随机算法

北京大学计算机系
蒋婷婷
2021年2月1日

中国计算机学会 China Computer Federation

什么是随机算法？

- 算法中加入随机性
  - 民意调查需要随机选择访问对象
- 对于很多问题，采用随机算法比采用确定型算法效率更高
- 随机算法的描述一般并不复杂，但是随机算法的分析比较复杂

概率论基础知识

- 随机变量X的加权平均值称为期望，记作$E[X]$
- 线性性质：

$$E[aX+bY]=aE[X]+bE[Y]$$

- 马尔科夫不等式

$$Pr[X\geq kE[X]]\leq 1/k$$

- 在事件B发生的条件下，事件A发生的概率称为条件概率，记作$Pr[A|B]$，计算公式为

$$Pr[A|B]=\Pr[A\cap B]\ /\ \Pr[B]$$

- 如果$Pr[A|B]=\Pr[A]$，则A和B是独立事件。
- 对于随机变量X和Y来说，如果所有可能的取值x和y，事件$\{X=x\}$和$\{Y=y\}$都是独立的，则称X和Y是独立随机变量

随机算法

Las Vegas 型随机算法

- 随机快速排序
- 随机选择
- 随机 n后放置

Monte Carlo型随机算法

- 主元素测试
- 串相等测试
- 模式匹配
- 素数测试

随机算法的分类与局限性

Las Vegas 型随机算法

随机快速排序

随机选择

随机 n后放置

中国计算机学会 China Computer Federation

随机快速排序算法

算法 随机快速排序算法

输入：包含 n 个元素的数组

输出：经过排序的 n 个元素的数组

1. 若数组包含 0 或 1 个元素则返回
2. 从数组中随机选择一个元素作为**枢轴**元素
3. 把数组元素分为三个子数组，并且按照 A, B, C 顺序排列

   A：包含比枢轴元素小的元素；

   B：包含与枢轴元素相等的元素；

   C：包含比枢轴元素大的元素.

4. 对 A 和 C 递归地执行上述步骤.

算法分析

定理 设数组含n个不同元素，随机快速排序算法的期望比较次数

$$T(n) \le 2\, n \ln n.$$

证明一： 求解递推式

随机选取枢轴元素，其位于排序后第 i 位置 (i=0,1,…,n-1)的概率是1/n，A和C的元素数分别是 i 个和 n–i–1个, 得

$$T(n) = (n-1) + \frac{1}{n}\sum_{i=0}^{n-1}[T(i) + T(n-i-1)] = (n-1) + \frac{2}{n}\sum_{i=1}^{n-1}T(i)$$

解为$\Theta(n\log n)$. 可归纳证明精确上界是 $T(n) \le 2n \ln n$.

$$T(n) = (n-1) + \frac{2}{n}\sum_{i=1}^{n-1} 2i\ln i \le (n-1) + \frac{2}{n}\int_1^n 2x\ln x\,dx$$

$\le$

$$\le (n-1) + \frac{2}{n}\left(n^2\ln n - \frac{n^2}{2} + \frac{1}{2}\right) \le 2n\ln n$$

随机选择算法

算法 RandSelect(A, p, r, k) //从$A[p..r]$中选第k小

1. **if** $p=r$ **then return** $A[p]$
2. $i \leftarrow$**Random**(p, r)
3. 以 $A[i]$ 为标准划分 A
4. $j \leftarrow$划分后小于等于 $A[i]$ 的数构成数组的大小
5. **if** $k \le j$
6. **then return RandSelect** (A, p, $p+j-1$, k)
7. **else return RandSelect** (A, $p+j$, r, $k-j$)

时间期望值估计

假设1.. n 中每个数被选的概率相等，并且假设第 k 个数总是出现在划分后两个数组中较大的数组，算法的期望时间为

$$T(n) \le \frac{1}{n}(T(n-1)+T(n-2)+\ldots+T(\frac{n}{2}+1)$$

$$+T(\frac{n}{2})+T(\frac{n}{2}+1)+\ldots+T(n-1))+O(n) \le \frac{2}{n}\sum_{i=n/2}^{n-1}T(i)+O(n)$$

