疑似乱数

乱数(Random Numbers)とは

- でたらめに生成される数の列
- 0から*N*-1までの整数乱数
  - 出現する順番がでたらめ
  - 各数字のでる頻度
    - 一様乱数：ほぼ等しい
    - ある分布に従う乱数

乱数は何に使う

- 確率過程のシミュレーション
  - 状態変化が決定的でない場合
- Monte Carlo法
  - 積分値の近似
  - 状態をサンプリングする

疑似乱数 (Pseudo Random Numbers)

- 本物の乱数
  - サイコロ
  - 熱雑音
  - 放射性原子の崩壊
- 疑似乱数
  - コンピュータで生成する
  - 生成アルゴリズムがあるので「偽物」
  - いかに良い乱数を生成するか

線形合同法
(Linear Congruential Method)

- **整数乱数** [0,*m*-1]

$$i_n, a, c, m \in N$$

$$i_n = \left(a\, i_{n-1} + c \right) \mod m$$

- **定数*a*, *c*, *m*の選び方へ経験則**
  - *a*=2416, *c*=374441, *m*=1771875

- **オーバーフローの危険性**

- *m* は範囲だけでなく最長周期でもある
  - ある数の次の数は一意に決まっている
  - シミュレーションでは多くの乱数が必要
- *m* はできるだけ大きく　$m = 2^{31} - 1$
  - C/C++の場合は符号なし整数を使う
  - Schrageの方法
- 発生した乱数を攪拌する

Schrageの方法

- 二つの整数をq とr を導入(c=0)

$$q = \lfloor m/a \rfloor, \quad r = m \mod a$$
$$m = aq + r$$
$$r < q$$

- $$a\,i_n \mod m = \left[a\,i_n - \lfloor i_n/q \rfloor (aq + r) \right] \mod m$$
$$= \left[a\left(i_n - \lfloor i_n/q \rfloor q\right) - \lfloor i_n/q \rfloor r \right] \mod m$$
$$= \left[a\left(i_n \mod q\right) - \lfloor i_n/q \rfloor r \right] \mod m$$

- **各項はオーバーフローしない**

$$a i_n \bmod m = \begin{cases} a(i_n \bmod q) - \lfloor i_n/q \rfloor r & \text{正の場合} \\ a(i_n \bmod q) - \lfloor i_n/q \rfloor r + m & \text{それ以外} \end{cases}$$

- **例**

$$a = 16807,\ \ c = 0,\ \ m = 2^{31} - 1$$
$$q = 127773,\ \ r = 2836$$

乱数の性質を調べる

- 例として分布の一様性を調べる
- 乱数は0から1 までの一様疑似乱数とする
  - 総数M 個
- N 個の等間隔の区間(bin)に分ける
  - 頻度分布を調べる
  - 各区間に乱数が発生する確率 $p=1/N$

- ある区間に乱数が入る確率 p
- その区間にk 個の乱数が入る確率

$$P(k)=\binom{M}{k}p^k(1-p)^{M-k}$$

$$\langle k\rangle=\sum_{k=0}^{M}kP(k)=\sum_{k=0}^{M}k\binom{M}{k}p^k(1-p)^{M-k}$$

$$=pM\sum_{k=1}^{M}\binom{M-1}{k-1}p^{k-1}(1-p)^{M-1-k+1}$$

$$=pM\sum_{l=0}^{M-1}\binom{M-1}{l}p^l(1-p)^{M-1-l}=pM$$

$$
\begin{aligned}
\left\langle k^2 \right\rangle &= \sum_{k=0}^{M} k^2 \binom{M}{k} p^k (1-p)^{M-k} \\
&= \sum_{k=0}^{M} \left[k(k-1) + k \right] \binom{M}{k} p^k (1-p)^{M-k} \\
&= pM + \sum_{k=2}^{M} k(k-1) \frac{M!}{(M-k)!\,k!} p^k (1-p)^{M-k} \\
&= pM + \sum_{k=2}^{M} \frac{M(M-1)(M-2)!}{(M-2-k+2)!(k-2)!} p^2 p^{k-2} (1-p)^{M-2-k+2} \\
&= pM + p^2 M(M-1)
\end{aligned}
$$

