S-PLUS における物理乱数の利用

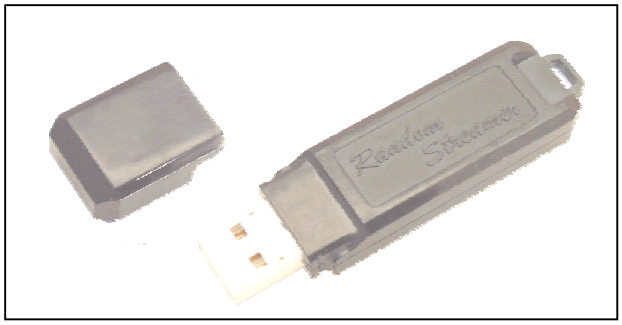
FDK 株式会社　清水　隆邦
上遠野　昌良

１．はじめに

統計的手法は情報処理、製造、金融から医療に至るまで、様々な分野で用いられています。そのような中で、Ｓ－ＰＬＵＳの様なデータ解析ソフトの役割は今後益々大きなものとなってゆくことでしょう。多くの分野で応用される統計ですが、そこでしばしば役に立つ便利な道具として”乱数”があります。乱数にはソフトで発生させる擬似乱数と呼ばれるものがありますが、確率的な物理現象を利用して発生する物理乱数というものもあります。ただ、物理乱数は高価でなかなか手が出せないという声もあり、実際に使った方はほとんどいないのではないでしょうか？

ＦＤＫ（株）では物理乱数に対する従来のイメージを大きく変えるような、低価格で使いやすい物理乱数生成ＵＳＢモジュール「Random Streamer」を開発しました。以下では、この Random Streamer から生成される物理乱数をデータ解析ソフトＳ－ＰＬＵＳで利用する方法について説明します。

２．物理乱数とは



Random Streamer (RPG102)

物理乱数は確率的な物理現象を利用して生成される乱数です。乱数源となる物理現象として主なものは”電気的なノイズ”と”放射線”ですが、Random Streamer では安全な電気的ノイズを用いています。そして独自の方法により効率よく乱数を生成し、小型化と高速性を実現しています。物理乱数の大きな特徴は、周期性を持たないことです。擬似乱数を用いる場合ではそれが持つ周期を考えて利用しないと誤った結果を導きかねませんが、物理乱数は周期を持たないので、いくら使い続けても特定パターンが不自然に繰り返すようなことはありません。質の良い物理乱数を用いることで、より信頼できる統計解析を行うことができます。

３．ソフトウエアへの取り込み

Random Streamer にはドライバの他にアプリケーション用のインターフェースが用意されています。

１）動作可能ＯＳ：　Microsoft Windows 2000 , Microsoft Windows XP

２）アプリケーションインターフェース

Windows 用　　：　RpgUsb.dll　(Windows システムにインストールされます。)

Microsoft Visual C++ 用　：　RpgUsb.lib / RpgUsb.h

４．RpgUsb.dll の拡張関数

RpgUsb.dll には乱数をパソコンに取り込む為の拡張関数が用意されています。Ｓ－ＰＬＵＳで使用する場合には以下の２つを使用してください。

4-1 GetRpgInt32ex

void　GetRpgInt32ex(DWORD **dwRand*)
[戻り値]　**void**　　[引数]　****dwRand***　**32** ビット整数の乱数値
説明　　**RPG102** から取得したデータから **32** ビット整数値を生成し、
引数****dwRand*** に返します。

4-2 GetRpgSRealex

void GetRpgSRealex(double **dbRand*)
[戻り値]　**void**　　[引数]　**double **dbRand***　単精度実数値
説明　　**RPG102** から取得した乱数データから単精度実数を生成し、引数 ****dbRand*** に返します。

５．Ｓ－ＰＬＵＳにおける乱数の取り込み

Windows API 対応のアプリケーションであれば Random Streamer の物理乱数を利用することができますが、データ解析ソフトＳ－ＰＬＵＳもその一つです。Ｓ－ＰＬＵＳでは外部のＣルーチンを呼び出す関数が用意されており、これを用いることで物理乱数を取得することができます。それには下記の３つのＳ関数を使います。

5-1 外部オブジェクトのロード

dyn.open ("オブジェクト名")
ＣまたはＦＯＲＴＲＡＮプログラムのオブジェクトをダイナミック・ロードします。
オブジェクト名として、前記ダイナミックライブラリ **RpgUsb.dll** を与えます。
ただし、このダイナミックライブラリ RpgUsb.dll はドライバーインストール時に Windows のシステムフォルダにインストールされます。
例）> dyn.open("C:￥￥WINNT￥￥system32￥￥RpgUsb.dll")

5-2 C ルーチンの呼び出し

.C("オブジェクト名" , 引数)
Ｃルーチンを呼び出します。オブジェクト名として、前記拡張関数名（例えば **GetRpgSRealex**）を与えます。引数の部分でＣルーチンの型と合せる必要があります。

5-3 型の指定

as.integer(x)

任意のオブジェクトｘが整数型の時はｘをそのまま返し、
そうでないときは整数型に変換してｘを返します。
GetRpgInt32ex を用いて整数型の乱数を取り込む場合にこの関数を使用します。

