第 2 题作业报告

PB18000341 范玥瑶

A. 作业题目

用 16807 产生器测试随机数序列中满足关系$X_{n-1} < X_{n+1} < X_n$的比重。讨论 Fibonacci 延迟产生器中出现这种关系的比重。

B. 算法及主要公式

B.1. 16807 产生器

用 16807 产生器测试随机数序列中满足关系$X_{n-1} < X_{n+1} < X_n$的随机数比重算法为：当 N 足够大时生成的随机数序列中满足关系$X_{n-1} < X_{n+1} < X_n$的随机数比重会接近生成无穷多随机数时随机数序列中满足关系$X_{n-1} < X_{n+1} < X_n$的随机数比重。因此输入种子值和一个很大的 N，用 x,y,z 三个变量分别储存X_{n-1}, X_n, X_{n+1},于用 Schrage 方法生成随机数的同时对符合条件的随机数数据进行计数，通过循环语句实现 n=1~N 时X_{n-1}, X_n, X_{n+1}的比较和 S 的计算，从而计算出满足关系$X_{n-1} < X_{n+1} < X_n$的随机数的比 S/N。

B.2. Fibonacci 延迟产生器

算法解释中 m 取 2^{31}，不同于源代码中的宏定义 m=2^{31}-1.

当 Xn=In/m 时$X_{n-1} < X_{n+1} < X_n$等价于$I_{k-1} < I_{k+1} < I_k$，当 N 足够大时生成的随机数序列中满足关系$X_{n-1} < X_{n+1} < X_n$的随机数比重会接近生成无穷多随机数时随机数序列中满足关系$I_{k-1} < I_{k+1} < I_k$的随机数比重。

自定义 p,q 和个数 N，在主函数里用 malloc（）函数开拓长为 L=max{p,q}+1 的动态数组，由用户填入前 max{p,q}个数，由公式 In=In-p⊕In-q mod m 计算 In 后填入数组，其中⊕即为 render，宏定义展开为+，选取其他含义如-、*、xor 时修改宏即可。此后在循环语句中，从 n=0 到 n=N-1，在一个周期中：先调用子函数 Fibonacci 通过数组指针、p、q 求 IL+n 作为 Ik+1，比较I_{k-1}、I_{k+1}、I_k后计数，调用子函数 arrange 对数组进行更新，进入下一周期。当循环语句结束时 N 个随机数中满足满足关系$I_{k-1} < I_{k+1} < I_k$的随机数计数为 S，则 S/N 即为比重。将 N 和比重存入文件 OriginDataFibonacci.txt。

其中子函数 Fibonacci 的算法是通过指针调用距离数组指针(p-1),(q-1)的数运算，利用整型变量的范围，将计算结果对 2^{31} 取模得 In=In-p⊕In-q mod m.此后返回计算结果，释放函数内存；arrange 的算法为从后往前依次将数组前 (l-1) 个元素的值依次赋给后一个元素，将 x 赋给第一个元素，从而更新数组。

C. 计算结果及具体分析、讨论

取 seed=1,p=1,q=2,I0=1,I1=1,分别求 $\log_{10}N$=3~9 的比重。将计算结果导入 Origin 作 S/N-N 图如图 1.由原始数据可以得到 16807 产生器比重趋于 0.1666，Fibonacci 产生器趋于 0.5.

以下计算比重的理论值。如果随机数产生器理想，由大数定律 N 很大时满足关系$X_{n-1} < X_{n+1} < X_n$的 N 的比重趋近于三个（0，1）之间的真随机数(x,y,z)满足 x<z<y 的概率。概率密度函数 $p(x,y,z)$满足

$$\iiint_0^0 p(x,y,z)dxdydz = 1,\quad p(x,y,z) = Const.$$

解得$p(x,y,z) = 1.$

则

$$P(X_{n-1} < X_{n+1} < X_n) = \iiint\limits_{0<x<z<y} p(x,y,z)dxdydz = \frac{1}{6} \approx 1.6667$$

对比原始数据，16807 产生器的随机性比 Fibonacci 产生器好。

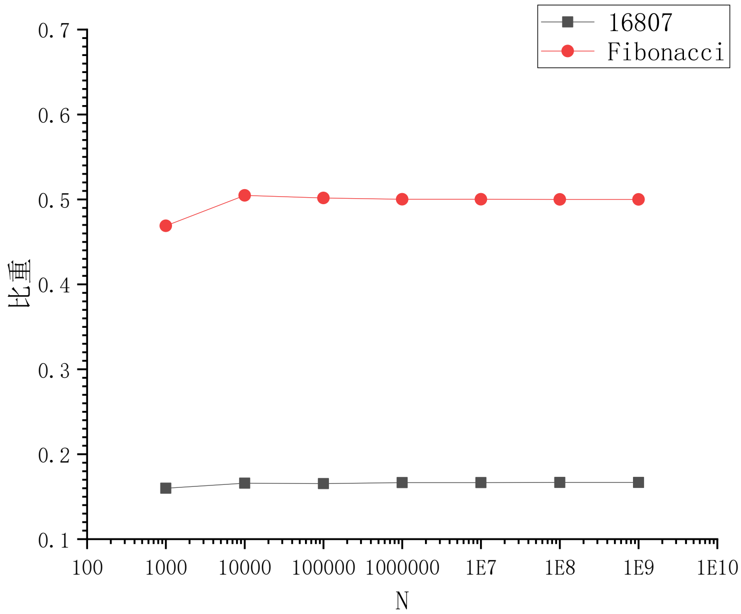

图1 比重随N数量级变化图

D. 总结

实验中通过编写 2 个程序分别验证了 16807 产生器和运算为+的 Fibonacci 产生器中满足满足关系$X_{n-1} < X_{n+1} < X_n$的比重。16807 产生器的结果比较接近理想随机数产生器假设下的比重。原因推测为 p,q 的选取过小。本实验中 p=1,q=2，应当选取 $p^2+q^2+1=prime$ 的较大的数对（p,q）更好。