดังกล่าวนี้ตัดสินว่า สมมติฐานนั้นเป็นจริงหรือไม่ ถ้าหลักฐานที่ได้จากตัวอย่างไม่สอดคล้องกับสมมติฐานที่ตั้งไว้ ก็จะทำให้สรุปได้ว่าปฏิเสธสมมติฐานนั้นและในทางตรงกันข้ามก็จะยอมรับสมมติฐานที่ตั้งขึ้น ทั้งนี้โดยเลือกสถิติเพื่อใช้ในการคำนวณหาค่าเพื่อให้สามารถสรุปว่าสมมติฐานนั้นเป็นจริงและยอมรับสมมติฐานนั้น ด้วยเหตุผลที่ไม่มีหลักฐานเพียงพอที่จะปฏิเสธ [2] โดยการทดสอบสมมติฐานเชิงสถิติมีขั้นตอนการทำงานห้าขั้นตอน ดังนี้

ขั้นตอนที่หนึ่ง ตั้งสมมติฐานสถิติ

สมมติฐานสถิติ คือ ข้อสมมติฐานหรือข้อความที่เกี่ยวข้องกับประชากรชุดเดียวหรือมากกว่า ซึ่งอาจเป็นจริงหรือไม่ก็ได้ โดยสมมติฐานที่ตั้งขึ้นมีสองแบบ ได้แก่ สมมติฐานหลัก(Null Hypotheses: H_0) และสมมติฐานอื่น (Alternative Hypotheses: H_1)

การสร้างข้อสมมติฐาน ถ้าต้องการทดสอบในทิศทางเชิงเดียว เช่น มากกว่า น้อยกว่า ดีกว่า หรือด้อยกว่า เป็นต้น การทดสอบนี้จะถูกสร้างข้อสมมติฐานอื่น H_1 โดยใช้สัญลักษณ์อสมการ (> หรือ <) ให้สอดคล้องกับทิศทางของการทดสอบ เช่น ในการทดสอบจำนวนสุ่ม จะทดสอบสมมติฐานที่คาดว่าจำนวนสุ่มที่นำมาทดสอบเป็นจำนวนสุ่มเทียมน้อยกว่าร้อยละสิบแล้วจะได้ข้อสมมติฐานอื่นว่า $H_1: p<0.1$ และสมมติฐานหลักคือ $H_0: p=0.1$ เป็นต้น

กรณีที่ต้องการทดสอบในสองทิศทางหรือสองสิ่งที่แตกต่างกัน เช่น ในการทดสอบจำนวนสุ่ม ต้องการทดสอบข้อสมมติฐานที่คาดว่าจำนวนสุ่มที่นำมาทดสอบไม่เป็นจำนวนสุ่มเทียม ดังนั้นจะได้ข้อสมมติฐานอื่นว่า $H_1: p\neq 0.1$ และสมมติฐานหลักคือ $H_1: p=0.1$ เป็นต้น

การกำหนดข้อสมมติฐานเพื่อต้องการทดสอบพารามิเตอร์ตัวใดจะทำให้ทราบว่าเป็นการทดสอบทางเดียวหรือสองทาง และการกำหนดระดับนัยสำคัญ (Significance level: α) จะเป็นการเลือกตัวสถิติทดสอบที่เหมาะสมเพื่อทดสอบสมมติฐาน การกำหนดบริเวณวิกฤตจะต้องทำให้สอดคล้องกับ H_1 α และตัวสถิติ จากนั้นคำนวณสถิติทดสอบ ซึ่งขั้นตอนในการทดสอบสมมติฐานสามารถสรุปได้ดังนี้

ขั้นตอนที่หนึ่งตั้งสมมติฐานหลัก $H_0\colon \theta=\theta_0$

ขั้นตอนที่สองตั้งสมมติฐานอื่น $H_1\colon \theta>\theta_0$ หรือ $H_1\colon \theta<\theta_0$ หรือ $H_1\colon \theta\neq\theta_0$

ขั้นตอนที่สามกำหนดระดับนัยสำคัญ α

ขั้นตอนที่สี่เลือกสถิติทดสอบที่เหมาะสมและกำหนดบริเวณวิกฤตหรือบริเวณปฏิเสธ H_0

ขั้นตอนที่ห้า คำนวณสถิติทดสอบจากตัวอย่างขนาดของจำนวนสุ่มที่ต้องการนำมาทดสอบ

ขั้นตอนที่หก การสรุปผล นั่นคือ ปฏิเสธ H_0 ถ้าสถิติทดสอบที่คำนวณได้อยู่ในบริเวณปฏิเสธ H_0 หรือยอมรับ H_1 ถ้าสถิติทดสอบที่คำนวณได้ อยู่ในบริเวณยอมรับ H_0

จากผลการทดสอบ กรณีที่ผลการทดสอบที่ได้แสดงว่าปฏิเสธสมมติฐาน นั่นหมายถึงสมมติฐานนั้นผิด ส่วนการยอมรับสมมติฐาน นั่นหมายความว่าไม่มีหลักฐานเพียงพอที่จะเชื่อถือเป็นอย่างอื่น ผลลัพธ์จากการทดสอบสมมติฐานเป็นการตัดสินใจเพื่อหาข้อยุติเกี่ยวกับสมมติฐานหลัก โดยจะมีคำตอบที่เป็นไปได้ทั้งหมดสี่แบบ คือ

