ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0005—2021
代替 GM/T 0005—2012

随机性检测规范

Randomness test specification

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号 …… 2
5　随机性检测方法 …… 3
5.1　单比特频数检测方法 …… 3
5.2　块内频数检测方法 …… 3
5.3　扑克检测方法 …… 4
5.4　重叠子序列检测方法 …… 4
5.5　游程总数检测方法 …… 5
5.6　游程分布检测方法 …… 6
5.7　块内最大游程检测方法 …… 6
5.8　二元推导检测方法 …… 7
5.9　自相关检测方法 …… 8
5.10　矩阵秩检测方法 …… 8
5.11　累加和检测方法 …… 9
5.12　近似熵检测方法 …… 9
5.13　线性复杂度检测方法 …… 10
5.14　Maurer 通用统计检测方法 …… 11
5.15　离散傅立叶检测方法 …… 12
6　随机性检测判定 …… 12
6.1　概述 …… 12
6.2　样本通过率判定 …… 13
6.3　样本分布均匀性判定 …… 13
6.4　随机性检测结果判定 …… 13
附录 A（规范性）　样本长度及检测设置 …… 14
附录 B（资料性）　随机性检测原理 …… 16
附录 C（资料性）　随机性检测结果示例 …… 23

前　言

本文件依据 GB/T 1.1—2020 给出的规则起草。

本文件代替 GM/T 0005—2012《随机性检测规范》，对随机性检测进行规范，为二元序列的随机性检测工作提供科学依据。与 GM/T 0005—2012 相比，除编辑性修改外主要技术变化如下：

a) 本文件适用范围由“适用于对随机数发生器产生的二元序列的随机性检测”改为“适用于对二元序列的随机性检测”(见第 1 章和 2012 年版的第 1 章)；

b) 删除了“随机数发生器”、“P 值”、“游程”的术语以及“单比特频数检测”等 15 个检测项的术语定义(见 2012 年版的第 2 章)，新增了术语“样本集”(见 3.6)；

c) 修改了符号 α、P_value 的说明(见第 4 章和 2012 年版的第 3 章)，增加了符号 α_T、Q_value 的说明(见第 4 章)；

d) 删除了“二元序列的检测”章节，新增“随机性检测方法”章节，分别从概述、检测步骤、结果判定对 15 项检测方法进行展开说明，其中每项检测方法的检测步骤中均增加 Q_value 的计算(见第 5 章和 2012 年版的第 4 章)；

e) 删除了“随机数发生器的检测”章节，新增“随机性检测判定”章节，分别从概述、样本通过率判定、样本分布均匀性判定、随机性检测结果判定进行说明，其中增加了对 Q_value 的样本分布均匀性判定要求[见第 6 章和 2012 年版的第 5 章)]；

f) 修改游程分布检测方法中的统计值构造方法(见 5.6.2 和 2012 年版的 4.4.7)；

g) 块内最大游程检测方法新增块内最大“0”游程检测模式(见 5.7)；

h) 累加和检测方法新增后向累加和检测模式(见 5.11)；

i) 删除“随机性检测参数设置表”(见 2012 年版的表 B.1)；

j) 新增三种样本长度及检测设置表(见附表 A.1、A.2、A.3)；

k) 删除“随机性检测结果分析表”(见 2012 年版的附录 C)；

l) 随机性检测原理调整为附录 B(见附录 B 及 2012 年版的附录 A)；

m) 修改块内最大游程的 π_i 取值(见附表 B.4 及 2012 年版的附表 A.3)；

n) 新增随机性检测结果示例(见附录 C)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件的附录 A 是规范性附录。本标准的附录 B、附录 C 是资料性附录。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：国家密码管理局商用密码检测中心、中国科学院软件研究所、中国科学院信息工程研究所、北京宏思电子技术有限责任公司、浙江大学。

本文件主要起草人：罗鹏、毛颖颖、陈华、范丽敏、马原、李亚威、张文婧、沈海斌、陈美会、朱少峰、张贺、朱双怡。

本文件的历次版本发布情况为：

——GM/T 0005—2012。

随机性检测规范

1 范围

本文件规定了适用于二元序列的随机性检测指标和检测方法。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

二元序列 binary sequence

由“0”和“1”组成的比特串。

注：如无特别说明，本文件所指的序列均为二元序列。

3.2

随机性假设 randomness hypothesis

对二元序列做随机性检测时，首先假设该序列是随机的，这个假设称为原假设或零假设，记为 H_0。与原假设相反的假设，即这个序列是不随机的，称为备择假设，记为 H_α。

3.3

随机性检测 randomness test

用于二元序列检测的一个函数或过程，可以通过它来判断是否接受随机性原假设。

3.4

显著性水平 significance level

随机性检测中错误地判断随机序列为非随机序列的概率。

3.5

样本 sample

用于随机性检测的二元序列。

3.6

样本集 sample group

多个样本的集合。

3.7

样本长度 sample length

样本的比特个数。

3.8

样本数量 sample size

样本集中的样本个数。