DESIGN AND ANALYSIS OF THE ALGORITHM FOR SOLVING FACTORIAL PROBLEM OF ANY REASONABLY LARGE NUMBER USING THE POWER-DECIMAL SYSTEM

NGUYEN BA HUNG

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR DEGREE OF
MASTER OF SCIENCE
(COMPUTER SCIENCE)

IN
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
1999

ISBN 974-662-349-4

4037887 SCCS/M: MAJOR: COMPUTER SCIENCE; M.Sc. (COMPUTER SCIENCE).
KEY WORDS : FACTORIAL/POWER-DECIMAL SYSTEM/REASONABLY LARGE NUMBER.

NGUYEN BA HUNG: DESIGN AND ANALYSIS OF THE ALGORITHM FOR SOLVING FACTORIAL PROBLEM OF ANY REASONABLY LARGE NUMBER USING THE POWER-DECIMAL SYSTEM. THESIS ADVISORS: DAMRAS WONGSAWANG, Ph.D., SUPACHAI TANGWONGSAN, Ph.D., 68 p., ISBN 974-662-349-4.

The computation of factorial of any small number is relatively simple, straightforward and easy to implement. However, in practical applications, factorial of very large numbers is needed, e.g., the using of factorial to the compute very large prime numbers will be used in RSA, one of the most popular public-key cryptosystems currently in use. For such a case, the straightforward algorithm of factorial computation can not be applied due to the overflow problem.

This thesis is intended to study the factorial problem of reasonably large numbers. The factorial computation technique and algorithm called Fast Factorial Algorithm (FFA), was proposed, analyzed and devised. The FFA introduced the use of Power-Decimal System as its main representation of very large numbers that allows arithmetic operations to be done on a normal computer such as PC without the overflow problem. The complexity of FFA was analyzed and its performance was tested. The experimental results were presented and recommendation for practical use was also suggested.

4037887 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม. (วิทยาการคอมพิวเตอร์)
คำสำคัญ : Factorial / Power-Decimal System / Reasonably Large Number

เหงียน บา ฮึม : การออกแบบและวิเคราะห์ ขั้นตอนวิธีสำหรับการแก้ปัญหา factorial ของตัวเลขขนาดใหญ่ โดยการใช้ระบบ Power-Decimal (DESIGN AND ANALYSIS OF THE ALGORITHMS FOR SOLVING FACTORIAL PROBLEM OF ANY REASONABLY LARGE NUMBER USING THE POWER-DECIMAL SYSTEM) คณะกรรมการควบคุมวิทยานิพนธ์ : ดำรัส วงศ์สว่าง, Ph.D., ศุภชัย ตั้งวงศ์ศานต์, Ph.D., 68 หน้า. ISBN 974-662-349-4

การคำนวณหาค่าของ factorial ของตัวเลขขนาดเล็กนั้น ค่อนข้างจะง่าย ตรงไปตรงมา และทำให้เป็นผลโดยคอมพิวเตอร์ได้สะดวก อย่างไรก็ตามในการประยุกต์ใช้ทางปฏิบัติ มักจะต้องการหาค่าของ factorial ของตัวเลขขนาดใหญ่มาก ๆ เช่น การใช้ factorial ในการหาเลข prime ขนาดใหญ่ สำหรับนำไปใช้ในระบบการเข้ารหัสแบบ RSA ซึ่งเป็นวิธีการเข้ารหัสแบบกุญแจสาธารณะที่นิยมใช้มากที่สุดในปัจจุบัน ในกรณีดังกล่าว วิธีการแบบตรงไปตรงมาในการหาค่าของ factorial จะไม่สามารถนำไปทำให้เกิดผลโดยคอมพิวเตอร์ได้ เนื่องจากจะเกิดปัญหาการล้นของตัวเลข

งานวิทยานิพนธ์นี้ได้ศึกษาปัญหาการคำนวณค่าของ factorial ของตัวเลขขนาดใหญ่ โดยไม่เกิดปัญหาการล้นของตัวเลข เทคนิคและวิธีการในการคำนวณที่มีชื่อว่า Fast Factorial Algorithm (FFA) ได้ถูกพัฒนาขึ้นมาศึกษาและวิเคราะห์ ระบบ Power-Decimal ได้ถูกนำมาใช้ใน FFA ในการแทนตัวเลขขนาดใหญ่ ซึ่งสามารถจะทำการดำเนินการคำนวณได้บนคอมพิวเตอร์ทั่ว ๆ ไป โดยไม่เกิดปัญหาการล้นของตัวเลข งานวิจัยนี้ได้ทำการวิเคราะห์ความซับซ้อนของ FFA ทดสอบประสิทธิภาพ และได้นำเสนอผลการทดลองกับตัวเลขขนาดใหญ่ นอกจากนี้ยังได้เสนอข้อแนะนำบางประการในการปรับปรุง FFA ให้ดีขึ้น สำหรับการประยุกต์ใช้ในทางปฏิบัติ