ยอมรับสมมติฐานหลัก เมื่อสมมติฐานหลักเป็นจริง

ปฏิเสธสมมติฐานหลัก เมื่อสมมติฐานหลักเป็นจริง เรียกว่า ความผิดพลาดประเภท *I*

ยอมรับสมมติฐานหลัก เมื่อสมมติฐานหลักไม่จริง เรียกว่า ความผิดพลาดประเภท *II*

ปฏิเสธสมมติฐานหลัก เมื่อสมมติฐานหลักไม่จริง

การพิจารณาตัดสินใจแต่ละครั้ง อาจจะทำความผิดพลาดประเภทใดประเภทหนึ่งเกิดขึ้น ดังนั้นการคำนวณพารามิเตอร์ของประชากรจะทำทราบว่าเกิดความผิดพลาดหรือไม่และเป็นความผิดพลาดประเภทใด แต่เมื่อไม่ทราบความจริงนั้น จึงตั้งสมมติฐานขึ้นมาและทำการทดสอบนั่นเอง โดยผลของการทดสอบจึงรวมเอาความผิดพลาดที่อาจจะเกิดขึ้นไว้ด้วย โดยมีความน่าจะเป็นของการกระทำความผิดพลาดประเภท *I* เรียกว่า ระดับนัยสำคัญของการทดสอบนั่นเอง

ขั้นตอนที่สอง การกำหนดระดับนัยสำคัญ

การกำหนดระดับนัยสำคัญ (Significance Level) หรือเรียกว่า บริเวณวิกฤต จะถูกกำหนดค่าไว้ล่วงหน้าก่อนการลงมือทำการทดสอบสมมติฐานทางสถิติ ซึ่งการกำหนดระดับนัยสำคัญจะเป็นการกำหนดค่าความน่าจะเป็นของการกระทำความผิดพลาดประเภท *I* ในการทดสอบสมมติฐาน โดยค่าที่นิยมใช้คือ 0.10 และ 0.05 ดังนั้นจึงถือว่าเป็นการกำหนดขอบเขตความผิดพลาดหรือความคลาดเคลื่อนที่จะยอมให้เกิดขึ้นได้นั่นเอง จากเนื้อหาข้างต้นแสดงให้เห็นว่าในการ

ทดสอบสมมติฐาน ถ้าเกิดความผิดพลาดหรือความคลาดเคลื่อนน้อยกว่าที่กำหนดไว้ก็จะทำการยอมรับสมมติฐานที่ตั้งไว้ (H_0)

ระดับนัยสำคัญเป็นสิ่งที่บ่งบอกถึงระดับความเชื่อมั่น (Confidence Level) ซึ่งหาได้จาก (1-α) x 100 % เช่น ที่ระดับนัยสำคัญ 0.10 แสดงว่ามีความน่าเชื่อมั่นร้อยละ 99 หมายถึงในการทดสอบอย่างใดอย่างหนึ่งจำนวน 100 ครั้ง ก็จะได้ผลดังที่ปรากฏนั้นไม่น้อยกว่า 99 ครั้ง โดยมีความผิดพลาดหรือความคลาดเคลื่อนไม่เกิน 1 ครั้ง เป็นต้น

ขั้นตอนที่สาม การกำหนดขอบเขตการทดสอบ

การกำหนดขอบเขตการทดสอบสมมติฐาน จะมีการแบ่งบริเวณการพิจารณาออกเป็นสองส่วนคือ บริเวณวิกฤต (Critical region) หมายถึงบริเวณของการปฏิเสธสมมติฐานหลัก H_0 และบริเวณยอมรับ (Acceptance region) หมายถึงบริเวณของการยอมรับสมมติฐานหลัก H_0 โดยมีค่าที่แบ่งบริเวณทั้งสอง เรียกว่า ค่าวิกฤติ (Critical value) และการทดสอบสมมติฐานจะมีการแบ่งขอบเขตการพิจารณาสองแบบ คือ การทดสอบสมมติฐานด้านเดียวและสองด้าน ซึ่งมีรายละเอียดดังนี้

การทดสอบสมมติฐานด้านเดียว (One-tailed Test) หรือการทดสอบทางเดียว เป็นการมองในแง่ของความแตกต่างที่มากกว่าหรือน้อยกว่าเพียงอย่างใดอย่างหนึ่งเท่านั้น ซึ่งอยู่ในลักษณะดังนี้

กรณีที่ 1 $H_0: \theta = \theta_0$
$H_1: \theta > \theta_0$

เมื่อถือว่า H_0 เป็นจริงบริเวณวิกฤตหรือบริเวณปฏิเสธ H_0 จะอยู่ที่ปลายหางด้านขวามือทั้งหมดของการแจกแจงของค่าสถิติทดสอบ $\hat{\theta}$ ด้วยขนาด α ดังรูป 4.4

กรณีที่ 2 $H_0: \theta = \theta_0$
$H_1: \theta < \theta_0$

เมื่อถือว่า H_0 เป็นจริงบริเวณวิกฤตหรือบริเวณปฏิเสธ H_0 จะอยู่ที่ปลายหางด้านซ้ายมือทั้งหมดของการแจกแจงของค่าสถิติทดสอบ $\hat{\theta}$ ด้วยขนาด α ดังรูป 4.5

สัญลักษณ์อสมการใน H_1 เป็นตัวชี้ทิศทางหรือตำแหน่งที่บริเวณวิกฤตอยู่

การทดสอบสมมติฐานสองด้าน (One-tailed Test)หรือการทดสอบสองทาง เป็นการมองในแง่ประเด็นที่แตกต่างกัน ซึ่งอยู่ในลักษณะ

$H_0: \theta = \theta_0$
$H_1: \theta \neq \theta_0$ ซึ่งหมายถึง $\theta < \theta_0$ หรือ $\theta > \theta_0$

เมื่อถือว่า H_0 เป็นจริงบริเวณวิกฤตหรือบริเวณปฏิเสธ H_0 จะอยู่ที่ปลายหางทั้งสองข้างของการแจกแจงของค่าสถิติทดสอบ $\hat{\theta}$ ด้วยขนาด $\frac{\alpha}{2}$ ดังรูป 4.6

