

VC 中的伪随机数 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/470/2021_2022_VC___E4_B8_AD_E7_9A_84_c67_470119.htm

为追求真正的随机序列，人们曾采用很多种原始的物理方法用于生成一定范围内满足精度（位数）的均匀分布序列，其缺点在于：速度慢、效率低、需占用大量存储空间且不可重现等。为满足计算机模拟研究的需求，人们转而研究用算法生成模拟各种概率分布的伪随机序列。伪随机数是指用数学递推公式所产生的随机数。从实用的角度看，获取这种数的最简单和最自然的方法是利用计算机语言的函数库提供的随机数发生器。典型情况下，它会输出一个均匀分布在0和1区间内的伪随机变量的值。其中应用的最为广泛、研究最彻底的一个算法即线性同余法。线性同余法LCG（Linear Congruence Generator）选取足够大的正整数M和任意自然数 n_0 ， a ， b ，由递推公式： $n_{i+1} = (a \cdot n_i + b) \bmod M$ $i=0, 1, \dots, M-1$ 生成的数值序列称为是同余序列。当函数 $f(n)$ 为线性函数时，即得到线性同余序列： $n_{i+1} = (a \cdot n_i + b) \bmod M$ $i=0, 1, \dots, M-1$ 以下是线性同余法生成伪随机数的伪代码：`Random(n, m, seed, a, b) { r0 = seed; for (i = 1; i <= n; i++) { ri = (a * ri-1 + b) mod m; }` 其中种子参数seed可以任意选择，常常将它设为计算机当前的日期或者时间；m是一个较大数，可以把它取为 2^w ，w是计算机的字长；a可以是 $0.01w$ 和 $0.99w$ 之间的任何整数。应用递推公式产生均匀分布随机数时，式中参数 n_0 ， a ， b ，M的选取十分重要。例如，选取 $M=10$ ， $a=b=n_0=7$ ，生成的随机序列为{6, 9, 0, 7, 6, 9,}，周期为4。取 $M=16$ ， $a=5$ ， $b=3$ ， $n_0=7$ ，

生成的随机序列为{6, 1, 8, 11, 10, 5, 12, 15, 14, 9, 0, 3, 2, 13, 4, 7, 6, 1.....}, 周期为16。取M=8, a=5, b=1, n0=1, 生成的随机序列为{6, 7, 4, 5, 2, 3, 0, 1, 6, 7.....}, 周期为8。Visual C 中伪随机数生成机制用VC产生随机数有两个函数, 分别为rand (void) 和srand (seed)。rand()产生的随机整数是在0~RAND_MAX之间平均分布的, RAND_MAX是一个常量(定义为: #define RAND_MAX 0x7fff)。它是short型数据的最大值, 如果要产生一个浮点型的随机数, 可以将rand()/1000.0, 这样就得到一个0~32.767之间平均分布的随机浮点数。如果要使得范围大一点, 那么可以通过产生几个随机数的线性组合来实现任意范围内的平均分布的随机数。其用法是先调用srand函数, 如srand((unsigned)time(NULL)) 这样可以使得每次产生的随机数序列不同。如果计算伪随机序列的初始数值(称为种子)相同, 则计算出来的伪随机序列就是完全相同的。要解决这个问题, 需要在每次产生随机序列前, 先指定不同的种子, 这样计算出来的随机序列就不会完全相同了。以time函数值(即当前时间)作为种子数, 因为两次调用rand函数的时间通常是不同的, 这样就可以保证随机性了。也可以使用srand函数来人为指定种子数。100Test 下载频道开通, 各类考试题目直接下载。详细请访问 www.100test.com