归纳证明 $T(n) \le cn$. 归纳步骤如下：假设对 $k<n$ 命题为真，

$$T(n) \le \frac{2}{n}[c\frac{n}{2}+c(\frac{n}{2}+1)+\ldots+c(n-1)]+tn=\frac{2c}{n}\frac{(\frac{n}{2}+n-1)\frac{n}{2}}{2}+tn$$

$$=\frac{3cn}{4}-\frac{c}{2}+tn \le \frac{3cn}{4}+tn=(\frac{3}{4}+\frac{t}{c})cn \le cn,\quad \text{取}c \ge 4t\text{ 即可}$$

n后放置的随机选择

算法BoolQueen(n)

1. $k \leftarrow 1$　　　　　　　　　　// k 放皇后的行号
2. $count \leftarrow 0$　　　　　　　　// $count$ 放好的皇后数
3. while $k \le n$ do
4. 　for $i \leftarrow 1$ to n do　　　　// i 为待选列号
5. 　　检查 i 与前面 k-1个皇后的相容性
6. 　　如果相容则将 i 加入S
7. 　if $S \ne \varnothing$ then
8. 　　$j \leftarrow \text{Random}(1,|S|)$
9. 　　$x_k \leftarrow S[j]$
10. 　　$count \leftarrow count+1$
11. 　　$k \leftarrow k+1$
12. 　else $k \leftarrow n+1$
13. return $count$

n后问题的随机算法

算法QueenLV(n) //重复调用随机算法BoolQueen

1. $p \leftarrow$ BoolQueen(n)
2. while $p<n$ do
3. $\quad p \leftarrow$ BoolQueen(n)