ขั้นตอนที่สี่ การเลือกสถิติทดสอบ

การเลือกสถิติทดสอบ (Test statistic) จะต้องเลือกให้เหมาะสมกับลักษณะของชุดประชากรที่จะศึกษา โดยมุ่งไปสู่คุณลักษณะของกลุ่มประชากร ซึ่งแสดงออกมาได้ด้วยตัวเลข เช่น ค่าเฉลี่ยเลขคณิตของประชากร (Mean) ส่วนเบี่ยงเบนมาตรฐานของประชากร(Standard deviation) หรือสัดส่วนของประชากร (Population proportion) เป็นต้น โดยมีรายละเอียดดังต่อไปนี้

การทดสอบสมมติฐานเกี่ยวกับค่าเฉลี่ย

เนื่องจากการทดสอบทางสถิติต้องใช้จำนวนสุ่มจำนวนมาก เพื่อให้ได้ผลการทดสอบที่ดีและให้ค่าที่ใกล้เคียงกับข้อมูลจริงมากที่สุดที่หน่วยประมวลผลสามารถรองรับได้ ดังนั้นวิทยานิพนธ์นี้ จึงสุ่มตัวอย่างจำนวน 1,000,000 จำนวน ดังนั้นจึงเป็นไปตามกทฤษฎีที่เกี่ยวข้องกับกรณีที่จำนวนตัวอย่าง $n \geqslant 30$ โดยแยกการทดสอบเกี่ยวกับค่าเฉลี่ยได้ดังนี้

การทดสอบสมมติฐานเกี่ยวกับค่าเฉลี่ยประชากรกลุ่มเดียว

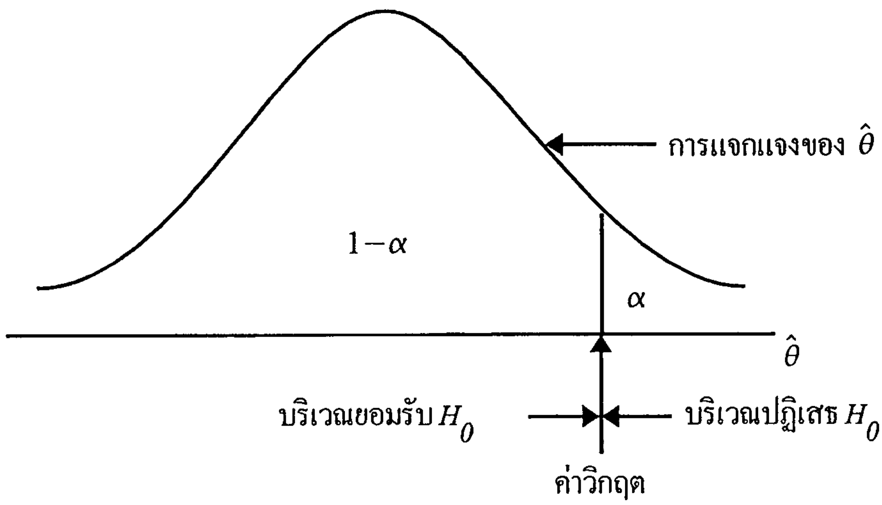
สถิติทดสอบ คือ
$$Z = \frac{(\bar{x} - \mu_0)}{(\frac{\sigma}{\sqrt{n}})} \tag{4.8}$$

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า Z ที่คำนวณได้ตกอยู่บริเวณวิกฤต

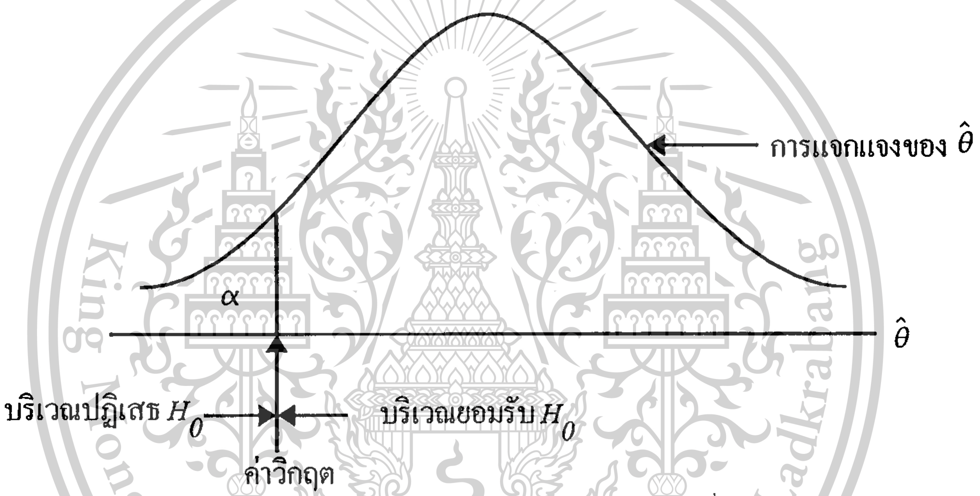
การทดสอบสมมติฐานเกี่ยวกับผลต่างระหว่างค่าเฉลี่ย ของประชากรสองกลุ่ม

สถิติทดสอบ คือ
$$Z = \frac{((\bar{X}_1 - \bar{X}_2) - d_0)}{\sqrt{(\frac{\sigma^2}{n} + \frac{\sigma^2}{n})}} \tag{4.9}$$

