计算机算法设计与分析
随机化算法

易凯

2017 年 5 月 28 日

班　　级	软件 53 班
学　　号	2151601053
邮　　箱	williamyi96@gmail.com
联系电话	13772103675
个人网站	https://williamyi96.github.io williamyi.tech
实验日期	2017 年 5 月 28 日
提交日期	2017 年 6 月 6 日

目录

插图

1 学习基本目标

1. 理解产生伪随机数的算法
2. 掌握数值概率算法的设计思想
3. 掌握蒙特卡洛算法的设计思想
4. 掌握拉斯维加斯算法的设计思想
5. 掌握舍伍德算法的设计思想

2 随机化算法类型

随机化算法共有四大类。分别为数值随机化算法，蒙特卡洛算法，拉斯维加斯算法和舍伍德算法。

2.1 数字随机算法

数值随机算法往往得到的是问题的近似解，其解的精度随计算时间的增加而不断提高。

2.2 蒙特卡洛算法

求问题的精确解，但是不保证得到的解的正确性。算法所用的时间越多，得到的正确解的概率越高。

2.3 拉斯维加斯算法

拉斯维加斯算法不会得到不正确的解，但是可能找不到解。其找到正确解的概率随着所用计算时间的增加而提升。

2.4 舍伍德算法

舍伍德算法总能求得问题的一个解，且所求的解总是正确的。它设法消除的是最坏情形行为与特定实例之间的关联性。

3 随机化计算

3.1 题目描述

试设计一个随机化算法计算 365!/340! 365^{25}, 并精确到 4 位有效数字。

3.2 题目解答

此题是生日问题的实例化，可以使用 Stirling 公式进行近似：

$n! = \sqrt{2\pi n}(\frac{n}{e})[1+\theta(\frac{1}{n})]$

可以得到

$n!/[(n-k)!n^k] \approx e^{-k^2/(2n)}$

进一步求解得到：

$n!/[(n-k)!n^k] \approx e^{-k(k-1)(2n-k^3)/(6n^2)\pm O(max(k^2/n^2),k^4/n^3)}$

最后带入 n=365，k=25 得到原式的大小为 0.4311。

4 易验证问题的算法

4.1 问题描述

一个问题是易验证的是指对该问题的给定实例的每一个解，都可以有效地验证其正确性。例如：求一个整数的非平凡因子问题是易验证的，而求一个整数的最小平凡因子就不是易验证的。在一般情况下，易验证问题未必是易解的。

1. 给定一个解易验证问题 P 的蒙特卡洛方法，设计一个相应的解问题 P 的拉斯维加斯算法；

2. 给定一个解易验证问题 P 的拉斯维加斯算法，设计一个相应的界问题 P 的蒙特卡洛算法。

4.2 问题解答

如果给定一个解易验证问题 P 的 MC，设计一个相应的解问题 P 的 LV 如下 (验证其正确性的算法为 Prove())：

```
    void Lv(LP x) {
        bool l = Mc(x);
        while(!Prove(x,l)) l = Mc(x);
```

```
}
```

如果给定一个解易验证问题 P 的 LV, 设计一个相应的解问题 P 的 MC 如下:

```
bool Mc(LP x) {
    Lv(x);
    if(timeused > maxt) return false;
    else return true;
}
```

5 整数因子分解

5.1 题目描述

假设已有一个算法 Prime(n) 可用于测试整数 n 是否为一个素数。另外还有一个算法 Split(n) 可以实现对合数 n 的因子分割。试利用这两个算法设计一个对给定整数 n 进行因子分解的算法。

5.2 问题解答

结合两个算法实现的对给定整数 n 的因子分解如下：

```
void fact(int n) {
    if(Prime(n)) {output(n); return;}
    int i = Split(n);
    if(i > 1) fact(i);
    if(n > i) fact(n/i);
}
```

6 算法的正确率

6.1 题目描述

设 mc(x) 是一致的 75% 正确的蒙特卡洛算法，考虑下面的算法：

```
mc3(x) {
    int t, u, v;
    t = mc(x);
```

```
        u = mc(x);
        v = mc(x);
        if((t==u) || (t==v)) return t;
        return v;
```

1. 试证明上述算法 mc3(x) 是一致的 27/32 正确的算法，因此是 84% 正确的。

2. 试证明如果 mc(x) 不是一致的，则 mc3(x) 的正确率可能低于 71%。

6.2 问题解答

由于 MC 返回的为 bool 类型，因此要么其正确，要么不正确。由上述的 t==u 和 t==v 的条件分析可以知道，一方面重复三次 MC 得到的各次正确的分布为 000,001,010,011,100,101,110,111。

其中 011, 101, 110, 111 可以返回正确解，从而返回正确解的概率为：

$0.25*0.75*0.75+0.75*0.25*0.75+0.75*0.75*0.25+0.75*0.75*0.75 = \frac{27}{32}$。

对于第二问，如果 MC(x) 是非一致的，那么 101 不能够保证返回正确解，从而返回正确解的概率可能为：

$0.25 * 0.75 * 0.75 + 0.75 * 0.75 * 0.25 + 0.75 * 0.75 * 0.75 = 0.703 < 0.71$,

因而 MC(x) 不一致，算法的正确率可能低于 0.71.

7 基于蒙特卡洛算法设计拉斯维加斯算法

7.1 题目描述

设算法 A 和 B 是解统一判定问题的两个有效的蒙特卡洛算法。算法 A 是 p 正确偏真算法，算法 B 是 q 正确偏假算法。试利用这两个算法设计一个解同一个问题的拉斯维加斯算法，并使所得到的算法对任何实例的成功率尽可能高。

7.2 题目解答

成功率最高的方法类似于将两者或起来。

```
bool Lv(LP x) {
    while(1) {
        if(A(x)) return true;
```

```
            if(!B(x)) return false;
        }
    }
```