一种基于硬件实现的游程检测算法

陈孟东，刘 鹏，徐亚君
（江南计算技术研究所，江苏 无锡 214083）

摘 要：在实际系统中对游程检测的实现速度、电路规模有很高的要求，而传统的检测方法性能较低。针对此问题提出了一种新的游程检测算法。该算法基于硬件实现，电路结构简单实现速度快，占用资源少。

关键词：随机性；游程；游程检测
中图分类号：TP39 **文献标识码**：A

Run-length detect algorithm based on hardware

CHEN Meng Dong, LIU Peng, XU Ya Jun
(Jiangnan Institute of Computing Technology, Wuxi 214083, China)

Abstract: Concerning the low performance of current methods and the high requirements of implementation time and the scale of electrocircuit, this article puts forward a new algorithm implementing run-length detect. This algorithm, which is based on hardware and fast in actualization, has a simple circuit framework and consumes little resources.

Key words: randomicity; run-length; run-length detect

随着计算机技术、通信技术、网络技术的迅速发展，信息在存储、传送、接收和处理过程中的安全问题已受到人们的广泛关注，随机数在信息安全系统中扮演着重要的角色，在基于计算机或 Internet 的通信和交易中有着广泛的应用，比如数据加密、密钥管理、公钥和私钥的产生、电子商务、数字签名、身份鉴定以及蒙特卡罗仿真等都要用到随机数[1]。

随机数序列的随机性能直接决定了信息安全系统的安全性能。因此，在使用随机数之前，必须对其随机性进行检测，而游程检测是序列随机性检测的一个重要方面。在分析了传统的游程检测方法后，本文提出了一种新的、基于硬件实现的游程检测算法。

1 游程检测

1 段 0、1 序列中，0 或者 1 连续地重复出现，即为游程，连续出现的个数称做游程长度[2]。游程长度是序列随机性的一个重要指标，它的大小可影响序列的随机性。通常，一个很大的游程长度将导致序列随机性的下降。因此，往往要求游程长度不能超过某一界限，检测一段序列中是否有超过游程界限的游程长度称为游程检测[3]。

在许多具体的系统中，随机数发生器产生的随机数要进行游程检测，然后才能使用。而游程检测需要以很少的资源、很快的速度实现，因此检测算法就变得非常重要，其优劣也会影响到整个系统的性能。

2 传统方法

传统的实现游程检测的方法有查表法和逐 bit 比较法等。以进行“1”的游程检测为例。

查表法是将随机数序列按 k bit 分段，逐段进行检测。对于 k bit 的序列，一共有 2^k 种，建立 1 个 2^k 长度的表格，每一种序列对应 1 个表格项，表内所存的是该种序列内所含有的游程长度，包括 k bit 内部“1”的游程长度以及左右两端连续“1”的长度。检测时，对每一个分段通过查表找到游程长度，通过考虑相邻段的“1”可以连接到一起，游程长度也可以相加，以判断是否有超过游程界限的情况。

逐 bit 比较法是将随机数序列串行地逐 bit 进行检验，判断是否为“1”来得到游程长度，判断是否超过游程界限。

查表法需要很大的存储空间，而且反复查表耗费时间；逐 bit 比较法同样所需时间较长、速度慢。这两种方法都耗费资源，不适于在集成的、高速的设备中使用。

3 新算法

3.1 算法流程

假设一随机数序列，要求游程界限为 t，游程长度超过 t 即为不合格。将随机数序列按 $k(k\leqslant t)$bit 分段，逐段进行检测。由于 $t\geqslant k$，所以仅在一段内部连续“1”的个数不可能超过界限 t，因此不予考虑。只需判断每段中左右两侧连续“1”的个数 cl、cr，因为 cl、cr 能够与相邻段中的 cr、cl 相加产生超过 t 的游程长度。具体流程如图 1 所示。其中，cr 前表示前一段中右侧连续“1”的个数。注意：当 $cl=cr$ 时，表示这 k 位全部为“1”，需要将 $c_{r\,前}$ 与本段的 cr 相加送入后面段的比较中。