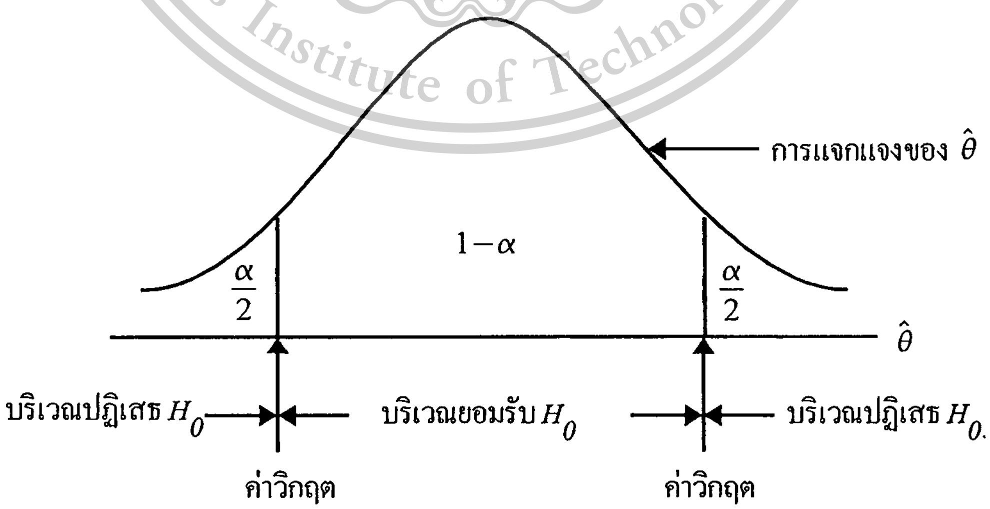
การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า Z ที่คำนวณได้ตกอยู่บริเวณวิกฤต



รูปที่ 4.4 การใช้ทฤษฎีขีดจำกัดสู่ศูนย์กลางกับตัวอย่างประชากร 3 รูปแบบ



รูปที่ 4.5 การใช้ทฤษฎีขีดจำกัดสู่ศูนย์กลางกับตัวอย่างประชากร 3 รูปแบบ



รูปที่ 4.6 การใช้ทฤษฎีขีดจำกัดสู่ศูนย์กลางกับตัวอย่างประชากร 3 รูปแบบ

การทดสอบสมมติฐานเกี่ยวกับสัดส่วนของประชากรกลุ่มเดียว

สถิติทดสอบ เมื่อ n มีค่ามากกว่า 30 และ p_0 ไม่เข้าใกล้ค่าศูนย์หรือหนึ่งมากจนเกินไป คือทั้ง np_0 และ $np_0 > 5$ สามารถหาสถิติทดสอบได้จาก

สถิติทดสอบ คือ $$Z=\frac{(\hat{p}-p_0)}{\sqrt{(\frac{(p_0 q_0)}{n})}}=\frac{(x-np_0)}{\sqrt{(np_0 q_0)}} \quad (4.10)$$

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า Z ที่คำนวณได้ตกอยู่บริเวณวิกฤต

การทดสอบสมมติฐานเกี่ยวกับผลต่างระหว่างสัดส่วนของประชากรสองกลุ่ม

เมื่อ $\hat{p}_1=\frac{X_1}{n}$ และ $\hat{p}_2=\frac{X_2}{n}$

สถิติทดสอบ คือ $$Z=\frac{(\hat{p}_1-\hat{p}_2)}{\sqrt{((\hat{p}\hat{q})(\frac{1}{n}+\frac{1}{n}))}} \quad (4.11)$$

สรุปผล จะปฏิเสธ H_0 ค่า Z ที่คำนวณได้ตกอยู่บริเวณวิกฤต

การทดสอบสมมติฐานเกี่ยวกับความแปรปรวนของประชากรกลุ่มเดียว

สถิติทดสอบ คือ $\chi^2=\frac{((n-1)S^2)}{\sigma_0^2}$ ที่มีการแจกแจงไคกำลังสอง ที่มี k=n-1 (4.12)

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า χ^2 ที่คำนวณได้ตกอยู่บริเวณวิกฤต

การทดสอบสมมติฐานเกี่ยวกับความแปรปรวนของประชากรสองกลุ่ม

สถิติทดสอบ คือ $f=\frac{S_1^2}{S_2^2}$ ที่มี $k_1=n_1-1$ และ $k_2=n_2-1$ (4.13)

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า f ที่คำนวณได้ตกอยู่บริเวณวิกฤต

ขั้นตอนที่ห้า การสรุปผลการทดสอบ

การสรุปผลการทดสอบว่าจะยอมรับหรือปฏิเสธสมมติฐานหลัก H_0 นั้น คือ จะปฏิเสธ H_0 ถ้าสถิติทดสอบที่คำนวณได้อยู่ในบริเวณปฏิเสธ H_0 หรือยอมรับ H_1 ถ้าสถิติทดสอบที่คำนวณได้ อยู่ในบริเวณยอมรับ H_0

นอกจากการทดสอบสมมติฐานที่ใช้สถิติทดสอบดังที่ได้นำเสนอไปข้างต้นแล้วนั้น วิทยานิพนธ์นี้ ได้นำการทดสอบไคกำลังสองมาประยุกต์ใช้เพื่อทดสอบว่าผลที่ได้จากการทดสอบมีความสอดคล้องกับทฤษฎีหรือไม่ โดยมีรายละเอียดการทดสอบดังนี้

4.5 การทดสอบไคกำลังสอง (Chi-Square Test)

จากการแจกแจงค่าความแปรปรวนของกลุ่มตัวอย่าง จะมีการแจกแจงไคกำลังสอง ซึ่งเป็นการแจกแจงที่ใช้อธิบายความสัมพันธ์ระหว่างความแปรปรวนของประชากรปกติ (σ^2) กับความแปรปรวนของตัวอย่าง (S^2) และใช้การแจกแจงนี้เพื่อประมาณค่าและทดสอบสมมติฐานเกี่ยวกับ σ^2 โดยใช้ S^2 ซึ่งการแจกแจงไคกำลังสองดังกล่าวเป็นการแจกแจงของค่าสังเกตที่ได้จากการวัด โดยข้อมูลถูกจัดในรูปของความถี่ และการทดสอบดังกล่าวนี้ส่วนใหญ่เป็นการศึกษาทางด้านคุณภาพ โดยค่าสังเกตได้มาจากการนับหรือการตรวจสอบคุณภาพ เป็นต้น