- **分散(2乗誤差)**

$$\sigma^2 = \left\langle \left(k - \langle k \rangle \right)^2 \right\rangle$$
$$= \left\langle k^2 \right\rangle - \left(\langle k \rangle \right)^2 = p(1-p)M$$

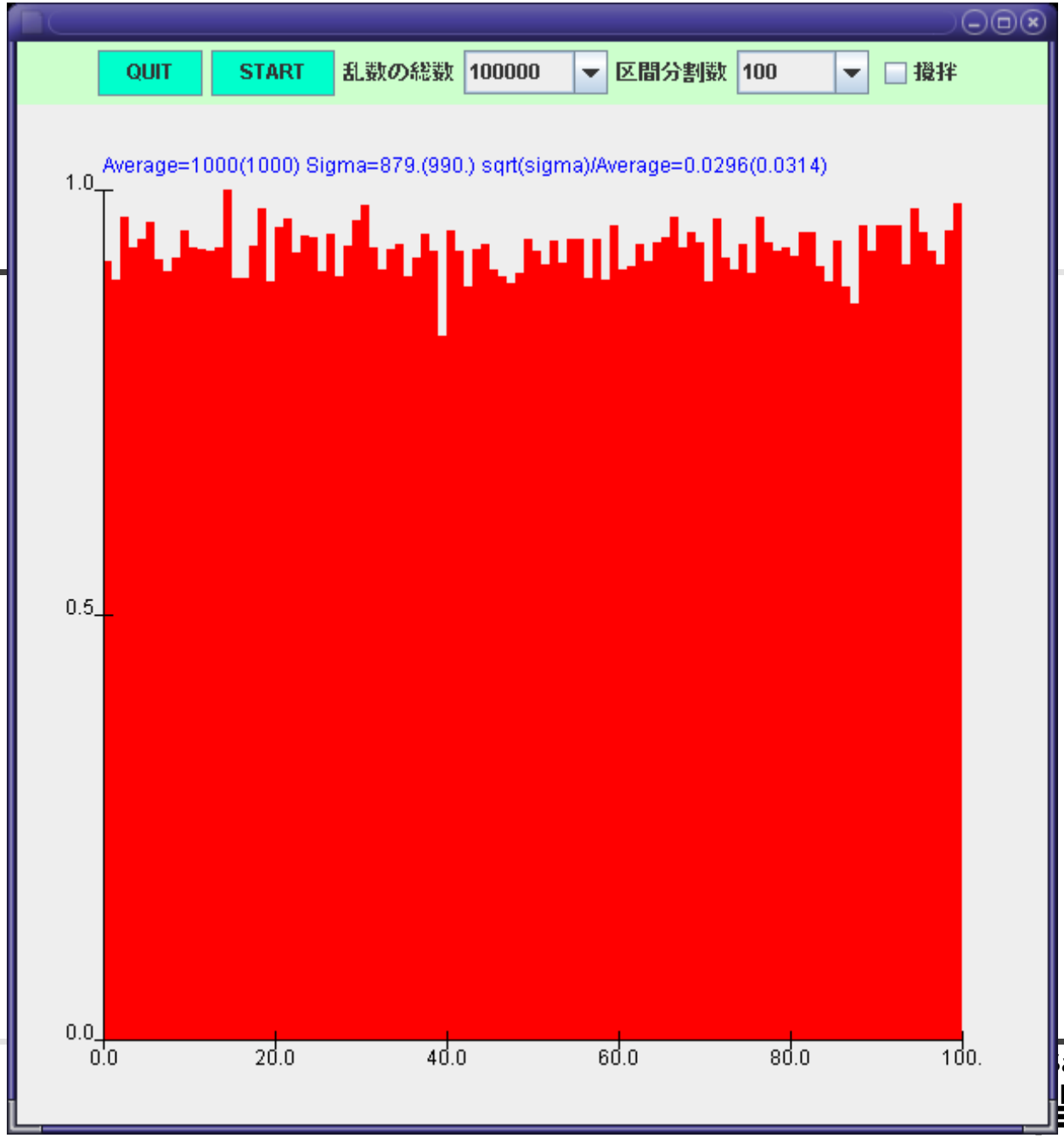
$$\frac{\sigma}{\langle k \rangle} = \left(\frac{1-p}{p} \frac{1}{M} \right)^{1/2}$$