改进算法---与回溯相结合

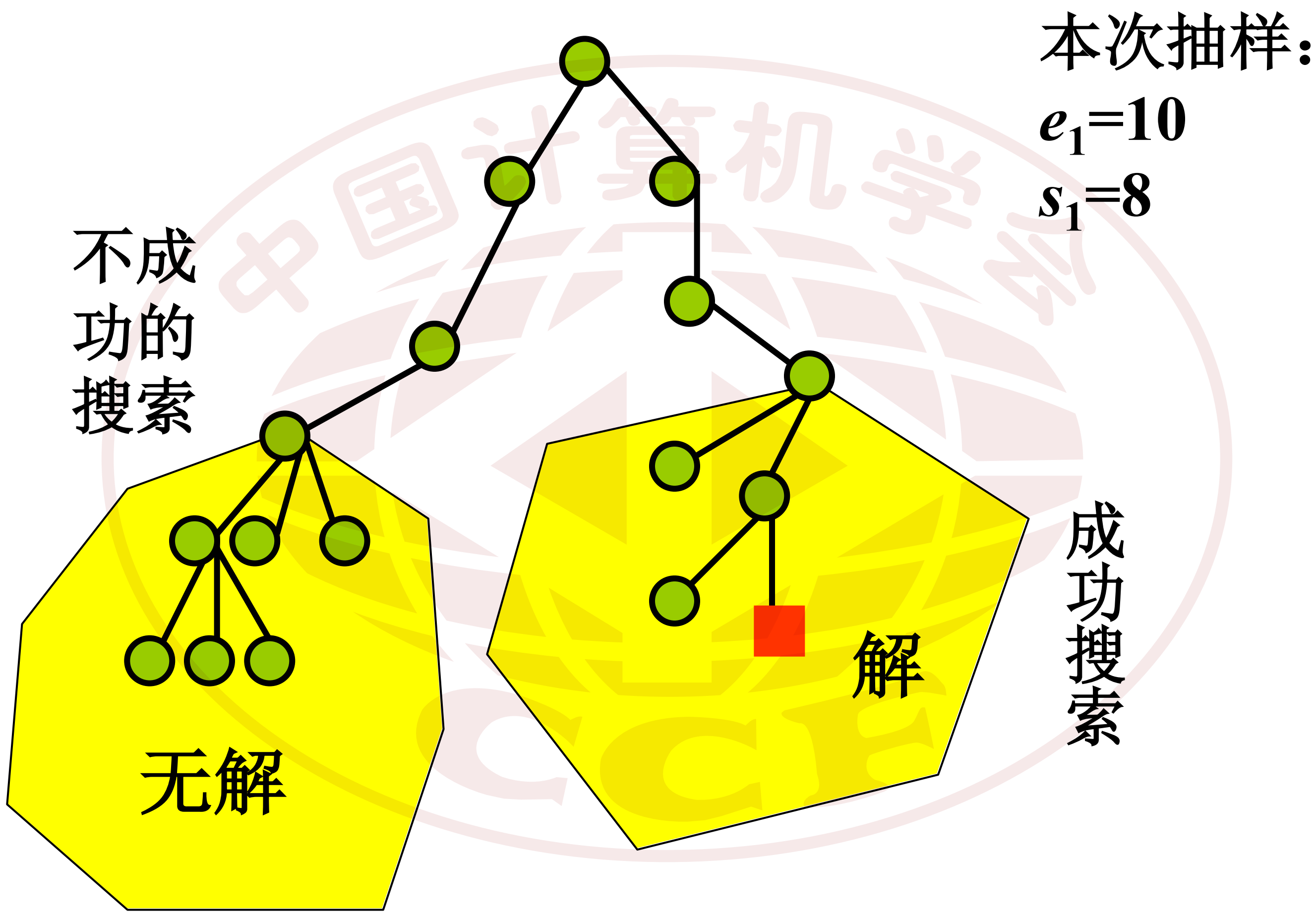
设 $stopVegas \le n$, 表示用QueenLV算法放置的皇后数

剩下 n - $stopVegas$ 个皇后用回溯方法放置

$stopVegas$ = 0 时是完全的回溯算法

$stopVegas$ = n 时是完全的Las Vegas算法

成功搜索与不成功搜索



改进算法的分析

对于不同的 *stopVegas* 值，设

- p 为算法成功概率
- s 为一次成功搜索访问的结点数的平均值
- e 为一次不成功搜索访问的结点数的平均值
- t 为算法找到一个解的平均时间

$$t = ps + (1-p)(e+t) \Rightarrow t = s + e\frac{1-p}{p}$$

n=12时的统计数据：*stopVegas* = 5时算法效率高

stopVegas	p	s	e	t
0	1.0000	262.00	-	262.00
5	0.5039	33.88	47.23	80.39
12	0.0465	13.00	10.20	222.11

LasVegas型随机算法总结

- 特点

  通过修改确定性算法得到，一般将算法的某步的确定型选择变成随机选择

  一次运行可能得不到解；若得到解，则解一定是正确的

  改进途径：与确定型算法相结合

  有可能改进确定型算法平均情况下的时间复杂度

- 有效的 LasVegas 算法

  运行时间是随机变量，期望运行时间是输入的多项式且总能给出正确答案的随机算法

Monte Carlo型随机算法

- 主元素测试
- 串相等测试
- 模式匹配
- 素数测试

主元素测试

问题

主元素：出现次数超过一半以上的元素

输入：n 个元素的数组 T

输出：如果存在主元素则输出“true”，否则“false”

算法 Majority(T,n)

1. $i \leftarrow \text{Random}(1,n)$
2. $x \leftarrow T(i)$
3. 计数 x 在 T 中出现的个数 k
4. if $k>n/2$ then return true
5. else return false

中国计算机学会 China Computer Federation

算法的正确性

若回答true：则T存在主元素，算法正确；若回答false，T仍可能存在主元素，算法可能出错. 回答正确概率大于1/2.

算法 BoolMajority(T,n)

1. if Majority(T,n) then return true
2. else return Majority(T,n)

BoolMajority 算法正确的概率为

$$p+(1-p)p=2p-p^2=1-(1-p)^2>\frac{3}{4}$$

调用 k 次Majority算法正确的概率为

$$p+(1-p)p+(1-p)^2p+\ldots+(1-p)^{k-1}p=1-(1-p)^k>1-2^{-k}$$

调用次数 k	1	2	3	4	5	6
正确概率大于	0.5	0.75	0.875	0.938	0.969	0.985

改进途径

对于任意给定的 ε>0, 如果要使出错的概率不超过 ε，则调用次数 k 满足

$$(\tfrac{1}{2})^k \le \varepsilon \Rightarrow k\log\tfrac{1}{2} \le \log\varepsilon \Rightarrow -k \le \log\varepsilon$$

$$\Rightarrow k \ge -\log\varepsilon \Rightarrow k \ge \left\lceil \log\tfrac{1}{\varepsilon} \right\rceil$$

出错概率不超过ε 的算法——MCMajority

算法 MCMajority(T,n,ε)

1. $k \leftarrow \lceil \log(1/\varepsilon) \rceil$
2. for $i \leftarrow 1$ to k
3.   if Majority(T,n) then return true
4. return false

串相等测试

问题：A 有一个长串 x, B 有长串 y，A 和 B 希望知道 $x=y$?