การแจกแจงไคกำลังสองที่นำมาใช้นี้ เป็นการประยุกต์เพื่อใช้เปรียบเทียบความถี่ที่สังเกต (Observed frequency) กับความถี่ที่คาดหวัง (Expected frequency) ซึ่งสอดคล้องกับความน่าจะเป็นของเหตุการณ์ที่ข้อมูลถูกจัดแบ่งตามกลุ่มดังที่กล่าวไว้ข้างต้น การแจกแจงไคกำลังสองประยุกต์นี้ จะถูกนำมาใช้เพื่อการทดสอบทางด้านคุณภาพเท่านั้นซึ่งคิดค้นโดย คาร์ล เพียร์สัน (Karl Pearson) (ค.ศ. 1857-1963) ซึ่งการทดสอบที่เกี่ยวข้องได้แก่ การทดสอบหลายสัดส่วน (Test for proportions) การทดสอบความเหมาะสมของการแจกแจง (Test for Goodness of Fit) และการทดสอบความเป็นอิสระ (Test for independence) ซึ่งในวิทยานิพนธ์นี้เน้นใช้การแจกแจงไคกำลังสองเพื่อการทดสอบสัดส่วนของการทดสอบคุณสมบัติของจำนวนสุ่ม และความเหมาะสมของการแจกแจงของชุดจำนวนสุ่ม ว่าสัดส่วนที่สังเกตและค่าทางทฤษฎีมีความแตกต่างกันมากน้อยเพียงใด และจำนวนสุ่มมีการแจกแจงตามที่ต้องการหรือไม่ ซึ่งจะกล่าวในรายละเอียดในลำดับถัดไป

การทดสอบหลายสัดส่วน (Test for proportions)

ในการทดสอบประชากรหนึ่งถ้ามีเหตุการณ์ที่สนใจ k เหตุการณ์ และอยากทราบว่าการเกิดขึ้นของเหตุการณ์ต่างเป็นเช่นไร ตัวอย่างเช่น ถ้ามีเหตุการณ์ที่สนใจจะทำการศึกษาเป็น $A_1, A_2, A_3, .., A_k$ จะทำการทดสอบเพื่อเปรียบเทียบว่ามีอัตราส่วนการเกิดขึ้นของเหตุการณ์ดังกล่าวเป็นไปตามอัตราส่วน $C_1, C_2, C_3, .., C_k$ หรือไม่ และจะสามารถสรุปได้โดยการทดสอบสมมติฐานด้วยสถิติไคกำลังสอง ซึ่งมีระดับความเป็นอิสระ เท่ากับ k-1 ทั้งนี้เนื่องจากภายใต้ความถี่

ที่ได้จากการสังเกตทั้งหมดของการทดสอบ จะมีความเป็นอิสระในการหาความถี่คาดหวัง จำนวน k-1 เหตุการณ์เท่านั้น โดยมีขั้นตอนการทดสอบเหมือนการทดสอบสมมติฐานดังที่ได้นำเสนอในหัวข้อที่ผ่านมา ดังนั้นจะหาสถิติทดสอบได้จาก

สถิติทดสอบ คือ $$\chi^2=\sum_{i=1}^{k}(\frac{(O_i-E_i)^2}{E_i}) \qquad (4.14)$$

โดย O_i คือ ความถี่ที่ค่าสังเกตที่เกิดขึ้นจากการทดลองจริง (Observed Frequency)

E_i คือ ความถี่ที่ค่าคาดหวังจะเป็นไปตามทฤษฎี (Expected Frequency)

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

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า χ^2 ที่คำนวณได้ตกอยู่บริเวณวิกฤต และสามารถสรุปได้ว่าข้อมูลที่รวบรวมได้นั้นมาจากประชากร ซึ่งการเกิดขึ้นของเหตุการณ์ต่างๆ ไม่เป็นไปตามอัตราส่วนของสมมติฐาน H_0

การทดสอบความเหมาะสมของการแจกแจง (Test for Goodness of Fit)

การทดสอบความเหมาะสมของการแจกแจง หมายถึงการเปรียบเทียบตัวเลขที่ได้จากตัวอย่างกับค่าที่ได้ตามทฤษฎีใดทฤษฎีหนึ่งว่าเหมือนกันหรือไม่ ซึ่งจะทดสอบว่าข้อมูลที่ทำการรวบรวมมานั้นจะมีการแจกแจงแบบที่ต้องการหรือไม่ ซึ่งสามารถหาสถิติทดสอบได้จาก

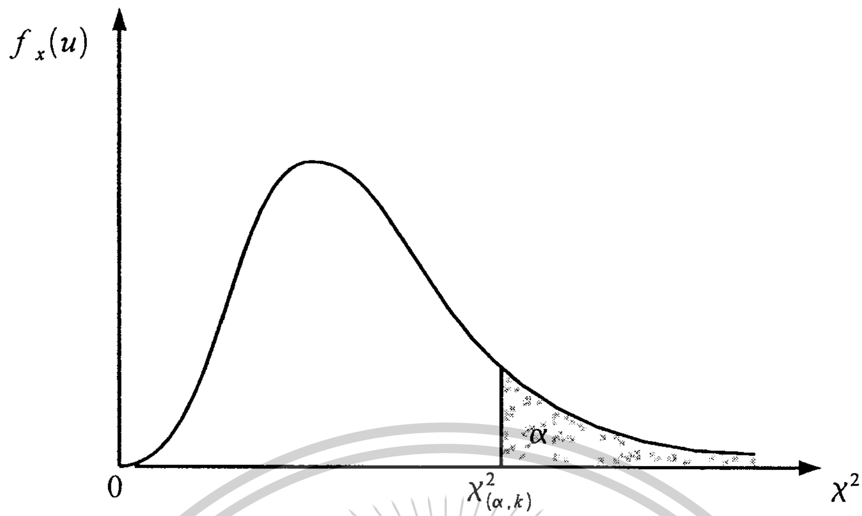
สถิติทดสอบ คือ $$\chi^2=\sum_{i=1}^{k}(\frac{(O_i-E_i)^2}{E_i}) \qquad (4.15)$$

โดย O_i คือ ความถี่ที่ค่าสังเกตที่เกิดขึ้นจากการทดลองจริง (Observed Frequency)