演習問題：分散$\sigma^2 = \left\langle \left(k - \langle k \rangle \right)^2 \right\rangle$が$\left\langle k^2 \right\rangle - \left(\langle k \rangle \right)^2$ と表されることを示しなさい

実験

- 実際に線形合同法で疑似乱数を生成する
- 頻度分布とその揺らぎを求める

頻度


QUIT
START
乱数の総数
100000
区間分割数
100
撹拌
Average=1000(1000) Sigma=879.(990.) sqrt(sigma)/Average=0.0296(0.0314)
1.0
0.5
0.0
0.0
20.0
40.0
60.0
80.0
100.

攪拌法

- 線形合同法の問題点の克服
  - 周期を長くする
  - ある値と次の値に関係を一意でなくする
- 生成した乱数をかき混ぜる

1. 大きさ*N*の配列*D*に乱数を格納する
   1. 乱数は 0から*M*-1とする
2. 新しい乱数を*a*とする
   1. 対応する配列の位置を計算する $k=\lfloor N \times a / M \rfloor$
   2. 格納されていた乱数を*b* とする $b \leftarrow D[k]$
   3. その場所に*a* を保存する $D[k] \leftarrow a$
   4. *b* を乱数として出力する
   5. 繰り返す

Javaでの撹拌法の実装例

```
/*  Random.java */
public interface Random {
    public int next();
    public double nextDouble();
    public int getM();
}
```

```
/* Shuffle.java */
public class Shuffle implements Random{
    private Random random;
    private int d[];
    private final int N=100;
    private int M;
    public Shuffle(Random random) {
        this.random=random;
        d=new int[N];
        M=random.getM();//整数乱数の最大値
        for(int i=0;i<N;i++)d[i]=random.next();
    }
```

```
public int next(){//次の整数乱数
    int a=random.next();
    double yy=(double)N*a/M;
    int k=(int)yy;
    int c=d[k];
    d[k]=a;
    return c;
}
public double nextDouble(){//次のダブル型乱数
    return (double)next()/M;}
public int getM(){return M;}
```

参考：別の計算方法

- 両辺をpで微分する　$1=\sum_{k=0}^{M}\binom{M}{k}p^k(1-p)^{M-k}$

$$0=\sum_{k=0}^{M}\binom{M}{k}\left[\frac{k}{p}-\frac{M-k}{1-p}\right]p^k(1-p)^{M-k}$$

$$=\sum_{k=0}^{M}\binom{M}{k}\left[\frac{k-Mp}{p(1-p)}\right]p^k(1-p)^{M-k}$$

$$=\frac{1}{p(1-p)}\sum_{k=0}^{M}\binom{M}{k}[k-Mp]\,p^k(1-p)^{M-k}$$

$$\therefore\ \sum_{k=0}^{M}k\binom{M}{k}p^k(1-p)^{M-k}=Mp$$

演習問題：同様に

$$1=\sum_{k=0}^{M}\binom{M}{k}p^{k}(1-p)^{M-k}$$

を二階微分することで

$$\sum_{k=0}^{M}k^{2}\binom{M}{k}p^{k}(1-p)^{M-k}$$

を求めなさい。