方法一：

A 将 x 发送给 B，B 测试 $x = y$?

发送消耗：长串占用信道资源大

方法二：

A 用 x 导出一个短串 $f(x)$ (fingerprints)

A 将 $f(x)$ 发送到 B

B 使用同样方法导出相对于 y 的短串 $f(y)$

B 比较 $f(x)$ 与 $f(y)$

如果 $f(x) \neq f(y)$，则 $x \neq y$;

如果 $f(x) = f(y)$，则不确定.

指纹产生

设 x 和 y 的二进制表示为正整数 $I(x), I(y)$

选择素数 p, 指纹函数为

$$I_p(x) = I(x) \bmod p$$

A 传送 p 和 $I_p(x)$ 给 B. 当 p 不太大时，传送一个短串.

存在问题:

$$x = y \Rightarrow I_p(x) = I_p(y)$$

$$I_p(x) = I_p(y) \nRightarrow x = y$$

出错条件：固定

$$p \mid (I(x) - I(y))$$

改进算法的途径

改进方法： 随机选择素数 p 进行测试

算法 StringEqualityTest

1. 随机选择小于 M 的素数 p //M为正整数
2. A 发送 p 和 $I_p(x)$ 给 B
3. B 测试是否 $I_p(x) = I_p(y)$

出错的必要条件：

x 的位数等于 y 的位数

$p \mid (I(x)-I(y))$

有关素数的性质

函数 $\pi(t)$：小于 t 的不同的素数个数，

例如，$\pi(20)=8$，素数8个：2, 3, 5, 7, 11, 13, 17, 19

两个相关结果：

(1) 素数定理 $\pi(t) \approx t / \ln t$

(2) 若 $k<2^n$，n不太小，整除 k 的不同素数个数小于 $\pi(n)$

n	10^3	10^4	10^5	10^6	10^7
$\pi(n)$	168	1229	9592	78498	664579
$t/\ln t$	145	1086	8686	72382	620421
比值	1.159	1.132	1.104	1.085	1.071

$k < 2^{10}=1024$，整除 k 的素数个数 $< \pi(10) = 4$，

例如 $k = 984$，整除 984 的素数只有 2, 3, 41

出错概率估计

n：x 和 y 的二进制表示的位数

$x, y \le 2^n$

若选择 $M \ge 2n^2$, 一次测试的出错概率估计：

$$\frac{|\{p \mid p\text{是小于}2^n\text{的素数，且 }p\text{ 整除 }I(x)-I(y)\}|}{\pi(M)}$$

$$\le \frac{\pi(n)}{\pi(M)} \approx \frac{n/\ln n}{2n^2/\ln(2n^2)} \approx \frac{n/\ln n}{2n^2/2\ln n} \le \frac{1}{n}$$

改进算法

重复执行 j 次，每次随机选择小于 M 的素数

算法 StringTest

输入：x, y，n位二进制数

输出：“Yes” (如果 $x = y$)；或者“No” (如果 $x \neq y$)

1. for $i \leftarrow 1$ to j
2. 随机选择小于 M 的素数 p // M为正整数
3. A 发送 p 和 $I_p(x)$ 给 B
4. B 测试
5. if $I_p(x) \neq I_p(y)$
6. then return “No”
7. return “Yes”

算法分析

令 $j=\lceil \log\log n \rceil$，则算法出错的概率

$$(\frac{1}{n})^j \le \frac{1}{n^{\lceil \log\log n \rceil}}$$

实例：x 和 y 是1000000位二进制数

$$n = 10^6$$

$$M = 2 \cdot 10^{12} = 2^{40.8631}$$

素数 p 的二进制表示至多 $\lfloor \log M \rfloor + 1 = 41$ 位

$I_p(x)$ 的位数至多 $\lfloor \log(p\text{-}1) \rfloor + 1 \le \lfloor \log M \rfloor + 1 = 41$

总共传送 82 位

中国计算机学会 China Computer Federation

模式匹配

问题：输入二进制串 $X=x_1x_2\ldots x_n$，$Y=y_1y_2\ldots y_m$，$m\le n$

输出：若 Y 在 X 中，Y 出现的第一个位置；否则为 “0”

算法一：顺序比较

初始 Y 与 X 的首元素对齐，依次从前到后比较 X 与 Y 的元素. 如果 X 与 Y 的所有元素都相等，输出 Y 的首位置 j；否则将 Y 的位置向后移动一个字符，重复原来过程.