E_i คือ ความถี่ที่ค่าคาดหวังจะเป็นไปตามทฤษฎี (Expected Frequency)

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

การสรุปผลการทดสอบจะทำการปฏิเสธ H_0 เมื่อค่า χ^2 ที่คำนวณได้ตกอยู่บริเวณวิกฤต และสามารถสรุปได้ว่าข้อมูลที่รวบรวมได้นั้นมาจากประชากร ซึ่งการเกิดขึ้นของเหตุการณ์ต่างๆ ไม่เป็นไปตามอัตราส่วนของสมมติฐาน H_0



รูปที่ 4.7 ค่าวิกฤตของการแจกแจงไคกำลังสอง $\chi^2 > \chi^2_\alpha$ บริเวณวิกฤตคือ χ^2 ที่คำนวณได้ [2]

การพิจารณาจึงใช้การแจกแจงไคกำลังสองโดยกำหนดบริเวณวิกฤตทางขวาเท่านั้น ดังรูป 4.7 สำหรับการทดสอบที่ต้องการทราบว่า O_i แตกต่างจาก E_i มากน้อยเพียงใด หรือต้องการทราบว่าผลที่ได้จากการทดสอบสอดคล้องกับทฤษฎีหรือไม่ นั่นคือต้องการทดสอบ สมมติฐานว่ามีความแตกต่างของ O_i และ E_i เป็นไปอย่างมีนัยสำคัญหรือไม่ ตามทฤษฎีหรือข้อกำหนดแล้ว ค่า O_i และค่า E_i จะใกล้เคียงกันหรือเท่ากัน เมื่อคำนวณค่า χ^2 แล้วได้ค่าที่เข้าใกล้ศูนย์ แต่ถ้าความถี่ที่สังเกตไม่สอดคล้องกับความถี่ตามทฤษฎีหรือข้อกำหนดแล้ว ค่า O_i และค่า E_i จะแตกต่างกัน โดยจะได้ค่า χ^2 ที่คำนวณได้จะมีค่ามาก

บทที่ 5
วิธีดำเนินการวิจัย

การพัฒนาโปรแกรมทดสอบคุณสมบัติจำนวนสุ่มนี้ เป็นการพัฒนาโดยอ้างอิงชุดทดสอบทางสถิติเอ็นไอเอสที โดยวัตถุประสงค์ของการทดสอบคือ ตรวจสอบหาคุณสมบัติของจำนวนสุ่มแท้และจำนวนสุ่มเทียมก่อนนำไปประยุกต์ใช้งาน เพื่อให้สามารถทราบว่าจำนวนสุ่มดังกล่าวมีคุณสมบัติเพียงพอที่จะนำไปใช้งานหรือไม่ ซึ่งการทดสอบโดยใช้หลักการทางสถิติจำเป็นจะต้องสังเกตคุณลักษณะของข้อมูลด้วยการเก็บข้อมูลจำนวนมาก เพื่อทำให้การประเมินหรือการวิเคราะห์ผลมีความคลาดเคลื่อนน้อยที่สุด ดังนั้นจึงเป็นสาเหตุที่ทำให้ใช้เวลานานในการทดสอบ จากการศึกษาชุดอ้างอิงชุดทดสอบทางสถิติเอ็นไอเอสที พบว่ากระบวนสำคัญของการทดสอบคือการคำนวณสถิติทดสอบและการสรุปผลว่าผ่านหรือไม่ผ่านการทดสอบนั้น จุดสำคัญที่นำมาพิจารณา คือ ค่าที่คำนวณได้จากสถิติทดสอบ (Test Statistic) และการคำนวณค่าพี (P-value) ซึ่งเป็นค่าที่ถูกใช้เป็นเกณฑ์ในการเปรียบเทียบว่ามีความผิดพลาดหรือความคลาดเคลื่อนเกินกว่าที่กำหนดไว้หรือไม่ ซึ่งจะส่งผลให้การพิจารณาการทดสอบคุณสมบัติของจำนวนสุ่มว่าเป็นไปตามเกณฑ์ดังกล่าวด้วย

5.1 การนำเสนอหลักการเพื่อการคำนวณและพิจารณาการผ่านการทดสอบ

จากชุดอ้างอิงชุดทดสอบทางสถิติเอ็นไอเอสที [2] พบว่าใช้สถิติทดสอบสองแบบที่สอดคล้องกับการแจกแจงของจำนวนสุ่ม แบบที่หนึ่ง สำหรับจำนวนสุ่มที่มีการแจกแจงแบบปกติ สถิติทดสอบและการพิจารณาการผ่านการทดสอบสามารถคำนวณได้จาก *Erfc* ดังสมการที่ 5.1 แบบที่สองสำหรับจำนวนสุ่มที่มีการแจกแจงไคกำลังสอง การพิจารณาการผ่านการทดสอบสามารถคำนวณได้จาก *Igamc* ดังสมการที่ 5.2

$$P-value=erfc(x) \quad \text{เมื่อ } x \text{ คือค่าที่สังเกต}$$

$$erfc(x)=\frac{2}{\sqrt{\pi}}\int_{x}^{\infty} e^{-t^2}\,dt \tag{5.1}$$

$$P-value=igamc(x) \quad \text{เมื่อ } x \text{ คือค่าที่สังเกต}$$

$$F(a,x)=\Gamma\frac{(a,x)}{(\Gamma(a))}=\frac{1}{(\Gamma(a))}\int_{x}^{\infty} u^{-t} e^{(a-1)}\,dt \tag{5.2}$$

