物理乱数・擬似乱数

田村　義保　　データ科学研究系　教授

［乱数とは］

乱数とは「独立した確率変数の列」のことです。例として0と1をそれぞれ0.5 の確率でとるような離散確率変数を考えることにします。公平なコイン投げを繰り返すことにより、この場合の「乱数」を作ることができることは容易に分かります。

［乱数発生器］

乱数を生み出す「仕組み」は乱数発生器と呼ばれています。何らかのアルゴリズムを用いて、計算機で発生させた乱数が擬似乱数です。通常、擬似乱数とは0 以上1 未満の値を同じ確率でとる一様乱数のことです。線形合同法、M 系列、メルセンヌ・ツイスター等がよく知られています。規則性が明らかにあるために真性乱数ではありません。物理現象を用いて発生させた場合は、その乱数は物理乱数と呼ばれ、真性乱数です。0と見なせる状態、1と見なせる状態が時間的に変化し、時間軸方向の相関がなく、 “ 0”と“１”の状態をそれぞれ0.5の確率で取り出すことができるような物理現象が用いられています。電気回路の熱雑音が用いられることが多いですが、半導体レーザーのカオス現象を用いる方法、磁気抵抗素子のスピン反転を用いる方法も提案されています。

［統計数理研究所での物理乱数発生装置の開発］

1956年に日本の商用計算機第一号であるFACOM128（リレー計算機）を導入しましたが、同時に物理乱数発生装置として放射線源を用いる装置も導入されました。その後、1963年、1971年、1989年とダイオード熱雑音をノイズ源とし、計数方式の装置を開発しました。図1は1989年に開発された装置で用いられているボードです。8枚で1.5MB/秒の発生速度を達成することができました。1998年に発生方式を見直しました。PCIボード化し、ダイオードの熱雑音増幅後、A/D変換を行う方式にしました。図2の1999年の初代ボードの発生速度は25MB／秒でした。現有の統計科学スーパーコンピュータシステムに導入されているボードの発生速度は640MB／秒で、世界最速です。これらの物理乱数装置が2016年3月に、情報処理学会の情報処理技術遺産に選ばれました。

［乱数の利用］

乱数はモンテカルロシミュレーション、粒子フィルタ、MCMC 法、ブートストラップ法等のために必要です。大規模問題解決のためには大規模計算が必要になります。当然、複数のCPU による並列計算が必要になります。異なったCPUが発生する乱数間に相関がある可能性もあり安心して使うことができないと思います。物理乱数の独立性は保証されていますので、安心して使うことができます。統計数理研究所では、乱数ポータル、http://random.ism.ac.jp/　を通じて物理乱数や擬似乱数をオンデマンドで取得できるようにしています。ご利用いただければ幸いです。

[Random Number]

Random number is defined a sequence of random variables. An example is a sequence of binary random variables with equal probability. We can get this random numbers form a result of finite number of honest coin tossing.

[Random number generator]

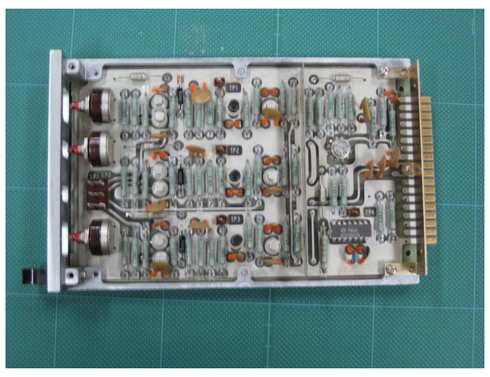
Methods to generate sequence of random variable are called random number generators. The sequence generated by an algorithm on the computer is called pseudo random number. The most popular pseudo random numbers have uniform distribution on [0, 1). There are linear congruential method, M-sequence, Mersenne Twister and so on. These random numbers are not true random number. The random number sequence generated by a physical phenomenon is called physical random number and can seem to be true random number. The most popular phenomenon which is used for a hardware random number generator is thermal noise of electronic circuit. Recently chaos phenomenon of semiconductor laser or magnetoresistive element is used.

[Development of Hardware Random Number Generator in our Institute]

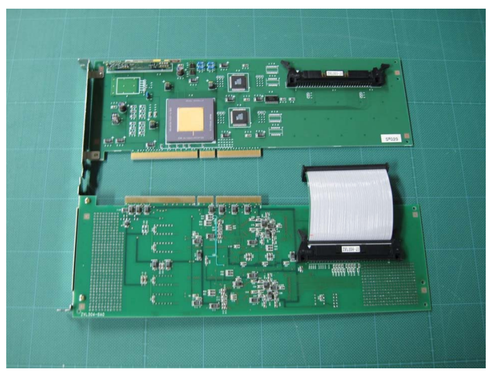
We introduced FACOM128 which is the first commercial computer system of Japan in 1956. We used hardware random generator whose noise source was radioactivity. In 1963, 1971, 1989 we introduced hardware random number generators whose noise sources are thermal noise of diodes and noise signal is digitized by using comparators. Fig.1 is a component of hardware random number generator which was developed in 1989. Generation speed is 1.5 MB/s by using 8 boards in parallel. In 1998 we changed generation method. A/D converters are used for digitizing analogue signal. Fig.2 is the generation board which was developed in 1999 whose speed is 25MB/s. Speed of the latest board is faster than 640MB/s. These hardware random number generators were certified as historical computer equipment by Information Processing Society of Japan in March 2016.

[Use of Random Numbers]

Random numbers are used for Monte Carlo method, bootstrap and so on. Large-scale computations are necessary for large-scale problems. Parallel computations must be conducted. We, however, cannot accept results free from care, since it is too difficult to confirm whether two random sequences have correlation or not. On the other hand we can use random numbers generated by hardware random number generator for parallel computing at ease. Users can download random numbers from our portal site http://random.ism.ac.jp/.

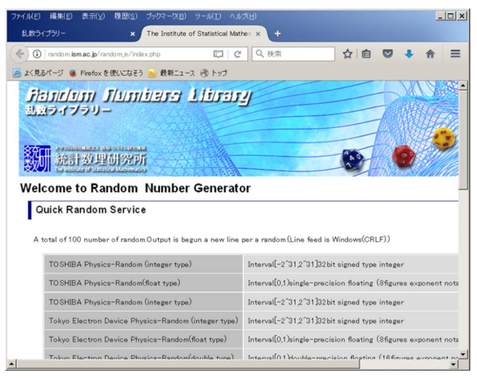


物理乱数発生部品　1989年
発生速度　1.5MB/s



SR8000用物理乱数発生ボード
1999年　発生速度　25MB/s

http://random.ism.ac.jp/



http://random.ism.ac.jp/random_e/index.php