运行时间：$O(mn)$

算法二：利用有限状态自动机的模式匹配算法

(Knuth,Morris,Pratt), Introduction to Algorithms

运行时间：$O(m+n)$

随机算法

算法三　利用串比较的随机算法

设计思想：设 $X(j) = x_j x_{j+1} \ldots x_{j+m-1}$，把 $X(j)$ $(j=1,2, \ldots, n-m+1)$ 与 Y 逐个字符的比较，改成对指纹 $I_p(X(j))$与 $I_p(Y)$ 的比较

$X(j)$与$X(j+1)$的关系

$$X(j) = 2^{m-1}x_j + \underline{2^{m-2}x_{j+1} + \ldots + 2x_{j+m-2} + x_{j+m-1}}$$

$$X(j+1) = \underline{2^{m-1}x_{j+1} + 2^{m-2}x_{j+2} + \ldots + 2x_{j+m-1}} + x_{j+m}$$

$$X(j+1) = 2X(j) - 2^m x_j + x_{j+m}$$

算法三的关键技术

由 $I_p(X(j))$ 求 $I_p(X(j+1))$ 的公式

$$I_p(X(j+1)) = (2I_p(X(j)) - W_p x_j + x_{j+m})(\bmod p)$$

$$W_p = 2^m (\bmod p)$$

该公式说明：由 $I_p(X(j))$ 计算 $I_p(X(j+1))$ 仅需要常数时间

公式的证明：

$$X(j+1) = 2X(j) - 2^m x_j + x_{j+m}$$

$$I_p(X(j+1)) = (2I_p(X(j)) - 2^m x_j + x_{j+m})(\bmod p)$$

令 $W_p = 2^m (\bmod p)$

$$I_p(X(j+1)) = (2I_p(X(j)) - W_p x_j + x_{j+m})(\bmod p)$$

算法

算法 PatternMaching

输入：串 X 和 Y, $|X|=n$, $|Y|=m$, $m \le n$

输出：如果 Y 在 X 中，Y 出现的第一位置；否则为“0”

1. 从小于 M 的素数集合中随机选择素数 p
2. $j \leftarrow 1$
3. $W_p \leftarrow 2^m (\mathrm{mod}\ p)$
4. $I_p(X(j)) \leftarrow I(X(j))(\mathrm{mod}\ p)$
5. $I_p(Y) \leftarrow I(Y)(\mathrm{mod}\ p)$
6. while $j \le n-m+1$ do
7.   if $I_p(X(j)) = I_p(Y)$ then return j
8. $I_p(X(j+1)) \leftarrow (2I_p(X(j)) - W_p x_j + x_{j+m})(\mathrm{mod}\ p)$
9. $j \leftarrow j+1$
10. return 0

算法分析

时间复杂度为 $O(m+n)$

W_p, $I_p(Y)$, $I_p(X(1))$ 计算 $O(m)$ 时间

从 $I_p(X(j))$ 计算 $I_p(X(j+1))$ 总共需要$O(n)$时间

出错条件：
$$Y \neq X(j) \wedge I_p(Y) = I_p(X(j))$$
$$\Leftrightarrow p \mid \prod_{\{j \mid Y \neq X(j)\}} |I(Y) - I(X(j))|$$

出错概率：乘积大小不超过 $(2^m)^n$，整除它的素数个数不超过 $\pi(mn)$，选 $M = 2mn^2$，则出错概率不超过

$$\frac{\pi(mn)}{\pi(M)} \approx \frac{mn/\ln(mn)}{2mn^2/\ln(mn^2)} = \frac{\ln(mn^2)}{2n\ln(mn)} < \frac{\ln(mn)^2}{2n\ln(mn)} = \frac{1}{n}$$

素数测试

- 求 x 的 m 次幂
- 求 a 的模 n 的 m 次幂
- Fermart小定理
- 测试算法分析

求 x 的 m 次幂

输入：x为实数

$m = d_k d_{k-1} \ldots d_1 d_0$ 为二进制自然数

输出：x^m

算法 Exp(x,m)

1. $y \leftarrow 1$;
2. for $j \leftarrow k$ downto 0 do
3. $\quad y \leftarrow y^2$
4. $\quad$ if $d_j=1$ then $y \leftarrow xy$
5. return y

