國 立 交 通 大 學

統計學系

碩 士 論 文

DX 亂數產生器之經驗分析研究

An Empirical Study on DX Random Number Generators

研 究 生：林季盈　　指導教授：洪志真　教授

中 華 民 國 九十三 年 七 月

DX 亂數產生器之經驗分析研究

An Empirical Study on DX Random Number Generators

研 究 生：林季盈　　Student：Chi-Ying Lin

指導教授：洪志真　　Advisor：Jyh-Jen Horng Shiau

國 立 交 通 大 學

統 計 學 系

碩 士 論 文

A Thesis

Submitted to Institute of Statistics

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

In Statistics

July 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年七月

DX 亂數產生器之經驗分析研究

學生:林季盈　　指導教授:洪志真 博士

國立交通大學統計學系研究所 碩士班

摘要

亂數產生器的用途在很多的應用上扮演一個非常重要的角色，像是加密系統，模擬， 統計方法的分析也都必須倚賴亂數。這些研究的品質及可信度必須要有一個好的亂數產生器來支持。且參數 B=16807，C=0，M=2147483647 之 LCG 是現在電腦套裝軟體中常見的基本亂數產生器，但是它的週期短，只能在一維空間均勻分佈，況且它無法通過 Diehard 這一套檢驗亂數產生器的系統檢驗。 DX-k-s 是一套高維均勻分佈，有效率，週期長，且可用來配備於各種電腦的亂數產生器。我們主要研究的目的就是要探討這一套亂數產生器用 Diehard 來檢驗的表現。根據我們的實驗結果報告，DX-k-s 幾乎通過了所有 Diehard 裡的檢驗法。而且分析檢驗結果，我們發現 DX 之參數 k，s，和 B 對 DX-k-s 在 Diehard 裡的表現並無顯著影響。我們也特別檢驗了參數 M= =2147427929 和 B=521816 的 DX-1511-4，這個亂數產生器的週期等於 ，而且它可以在 1511 維以內的空間均勻分佈。現今鮮少有亂數產生器可以通過 Diehard 裡的所有檢驗法，而 DX-1511-4 辦到了。 總而言之，由我們的檢驗結果來評估，DX 是一套相當好，值得推薦的亂數產生器。

An Empirical Study

of

DX Random Number Generators

Student: Chi-Ying Lin Advisor: Dr. Jyh-Jen Horng Shiau

Institute of Statistics
National Chiao Tung University

ABSTRACT

Random numbers are used in many modern applications, such as computer games, the generation of cryptographic keys, simulation studies, and many scientific experiments. Quality of these applications and studies rely heavily on the quality of the random number generator (RNG) used. LCG with B=16807, C=0, M=2147483647 is very popular and used as a default RNG in many computer systems; but it does not pass all the tests in the Diehard test suite [19]. DX-k-s generators, proposed recently by Deng and Xu [4], is a system of High-dimensional uniformly, Efficient, Long-cycle, and Portable uniform random number generators. The main objective of this study is to investigate the empirical performance of the DX-k-s random number generators. We test DX-k-s random number generators by the Diehard test suite with a well-planned experimental design. According to the results of our experiments, DX family generators pass almost all the tests in Diehard and the parameters, k, s, and B do not significantly affect the performances of the RNGs under study. We also test a particular generator DX-1511-4 with M= =2147427929 and B=521816. This generator has a very long period of and is equi-distributed up to 1511 dimensions. In particular, DX-1511-4 passes all the tests in Diehard. We conclude that, based on our empirical study, DX-k-s generators is a very good family of RNGs.

Acknowledgement

我終於畢業了！首先我由衷感謝我敬愛的洪志真老師，感謝她這幾年來的耐心；有些時候，她像個朋友，讓我毫無戒心的把心事、生活中遇到的困擾一一向她傾訴，有些時候她像個心靈嚮導，給我一些建議，舒緩我心裡的障礙。這一次論文能夠順利的完成，賴於老師的殷殷叮囑，時時刻刻提醒我不要放棄；我永遠也不會忘記老師幫忙批改，糾正論文寫法這一段時間，陪我到晚上 10 點多，讓我心裡諸多過意不去。老師之於我的一切，我都只有感動與無限感激。

另外，我要感謝 Joy，謝謝她在我寫論文的時期，給予無數的意見與信心建立，PowerPoint 的製作，沒有她從旁幫忙，我還真欲哭無淚！接下來一段時間是 Joy 要拿博士學位的關鍵時期，希望老天爺庇祐她順利拿到博士學位。當然有需要我的地方，我一定也會義不容辭；比如說，幫忙倒茶水！

由於爸爸媽媽是公務人員，我是由阿媽一手帶大的，精明的阿媽影響我很多，如今她九十六歲高齡需要人照顧，我很慶幸寫論文這段期間有機會親手反哺她對我的恩情，也希望老天爺保佑她每一天能夠心安且身無病痛；最終，我要感謝的是我最摯愛的家人，爸爸以禪的智慧來面對我的狀況，媽媽總是以最樂觀的態度引導我，弟弟最愛與我分享他讀過的名人經驗來鼓勵我，而最可愛美麗的妹妹常用她甜美的笑容來支持我，並告訴我：「姊！我相信妳一定可以的！」家永遠是最溫暖的避風港，我有一個可愛健康的家庭，這裡的每一個小孩都會愈來愈成長茁壯！我親愛的弟弟、妹妹，咱們一起加油！

僅此向所有關心我的朋友致上最誠摯的謝意！

季盈 2004.7

CONTENTS

List of Tables

List of Figures