【文章编号】 1004-1540(2007)03-0225-03

超大 Fibonacci 数的快速迭代算法

陈莲娜[1]，梁自力[2]

(1. 中国计量学院 信息工程学院，浙江 杭州 310018；
2. 浙江省人口与计划生育信息中心，浙江 杭州 310012)

【摘　要】 Fibonacci 序列在信息隐藏、密码学等领域具有广泛的应用，现提出一种能计算超大 Fibonacci 整数的快速算法，最大可以精确地计算第 30 万个 Fibonacci 整数，可以完全满足信息隐藏和密码学领域实时计算的需要.

【关键词】 Fibonacci 数；迭代；超大整数
【中图分类号】 TP311　　【文献标识码】 A

A fast iterative algorithm for very large Fibonacci numbers

CHEN Lian-na[1], LIANG Zi-li[2]

(1. College of Information Engineering, China Jiliang University, Hangzhou 310018, China;
2. Information Centre of Zhejiang Family Planning Commission, Hangzhou 310012, China)

Abstract: A fast iterative algorithm for very large Fibonacci numbers is proposed. By using this algorithm, the 300 000th Fibonacci number can be calculated. The algorithm is adequate in applications.

Key words: Fibonacci number; iterative; very large integer

斐波那契(Fibonacci)序列源自古老的兔子序列，是所有通俗趣味数学的典型题材. 本文用 $F[n]$表示第 n 个 Fibonacci 数，其数学定义如下：

$F[1]=1, F[2]=1$,

$F[n]=F[n-1]+F[n-2]$　$(n>2)$.

Fibonacci 序列具有很多应用事例. 在信息隐藏的图像水印和音频置乱中的应用参见文献[1,2]，在密码学中的应用参见文献[3-5]. 在这些应用中，我们需要的是 Fibonacci 序列. 所谓序列，在理论上是一个无限的序列，在实际使用上，需要较大 n 的 Fibonacci 数 $F[n]$. 比如，在文[1,2]中使用所谓斐波那契变换

$$S[k]=(k * F[n]+r) \bmod F[n+1],$$

此处 r 为算法中的密钥. 在图像置乱中，一幅并不算大的图像，比如 256×256 的图像有 65 536 个像素. 因而至少需要 65 536 个 Fibonacci 数. 然而，对于目前的 int 型，32 位计算机只能计算 $F[46]$，对于 unsigned 型也只能算出 $F[47]$，而 F

【收稿日期】 2007-04-17
【基金项目】 浙江省科技厅基金资助项目(No. 2006C23058)
【作者简介】 陈莲娜(1965－)，女，甘肃兰州人，副教授. 主要研究方向为模式分类、人工智能、数据库.

[48]已经溢出了.因此,为适应应用上的需要,有必要快速地计算 $F[48]$以后的 Fibonacci 整数.本文称 32 位计算机不能计算的整数为超大整数.

显然,计算 Fibonacci 整数的实用算法不能用递归算法,因为其速度太慢;也不用直接计算的比纳(Binet)公式

$$F(n)=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right],$$

因其速度仍然慢且使用开方和乘法运算不便于程序的硬化.为便于硬化程序,我们只采用全加法的迭代算法.

本文设计了超大整数的加法,整个算法不用乘法,以便硬化处理满足实时快速产生超大 Fibonacci 整数的需要.

1 算法设计与原理

1.1 超大数的加法设计及原理

取 $N=100\ 000\ 000$ 作为超大数的进位单位,就是用数组定义了一个亿进制,用亿进制原理解决计算机中超大数的截断.下面是超大数加法函数.

```
/**********************************
r[]        函数 add(a[],b[])运行结果数组,数
           组间的权值是 N
fa[], fb[]计算 Fibonacci 数 f[n]需要的数组
flag       进位标志,flag=1 进位,flag=0 不进位
rnum       结果数组的长度
**********************************/
#define N 100 000 000
unsigned r[10 000];
int flag;
int rnum=1;            //数组 r[]长度初始化
void add(unsigned a[],unsigned b[]){
  flag=0;
  for(int i=0;i<=rnum;i++){
    r[i]=a[i]+b[i]+flag;
    if(r[i]>N-1){ //进位
      r[i]=r[i]-N; flag=1;
    }
    else flag=0;
  }
  if(flag==1){
    rnum++; r[rnum]=1;
    //进位,且设置的位数 rnum 增加 1
  }
}
```

1.2 计算 Fibonacci 整数的算法

计算 Fibonacci 整数的算法,采用分段迭代算法.对于 $n<48$ 的 Fibonacci 数,用通常的迭代算法

```
unsigned cur, old2=1, old1=1;
for(int i=3; i<=n; i++){
  cur=old2+old1;
  old1=old2; old2=cur;
}
```