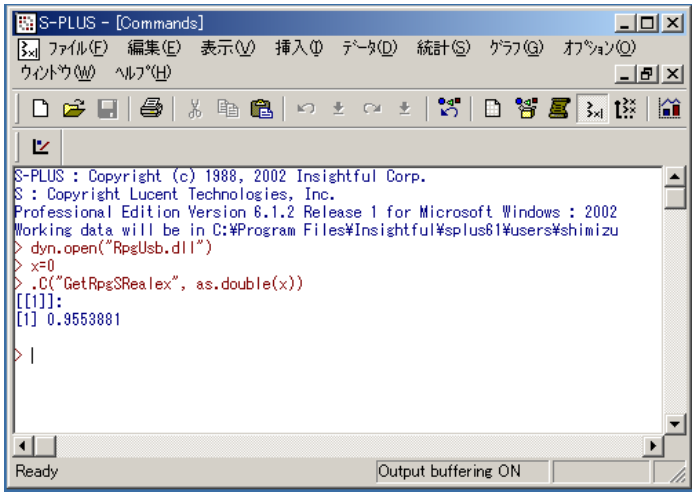
as.double(x)

任意のオブジェクトｘが倍精度実数型の時はｘをそのまま返し、
そうでないときは倍精度実数型に変換してｘを返します。
GetRpgSRealex を用いた実数型の乱数を取り込む場合にこの関数を使用します。

【　乱数取得の例　】

```
> dyn.open("C:￥￥WINNT￥￥
      system32￥￥RpgUsb.dll ")
>x = 0
>.C("GetRpgSRealex",
            as.double(x))
```

乱数が一つ生成されます。 →



６．物理乱数の利用

Ｓ－ＰＬＵＳにおいて物理乱数をより使いやすくするには、擬似乱数生成関数と同様に、指定した個数の乱数を一つのリストとして出力する関数があると良いでしょう。その後は用途に応じてより高度なプログラムを組んで活用いただけると思います。

6-1 物理乱数生成関数の作成

物理乱数のリストを出力する関数の例です。乱数の範囲は[0,1)となっています。

（一様乱数の例）

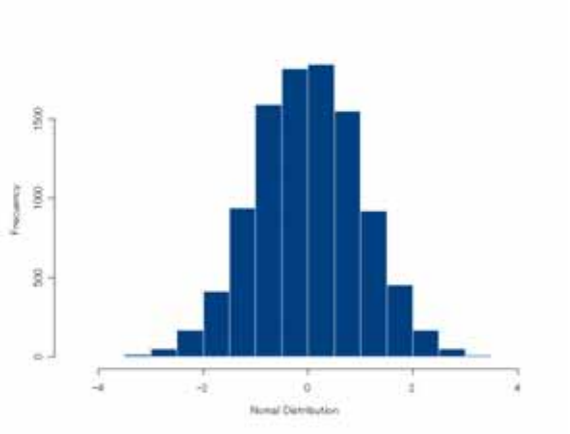
```
>fdkrunif<-function(j){i=0;r=list();x=0;while(i<j){i<-i+1;
  r[i]<-.C("GetRpgSRealex",as.double(x))};return(unlist(r))}
> fdkrunif(10)      ・・・乱数を１０個生成
   [1] 0.2878807 0.1784678 0.6987097 0.2279889 0.2196139 0.8387640 0.2459043
   [8] 0.2736715 0.8199442 0.6292390
```

6-2 様々な分布に従う乱数

Ｓ－ＰＬＵＳには多くの確率分布関数が用意されています。一様分布以外の乱数が必要な場合はこれらの関数を使い、逆関数法によって各分布乱数を得ることができます。

（標準正規分布に従う乱数の例）

```
> fdkrnorm <- function(j) qnorm(fdkrunif(j))
> fdkrnorm(10)
 [1] 0.85775057 -0.19826742 -0.59443192
     1.19662472  0.35409554  1.15936101
 [7] -1.90183671  2.46002764 -0.06514452
     0.94019136
```



標準正規分布の物理乱数

6-3 物理乱数の応用例

物理乱数が扱いやすくなったことで、これから様々な用途に用いられると思います。例えばランダムサンプリングなどに用いるのも良いかもしれません。下記はブートストラップ法による標本平均の分散推定の例です。

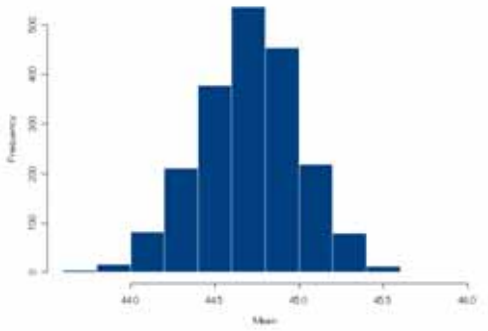
（FDK IC 内部クロックの Delay Time）

[1] 44.0854 44.2252 44.4474 41.7716 44.3998 43.3848 46.7283 45.1084 45.1249

[10] 46.3785 45.3739 43.9255 45.1004 45.2500 45.2152

〔Delay 平均値の分散推定〕

サンプル数	15
平均値	44.70129
ブートストラップ反復回数	2000
ブートストラップ分散推定量	0.09056824



Delay 平均値の Bootstrap 分布

７．まとめ

従来の物理乱数は高価なもので、個人レベルでの利用がとても困難でした。Random Streamer の登場で物理乱数の個人利用が現実的になりましたが、より身近な存在となるにはソフトウエアとのリンクが欠かせません。Ｓ－ＰＬＵＳは外部ＤＬＬとのリンク機能をもっており、これによって物理乱数をソフト上で生成することが可能となります。Ｓ－ＰＬＵＳの強力なデータ解析機能との組み合わせでより便利になり、物理乱数が様々な分野で幅広く応用されるようになれば幸いです。

[本件に関するお問い合わせ]

ＦＤＫ株式会社　開発営業部

URL http://www.fdk.co.jp

TEL 03-5473-4668　FAX 03-3431-9436

今村　恒明　E-mail: imamu@fdk.co.jp

[ご購入先]

日本テクノ･ラボ株式会社

URL http://randomstreamer.ntl.co.jp

TEL 03-5276-2810　FAX 03-5276-2820

E-mail: randomstreamer@ntl.co.jp