เมื่อ $\Gamma(a)$ คือแกมมาฟังก์ชัน (Gamma Function)

$$\Gamma(a)=\int_{0}^{\infty} t^{(a-1)} e^{(-t)} dt \tag{5.3}$$

แกมมาฟังก์ชันเป็นฟังก์ชันพิเศษ (Special Function) ที่มีรูปสมการซับซ้อน ส่งผลให้กระบวนการคำนวณและการพิจารณาการผ่านการทดสอบนั้นมีขั้นตอนและระยะเวลาของการประมวลผลนาน โดยเฉพาะอย่างยิ่งกรณีที่เก็บข้อมูลจำนวนมากและทดสอบจำนวนหลายครั้งเช่นการทดสอบทางสถิติที่ต้องการความแม่นยำสูง ดังนั้นจึงจะส่งผลทำให้การทดสอบมีความล่าช้า ดังนั้นวิทยานิพนธ์นี้จึงมุ่งการพัฒนาการทดสอบให้มีรูปแบบที่ง่าย ความซับซ้อนต่ำและลดการใช้เวลาในการคำนวณ รวมทั้งเป็นแนวทางพัฒนาการให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์(Web Service) และสามารถพิสูจน์ได้ว่าจำนวนสุ่มนั้นเป็นจำนวนสุ่มเพียงพอที่จะนำมาประยุกต์ใช้งานด้านวิทยาการรหัสลับได้ โดยนำเสนอสองส่วน ได้แก่ ส่วนแรกสำหรับจำนวนสุ่มที่มีการแจกแจงแบบปกติ โดยนำเสนอสถิติทดสอบและการผ่านการทดสอบที่จะคำนวณได้จากค่ามาตรฐาน *(Z)* ดังสมการที่ 3.30 และส่วนที่สองสำหรับจำนวนสุ่มที่มีการแจกแจงแบบไคกำลังสอง โดยนำเสนอสถิติทดสอบและการผ่านการทดสอบที่จะคำนวณได้จากสถิติทดสอบไคกำลังสอง χ^2 ดังสมการที่ 4.15

5.1.1 หลักการที่หนึ่ง

ถ้าให้ X เป็นตัวแปรสุ่มที่มีการกระจายตัวเป็นเส้นโค้งปกติ มีค่าเฉลี่ยเท่ากับ $\mu(-\infty<\mu<\infty)$ และมีความแปรปรวนเป็น $\sigma^2(\sigma^2>0)$ จะสามารถหาฟังก์ชันความหนาแน่นดังสมการที่ 5.4

$$p(x)=\frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu)^2/2\sigma^2} \tag{5.4}$$

การหาพื้นที่ใต้เส้นโค้งปกติสามารถหาได้จากการแจกแจงปกติสะสม (The Cumulative distribution function: CDF) ซึ่งเป็นการปริพันธ์ (Integration) ฟังก์ชันความหนาแน่น ดังแสดงตามสมการที่ 5.6

$$F(X)=P(X\leqslant x)=\int_{-\infty}^{x} p(u)\,du \tag{5.5}$$

$$F(X)=\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{x} e^{-(x-\mu)^2/2\sigma^2}\,du \tag{5.6}$$

จากหลักการข้างต้นการคำนวณสถิติทดสอบของชุดอ้างอิงเอ็นไอเอสที สามารถคำนวณจากส่วนเติมเต็มฟังก์ชันค่าคลาดเคลื่อน (*Erfc*) ซึ่งสามารถหาความสัมพันธ์ระหว่าง CDF และ *Erfc* เมื่อให้ค่าเฉลี่ยเลขคณิตเท่ากับศูนย์และมีค่าเบี่ยงเบนเฉลี่ยเท่ากับหนึ่ง จะได้ความสัมพันธ์เป็นดังนี้

$$F(X)=\frac{1}{2}\frac{1}{\sqrt{\pi}}\int_{-\infty}^{(x-\mu)/\sqrt{2\sigma}} e^{-t^2}\,dt$$

$$F(X)=\frac{1}{2}+\frac{1}{2}erf\left(\frac{x-\mu}{\sqrt{2}\sigma}\right)$$

จากสมการของฟังก์ชันความคลาดเคลื่อน(*Erf*)

$$erf(x)=\frac{2}{\sqrt{\pi}}\int_{0}^{x} e^{-t^2}\,dt \tag{5.7}$$

สามารถหาความสัมพันธ์ระหว่าง *Erf* กับ *Erfc* ดังนี้

$$erf=1-erfc \tag{5.8}$$

ดังนั้นจึงสามารถเขียนสมการ CDF ในรูปสมการของ *Erfc* ดังนี้

$$F(x)=1-\frac{1}{2}erfc\left(\frac{x-\mu}{\sqrt{2}\sigma}\right) \tag{5.9}$$

เพราะฉะนั้นสามารถหาค่า *Erfc* ได้จากสมการ

$$erfc(x)=\frac{2}{\sqrt{\pi}}\int_{x}^{\infty} e^{-t^2}\,dt \tag{5.10}$$

จากสมการ 5.10 จะเห็นได้ว่าการหาค่า *Erfc* เพื่อคำนวณสถิติทดสอบของชุดทดสอบอ้างอิงนั้น เป็นการหาปริพันธ์เป็นสมการที่มีความซับซ้อน โดยเฉพาะอย่างยิ่งในกรณีที่ต้องเก็บข้อมูลจำนวนมากและทดสอบจำนวนหลายครั้งเช่นการทดสอบทางสถิติเพื่อให้มีต้องการความแม่นยำสูง

แล้วนั้น จะส่งผลทำให้การทดสอบมีความล่าช้า ไม่เหมาะสมสำหรับพัฒนาชุดทดสอบเพื่อให้บริการทดสอบคุณสมบัติของจำนวนสุ่มผ่านระบบออนไลน์(Web Service)ได้ ดังนั้นวิทยานิพนธ์นี้ได้นำเสนอการหลักการพิจารณาที่มีรูปสมการที่เรียบง่ายและมีความซับซ้อนต่ำ โดยมีรายละเอียดดังนี้

