様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月５日現在

研究種目：基盤研究（C）
研究期間：2006～2008
課題番号：18500006
研究課題名（和文）　定量的計算資源としてのランダムネス：
効率的利用法の開発と限界の解明
研究課題名（英文）　Randomness as Quantitative Computational Resource:
Efficient Usage and Limitations

研究代表者
垂井　淳（TARUI Jun）
電気通信大学・電気通信学部・准教授
研究者番号：00260539

研究成果の概要：ネットワークを流れて次から次にやってくる膨大なデータに対する効率的計算が可能なのはどのような場合か？このような『ストリーム計算』と呼ばれる計算モデルにおいて、重複データを特定する問題を解析した。アルゴリズムが使えるランダムビット数と計算に必要なメモリー量のトレードオフを数学的に解明することに成功した。この他にもいくつかの具体的計算課題において計算に必要なランダムネスの量を解明すること成功した。関連する回路計算量の問題についてもいくつかの興味深い結果を得ることに成功した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,000,000	0	1,000,000
２００７年度	900,000	270,000	1,170,000
２００８年度	900,000	270,000	1,170,000
総　計	2,800,000	540,000	3,340,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：計算量理論、ランダマイズドアルゴリズム、乱拓計算、回路計算量、領域計算量

１．研究開始当初の背景

研究代表者は、本研究に先んじて、限定独立ランダムネスに関わる興味深い結果をいくつか得ることに成功していた。これらの結果をふまえて、研究代表者がよく知る回路計算量の手法の応用も探りつつ、ランダムネスの計算量解析を新たに展開しようという着眼だった。

２．研究の目的

（１）研究の対象・目的：　確率的アルゴリズムの用いるランダムネスの量、すなわち、用いるランダムビット数を、計算時間・記憶容量・ネットワーク帯域と同様に定量的計算資源と捉え、以下の課題の研究を展開する。

（A）ランダムネスの量を節約する一般的手法と応用法を開発し分析する。

（B）必要なランダムネスの量に対する下界、すなわち、節約できる限界を示し、計算資源

としてのランダムネスに対する理解を深める。

（Ｃ）計算論的擬似ランダムネス(computational pseudorandomness)について、その生成可能性と生成可能である場合の応用を解析し、計算資源としてのランダムネスの本質的意味の解明を進める。

本研究は、理論計算機科学の計算量理論の中に位置づけられるものである。

（2）研究の意義・位置付け：　ランダムビット列を用いる確率的アルゴリズムの有用性はよく認識されている。多様な計算課題とネットワークプロトコル課題に対して、決定的アルゴリズムに較べて以下の利点をもつ確率的アルゴリズムが知られている。

(a)アルゴリズムの構造が単純でコンパクトな実装が可能である。

(b)より短い時間・より小さな記憶容量・より狭いネットワーク帯域で計算できる。

(c)プロトコルの暗号論的セキュリティに関して、より確かな裏づけが得られる。

一方、一様ランダムで独立なビット列を自由に用いることができるという仮定の物理的・工学的裏づけは難しい。したがってランダムビットは得るのにコストがかかると考えるのが現実的であり、用いる量を減らす一般的手法の開発・分析とその限界の解明が重要な課題となる。

そもそも「多項式時間計算において、ランダムネスを用いることで真に計算パワーが増大するのか？」という根源的問題は、計算量の理論において最重要未解決問題のひとつである。多項式時間計算に関しては、ランダムネスを用いることによる計算パワーの増大はない、すなわち、計算可能なブール関数のクラスはランダムネスの使用によって真に大きくはならない(クラス P とクラス BPP は等しい）と予想されている。この予想は、計算論的擬似ランダムネス(computational pseudorandomness)に関する理論の中心問題である。この理論と計算機科学における最重要未解決問題 P vs NP 問題との深い関連が、過去７年ほどの間の非常に活発な研究により徐々に明らかにされつつあり、最近の Kabanet-Impagliazzo によるブレイクスルーが新たな展開を与えた[STOC03: Proceedings of the 35th Annual ACM Symposium on Theory of Computing, 355-364, 2003]。現在計算量の理論において最重要分野のひとつである計算論的擬似ランダムネスの理論について、本研究ではすでに生成可能であることがわかっている対数記憶容量計算に関する擬似ランダムネスに着目し、この場合に関する詳しい分析を足場として解析を進める。

３．研究の方法

研究の性格は理論的・数理的なものである。研究代表者が本研究に先んじていくつかの結果を得ていた次の２つの切り口からの解析を進めた。ランダムな置換に関するアルゴリズムを解析し、また、限定独立なランダネスを用いたアルゴリズムについて解析した。ランダムネに対する計算量解析は通信計算量の枠組みで行うのが一般的であったが、本研究により、回路計算量の手法の応用という新しい解析法を見つけることができた。

