行政院國家科學委員會專題研究計畫　期中進度報告

隨機計算與量子計算之研究(2/3)

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-009-057-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：國立交通大學資訊工程學系

計畫主持人：蔡錫鈞

計畫參與人員：吳信龍, 唐偉清,鄧欣元,張中芸

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 92 年 5 月 23 日

行政院國家科學委員會專題研究計畫期中報告

隨機計算與量子計算之研究(2/3)

On randomized computation and quantum computation (2/3)

計畫編號：NSC 91-2213-E-009-057

執行期限：91 年 8 月 1 日至 92 年 7 月 31 日

主持人：蔡錫鈞

執行機構及單位名稱 交通大學 資訊工程學系

一、中文摘要

本計畫第二年計畫探討隨機計算中的重要課題—Kolmogorov complexity,首先我們探討使用具有高度 Kolmogorov complexity 的字串來產生一些亂數進而達到解隨機化的應用,本年計畫主要探討利用不可壓縮的字串來產生亂數的可能性.在本計畫執行中,我們發現 Kolmogorov Complexity 與 Bounded Storage security 似乎有相當的關聯,在此我們將進一步探討其相關的性質.

關鍵詞：Kolmogorov Complexity、de-randomization、bounded storage security

Abstract

In the second year of the project, we study issues on Kolmogorov complexity. We study de-randomization via Kolmogorov complexity. We study the possibility of generating pseudo random number from the incompressible strings. Along the way with recent developments in bounded storage security, we find a possible connection to Kolmogorov complexity. We'll investigate several related issues.

Keywords: Kolmogorov complexity, bounded storage security、de-randomization

二、緣由與目的

This three-year project targets at three major topics in computational complexity, that is, (1) randomized computation, (2) Kolmogorov complexity and (3) quantum computation. Recently there have been many progresses done in related areas, especially in the quantum computation. One of the purposes of this project is to give interested students in Taiwan opportunities to experience related researches, such that the students will have the chance to interact with the experts in these areas.

Randomized computation is the only

known way for many difficult problems, such as permanent approximating. BPP is the class of problems that can be solved with polynomial time randomized algorithms with bounded errors. The “de-randomizing BPP problem” is to study the feasibility of eliminating the randomness used in efficient randomized algorithms. In other words, we want to study “if BPP=P?”. A key step for de-randomization is using a pseudo-random generator, which uses few truly random bits and generates a sequence of long strings that can be used as random numbers. A commonly used method is using a hard function or a boosted mildly hard function to generate random bits from some weak random source.

In the first year of the project, we will consider “timed Turing machines”, where each transition step is timed. Given two different timed Turing machines of different speeds, we want to study the feasibility of utilizing the speed of the faster Turing machine to generate pseudo-random numbers for the slower machine. The second problem that we try to tackle is study the feasibility of using the un-solvable problems to generate pseudo-random strings. It has been proved to be hard for those unsolvable problems. Our goal in the first year is to answer the above problems.

In the second year of the project, we focus on some issues related to Kolmogorov complexity and de-randomization. Intuitively, a string with high Kolmogorov complexity carries more information than those with lower complexity. We study the possibility of utilizing the informatic technique to tackle issues in randomized computation.

三、期中進度

In order to apply the concept of Kolmogorov complexity to de-randomization, we need to modify the definition of Kolmogorov Complexity for any x: d(x,e) is defined to be smallest program P such that Pr(P produces x) > 0.5 + e, where 0< e <0.5. Let x=x_1..x_n. We can modify the above definition as: d(x,e) is defined to be smallest program P such that for all i in [n],Pr(P produces x_i| given x_1..x_{i-1}) > 0.5 + e, where 0< e <0.5.

Recently the work on everlasting security has been studied under the bounded-storage model by several researchers [1,2]. The bounded storage model for key-expansion is defined as: In the first phase, a t-bit strings is broadcast and available to all parties. Alice and Bob apply a known key-derivation function f: R x K → {0, 1}^n to compute the derived ket as X=f(R,K), where f is an efficiently computable. Even can store arbitrary s bits of information about R, i.e., it can be computed by an arbitrary storage function h: R→ U, where |U| <= 2^s. Even store U=h(R). Suppose Eve knows K, f is secure in the bounded storage model if the conditional probability distribution of Pr(X|U=u, K=k) is very close to the uniform distribution.

Lu [2] recently shows that with strong randomness extractor, i.e., a function which extracts randomness from a slightly random source, the above encryption scheme can be derived easily.

Basically, the bounded storage model is based on the information theory, so is

Kolmogorov complexity. We believe there exists a tight connection between these two concepts. Although, we still need to fill in some of the missing links. We are working on this. Probably, we should be able to obtain some concrete result in this summer. Besides, we have made some progress on proving that Maurer's result actually implies a method of designing extractors. First, by modified their method and consider flat source, we can prove that it does produce an extractor. Then, we give a method on how to simulate a specific weak random source with flat source. Thus, from any weak random source, we can construct an extractor as well by modifying Maurer's method.

Along the way, we want to study some issue between extractor via Kolmogorov complexity. We expect to complete 1-2 technical papers on related topics in the coming months.

This year, we also study the possible applications of extractors on fault tolerant storage devices, such as RAID. In this direction, we thoroughly study soft decoding with extractor codes. We find the widely used RAID architecture based on Reed Solomon code can be further extended by using the approach of soft decoding. We apply the extractor code to RAID architecture, which can recover severe damages on the disks that is way beyond the recovering limit of Reed Solomon code. Based on the theory foundation, we give a feasible design on RAID systems. We expect to publish a paper on this application.

四、參考文獻

[1] Dziembowski and Maurer, STOC 2002, Tight Security Proofs for the bounded-storage Model.

[2] Lu, Crypto 02, Hyper-encryption against space-bounded adversaries from online strong extractors.

[3] M. Li and P. Vitanyi, An Introduction to Kolmogorov Complexity and its Applications, Springer-Verlag.

[4] Motwani and Raghavan, Randomized algorithms, Cambridge Univ. Press, 1995.

[5] Nisan and Wigderson, Hardness v.s. Randomness, FOCS 1988.

[6] M. Sudan, Decoding of Reed-Solomon codes beyond the error-correction bound, J. of Complexity, 1997.

[7] A. Ta-Shma and D. Zuckerman, STOC 2001, Extractor Codes.

[8] Trevisan, Construction of extractors using pseudo-random generators, STOC 1999.

[9] Vadhan, Extracting all the randomness from a weakly random source, 1999.

五、計畫內完成及發表之論文：

1. C.-C. Lu and S.-C. Tsai, A note on unscrambling address lines, Information Processing Letters (EI, SCI Expanded), 85(4): 185--189, 2003.
2. J.-C. Chang, R.-J. Chen, T. Klove and S.-C. Tsai, Distance preserving mappings from Binary vectors to permutations, IEEE Transactions on Information Theory, 49(4): 1054--1059, 2003.
3. More On Assessing Randomized Computations, submitted for publication.