当 $n>=48$ 时,用前面的超大整数加法函数 add(),进行迭代,利用 $F[46]=1\ 836\ 311\ 903$,$f[47]=2\ 971\ 215\ 073$:

```
fa[0]=36 311 903; fa[1]=18; fa[2]=0;
fb[0]=71 215 073; fb[1]=29; fb[2]=0;
for(int i=48; i<=n; i++){
  add(fa, fb);
  for(int j=0; j<= rnum; j++){
    fa[j]=fb[j]; fb[j]=r[j];
  }
  fb[rnum+1]=0;
  //最高位外的位,赋值 0,否则将出错
}
```

1.3 超大数的减法设计

为了验证所得的 Fibonacci 整数的正确性,本文用 Fibonacci 整数逆运算

$$F[n-2]=F[n]-F[n-1]$$

用超大数的减法验证 $f[3]=2$. 是否成立.若成立,所得的 Fibonacci 数正确,否则不正确.减法算法如下:

```
//超大数减法函数
void minus(unsigned a[],unsigned b[]){
  flag=0;
  for(int i=0; i< rnum; i++){
    if((a[i]-flag)>=b[i]){
        r[i]= a[i]-flag-b[i];
        flag=0;
    }
    else{
```

```
        r[i]=N+a[i]-flag-b[i];
        flag=1;
      }
    }
  if(r[rnum-1]==0) rnum--;
}
```

2　实验结果和结论

以下是在 CPU 为 Pentium-III，内存 64M 的计算机上运行分别用递归算法、直接计算法、对分迭代算法和使用超大整数分段迭代算法的实验结果(表 1). 实验结果表明，递归算法、直接计算法、对分迭代算法由于使用通常的加法最多只能计算 $F[46]=1\ 836\ 311\ 903$，对于计算 $F[47]$已发生溢出错误. 而本文的算法可以计算到第 30 万个 Fibonacci 数 $F[300\ 000]$. 在计算所耗费的时间上，对于递归算法是完全不实用的. 用递归算法计算 $F[45]$所耗费的时间几乎是用本文算法计算 $F[300\ 000]$的 3 倍. 本文的算法计算到 $F[2\ 000]$仅用 20 ms，完全满足实时进行图像置乱的要求.

表 1　几种算法计算 Fibonacci 数的时间　　ms

N	45	2 000	1 万	10 万	30 万
递归算法	128 554	—		—	—
直接计算	0.02	—	—	—	—
迭代算法	0.01	10	110	4 877	42 051

注："—"表示不能计算.

【参　考　文　献】

[1] 商艳红，李　南，邹建成. Fibonacci 变换及其在数字图像水印中的应用[J]. 中山大学学报，2004，43(增刊)：148-151.

[2] 李　南，商艳红，邹建成. 基于 Fibonacci 变换的音频置乱方法[J]. 北方工业大学学报，2004，16(3)，8-12.

[3] 顾乃杰. 基于斐波那契序列的多播算法[J]. 计算机学报，2002(4)：365-372.

[4] 王丽萍. 基于 Fibonacci-Lucas 序列的两种公钥分配密码体制[J]. 保密通信，2000(2)：45-47.

[5] 孙燮华. 关于 Chomsky 范式的算法及其实现[J]. 中国计量学院学报，2006(9)：239-242.

(上接第 210 页)

[4] 王　英，叶忠民，陈绍聂，等，浙江省光通信仪表的计量测试[J]. 中国计量学院学报，2003，14(2)：97-99.

[5] 魏会敏，罗风光，曹明翠，等. 基于低电压驱动 MEMS 的可调光衰减器的设计与性能分析[J]. 光电子·激光，2006，17(6)：685-687.

[6] SALEHEEN H I. Closed cycle lasing of ASE noise in a WDM ring network[A]// The 4th Pacific Rim Conference on, Lasers and Electro-Optics CLEO/Pacific Rim [C]. USA, New York, IEEE, 2001：558-559.

[7] UNAMUNO A, UTTAMCHANDANI D. MEMS variable optical attenuator with vernier latching mechanism [J]. IEEE Photon Technol Lett，2006，18(1)：88-90.

[8] 袁　野，曹钟慧，鲍俊峰，等. 一种 MEMS 可调光衰减器性能测试及动态响应分析[J]. 光子学报，2004，33(4)：439-442.

[9] HIRABAYASHI K, WADA M. AMANO C. Liquid crystal variable optical attenuator integrated on planar lightwave circuits[J]. IEEE Photon Technol Lett，2001，13(6)：609-611.

[10] LENZI M, TEBALDINI S, MOLA D D, et al. Power control in the photonic domain based on integrated arrays of optical variable attenuators in glass-on-silicon technology [J]. IEEE J Select Topics Quantum Electron，1999，5：1289-1297.

[11] SHI Y Q, ZHANG C, ZHANG H, et al. Low (sub-1-volt) halfwave voltage polymeric electro-optic modulators achieved by controlling chromophore shape[J]. Science，2000，288：119-122.

[12] CHUNG Y, DAGLI N. An assessment of finite difference beam propagation method[J]. IEEE Journal of Quantum Electronics，1990，26(8)：1335-1339.