实例

x^{101}: $d_2=1, d_1=0, d_0=1$

$y=1$

$j=2$	$j=1$	$j=0$
$y=1$	$y=x^2$	$y=x^4$
$y=x$		$y=x^5$

a模n的m次幂

输入：$a, m, n \in Z^+$， $m \le n$,

$m = b_k b_{k-1} \ldots b_1 b_0$为二进制自然数

输出：$a^m \pmod n$

算法ExpMod(a, m,n)

1. $c \leftarrow 1$
2. for $j \leftarrow k$ downto 0 do
3. $\quad c \leftarrow c^2 \pmod n$
4. $\quad$ if $b_j=1$ then $c \leftarrow ac \pmod n$
5. return c

$T(n)=O(k\log^2 n)=O(\log^3 n)$ 以位乘作为基本运算

Fermart小定理:测试原理

定理1： 如果 n为素数，则对所有的正整数 $a \neq 0 \pmod n$有

$$a^{n-1} \equiv 1 \pmod n$$

素数测试原理：检测 $2^{n-1} \equiv 1 \pmod n$. 如是，输出“素数”否则输出“合数”

算法 Ptest1(n)

输入：奇整数 n, $n > 5$

输出：“prime”或者“composite”

1. if ExpMod(2,n–1,n) =1 then return prime
2. else return composite

问题：算法 Ptest1只对a=2进行测试. 如果 n为合数且算法输出“素数”，则称 n 为基2的伪素数. 例如341.

改进算法(一)

改进算法：随机选取2--n-1中的数，进行测试. 如取a=3，$3^{340}(\text{mod } 341) \equiv 56$，341不是素数.

算法Ptest2(n)

1. $a \leftarrow$ Random(2, n-2)
2. if Expmod(a, n-1, n)=1 then return prime
3. else return composite

- Fermat 小定理是必要条件，不是充分条件，满足该条件的也可能是合数. 对所有与 n 互素的正整数 a 都满足条件的合数 n 称为Carmichael数，如561，1105，1729，2465等. Carmichael数非常少，小于 10^8 的只有255个.
- 由初等数论可以证明：如果n为合数，但不是Carmichael数，算法Ptest2 测试 n为合数的概率至少为1/2.

素数的另一个必要条件

定理2 如果 n为素数，则方程 $x^2 \equiv 1(\mathrm{mod}\ n)$ 的根只有两个，即 $x = 1$，$x = -1$（或 $x = n-1$）.

证明 $x^2(\mathrm{mod}\ n) \equiv 1$

$\Leftrightarrow x^2-1 \equiv 0\ (\mathrm{mod}\ n)$

$\Leftrightarrow (x+1)(x-1) \equiv 0\ (\mathrm{mod}\ n)$

$\Leftrightarrow x+1 \equiv 0$ 或 $x-1 \equiv 0$ （域中没有零因子）

$\Leftrightarrow x = n-1$ 或 $x=1$

称 $x \neq \pm 1$ 的根为非平凡的.

判别方法： 如果方程有非平凡的根，则 n 为合数.

例如： $x^2(\mathrm{mod}\ 12) \equiv 1 \Leftrightarrow x = 1$ 或 $x = 11$ 或 $x = 5$ 或 $x=7$

结论：由于5 和 7 是非平凡的根，12是合数

测试方法

设 n为奇素数，存在 q, m 使得 $n-1=2^q m$,（$q\geq 1$).

构造序列：

$$a^m \pmod n), a^{2m} \pmod n), a^{4m} \pmod n), \ldots, a^{2^q m} \pmod n)$$

其最后一项为 $a^{n-1} \pmod n)$，而且每一项是前面一项的平方.

测试方法：

1. 对于任意 i（$i = 0,1,\ldots, q-1$）, 判断

$$a^{2^i m} \pmod n)$$

   是否为 1 和 n-1, 且它的后一项是否为1.

2. 如果其后项为1，但本项不等于 1 和 $n-1$, 则它就是非平凡的根，从而知道 n不是素数.

3. 随机选择 $a\in\{2, 3, \ldots, n-1\}$，进行上述测试.