จากการแจกแจงแบบปกติและการหาพื้นที่ใต้โค้งปกติโดยการหาค่า CDF ของการแจกแจงดังสมการที่ 5.6 สมการดังกล่าวสามารถแปลงรูปฟังก์ชันให้อยู่ในรูปสมการที่สามารถหาปริพันธ์อย่างง่าย เรียกว่าค่ามาตรฐาน ซึ่งมีค่าเฉลี่ย $\mu=0$ และค่าเบี่ยงเบนมาตรฐาน $\sigma=1$ และสามารถหาได้ค่าปกติมาตรฐานดังสมการที่ 5.11

$$Z=\frac{x_i-\mu}{\sigma} \tag{5.11}$$

สมการที่ 5.5 5.6 และ 5.11 สามารถหาปริพันธ์ของตัวแปรสุ่มแบบปกติมาตรฐานได้ดังนี้

$$F(X)=P(X\leqslant x) \tag{5.12}$$

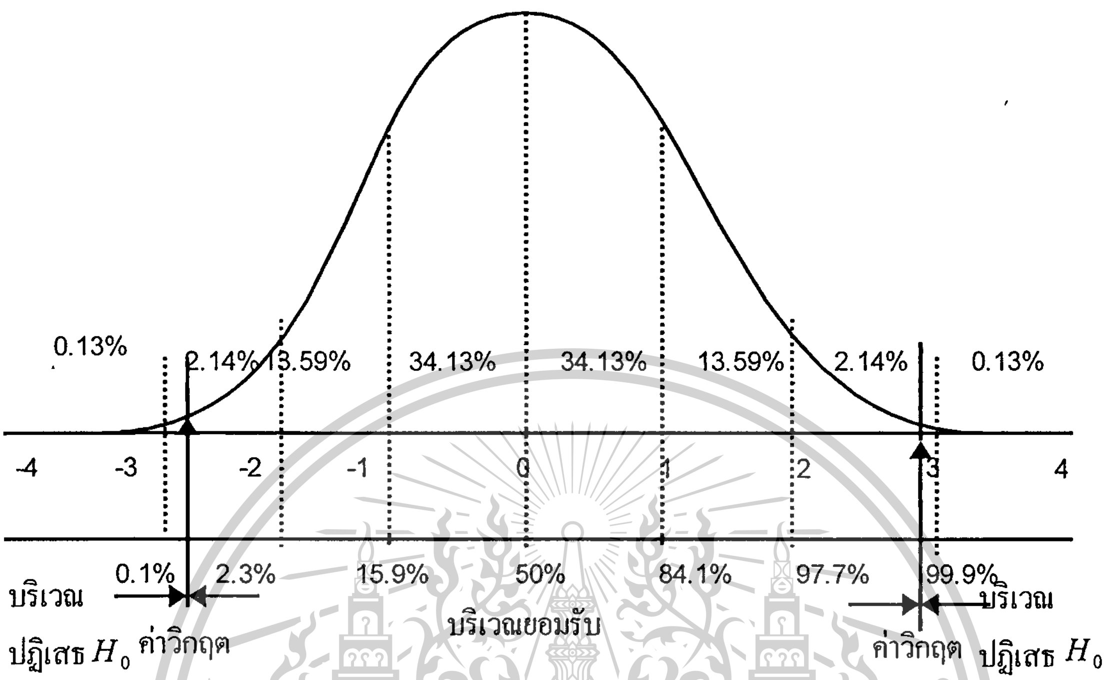
$$F(Z)=P(Z\leqslant\frac{x_i-\mu}{\sigma}) \tag{5.13}$$

$$F(Z)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{(x_i-\mu)/\sigma} e^{-z^2}\,dz \tag{5.14}$$

ซึ่งความสัมพันธ์ระหว่าง *Erfc* และ *Z* สามารถหาได้จากสมการที่ 5.11 และ 5.14 ดังนี้

$$F(Z)=\frac{1}{2}(erfc\left(\frac{Z}{\sqrt{2}}\right)) \tag{5.15}$$

จากหลักการที่นำเสนอ จะเห็นว่าการหาสถิติทดสอบนี้อยู่ในรูปสมการที่มีความซับซ้อนต่ำ โดยมีประเด็นที่สำคัญคือสามารถเปรียบเทียบระหว่างลักษณะของข้อมูลและค่าทางสถิติได้โดยตรง โดยอ้างอิงการลักษณะของการแจกแจงของชุดจำนวนสุ่ม ทำให้สามารถพิจารณาการผ่านการทดสอบ โดยสามารถเปรียบเทียบการพิจารณาขอบเขตวิกฤตที่ใช้ในการตัดสินใจยอมรับหรือปฏิเสธข้อสมมติฐานที่ตั้งไว้เป็นร้อยละของพื้นที่ ดังรูปที่ 5.1 ทำให้สามารถพิจารณาการผ่านการทดสอบและทราบถึงระดับความเชื่อมั่นได้ทันที ซึ่งจะส่งผลให้การทดสอบคุณสมบัติของจำนวนสุ่มมีระยะเวลาในการประมวลผลการทดสอบสั้นลงได้



รูปที่ 5.1 การแปลงค่าพื้นที่ใต้โค้งปกติในให้อยู่ในระบบค่ามาตรฐาน (*Z*) และระบบเปอร์เซนต์ไทล์ (Percentiles)

5.1.2 หลักการที่สอง

จากการแจกแจงแบบไคกำลังสอง สามารถหาฟังก์ชันความหนาแน่นจากสมการ

$$f(X^2)=\frac{1}{2_{k/2}\Gamma(\frac{k}{2})}u^{(k/2)-1}e^{-u/2} \quad ; \quad \mu>0 \qquad (5.16)$$

$$=0 \quad ; \quad \mu \text{ มีค่าอื่นๆ}$$

เมื่อ $\Gamma(a)$ คือ แกมมาฟังก์ชัน (Gamma Function) และการแจกแจงไคกำลังสองมีระดับขั้นความเสรี k เขียนแทนด้วย X_k^2

$$\Gamma(a)=\int_0^{\infty} t^{(a-1)}e^{(-t)}dt \quad ; \quad x>0$$