統数研における物理乱数発生装置の開発

田村　義保　　モデリング研究系　教授

統計数理研究所においては1956年に日本の商用計算機の第一号であるFACOM128を導入した。この時から、物理乱数の重要性に注目し、放射能を用いた発生装置を用いていた。Fig.1は放射線のディテクタである。その後、1963年からは、ダイオードの熱雑音をコンパレータで計数する方式を用いるようになった。Fig.2はこの方式の初代（発生速度：12,000bit/秒）の部品である。1971年から1988年までは発生速度200KB/秒の装置を使っている。日立製の汎用計算機のチャネル接続であった。1989年から1998年までは発生速度1.5MB/秒の装置を使っていた。Fig.4aのボードを64枚用いていた。8枚が一組となっており、ランダムにいずれかを選び、一ビットの物理乱数を発生させていた。8組あるので、1バイトの乱数を発生できる装置となっていた。日立のチャネルの他にRS232Cポートも有しているので、今でも、乱数を取り出すことができる。コンパレータを用いて計数し、その偶奇により0か1かを、判断しているので、0と1との等確率性には優れている。しかし、計数方法は、高速な発生が不可能であるために、1998年から、熱雑音をA/D変換して、その一部のビットを使う方式を用いることにした。0と1を定常的に等確率にするための工夫が特許となっている。各社それぞれで用いている方式が異なっている。1999年から利用したFig.5aに示す日立製の発生速度が25MB/秒であるのに対して、2010年から利用した東芝製の発生速度は640MB/秒となっている。A/D変換器のサンプリング速度が速くなったことビット幅が広くなったことによる。

統数研においては北川敏男先生を中心にして統計数値表の乱数表を作成する時に、Fig.8に示すコインを用いたと聞いている。写真は一部のみを抜き出しているものであり、この100倍以上のコインを用いていた。この乱数表作成は、後年も引き継いでおり、Fig.9に示す装置は、JIS規格の付表として掲載された乱数表を作成するために用いた装置である。

Fig.10は公開中の乱数ポータルのページである。多くの方に利用していただければ幸いである。

Fig.1
放射線利用物理乱数発生装置部品
1956年

Fig.2
初代物理乱数発生機部品
1963年
発生速度　12,000bit/秒
HIPAC103を中心としたシステムで利用

Fig.3　第2代物理乱数発生機
1971年
発生速度　200KB/秒
HITAC8500を中心としたシステムで利用（M280Hを中心としたシステムまで利用）

Fig.4-a
第3代物理乱数発生機部品
1989年
日立製作所

Fig.4-b
第3代物理乱数発生機
1989年
発生速度　1.5MB/秒
M682Hを中心とした統計科学コンピュータシステムで利用（HITAC　S3800/162を中心としたシステムまで利用）

Fig.-5a　第1世代物理乱数発生ボード　1　1999年　日立製作所
発生速度　25MB/秒
SR8000を中心とした統計科学スーパーコンピュータシステムに6枚のボードを装着して利用

Fig.-5b　第1世代物理乱数発生ボード　2　1999年　東芝
発生速度　32MB/秒
ブートストラップシステム（100台のパソコンクラスタ）で利用

Fig.-6　第2世代物理乱数発生ボード　2004年　東芝
発生速度　133MB/秒
Altix2800を中心とした統計科学スーパーコンピュータシステムに6枚のボードを装着して利用

Fig.-7a　第3世代物理乱数発生ボード 1　2010年
東京エレクトロンデバイス　発生速度　400MB/秒
Fujitsu PRIMERGY RX200S5を中心とした統計科学スーパーコンピュータシステムに装着して利用

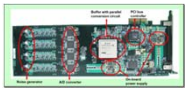

Fig.-7b　第3世代物理乱数発生ボード 2　2010年　日立製作所
発生速度　200MB/秒
日立 EP8000 を中心とした物理乱数発生システムに装着して利用

Fig.-7c　第3世代物理乱数発生ボード 3　2010年　東芝
発生速度　640MB/秒
SGI　UV100 を中心とした物理乱数サーバーシステムに装着して利用

Fig.-8
昭和20年代に統計数値表の乱数表を作成するために用いたコイン

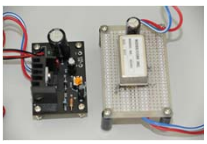

Fig.-9
JISZ9031:2001の乱数表を作成するために用いた発生装置

Fig.-10　乱数ポータル
オンデマンド取得ページ
http://random.ism.ac.jp/info02.html