４．研究成果

概要：　ネットワークを流れて次から次にやってくる膨大なデータに対する効率的計算が可能なのはどのような場合か？このような『ストリーム計算』と呼ばれる計算モデルにおいて、重複データを特定する問題を解析した。アルゴリズムが使えるランダムビット数と計算に必要なメモリー量のトレードオフを数学的に解明することに成功した。この他にいくつかの具体的計算課題において、計算に必要なランダムネスの量を明らかにした。関連する回路計算量の問題についていくつかの興味深い結果を得ることが出来た。

（１）下記雑誌論文-(III)では、{1,…,n}の置換の集合で 3-scrambling という性質をもつものの最少サイズに対する新たな上界と下界を与えることに成功した。

（２）下記雑誌論文-(I),(II)では、否定限定回路に対する回路計算量解析をした。すなわち、論理回路において使ってよい否定ゲートの数に制限を加えた場合に注目するブール関数を計算する回路の最小サイズを会席した。

論文-(II)では、パリティ関数とインバーター関数に対して精密な下界を与えることに成功し、許す否定ゲート数と回路サイズの

トレードオフを正確に決定することに成功した。
論文-(I)では、入力ビット列が k-tonic である場合に限定したインバーター関数について、少ない数の否定ゲートのみ用いて小さいサイズと深さで計算できることを示した。

（３）国際会議論文-(III)ではストリーム計算モデルにおいて重複データ特定問題を解析した。1 以上 n 以下の整数がストリーム状に全部で m 個流れてくるとし、m > n と仮定する。鳩の巣原理より２回以上出現する数が少なくともひとつ存在する。この重複して出現する数（のうちのひとつ）を特定するのに必要な記憶領域量について良い下界を与えることに成功した。また、ランダムネスを使ってよい場合と使わない場合の領域計算量の違いを解明することに成功した。

（４）国際会議論文-(I)では、２のべき乗個の入力ビットのパリティを計算する最小サイズフォーミュラが本質的に一意であることを示した。最適アルゴリズムが一意であって、かつそのことが証明できているケースというのは珍しい。この意味で興味深い結果と言える。

（５）国際会議論文-(II)では、回路計算量における次の結果を与えた。回路サイズに対する現在まで知られている最大の下界は Iwama-Morizumi-Lachish-Raz による 5n であるが、Iwama らによる証明の中の分析をさらに精密化することで下界をより大きくできるのではないかという自然な予想があった。我々はこの予想は成立しないことを示した。ｓｄすなわち、我々は Iwama らの枠組みの中のブール関数でサイズ 5n の回路で計算可能なものが存在することを証明した。この結果により、5n より大きな下界を与えるためには根本的に新しい枠組みが必要であることが明らかとなった。

５．主な発表論文等　（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

(I) H. Morizumi and J. Tarui: Linear-size log-depth negation-limited inverter for k-tonic binary sequences. Theoretical Computer Science, 410(11), 1054--1060, 2009. 査読有り.

(II) K. Iwama, H. Morizumi, and J. Tarui: Negation-Limited Complexity of Parity and Inverters. Algorithmica, 54(2), 256-267, 2009. 査読有り.

(III) J. Tarui: On the Minimum Number of Completely 3-scrambling Permutations. Discrete Mathematics, 308(8), 1350--1354, 2008. 査読有り.

(IV) K. Iwama, H. Morizumi, and J. Tarui: Reductions for Monotone Boolean Circuits. Theoretical Computer Science, 408(2--3), 208--212, 2008. 査読有り.

〔学会発表〕（計５件）

(I) J. Tarui: Smallest Formulas for Parity of 2k. Proc. of COCOON08: LNCS vol 5092, 92-99, 2008. 発表：2008 年 6 月 29 日

(II) K. Amano and J. Tarui: A Well-Mixed Function with Circuit Complexity 5n±o(n): Tightness of the Lachish-Raz-Type Bounds. Proc. of TAMC08: LNCS vol 4978, 342-350, 2008. 発表：2008 年 4 月 27 日

(III) J. Tarui: Finding a Duplicate and a Missing Item in a Stream. Proc. of TAMC07: LNCS vol 4484, 128-135, 2007. 発表：2007 年 5 月 22 日

(IV) H. Morizumi and J. Tarui: Linear-Size Log-Depth Negation-Limited Inverter for *k*-Tonic Binary Sequences. Proc. of TAMC07: LNCS vol 4484, 605-615, 2007. 発表：2007 年 5 月 25 日

(V) K. Iwama, H. Morizumi, and J. Tarui: Negation-Limited Complexity of Parity and Inverters. Proc. of ISAAC06: LNCS vol 4288, 223-232, 2006. 発表：2006 年 12 月 18 日

〔その他〕
ホームページ
http://www.jtlab.ice.uec.ac.jp/

６．研究組織

(1)研究代表者
垂井　淳（TARUI Jun）
電気通信大学・電気通信学部・准教授
研究者番号：00260539

(2)研究分担者　なし

(3)連携研究者　なし