物理乱数と擬似乱数

田村　義保　　データ科学研究系　教授

「物理乱数」を中心に、擬似乱数を含めた新しい乱数の発生法、その応用と評価について研究している。物理乱数は数式で発生させる擬似乱数とは異なり、周期が無く、そのほかの性質についても高品質である。高精度の乱数としての物理乱数の研究・開発・実用化はそれ自身重要であるが、近年の情報技術の進展によって、あらたな用途が期待されている。特に重要なのは

（1）並列計算における利点

（2）セキュリティ技術における利点

である。

物理乱数についてのこれまでの研究成果と現状

平成17年度に、小型であるが高速（24MB/秒）のUSB接続可能な装置をFDKと共同開発した。また、FDKと共同で１GB/秒の発生速度が可能なボードの特許申請(2006年12月28日)を行い、プロトタイプとして128MB/秒の性能を有するボードを開発している（2008年3月完成）。このボードのテストを現在も行っている。

また、小野寺客員准教授、泰地客員教授（当時）の協力を得て、平成17年度に東京エレクトロンデバイスと共同で乱数発生ボード開発し・性能評価を行った。この評価結果に基づき、新たな乱数発生回路を設計し、東京エレクトロンデバイスにボードの開発を依頼した。この開発が後述の2010年1月導入のボードに活かされている。

2010年1月導入の統計科学スーパーコンピュータシステム、2010年3月導入の物理乱数発生システム、2010年7月導入の物理乱数サーバーシステムにおいては、それぞれ、東京エレクトロンデバイス製、日立製作所製、東芝製のPCI-EX仕様の物理乱数ボードを装着した計算機を構成に含めている。どのボードも、ユーザアプリケーションでの実効値で、400MB/秒以上の発生速度を有しており、現時点で世界最高性能を有している。3種のボードにより生成される物理乱数を乱数ポータルからダウンロードできるようにする予定である。3社のボードともノイズ源としてツェナーダイオードを用いていることは共通であるが、各ビットで0、1をとる確率を0.5にする方法が異なっている。

並列計算機と擬似乱数

先端的科学技術計算のためには並列計算機と乱数が不可欠である。擬似乱数の並列利用のためには、(1)中心サーバー法　(2)周期分割法　(3) Cycle Parameterization法 (4) Parameterized Iteration法　等が提案されている。異なったCPU(コア)で発生させる乱数間の相関があるかないかを調べることは非常に難しい。しかしながら、メルセンヌ・ツイスターでは、異なったパラメータにより発生させた系列が互いに独立であることが証明されている。

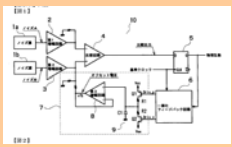
17年度開発の小型装置

17年度開発のボード

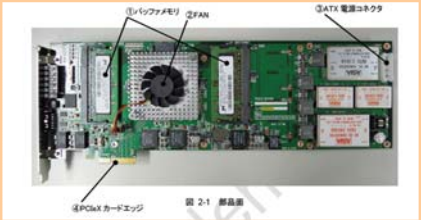
18年度開発の装置

19年度開発の装置

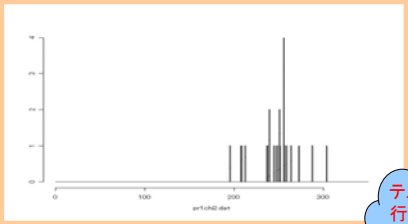
19年度開発の装置の回路図



東京エレクトロンデバイス製の乱数ボード



データ長10,240の乱数25系列の一様性の検定結果

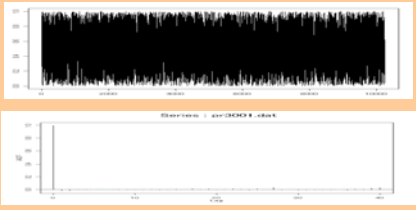


乱数ポータルトップページ

テストは進行中。高品質であると考える。

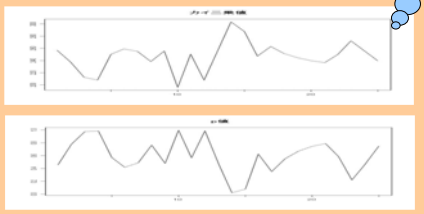
東エレ、日立のボードの乱数は現状で取得可。

上記ボードのサンプルデータ（上のグラフ）と自己相関関数（下のグラフ）　データ長10,240



25系列のカイ二乗値の変化（上のグラフ）

P値の変化（下のグラフ）



乱数オンデマンド取得ページ