**【★】浅谈计算机与随机数**

       闲来无事，看到关于人工智能的新闻，想到现在好多产品都喜欢给自己贴上“智能”的标签，因而又想到我高中时期的一次研讨会上大家由这个话题延伸至“计算机如何生成随机数”。现在我想把对随机数生成器的理解写下来。

       首先需要声明，计算机是不会产生绝对随机的随机数，它只能产生“真随机数”。

       真正意义上的随机数是一个个相互独立，具有一定发生概率且不可预计的数。而现代计算机的程序和算法本身不能产生真随机数。计算机可以知识渊博（海量存储嘛），也可以很智能（按照植入的程序高速计算），但不论它的运算速度有多快，都还是按照事先设计好的算法逻辑来运行的。仅依靠计算机内部的程序只能生成伪随机数，伪随机数发生的概率极不稳定，实验表明：当试验次数越来越多，伪随机数样本就越来越不服从均匀分布。不难理解，伪随机数只是按照数学家们精心构造的规则而生成的（比如C语言中的随机数生成函数），它们是通过一个固定的、可以重复的计算方法产生的，只是具有很长的周期性罢了。因此，人类不断改造计算机，试图使其有生成真随机数的能力。

       电脑自然是没有人脑聪明的。就存储能力而言，计算机硬盘采用一维存储（二进制数的依次排列）以及二维检索（坐标查找）的方式来实现输入与输出；而众所周知，人的大脑是由神经元构成的，神经细胞相互之间通过神经突触相互影响，形成极其复杂的相互联系，记忆就是无数脑神经细胞之间相互呼叫所形成的一种多维的存储方式，人脑计算功能也是如此。经科学家计算，每10个神经元就相当于1TB硬盘的存储容量，人脑上千亿个神经元的存储力可想而知。但是，人脑能产生真随机数吗？随便一个人，让他随机说出10以内的整数：2,3,7,9,5……。当说出足够多的数后，研究人员统计发现，每个数字出现的次数比例不尽相同且差距很大，完全不符合随机分布，且不同的人有不同的情况。因此人脑也不能产生正真的随机数，比如我们说出下一个随机数之前，潜意识已经被上一个数影响，单这一点就违背了随机数的定义。

       那计算机的真随机数发生器是怎么做到的呢？关键还是在于它的算法。虽然人脑不能生成真随机数，但人类可以设计出各种方案以产生随机性很高的随机数。比如随便想出一个汉字，数它的笔划数：奇数代表是，偶数代表否。如此是和否的概率都近似50%。再比如拿一本书从中间翻开观察页数；抬起头看看时钟的指针位置；找一个英文单词观察长度；找一张现成的表格（比如全市人民身份信息表），等等方法都可以生成相当准确的随机数。计算机的随机数发生器就是利用了一张巨大的“表格”：其中的每个元素覆盖了所需随机数的范围，元素的坐标既是来自外界的随机因子（称之为随机种子）。这张表类似于密码学中的秘钥，是一种并不复杂的算法。

       来自外界（cpu以外）的随机种子可以是任何计算机可识别的因素：从键盘敲击速度，鼠标位置变化，内存占用大小，磁盘读写速率到IO请求的响应时间，硬件中断的时间间隔，风扇的旋转功率，当时的时间和日期，邻居家无线信号强度变化，甚至此时的气温湿度和磁场，它们都可以被用来参与随机数的计算。这才是未来程序语言和软件中真随机数生成函数的工作原理。

       然而正如刚开始所说，计算机无法生成绝对随机的随机数，随机只是理想化的。事实上，世上本无概率之说，全宇宙都不存在随机的东西，世间万物的发展与变化都遵循着其固有的规律，包括人类。至于刚才所说的利用外界因素和计算机系统作为整体迂回产生的随机数也并不是100%的随机，只要试验次数足够多（可能天文数字都无法衡量），随机分布状态便会瓦解。当然，这是个无尽的话题，如果更深入的话，还需要论及宇宙的本质之类的哲学命题，暂且不表。

       对计算机与随机数的思考，让我联想到如今高速发展的人工智能。你觉得机器人还有机会超越人类吗？它们的“大脑”连生成真随机数的本领都没有（至少目前没有）。当代计算机只有绝对服从的程序语言，不会有自己的思想，不会具有人类的情感，不会有喜怒哀乐，更不会有曾经谣传的超级计算机“愤怒”而杀人的事件。如果在遥远的未来人成功得将计算机改造拥有能够匹敌21世纪人类大脑智慧的力量，那么此时人类的大脑必然已进化到一个更高更智慧的状态。

——by Jim