实例

例如 n=561, n–1=560=$2^4\cdot 35$，假设 a=7，构造的序列为

$$7^{35}(\mathrm{mod}\,561)=241,$$

$$7^{2^1 35}(\mathrm{mod}\,561)=7^{70}(\mathrm{mod}\,561)=298,$$

$$7^{2^2 35}(\mathrm{mod}\,561)=7^{140}(\mathrm{mod}\,561)=166,$$

$$7^{2^3 35}(\mathrm{mod}\,561)=7^{280}(\mathrm{mod}\,561)=67,$$

$$7^{2^4 35}(\mathrm{mod}\,561)=7^{560}(\mathrm{mod}\,561)=1$$

第 5 项为 1，但是第 4 项等于 67，它既不等于 1 也不等于 560，是个非平凡的根，因此可以判定 n 为合数.

根据这个思想设计的计算机算法称为 **Miller-Rabin 算法**，它随机选择正整数 $a\in\{2,3,\ldots,n-1\}$，然后进行上述测试.

算法子过程(一)

算法 findq-m(n)　//找 q, m 使得 n-1=$2^q m$

1. $q \leftarrow 0$; $m \leftarrow n-1$
2. repeat
3. 　$m \leftarrow m/2$
4. 　$q \leftarrow q+1$
5. until m是奇数

运行时间：$O(\log n)$

China Computer Federation 中国计算机学会

算法子过程（二）

算法 test(n, q, m) //检测序列是否存在非平凡的根

1. $a \leftarrow$ Random(2, n-1)
2. $x_0 \leftarrow$ ExpMod(a, m, n) //$x_0=a^m$(mod$n$), $O(\log^3 n)$
3. for $i \leftarrow 1$ to q do //$q=O(\log n)$
4. $x_i \leftarrow x_{i-1}^2$ (mod n) //$O(\log^2 n)$
5. if $x_i = 1$ and $x_{i-1} \neq 1$ and $x_{i-1} \neq n-1$
6. then return composite
7. if $x_q \neq 1$ then return composite
8. return prime

性能分析：

- 1 次测试运行时间 $O(\log^3 n)$
- 可证明1次测试出错的概率至多 1/2.
- 重复运行 k 次，可将出错概率降到至多2^{-k}.

Miller-Rabin算法

令$k=\lceil \log n \rceil$, 出错的概率小于等于$2^{-k}\le 1/n$. 即算法给出正确答案的概率为$1-1/n$. 换句话说，如果 n为素数，则算法输出素数. 如果n为合数，则算法以$1-1/n$的概率输出“合数”.

算法 PremalityTest(n) // $n \ge 5$，奇整数

1. findq-m(n)
2. $k \leftarrow \lceil \log n \rceil$
3. for $i \leftarrow 1$ to k //重复执行$\log n$次
4. test(n, q, m)

时间：$T(n) = O(\log^4 n)$ // 按位乘统计

Las Vegas型与 Monte Carlo型随机算法

- **Las Vegas型随机算法**
  - 如果得到解，总是给出正确的结果，区别只在于运行时间的长短.
  - 拉斯维加斯型随机算法的运行时间本身是一个随机变量
  - 期望运行时间是输入规模的多项式且总是给出正确答案的随机算法称为有效的拉斯维加斯型算法.
- **Monte Carlo型随机算法**
  - 这种算法有时会给出错误的答案.
  - 其运行时间和出错概率都是随机变量，通常需要分析算法的出错概率.
  - 多项式时间内运行且出错概率不超过1/3的随机算法称为有效的蒙特卡洛型算法

单侧错误和双侧错误

- 弃真型单侧错误
  - 当算法宣布接受时，结果一定是对的
  - 当算法宣布拒绝时，结果有可能是错的
  - 例如主元素测试算法
- 取伪型单侧错误
  - 当算法宣布拒绝时，结果一定是对的
  - 而当算法宣布接受时，结果有可能是错的
  - 例如素数测试
- 双侧错误
  - 在所有的输入上同时出现上述两种不同的错误

随机算法的分类与局限性

- 拉斯维加斯型随机算法
  - 零错误概率多项式时间算法(有效的)，ZPP
- 蒙特卡洛型随机算法
  - 错误概率有界的有效算法(多项式时间)，BPP
  - 弃真型单侧错误概率有界的有效算法，RP
  - 取伪型单侧错误概率有界的有效算法，coRP
- 随机算法的局限性
  - 错误概率有界的多项式时间随机算法不太可能解决NP完全问题

中国计算机学会
China Computer Federation

总结

- 随机算法的两种类型
- 随机算法的分析方法