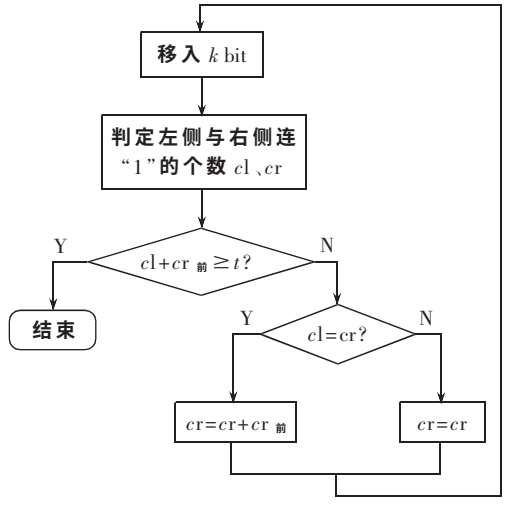

图 1 新算法流程图

3.2 cl、cr 的检测方法

以检测一段 data(k bit)中左侧起连续“1”的个数 cl 为例(cr 的检测与此类似)。

检测方法是：将这一段 data 与检验序列 $\underbrace{11\cdots1}_{n}\,\underbrace{00\cdots0}_{k-n}$($n=k,k-1,k-2,\cdots1$)分别相与，使其右侧 $k-n$ 位变为 0，保留最左侧 n 位，检测 n 位是否为全“1”。若 k 个与完的结果中存在最大的 n，使 data& $\underbrace{11\cdots1}_{n}\,\underbrace{00\cdots0}_{k-n}=\underbrace{11\cdots1}_{n}\,\underbrace{00\cdots0}_{k-n}$，则 $cl=n$。否则，这 k bit 中最左侧一位为 0，即 $cl=0$。其流程如图 2 所示。

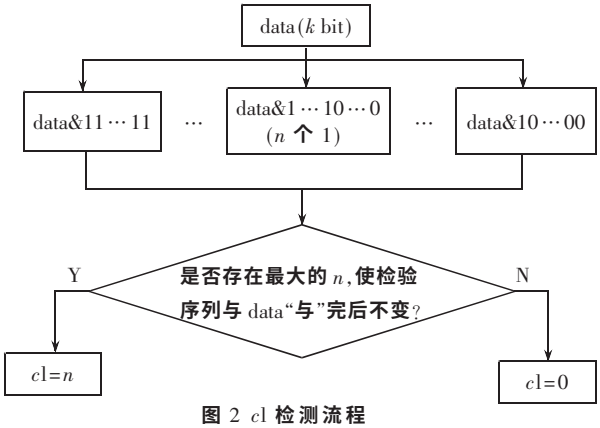

图 2 cl 检测流程

3.3 算法的分析

该游程检测算法适于硬件实现，只需设计 1 个 k 位的寄存器，将 k 位的 data 依次移入该寄存器，然后进行检测。每一段的移入、判断在 1 个时钟周期内就可以完成，且只需少量组合逻辑电路即可实现，电路简单、检测效率高。

4 算法的扩展

当游程界限 t 变小时，可以缩小寄存器的长度 k，让 k 始终$\leqslant t$，这样就可以保证在 k bit 序列中部的连续“1”的个数不会超过界限 t。不必检测 k bit 中部的“1”的游程长度，算法即可适用于任意的游程界限。

k 值的选取还需要考虑寄存器的长度等因素，需要选取一个适中的值。进行“0”的游程检测时，方法与此算法类似。

游程检测是序列随机性检测的一个重要方面，是在使用随机数之前必须进行的一项工作，在工程实践中具有重要的作用。尤其是在一些实时的系统中，检测算法的速度至关重要。本文提出了一种新的进行游程检测的算法，主要针对硬件实现中需要快速进行检测的需求而设计的。它将随机数序列分成合适长度的段，并利用基本的“与”电路和比较电路逐段进行判断，每一段的判断可以在 1 个时钟周期内完成，非常适合硬件实现，而且电路结构简单，具有实现速度快、节省资源等优点。

参考文献

[1] 胡涛，郭立，黄昊. 一种新的混沌随机数生成器实现方案[J]. 电子技术应用，2006,32(6):51-53.

[2] 智库百科.什么是游程检验[EB/OL]. http://wiki.mbalib.com/wiki. 2009-08-18.

[3] 万艳. 林晓伟. 李炜. 真随机数发生器芯片的设计[J]. 大众科技，2006(2):70,72.

(收稿日期：2009-08-18)

作者简介：

陈孟东，男，1984 年生，硕士研究生，助理工程师，主要研究方向：信息安全。

刘鹏，男，1982 年生，助理工程师，硕士，主要研究方向：信息安全。

徐亚君，女，1965 年生，高级工程师，硕士，主要研究方向：信息安全。